Am 09.03.2017 freigegebene Version

ELGA GmbH

ELGA-Gesamtarchitektur

Datum: 28.02.2017

Version: **2.30b**

Inhaltsverzeichnis

113

1. Management Summary

Das vorliegende Dokument beschreibt die allgemeine Architektur der elektronischen Gesundheitsakte ELGA in Österreich und deckt insbesondere folgende Aspekte ab:

- Übersicht der ELGA-Benutzer
- Übersicht der Komponenten von ELGA
- Zusammenwirken der ELGA-Komponenten sowie der zum Einsatz kommenden Schnittstellen
- Nicht-funktionale Anforderungen an die Gesamtarchitektur sowie die daraus resultierenden Anforderungen an die einzelnen Systemkomponenten
- Technische Konzepte für die Umsetzung der nicht-funktionalen Anforderungen

Dieses Kapitel enthält eine Zusammenfassung der im Weiteren diskutierten und präzise ausgelegten Details der ELGA-Architektur.

1.1. Ziel des Dokumentes

Dieses Dokument soll einen Überblick über die Gesamtarchitektur der elektronischen Gesundheitsakte ELGA vermitteln. Es dient der Definition der grundsätzlichen Aufgaben von ELGA und beschreibt die vorgesehene Funktionalität sowie die Beziehungen der interagierenden logischen ELGA-Komponenten. Ziel des Dokuments ist es, einen technischen Überblick der ELGA-Architektur zu geben. Einzelne Details, notwendige Präzisierungen, Ergänzungen und eventuelle Abweichungen sind in den jeweiligen Pflichtenheften sowie sonstigen Realisierungsdokumenten konkret begründet und erklärt (mit Referenz auf die entsprechenden Passagen der Gesamtarchitektur).

1.2. Übersicht der ELGA-Benutzer

Als ELGA-Benutzer werden alle Personen bezeichnet, die aufgrund ihrer Befugnisse Zugang zu im Wege von ELGA gespeicherten Daten haben. Darunter fallen verschiedene Akteure wie ELGA-Teilnehmer bzw. deren Bevollmächtigte und gesetzliche Vertreter, Mitarbeiter des ELGA-Service (wie z.B. ELGA-Regelwerk- und Sicherheitsadministratoren) sowie ELGA-GDA (ELGA-Gesundheitsdiensteanbieter) als Person oder Organisation. *Abbildung 1* zeigt die Gliederung der ELGA-Benutzer auf hoher Ebene.

Die Identitäten der ELGA-Teilnehmer sind durch den Zentralen Patientenindex (Z-PI) verwaltet. Darüber hinaus speichert der Z-PI gemäß § 15 Abs. 1 GTelG 2012 auch alle natürlichen Personen, die einer ELGA-Teilnahme widersprochen haben. Identitäten von ELGA-GDA sowie die Identität der ELGA-Ombudsstelle (ELGA-OBST), welche in Vertretung eines ELGA-Teilnehmers agiert, werden durch den GDA-Index verwaltet. Die Identität der

ELGA-Widerspruchstelle (ELGA-WIST) wird explizit im Berechtigungssystem geführt. Identitäten der Servicemitarbeiter und Sicherheitsadministratoren werden durch vertrauenswürdige lokale Verzeichnisdienste (etwa im Bundesrechenzentrum (BRZ)) verwaltet.

Entsprechende Begriffsdefinitionen sind gesetzlich durch das Elektronische Gesundheitsakte Gesetz (ELGA-G) festgelegt.

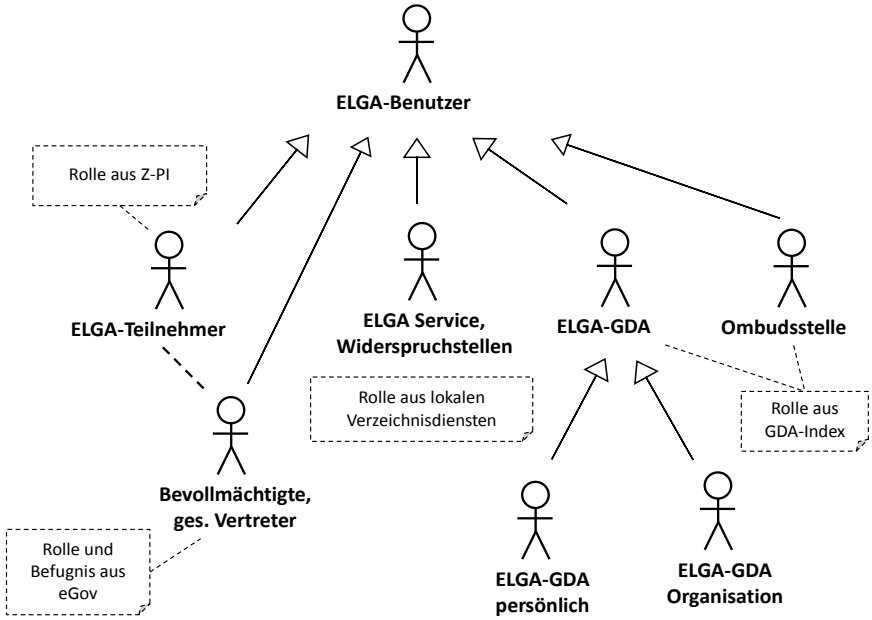


Abbildung 1: ELGA-Benutzer Hierarchie

1.3. Übersicht der Architektur

Die Architektur von ELGA baut auf der ersten Version des ELGA-Lastenheftes zur Gesamtarchitektur aus dem Jahr 2008 [1] auf und berücksichtigt darüber hinaus die evolutionäre Entwicklung der entsprechenden Sicherheitsstandards, etwa WS-Trust Version 1.4 von 2009 oder XSPA Profil of WS-Trust aus dem Jahr 2010.

Im Hinblick auf die Integration bereits existierender elektronischer Gesundheitsdaten zu einer österreichweiten elektronischen Gesundheitsakte wurde das Konzept eines ELGA-Bereichs eingeführt. Ein ELGA-Bereich zeichnet sich durch eine Menge von funktionalen Komponenten und entsprechenden Interaktionen zwischen diesen aus, welche durch das Kommunikationsframework der *Integrating the Healthcare Enterprise Initiative* (IHE) im Allgemeinen bzw. durch ELGA im Speziellen festgelegt sind. Das ELGA-Berechtigungssystem steuert, führt und überwacht das Zusammenspiel innerhalb eines ELGA-Bereichs sowie die Interaktion zwischen den ELGA-Bereichen.

Demnach umfasst ein ELGA-Bereich zumindest folgende Komponenten:

- Akteure, die im IHE Integrationsprofil *Cross-Enterprise Document Sharing* (XDS) spezifiziert sind:
  - genau eine ELGA-Registry (XDS Document Registry)
  - optional ein oder mehrere ELGA-Repositories (XDS Document Repository)
  - zumindest eine Anbindung eines Informationssystems eines ELGA-Benutzers (XDS Document Consumer bzw. Document Source)
- Akteure gemäß dem IHE Integrationsprofil *Patient Identifier Cross-Reference HL7 V3* (PIXV3), *Patient Demographic Query HL7 V3* (PDQV3)
  - genau ein lokaler Patientenindex (L-PI)
- Akteure gemäß dem IHE Integrationsprofil *Cross-Community Access* (XCA)
  - genau ein ELGA-Gateway (beinhaltet XCA Initiating bzw. Responding Gateways)
- Dezentraler Teil des verteilten ELGA-Berechtigungssystems zur einheitlichen Umsetzung der gesetzlichen und individuellen Bestimmungen

Die österreichische ELGA ermöglicht die Integration personenbezogener medizinischer Dokumente, die dezentral durch die Komponenten eines ELGA-Bereichs persistiert werden. Die tatsächliche Anzahl an ELGA-Bereichen variiert in Abhängigkeit regionaler, fachlicher bzw. organisatorischer Kriterien.

Abbildung 2 illustriert sowohl ELGA-Bereiche als auch bereichsübergreifende (zentrale) Komponenten als Fundament der ELGA-Gesamtarchitektur.

Um die Funktionalitäten von ELGA nutzen zu können, sind die einzelnen ELGA-Gesundheitsdiensteanbieter (ELGA-GDA) verpflichtet, selbst für die Anbindung an einzelne ELGA-Bereiche Sorge zu tragen, etwa über Service-Provider, die solche Dienste und Anbindungen anbieten, oder direkt über klar definierte, auf internationalen Standards aufbauende Schnittstellen (z.B. OASIS, W3C, IHE Profile), die von den ELGA-Bereichsbetreibern verpflichtend anzubieten sind. Die hierfür nötigen Informations- und Kommunikationstechnologien werden durch die in dieser Beschreibung spezifizierten Schnittstellen klar festgelegt.

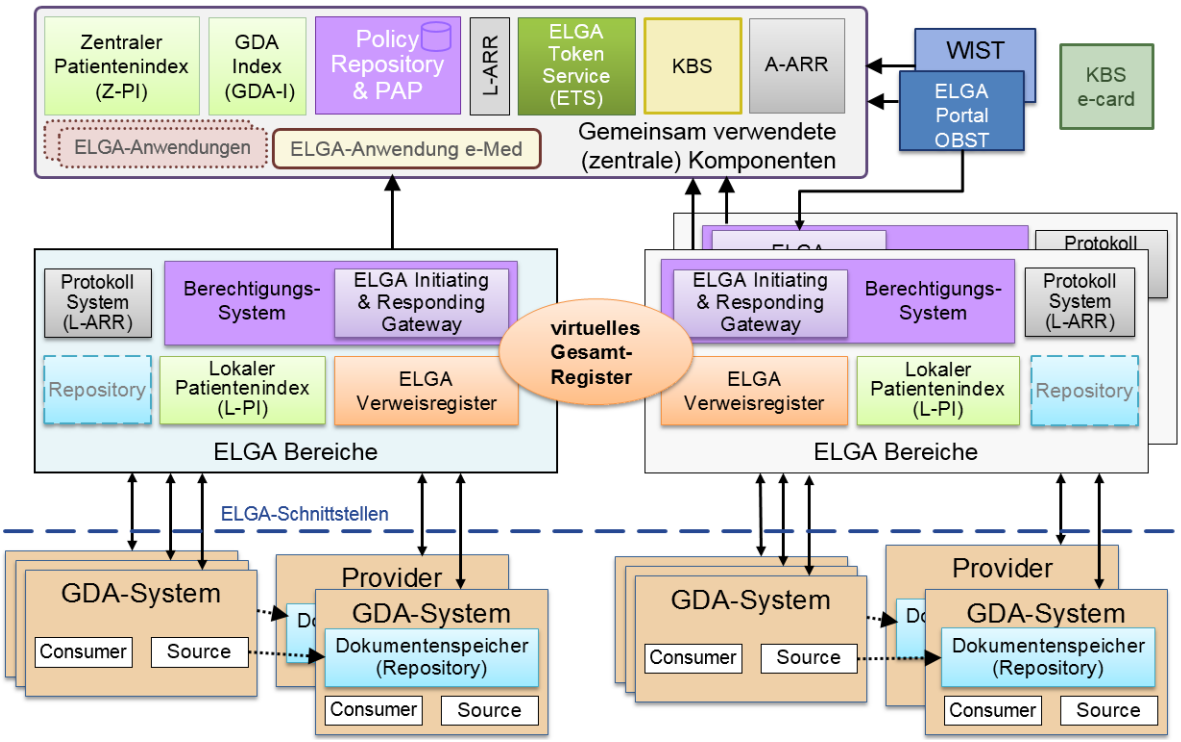


Abbildung 2: Darstellung der Architektur von ELGA[1]

Jeder ELGA-Bereich umfasst ein ELGA-Gateway gemäß dem IHE Integrationsprofil Cross-Community Access (XCA), das sowohl bereichsintern als auch bereichsübergreifend die Suche und den Abruf von ELGA-CDA-Dokumenten ermöglicht. Ein Gateway wird somit durch einen ELGA-Benutzer (bzw. durch dessen genutzten Document Consumer) für die transparente Suche und den anschließenden Abruf von ELGA-CDA-Dokumenten genutzt. Zudem wird das prinzipielle Konzept eines XCA Gateways in ELGA durch wesentliche Mechanismen der Zugriffssteuerung ergänzt und als ELGA-Anbindungsgateway (E-AGW im Weiteren kurz nur AGW) detailliert spezifiziert, um die Zulässigkeit von Operationen auf personenbezogene medizinische Daten einheitlich sicherzustellen.

Im Zuge der Veröffentlichung eines ELGA-CDA-Dokuments übermittelt das lokale System eines ELGA-GDA als XDS Document Source ein Dokument an die, seitens des ELGA-GDAs bereitzustellende, XDS Document Repository Komponente. Anschließend übernimmt die XDS Repository Komponente die Aufgabe der Übermittlung entsprechender Dokument-Metadaten an eine (ELGA) XDS Registry. Das XDS Repository kann, unter Gewährleistung der Verfügbarkeitsanforderungen, als Teil eines GDA Systems bzw. als dedizierte Komponente durch einen Provider realisiert werden. Beide Varianten sind in der Abbildung 2 dargestellt.

[1] Farbschemas siehe Anhang A „Verwendete Farbschemas“

Die Komponente *lokaler Patientenindex (L-PI)* eines ELGA-Bereichs bildet (bereichsübergreifend betrachtet) gemeinsam mit allen lokalen Patientenindizes weiterer ELGA-Bereiche, eine hierarchische Struktur, der ein zentraler Patientenindex übergeordnet ist. Diese Hierarchie dient der übergreifenden Identifikation von ELGA-Teilnehmern durch Zusammenführung der Informationen aus den einzelnen ELGA-Bereichen. Der L-PI eines ELGA-Bereichs enthält insbesondere Identifikatoren der ELGA-Teilnehmer, die durch ELGA-GDA desselben ELGA-Bereichs medizinisch versorgt werden.

Der zentrale Patientenindex (Z-PI) deckt folgende Funktionen ab:

- Herstellung der Verknüpfung unterschiedlicher lokaler Identifikatoren ein und desselben ELGA-Teilnehmers mittels qualitätsgesicherter personenbezogener Daten aus externen Registern (z.B. Zugriff auf die Daten des zentralen Melderegisters (ZMR) im Wege der Zentralen Partnerverwaltung der Sozialversicherung (ZPV)).
- Bereitstellung des Patient Identifier Cross-Referencing Query (PIX-Query) Service, welches zur Abfrage jener ELGA-Bereiche dient, in denen der ELGA-Teilnehmer registriert wurde und in denen somit medizinische Dokumente des ELGA-Teilnehmers registriert sein könnten (wobei nicht zwingend Dokumente vorliegen müssen).
- Bereitstellung qualitätsgesicherter demographischer Daten von Personen und Identitätsdaten gemäß § 18 Abs. 2 GTelG 2012 (PDQ).

Das ELGA-Portal (Abbildung 2) ist durch ein speziell vorkonfiguriertes, dediziertes ELGA-Gateway angebunden. Dadurch entsteht ein „virtueller“ ELGA-Bereich für das Portal zwar ohne L-PI, ohne Verweisregister und Repositorien, aber in der Kommunikation mit ELGA strikt den Vorgaben des IHE XCA-Profils folgend.

Die ELGA-Anwendung e-Medikation ist in der Abbildung 2 im Bereich der zentralen Komponenten angeführt, um zu zeigen, dass diese Dienstleistung für ELGA als gemeinsam zu verwendende Komponente zur Verfügung gestellt wird. Weiters ist anzumerken, dass die Anbindung der e-Medikation nicht dem IHE XCA-Profil folgt. Nähere Details sind im Kapitel 11.3 erörtert.

1.4. Übersicht über das Berechtigungs- und Protokollierungssystem

Das Berechtigungssystem repräsentiert die technische Umsetzung legistischer und datenschutzrechtlicher Anforderungen bezüglich der elektronischen Verarbeitung und Übermittlung personenbezogener medizinischer Daten. Es dient primär der Autorisierung von ELGA-Benutzern sowie der Autorisierung von deren Zugriffen auf personenbezogene medizinische Daten in ELGA. Basierend auf, mittels elektronischer Signaturen verifizierten, Identitäts- und Rolleninformationen sowie einer Kombination von gesetzlich und individuell festgelegten Zugriffsberechtigungen, wird die Zulässigkeit von Aktionen der ELGA-Benutzer

durch das Berechtigungssystem validiert, erteilt oder im Falle fehlender bzw. widerrufener Berechtigungen abgelehnt.

Im Allgemeinen setzt sich das ELGA-Berechtigungssystem aus den zentralen Komponenten ELGA-Token-Service (ETS), Kontaktbestätigungsservice (KBS), Policy Administration Point (PAP) und mehreren dezentralen ELGA-Anbindungsgateways (AGW) zusammen. Das ETS nutzt die Dienste des Zentraler Patientenindex (Z-PI), Policy Administration Point (PAP) und Gesundheitsdiensteanbieter-Index (GDA-I) sowie des Kontaktbestätigung-Services (KBS), um identitäts-, rollen- sowie weitere autorisierungsbezogene Attribute (generelle und individuelle Berechtigungen) in standardisierter Form als sogenannte ELGA-Authorisation-Assertion strukturiert abzubilden (siehe Abbildung 3). Diese benutzerspezifische ELGA-Authorisation-Assertion ist Teil jeder Aktion in ELGA und wird zum Zweck der Autorisierung durch die AGW verarbeitet.

Obige zentrale Dienste werden über entsprechende Komponenten den damit unmittelbar verbundenen ELGA-Bereichen (siehe Abbildung 2) zur Verfügung gestellt.

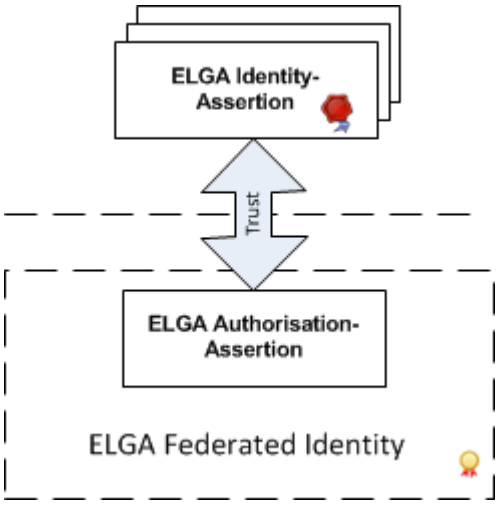


Abbildung 3: Beziehung zwischen ELGA-Identity- und Authorisation Assertion

Das ELGA-Protokollierungssystem dient der Wahrung von Transparenz und Nachvollziehbarkeit aller erfolgten Aktionen auf personenbezogene medizinische Dokumente in ELGA. Protokollnachrichten werden in lokale Audit Record Repositories (L-ARR) der ELGA-Bereiche und im L-ARR der zentralen Komponenten persistiert (Z-L-ARR). Darüber hinaus werden relevante Teile der Audits in einem zentral aufgestellten, aggregierten Audit Record Repository (A-ARR) für die Bedürfnisse des ELGA-Portals bereitgestellt. Folglich werden inhaltliche Protokollaufbereitungen ermöglicht, die der übersichtlichen und verständlichen Darstellung von Protokollinhalten für ELGA-Teilnehmer dienen. Die Gesamtmenge der in den einzelnen L-ARR, Z-L-ARR und A-ARR geführten Protokolle dient einer lückenlosen, forensisch nachvollziehbaren Aufzeichnung aller lesenden, schreibenden und modifizierenden Aktionen in ELGA. Diese Tatsache entbindet die IHE-Akteure

Document Consumer (Konsument), Document Source (Dokumentenquelle) sowie Registry (Verweisregister) und Repository (Datenspeicher) **nicht** von ihren Pflichten, die durchgeführten Transaktionen gemäß IHE-ATNA vollständig zu protokollieren.

2. Einführung

2.1. Festlegungen zur Notation

Um verbindliche Anforderungen eindeutig hervorzuheben werden die in IETF RFC 2119 beschriebenen Schlüsselwörter verwendet. Die in Großbuchstaben geschriebenen Schlüsselwörter kennzeichnen, welche Teile der Spezifikation bei einer Implementierung unbedingt zu berücksichtigen sind und welche Aspekte optionale Erweiterungen darstellen.

Die unten angeführte Tabelle gibt eine Übersicht der Übersetzung der verwendeten Schlüsselwörter ins Deutsche.

Schlüsselwort DE	EN lt. RFC2119	Beschreibung
MUSS	MUST	Umsetzung der Festlegung erforderlich
DARF NICHT	MUST NOT	Umsetzung der Festlegung definitiv untersagt
ERFORDERLICH	REQUIRED	Umsetzung der Festlegung erforderlich
SOLL	SHALL	Umsetzung der Festlegung erforderlich
SOLL NICHT	SHALL NOT	Umsetzung der Festlegung definitiv untersagt
SOLLTE	SHOULD	Umsetzung der Festlegung empfohlen
SOLLTE NICHT	SHOULD NOT	Umsetzung der Festlegung nicht empfohlen
EMPFOHLEN	RECOMMENDED	Umsetzung der Festlegung empfohlen
KANN	MAY	Umsetzung der Festlegung optional
OPTIONAL	OPTIONAL	Umsetzung der Festlegung optional

Tabelle 1: Notation nach IETF RFC 2119

2.2. Grundlagen der Elektronischen Gesundheitsakte

Die ELGA-Architektur basiert auf den auf der Homepage der ELGA GmbH (http://www.elga.gv.at/) veröffentlichten Grundlagen. Diese gliedern sich in die rechtlichen und technischen Grundlagen und in die Harmonisierungsarbeit.

Als rechtlichen Grundlage ist allen voran das Bundesgesetz BGBl. Nr. 111/2012: Elektronische Gesundheitsakte-Gesetz (ELGA-G) zu nennen. Weitere sind unter anderem das Datenschutzgesetz und das e-Governmentgesetz.

Die technische Grundlage bildet die Integrating the Healthcare Enterprise (IHE) Initiative, die die interoperable Anwendung von Standards wie Health Level 7 (HL7) und Digital Imaging and Communications in Medicine (DICOM) zum Ziel hat. IHE definiert zu ausgewählten

Anwendungsfällen so genannte Integrationsprofile. Diese legen die anzuwendenden Standards fest und definieren einen technischen Leitfaden für die Umsetzung um die nahtlose Zusammenarbeit sicherzustellen. Hersteller testen auf dem „Connectathon“ die Systeme untereinander um die Interoperabilität der entwickelten IHE-Lösungen (und Profilen) nachzuweisen.

In einem Integrationsprofil werden Akteure (Actors) definiert, die die Aufgabe eine Software-Applikation im Kontext des Profils benennen, und Transaktionen (Transactions), die konkrete Schnittstellen spezifizieren.

Die Harmonisierungsarbeit standardisiert die Metadaten und den Inhalt der medizinischen Dokumente und sorgt damit für die Austauschbarkeit und eine einheitliche Suche.

Die folgenden Unterkapitel liefern eine Übersicht über die technischen Grundlagen und deren Benutzung in der ELGA-Gesamtarchitektur.

2.3. Dokumentenaustausch auf regionaler Ebene – XDS Profil

Für den Austausch von Dokumenten innerhalb eines klar definierten Bereichs (XDS Affinity Domain) definiert IHE das Cross-Enterprise Document Sharing (XDS) Profil. In der aktuellen Variante (XDS.b) bildet dieses im Rahmen der ELGA die Basis für den regionalen Dokumentenaustausch.

Das Profil definiert, wie Dokumente von einer Dokumentenquelle (Document Source) in einem Datenspeicher (Document Repository) abgelegt werden, in einem Verweisregister (Document Registry) registriert werden und wie ein Konsument (Document Consumer) die Dokumente suchen und abrufen kann. Weiters definiert das Profil, wie die Patienten in diesem Zusammenhang identifiziert werden und berücksichtigt daher auch einen Akteur, der „Patient Identity Source“ bezeichnet wird. Dieser liefert Informationen zu den Identifikatoren, mit denen Dokumente registriert werden.

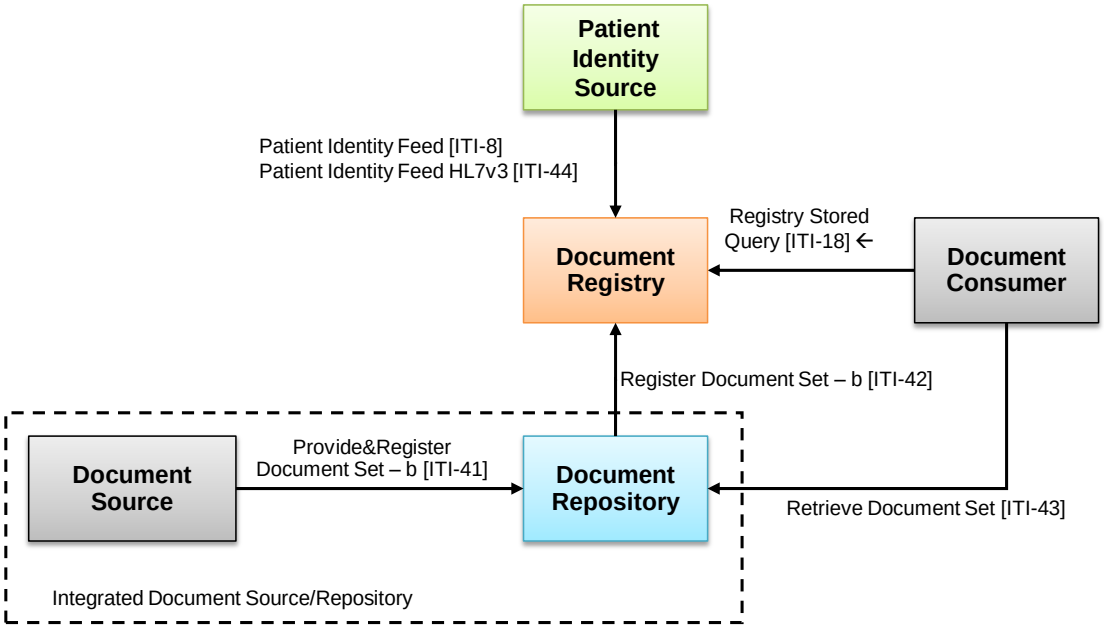


Abbildung 4: Cross-Enterprise Document Sharing – b (XDS.b)

Die *Abbildung 4* zeigt die Akteure und Transaktionen des Profils sowie im IHE Technical Framework [11] dargestellt, wobei die hier im Dokument verwendete Farbgebung ergänzt wurde.

Das Profil legt die Prozesse zum Ablegen von Dokumenten, zum Registrieren von Metadaten und Verweisen und zum Suchen von Dokumenten fest. Es gilt für Dokumente beliebigen Inhalts, wobei für den Austausch von Bildern das Profil Cross-Enterprise Document Sharing for Imaging (XDS-I.b) zur Anwendung kommt, welches analog aufgebaut ist.

In ELGA werden auf Basis der Harmonisierungsarbeit grundsätzlich CDA Dokumente (ELGA-CDA-Dokumente) verwendet, bei denen die Metadaten für die Registrierung teilweise im Dokument vorhanden und teilweise explizit durch die Document Source anzugeben sind. Die Document Registry wird in Anlehnung an das ELGA-Gesetz als „ELGA-Verweisregister“ bezeichnet. Dies streicht auch heraus, dass hier nur ELGA Dokumente sichtbar sein dürfen. Der Akteur „Patient Identity Source“ wird aufgrund der im Kapitel Patientenindex näher beschriebenen Hierarchie als Funktion des „Lokalen Patientenindex“ (L-PI) betrachtet.

2.4. Österreichweiter Zusammenschluss: XCA-Profil

Für die Suche und den Abruf von Dokumenten über XDS Affinity Domains hinweg definiert die IHE das Profil „Cross Community Access (XCA)“. Die Akteure und Transaktionen sind in *Abbildung 5* dargestellt.

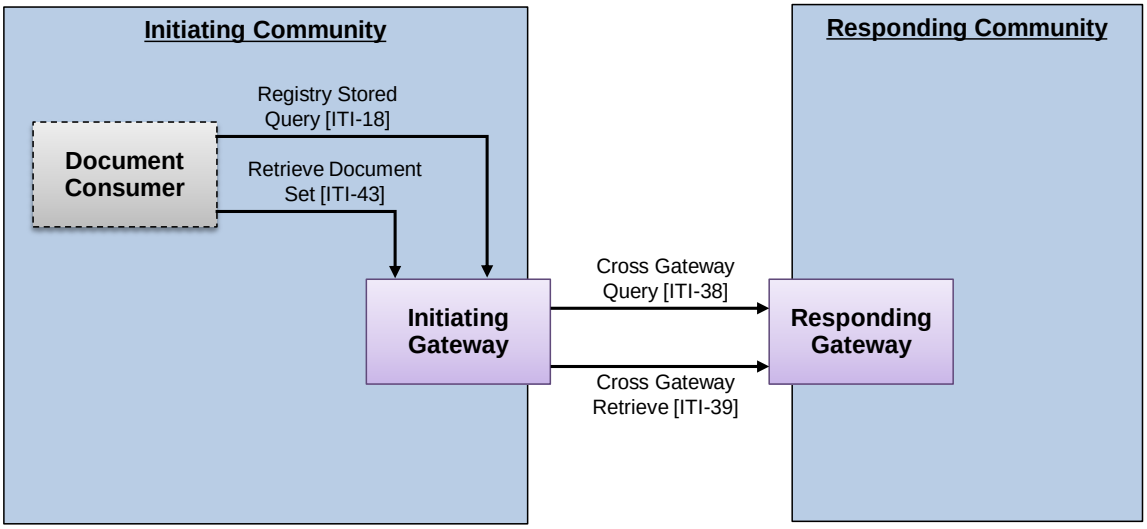


Abbildung 5: Cross Community Access (XCA)

Das Profil legt die Schnittstellen zur Suche (ITI-38) und zum Abruf von Dokumenten über sogenannte Communities fest. Für den Konsumenten (Document Consumer) bietet das Profil die Möglichkeit mit den gleichen Transaktionen zu arbeiten, wie in der eigenen XDS Affinity Domain.

Bei der Umsetzung des XCA Profils müssen die Partner (Communities) im Wesentlichen folgende Punkte festlegen:

- Gemeinsame Sicherheitskonzepte und Berechtigungsregeln
- Gemeinsame Standards für Dokumente und Metadaten
- eine gemeinsame Strategie zur Identifikation von Patienten bzw. zur Auffindung von anzufragenden Communites bei der Dokumentensuche.

In ELGA werden die Punkte folgendermaßen umgesetzt:

- Es gibt ein gemeinsames Informationssicherheitsmanagement (ISMS) und das Berechtigungs- und Protokollierungssystem sorgt für die einheitliche Durchsetzung und Überwachung von allgemeinen und individuellen Berechtigungsregeln.
- Durch die Harmonisierungsarbeit werden gemeinsame Standards für Dokumente und Metadaten definiert.
- Der Zentrale Patientenindex sorgt für die österreichweit eindeutige Identifikation der ELGA-Teilnehmer und bildet zugleich die Basis für das übergreifende Auffinden der Dokumente.

Um den Zusammenschluss von existierenden XDS Affinity Domains zur ELGA zu beschreiben, wird der Begriff „ELGA-Bereich“ eingeführt. Ein ELGA-Bereich implementiert

die gemeinsamen Richtlinien für den Zusammenschluss, die weiter unten im Dokument detailliert beschrieben sind. Aus Sicht des XCA-Profils stellt er eine „Community“ dar.

Auch der „Initiating Gateway“ bzw. der „Responding Gateway“ muss im Rahmen von ELGA die festgelegten Richtlinien implementieren und wird daher mit ELGA-Gateway bezeichnet. In ELGA-Terminologie ergibt sich das in *Abbildung 6* gezeigte Bild für den Zugriff auf ELGA Dokumente.

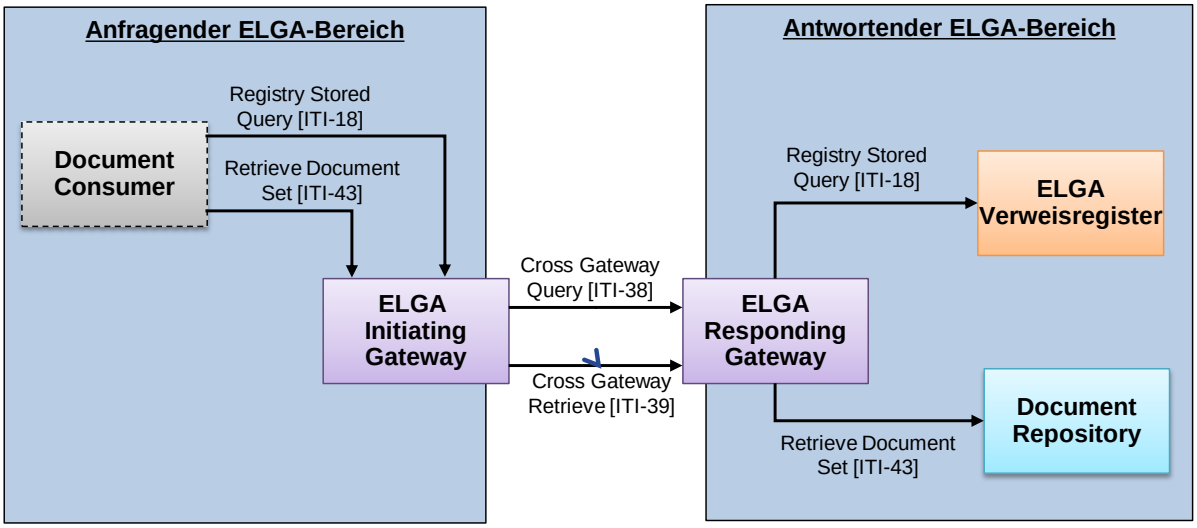


Abbildung 6: Dokumentensuche und Abruf auf Basis XDS.b / XCA

Die Dokumente bleiben im ELGA-Bereich, in dem sie anfallen, gespeichert.

IHE-konforme Lösungen waren zur Zeit der Ersterfassung dieses Dokumentes (in den Jahren 2008 bis 2011) insbesondere in folgenden Einrichtungen im Einsatz:

- Projekt NÖ ELGA (vormals NÖMED WAN): Gesundheitsnetz Niederösterreich
- Projekt GNT: Gesundheitsnetz Tirol
- Projekt eGOR: Elektronische Gesundheitsplattform der Ordenseinrichtungen
- Projekt eGP: Elektronische Gesundheitsplattform OÖ, Betreiber gespag

Im Rahmen des Zusammenschlusses können existierende IHE basierende Systeme entweder weitergeführt oder migriert werden. Eine Weiterführung ist durchaus sinnvoll, wenn regionale gesetzliche Richtlinien umgesetzt werden müssen. Eine Migration demgegenüber ist überall dort vorstellbar, wo regionale Bedürfnisse durch das ELGA-Gesetz vollständig erfüllt sind.

Darüber hinaus ermöglicht die Einführung von ELGA den Zugriff des ELGA-Teilnehmers auf seine eigenen ELGA-Gesundheitsdaten. Hierzu nutzen ELGA-Teilnehmer das ELGA-Portal über das Internet.

2.5. Identifikation von ELGA-Teilnehmern

Die Identifikation von ELGA-Teilnehmern erfolgt gemäß ELGA-Gesetz, §18 durch den Patientenindex. Aus technischer Sicht implementiert der Patientenindex

- den Akteur „Patient Demographics Supplier“ des IHE-Profils „Patient Demographics Query HL7 V3 (PDQV3)“
- den Akteur „Patient Identifier Crossreference Manager“ des IHE-Profils „Patient Identifier Cross-referencing HL7 V3 (PIXV3)“

Die *Abbildung 7* zeigt das Diagramm mit den Akteuren und Transaktionen für beide Profile gemeinsam.

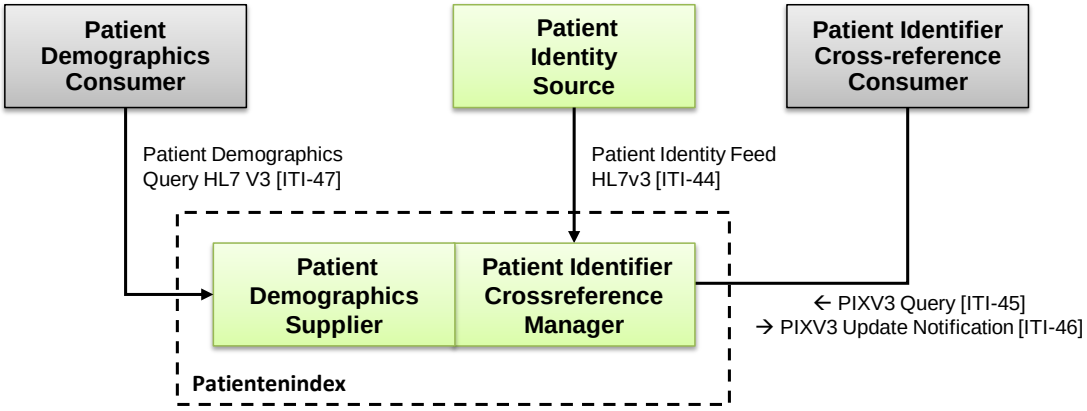


Abbildung 7: Profile PIXV3 und PDQV3

Das PIXV3 Profil wird nicht nur zur Befüllung des Patientenindex verwendet, sondern spielt auch eine wesentlich Rolle bei der Anwendung des XDS.b und XCA Profils in ELGA. Das XDS Profil legt fest, dass Dokumente mit einer sogenannten *XDS Affinity Domain Patient ID* (XAD-PID), einem eindeutigen Identifikator für den Bereich, registriert werden. Dieser Identifier wird in ELGA als L-PID (Lokaler Patienten Identifier) bezeichnet. Dieser Identifikator wird nun mit „Patient Identity Feed (ITI-44)“ an den zentralen Patientenindex (Z-PI) gemeldet, der die eingemeldeten Identitäten verknüpft und damit die Basis für die übergreifende Suche bereitstellt. Weitere Details sind in Kapitel 6 Patientenindex beschrieben.

2.6. Einheitliche Berechtigung und Protokollierung

Das ELGA-Gesetz definiert wesentliche Anforderungen bezüglich Datenschutz, Zugriffschutz und Protokollierung. Dieses Kapitel gibt einen Überblick über die Umsetzung der Gesamtarchitektur, um den Leser mit den im Folgenden verwendeten Begriffen vertraut zu machen. Eine detaillierte Beschreibung ist dem Kapitel 9 „Berechtigungs- und Protokollierungssystem“ zu entnehmen.

Ausgangspunkt für die Umsetzung sind folgende IHE-Profile:

- Audit Trail and Node Authentication (ATNA) und
- Cross-Enterprise User Assertion (XUA)

ATNA definiert die grundlegenden Sicherheitsanforderungen an die in einem Netzwerk kommunizierenden Systeme und wird in ELGA grundsätzlich als Sicherheitsinfrastruktur vorausgesetzt. Technisch werden folgende Transaktionen definiert:

- „Maintain Time [ITI-1]“ dient zur Zeit-Synchronisation der Systeme
- „Node Authentication [ITI-19]“ definiert zertifikatsbasierte, wechselseitige Authentisierung für alle beteiligten Systeme.
- „Record Audit Event [ITI-20]“ definiert wie Audit-Nachrichten an ein „Audit Repository“ übertragen werden sollen. Ergänzt wird diese Transaktion durch Audit Anforderungen in der Beschreibung der einzelnen Profile, die festlegen, welchen Inhalt Audit Nachrichten haben müssen. Diese stellen in ELGA Mindestkriterien dar.

Hinweis: Im Folgenden wird für das „Audit Repository“ häufig die Abkürzung ARR („Audit Record Repository) verwendet.

Das XUA Profil unterstützt die übergreifende Authentisierung und Autorisierung von Benutzern. Es beschränkt sich im Wesentlichen auf die Definition, wie bestimmte Attribute innerhalb Web Service basierter IHE-Transaktionen als SAML 2.0 Assertion übertragen werden und wie die Audit Protokollierung erfolgt. Die *Abbildung 8* zeigt das „Actor Diagram“ aus dem IHE Framework.

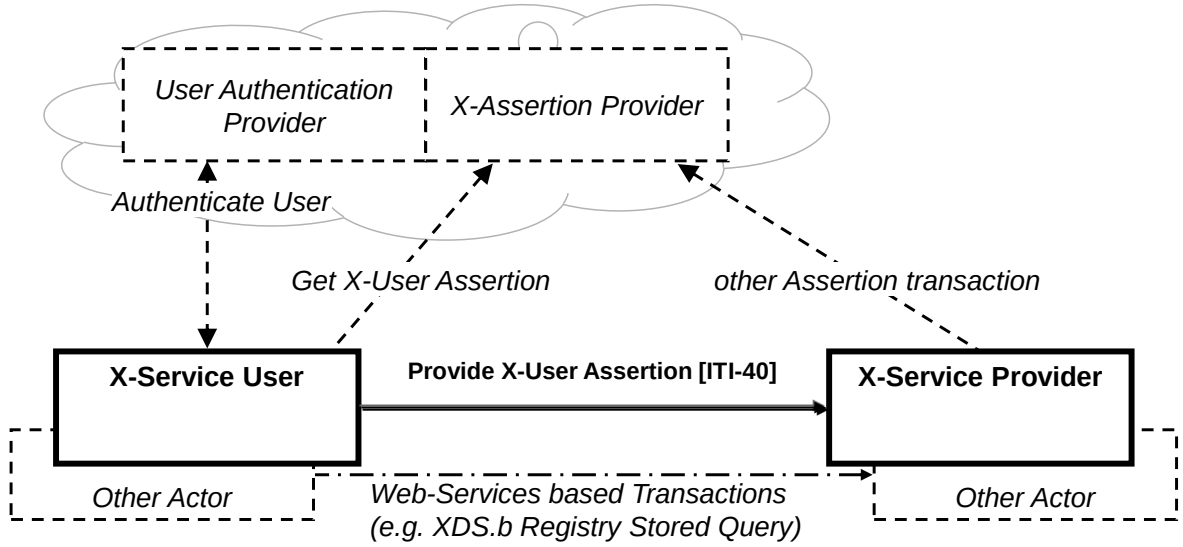


Abbildung 8: Cross Enterprise User Authentication – Akteure und Transaktionen

Die ELGA Architektur baut auf diesem Profil auf, indem ein einheitlicher *X-Assertion Provider*, das ELGA Token Service (ETS) definiert wird. Das Anfordern der Assertion erfolgt in ELGA

grundsätzlich auf Basis des Oasis Standards WS-Trust, Version 1.4. Um die erforderlichen Informationen zu transportieren, werden in die XUA Assertion zusätzliche Attribute aufgenommen (siehe IHE ITI Rev 12) und damit eine Klassenhierarchie von in ELGA angewendeten Assertions definiert.

In ELGA wird der User Authentication Provider mit „Identity Provider (IdP)“ bezeichnet. Es werden mehrere IdP unterstützt. Das ELGA Token Service föderiert die Identitäten, sodass beim Zugriff mit einer eindeutigen Benutzeridentität gearbeitet wird. Für Gesundheitsdiensteanbieter (und Benutzer der Ombudsstelle) erfolgt durch das ETS auch der in §19 geforderte Abgleich mit dem Gesundheitsdiensteanbieterindex (GDA-I). Dadurch wird sichergestellt, dass ausschließlich ELGA-GDA Zugriff auf ELGA-Gesundheitsdaten gewährleistet wird.

Für die Autorisierung des Zugriffs gemäß den gesetzlichen Anforderungen sind über die IHE-Profile hinausgehende Festlegungen erforderlich. Im Wesentlichen sind dies

- Die Berücksichtigung von Kontaktbestätigungen bzw. die Einführung eines durch das ELGA-G implizit geforderten Kontaktbestätigungsservices (KBS).
- Die Verwendung von allgemeinen und individuellen Berechtigungsregeln. Individuelle Berechtigungsregeln können über das ELGA-Portal vom Bürger festgelegt werden. Technisch werden die Berechtigungsregeln in einem „Policy Repository“ (PAP – Policy Administration Point) abgelegt.
- Die Autorisierung, also die Implementierung des Zugriffschutzes wird bei ELGA von der Geschäftslogik getrennt und in einer herausgezogenen Zugriffsteuerungsfassade (ZGF) durchgeführt. Diese hat nicht nur die Aufgabe, Aufrufe auf Basis der Berechtigungsregeln zuzulassen oder abzuweisen, sondern muss im Fall der Dokumentensuche auch das Suchergebnis filtern. In der Trefferliste scheinen damit nur Verweise auf Dokumente auf, die für den authentisierten Benutzer sichtbar sind.
- Um eine rasche und standardisierte Anbindung von existierenden XDS-Affinity Domains und von ELGA-GDA an ELGA zu ermöglichen, sieht die Architektur ein ELGA-Anbindungsgateway vor, das die erforderlichen Zugriffsteuerungsfassaden und die Funktionen von XCA Initiating- und Responding Gateway in sich vereint. Darüber hinaus sorgt das ELGA-Anbindungsgateway für die Protokollierung der Zugriffe auf Gesundheitsdaten und liefert damit in hinreichender und einheitlicher Weise die Informationen für die Anzeige am ELGA-Portal.

Die folgende *Abbildung 9* zeigt nun die Dokumentensuche und den Abruf (vgl. *Abbildung 6*) mit den Komponenten des Berechtigungssystems, wobei die Datenflüsse für einen Standard-Ablauf dargestellt sind. Die Darstellung dient dazu, den Leser mit allen relevanten Komponenten vertraut zu machen und den Bezug zu den implementierten Standards

herzustellen. Details sind dem Kapitel „Berechtigungs- und Protokollierungssystem“ zu entnehmen.

Die Abbildung zeigt, dass aus der Zugriffsteuerungsfassade des ELGA-Anbindungsgateways im anfragenden ELGA-Bereich nur ein Zugriff auf das ELGA Token Service erfolgt.

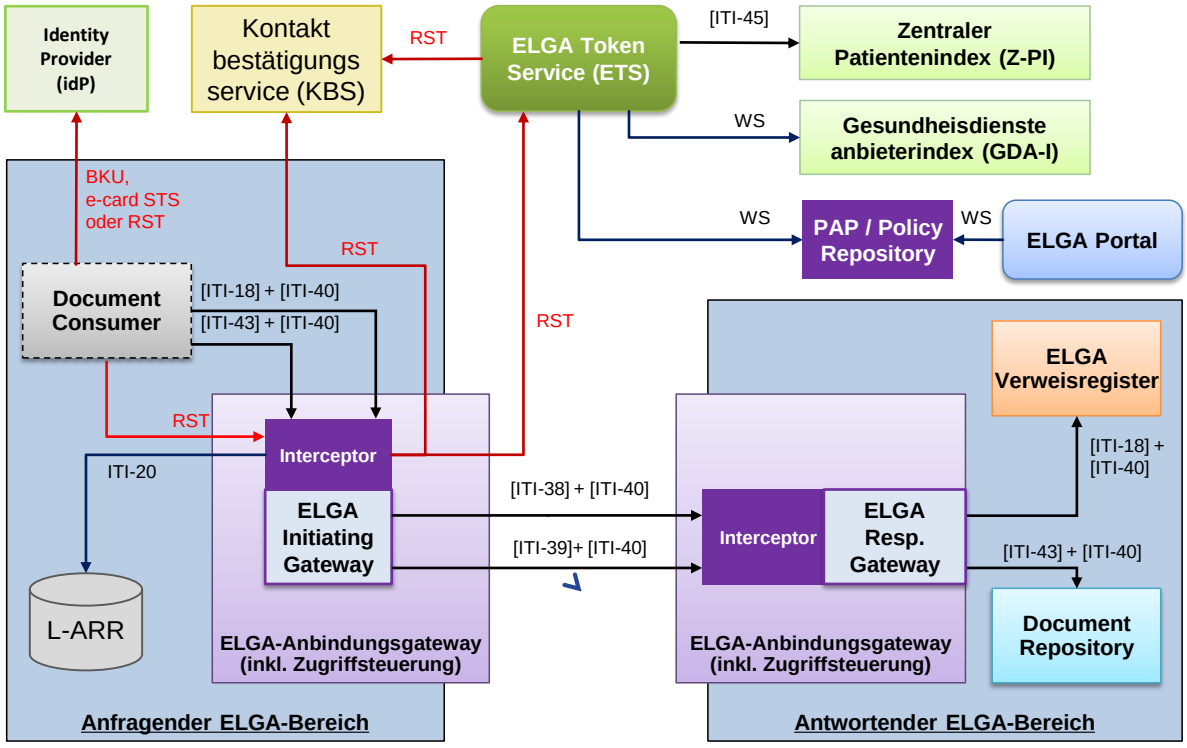


Abbildung 9: Dokumentensuche und Abruf mit Berechtigungssystem (beispielhaft). WS = Web Service Zugriff symbolisch

Das ETS führt alle erforderlichen Prüfungen durch, ruft bei einer Suchanfrage die Identifier der anzufragenden ELGA-Bereiche aus dem Z-PI ab und übermittelt die relevanten Autorisierungsattribute einschließlich der zutreffenden Berechtigungsregeln in einer Assertion je Ziel-ELGA Bereich. Damit kann das XCA-Gateway des anfragenden ELGA-Bereichs die Ziele ermitteln, die „Cross Gateway Query [ITI-38]“ Aufrufe erzeugen, und im Soap Header die Assertion für das Ziel mitgeben („Provide X-User Assertion [ITI-40]“). Im Ziel erfolgt die Autorisierung dann auf Basis der Assertion, wobei bei „Retrieve Document Set [ITI-43]“ ggf. zusätzlich Attribute aus der Registry abgerufen werden müssen.

Die Grundlage für die Protokollierung liefert die Transaktion „Record Audit Event [ITI-20]“. Für ELGA werden folgende zusätzlichen Festlegungen getroffen:

- In den Daten der vom jeweiligen IHE-Profil definierten Audit-Nachricht werden zusätzliche Daten für ELGA ergänzt, etwa der Name der zugreifenden Person.
- Die Audit Nachrichten werden lokal gespeichert (d.h. im jeweiligen ELGA-Bereich oder beim Betreiber von zentralen ELGA-Komponenten).

- Die Audit Nachrichten des ELGA-Anbindungsgateways werden zwecks Protokollauskunft im ELGA-Portal in einem zentralen aggregierten Audit Repository gesammelt und aufbereitet (A-ARR).

2.7. Übersicht der Anwendungsfälle

Die nachfolgenden Tabellen fassen die grundlegenden logisch-funktionalen Anwendungsfälle für ELGA-Teilnehmer, Vollmachtnehmer & Vertreter, ELGA-GDA, ELGA-Widerspruchstelle (ELGA-WIST), ELGA-Ombudsstelle (ELGA-OBST) bzw. ELGA-Sicherheits- und Regelwerkadministratoren zusammen.

Die in den folgenden Tabellen 2 und 3 (ELGA-Teilnehmer und Vertreter) angeführten Anwendungsfälle sind in enger Anlehnung an die involvierte e-Government Infrastruktur (MOA-ID Komponenten) gestaltet. Eine Autorisierung für den ELGA-Zugriff ist nur dann möglich, wenn dem ELGA-Berechtigungssystem ein vom e-Government ausgestellter und entsprechend digital signierter SAML 2.0 Token präsentiert wird. In Vertreterszenarien ist auch eine in den Token integrierte elektronische Vollmacht erforderlich.

In den anderen Anwendungsfällen (Tabellen 4, 5, 6) ist für den ELGA-Zugang und die Autorisierung eine Identity Assertion in Form vom SAML 2.0 zu präsentieren, welche von einem vertrauenswürdigen Identity Provider ausgestellt wurde. Über Vertrauenswürdigkeit von externen Identity Provider entscheidet die ELGA Sicherheitskommission (E-SIKO).

Eine weit detaillierte Beschreibung der hier angeführten Anwendungsfälle ist im Kapitel 9.1.4 zu finden. Darüber hinaus werden einige ausgewählte Anwendungsfälle, die aus Sicht des Berechtigungssystems von entscheidender Bedeutung sind, auch in Form von Workflow-Diagrammen im Anhang A „Beschreibung der Anwendungsfälle“ angeführt.

Die tabellarisch zusammengefassten Anwendungsfälle sind in der ersten Spalte mit Präfix und Nummer gekennzeichnet (siehe z.B. ET.1.1 oder BET.2.2 usw.). Diese hier eingeführte Identifikation der Anwendungsfelle muss in jeglicher ELGA-relevanten Dokumentation bei Referenzen auf die Anwendungsfälle entsprechend verwendet werden.

2.7.1. Anwendungsfälle von ELGA-Teilnehmern

Akteur / User-Agent	No	Anwendungsfall	Anmerkung / Beispiel
ELGA-Teilnehmer via Web-Browser oder Touch-Screen Applikation (Zugriff vom Internet)	ET.1.1	ELGA-Login Teilnehmer	Bürgerkarte (bzw. Handy-Signatur) erforderlich
	ET.1.2	Login-Token erneuern Teilnehmer	Token vorm Ablauf erneuern
	ET.1.3	Zugriffsrechte verwalten und anschließend Consent Dokument (PDF) signiert speichern	Opt-Out/Widerruf erklären, Dokumente ausblenden, löschen, GDA Zugriffsrechte einschränken, erweitern
	ET.1.4	Liste der gültigen GDA-Kontakte holen und einsehen	Das Kontaktbestätigungsservice muss kontaktiert und befragt werden
	ET.1.5	GDA vor einer Konsultation suchen (Name, Fach, Ordinationsadresse, etc.) und Berechtigungen setzen	Dieser Geschäftsfall wird nicht realisiert, da vom Gesetz nicht vorgesehen und eine mengenmäßige Begrenzung nicht erlaubt ist (Policies könnten mit tausenden GDA-Einträgen überfrachtet werden)
	ET.1.6	Ausgewählte Protokolle über stattgefundene Zugriffe auf die Gesundheitsdaten durch GDA ansehen	Selektion beispielsweise via Datumfilter, GDA-Filter, etc. einschränken
	ET.1.7	Ausgewählte Teile des Protokolls als PDF herunterladen/ausdrucken	Bedingungen am Client sind zu erheben (Adobe Reader Plugin installiert?)
	ET.1.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken
	ET.1.9	Ein bestimmtes CDA-Dokument auswählen, öffnen	Angezeigt wird eine via XSLT erzeugte HTML-View
	ET.1.10	Eigene Medikationsliste einsehen	On-Demand Dokument stellt e-Medikation zur Verfügung, Darstellung am Portal
	ET.1.10a	Abgelaufene Verordnungen als PDF herunterladen	Diese Liste der abgelaufenen Verordnungen wird am EBP nicht dargestellt
	ET.1.11	Ein bestimmtes Bildmaterial oder ganze Studie/Serie, das/die in einem Befund referenziert ist, auswählen, öffnen, anschauen	HTML5 freundliche **Darstellung** am Portal

	ET.1.12	Vorversionen eines bestimmten CDA-Dokumentes öffnen	Ausgehend von einer geöffneten aktuellen Version
	ET.1.13a	Ein bestimmtes Dokument als PDF herunterladen (oder drucken)	Adobe/PDF-Bedingungen am Client sind zu prüfen
	ET.1.13b	Ein oder mehrere Bilder der bildgebenden Diagnostik als JPEG herunterladen bzw. drucken (siehe diesbezüglich auch ET.1.11)	Das Portal bietet dem ELGA-Teilnehmer das Herunterladen der eigenen Bilder an
	ET.1.14	ELGA-Logout Teilnehmer	Session-Zeit ist limitiert (einige Stunden bei Aktivität bzw. wenige Minuten bei Untätigkeit). Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout). Noch gültige Token sind explizit zu invalidieren
	ET.1.15	Optional: Personalisierte Oberfläche, bestimmte Daten zwischenspeichern	CDA-Dokumente werden online jederzeit schnell zugreifbar. Geeignet z.B. für eine Merkliste

525 *Tabelle 2: Anwendungsfälle eines ELGA-Teilnehmers am ELGA-Portal*

526

2.7.2. Anwendungsfälle von bevollmächtigten Vertretern

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
Bevollmächtigter ELGA-Teilnehmer via Web-Browser oder Touch-Screen Applikation (Zugriff vom Internet)	BET.2.1	ELGA-Login als Vertreter	Bürgerkarte bzw. BKU erforderlich. Die Vollmacht bzw. die Vertretungsbefugnis muss via e-Government elektronisch abgebildet sein.
	BET.2.1a	ELGA-Login, Eltern für ihre Kindern	Berechtigte Eltern, können diese Möglichkeit für Kinder die jünger als 14 Jahre sind, via Vertretungsmodul nutzen (siehe Kapitel 10.2.3.2)
	BET.2.2	Login-Token erneuern bevollmächtigter Teilnehmer	Token vorm Ablauf erneuern
	BET.2.3	Zugriffsrechte verwalten und anschließend Consent Dokument (PDF) signiert speichern (im Namen des Vertretenen)	Opt-Out/Widerruf erklären, Dokumente ausblenden, löschen, GDA Zugriffsrechte einschränken, erweitern
	BET.2.4	Liste der gültigen GDA-Kontakte holen und einsehen (im Namen des Vertretenen)	Das Kontaktbestätigungsservice muss kontaktiert und befragt werden
	BET.2.5	GDA suchen (Name, Fach, Ordinationsadresse, etc.) (im Namen des Vertretenen)	Wird nicht umgesetzt. Siehe Kommentar bei ET.1.5
	BET.2.6	Ausgewählte Protokolle über stattgefundene Zugriffe auf die Gesundheitsdaten durch GDA ansehen (im Namen des Vertretenen)	Selektion beispielsweise via Datumfilter, GDA-Filter, etc. einschränken
	BET.2.7	Ausgewählte Teile des Protokolls als PDF herunterladen/ausdrucken (im Namen des Vertretenen)	Bedingungen am Client sind zu erheben (Adobe Reader Plugin installiert?)
	BET.2.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen (im Namen des Vertretenen)	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken

	BET.2.9	Ein bestimmtes CDA-Dokument auswählen, öffnen (im Namen des Vertretenen)	Angezeigt wird eine via XSLT erzeugte HTML-View
	BET.2.10	Medikationsliste im Namen des Vertretenen einsehen	Stellt e-Medikation zur Verfügung
	BET.2.11	Ein bestimmtes Bildmaterial oder ganze Studie/Serie auswählen, öffnen und anschauen	HTML5 freundliche Darstellung am Portal.
	BET.2.12	Vorversionen eines bestimmten CDA-Dokumentes öffnen (im Namen des Vertretenen)	Ausgehend von einer geöffneten aktuellen Version
	BET.2.13.a	Ein bestimmtes Dokument im Namen des Vertretenen als PDF herunterladen (drucken)	Adobe/PDF-Bedingungen am Client sind zu prüfen. Das Portal bietet dem Vertreter das Herunterladen der Bilder des Vertretenen an
	BET.2.13.b	Instanzen der bildgebenden Diagnostik im Namen des Vertretenen als JPEG herunterladen (bzw. drucken)	Das Portal bietet dem Vertreter das Herunterladen der Bilder des Vertretenen an (siehe auch BET.2.11)
	BET.2.14	ELGA-Logout als Vetreter	Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout). Noch gültige Token sind explizit zu invalidieren (Siehe ET.1.14)

Tabelle 3: Anwendungsfälle eines bevollmächtigten ELGA-Teilnehmers (gewillkürte Vollmacht)am ELGA-Portal

2.7.3. GDA-Anwendungsfälle

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-GDA via KIS-System oder Arztsoftware (Kein Internet-Zugriff erlaubt)	GDA.3.1	ELGA-Login GDA	Basierend auf erfolgter Authentifizierung durch vertrauenswürdigen IdP ohne zusätzliche Anwenderaufforderung.
	GDA.3.2	Login-Token erneuern (Renew) GDA	Beim Login ausgestellten Token vorm Ablauf der Gültigkeitsdauer erneuern
	GDA.3.3	Demografische Patientensuche	Via L-PI und indirekt zu Z-PI oder optional unmittelbar via Z-PI (PDQ)
	GDA.3.4	Situatives Opt-Out umsetzen	Dieser Anwendungsfall wird in der Gesamtarchitektur nicht behandelt, da die Umsetzung des situativen Opt-Outs Angelegenheit des lokalen Systems des GDA ist. Details dazu siehe im Organisationshandbuch.
	GDA.3.5	Patient identifizieren und einmelden	Identifikation des Patienten vor Ort und PIF
	GDA.3.6	Behandlungszusammen-hang schaffen	Für eindeutig identifizierten Patienten wird ein Kontakt gemeldet bzw. ein Kontakt bestätigt.
	GDA.3.7	Behandlungszusammenhang (Kontakt) delegieren	Ein Kontakt kann an einen GDA weitergereicht werden, der in die Behandlung explizit involviert wird. Siehe hierfür Kontaktbestätigungs-Service.
	GDA.3.8	Behandlungszusammenhang (Kontakt) stornieren	Ein Kontakt kann vom GDA storniert werden (z.B. administrativer Fehler etc.)
	GDA.3.9	Dokumentenliste zu einem Patienten abrufen	Registry Stored Query [ITI-18] wird ausgelöst
	GDA.3.10	Dokument(e) zu einem Patienten abrufen	Retrieve Document Set [ITI-43] wird ausgelöst. Das Dokument wird lokal nur temporär zwischengespeichert
	GDA.3.11	Medikationsliste des Patienten abrufen	siehe auch Anforderungsdokument e-Medikation
	GDA.3.12a	Ein oder mehrere e-Med-ID holen	[EMEDAT-1] Anfrage an e-Medikation stellen
	GDA.3.12b	Verordnung bzw. Advice eines oder mehrerer Medikamente speichern	siehe auch Anforderungsdokument e-Medikation

	GDA.3.12c	e-Med-ID Token holen	[EMEDAT-1] RST-Anfrage. Der e-Med STS wird kontaktiert
	GDA.3.13	Abgabe eines oder mehrerer Medikamente speichern	siehe auch Anforderungsdokument e-Medikation
	GDA.3.14	DICOM-Instanzen (Studien/Serien/Einzelbilder) der bildgebenden Diagnostik abrufen	Retrieve Imaging Document Set wird ausgelöst. Eventuelles Speichern im lokalen Bereich ist nicht vorgesehen (Speichern außerhalb von ELGA in PACS).
	GDA.3.15	Vorherige Version eines bestimmten Dokumentes abrufen	Verlinkte ältere Version des Dokumentes kann abgerufen werden
	GDA.3.16	Ausgewählte Dokumente des Patienten herunterladen und lokal speichern	Wie GDA.3.10 mit anschließendem Speichern.
	GDA.3.17	Registrieren (freigeben) eigener Dokumente in ELGA	Provide and Register Document Set bzw. NonVersioningUpdate wird ausgelöst (siehe Kapitel 9.7.3)
	GDA.3.18.a	Updaten von ELGA-Dokumenten	Einstellen neuer Versionen von CDA-Dokumenten
	GDA.3.18.b	Storno von ELGA-Dokumenten	Dokumente stornieren und dadurch unzugänglich machen
	GDA.3.19	ELGA-Logout GDA	Explizites oder automatisches (Timeout) Abmelden von ELGA
	GDA.3.20	Update von ELGA-Dokumenten bei abgelaufener Kontaktbetätigung	Wie Anwendungsfälle GDA.3.18.a und 3.18.b mit dem Unterschied, dass eine abgelaufene (bis zu einem Jahr) Kontaktbestätigung ausreichend ist
	GDA.3.21	Zugriffe auf Gesundheitsdaten für ELGA-Teilnehmer protokollieren	Diese Aufgabe wird von der ZGF transparent erledigt. Siehe 2 Phasen Protokollierungskonzept im A-ARR
	GDA.3.22	Clearing von Metadaten (Link-Change bzw. Move von Dokumenten)	Clearing ist via XAD-PID Link Change und ELGA-1 Transaktionen durchzuführen (siehe Kapitel 9.7)

533 *Tabelle 4: Anwendungsfälle eines ELGA-GDA*

2.7.4. Anwendungsfälle der Widerspruchstelle

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Widerspruchstelle (Zugriff über gesichertes Netzwerk)	WIST.4.1	ELGA-Login WIST (Vorgesehen ist ein automatischer Prozess)	Prozess (oder Batch-Job) läuft unter einen authentifizierten und in ELGA föderierten Account. Mitprotokolliert wird der Account.
	WIST.4.2	Vertretenen ELGA-Teilnehmer eindeutig identifizieren (durch Mitarbeiter der WIST). ELGA Anmeldung ist nicht erforderlich. Z-PI Zugriff über ITSV-interne Schnittstelle.	Der Vertretene muss eine Kopie eines gültigen Lichtbildausweises zusätzlich zur von ihm unterschriebenen gewünschten Policy mitschicken. PDQ zwecks Identifizierung durch Z-PI erforderlich (bPK-GH des ELGA-Teilnehmers ist notwendig)
	WIST.4.3	Opt-Out, Opt-Out Widerruf, partieller Opt-Out oder partieller Opt-Out Widerruf wird durchgeführt	Policy Administration Point (PAP) wird kontaktiert und die neue Policy samt amtssignierten Policy-Consent Document (PDF) online gespeichert
	WIST.4.4	ELGA-Logout WIST	Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout)

Tabelle 5: Anwendungsfälle der ELGA-Widerspruchstelle

2.7.5. Anwendungsfälle der ELGA-Ombudsstelle

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Ombudsstelle via Web-Browser (Zugriff über das ELGA-Portal vom gesicherten Netzwerk)	OBST.5.1	ELGA-Login als OBST (Anmelden am Portal, genaue Spezifizierung ist in Bearbeitung)	Bestandsgeber Zertifikat etwa auf Bürgerkarte (oder gleichwertiges) erforderlich. Berechtigungen via entsprechende ELGA-Rolle in GDA-Index. Protokolliert wird namentlich.
	OBST.5.2	Vertretenen ELGA-Teilnehmer eindeutig identifizieren	Der Vertretene muss einen gültigen Lichtbildausweis vorzeigen können. PDQ zwecks Identifizierung durch Z-PI erforderlich (bPK-GH des ELGA-Teilnehmers)
	OBST.5.3	Zugriffsrechte verwalten und anschließend Consent Dokument (PDF) signiert speichern (im Namen des Vertretenen)	Opt-Out/-Widerruf erklären, Dokumente ausblenden, löschen, GDA Zugriffsrechte einschränken, erweitern
	OBST.5.4	Liste der gültigen GDA-Kontakte holen und einsehen (im Namen des Vertretenen)	Das Kontaktbestätigungsservice muss kontaktiert und befragt werden
	OBST.5.5	GDA im Namen des Vertretenen vor einer Konsultation suchen (Name, Fach, Ordinationsadresse,...)	Wird nicht realisiert. Siehe Kommentar bei ET.1.5
	OBST.5.6	Ausgewählte Protokolle über stattgefundene Zugriffe auf die Gesundheitsdaten durch GDA ansehen (im Namen des Vertretenen)	Selektion beispielsweise via Datumfilter, GDA-Filter, etc. einschränken
	OBST.5.7	Ausgewählte Teile des Protokolls als PDF herunterladen/ausdrucken (im Namen des Vertretenen)	Bedingungen am Client sind zu erheben
	OBST.5.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen (im Namen des Vertretenen)	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken

	OBST.5.9	Ein bestimmtes CDA-Dokument auswählen, öffnen (im Namen des Vertretenen)	Angezeigt wird eine via XSLT erzeugte HTML-View
	OBST.5.10	Eigene Medikationsliste einsehen (im Namen des Vertretenen)	Stellt e-Medikation zur Verfügung
	OBST.5.11	Instanzen der bildgebenden Diagnostik im Namen des Vertretenen auswählen bzw. öffnen	HTML5 freundliche Darstellung am Portal
	OBST.5.12	Vorversionen eines bestimmten CDA-Dokumentes öffnen (im Namen des Vertretenen)	Ausgehend von einer geöffneten aktuellen Version
	OBST.5.13a	Ein bestimmtes Dokument im Namen des Vertretenen als PDF herunterladen (eventuell drucken)	Adobe/PDF-Bedingungen am Client sind zu prüfen
	OBST.5.13b	Ein bestimmtes Bild im Namen des Vertretenen als JPEG herunterladen (eventuell drucken)	Das Portal bietet dem Vertreter das Herunterladen der Bilder des Vertretenen an
	OBST.5.14	ELGA-Logout OBST	Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout)

537 *Tabelle 6: Anwendungsfälle ELGA-Ombudsstelle*

538

2.7.6. Anwendungsfälle der Administration

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Regelwerk-administrator (direkter Zugriff auf Server)	RADM.6.1	ELGA-Login eines Regelwerkadministrators (Anmelden lokal)	Autorisierung im lokalen Verzeichnisdienst notwendig. Auditing im lokalen System erforderlich. Administrator hat keine Rechte Auditing Einstellungen zu verändern.
	RADM.6.2	Policy Administration Point & Repository-Daten (PAP) verwalten, warten, Probleme identifizieren und beheben. Generelle Policies einpflegen.	Voller Zugriff auf die im PAP gespeicherten Daten, welche jedoch keine namentliche Zuordnung ermöglichen. Bei individuellen Policies bPK-GH als Fremdschlüssel vorhanden.
	RADM.6.3	PAP-Zugriffsprotokolle einsehen und auswerten	Zugriffe des Administrators werden im lokalen Auditing System mitprotokolliert.
	RADM.6.4	ELGA-Logout Regelwerkadministrator	Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout)

Tabelle 7: Anwendungsfälle eines ELGA-Regelwerkadministrators

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Sicherheits-administrator (direkter Zugriff auf Server)	SADM.7.1	ELGA-Login Sicherheitsadministrator (Anmelden lokal)	Autorisierung im lokalen Verzeichnisdienst notwendig. Administrator hat volle Rechte Auditing Einstellungen zu verändern. Keine Zugriffsrechte auf die im PAP gespeicherten Daten. Keine Zugriffsrechte auf Systemressourcen, die außerhalb der Protokollierung liegen.
	SADM.7.2	ELGA-bezogene Audits verwalten, warten, Probleme identifizieren und beheben	Voller Zugriff auf Audit-Protokolle, welche die Tätigkeit der ELGA-Regelwerkadministratoren erfassen.
	SADM.7.3	A-ARR bzw. sonstige ELGA-relevante ATNA und nicht ATNA Zugriffsprotokolle einsehen	Zugriffe des ELGA-Sicherheitsadministrators müssen im lokalen Auditing System mitprotokolliert werden
	SADM.7.4	ELGA-Logout Sicherheitsadministrator	Aktiv durch Benutzer oder nach gewisser Zeit der Untätigkeit automatisch (Timeout)

Tabelle 8: Anwendungsfälle eines ELGA-Sicherheitsadministrators

Es ist anzumerken, dass weitere (neue) Anwendungsfälle durch ELGA-Anwendungen (z.B. e-Medikation) möglich sind. Diese Anwendungsfälle werden in der entsprechenden Dokumentation der einzelnen ELGA-Anwendungen beschrieben.

3. Darstellung der Gesamtarchitektur

3.1. Rahmenwerk und Standards

Die Architektur der ELGA basiert generell auf den im Einführungskapitel 2 beschriebenen IHE Integrationsprofilen XDS und XCA sowie im Bereich der Zugriffsberechtigungssteuerung auf XUA.

Die Konzepte des IHE Kommunikationsframeworks werden basierend auf der **Revision 12** des Integrationsprofils IT Infrastructure Technical Framework Volume 1-4 [11] umgesetzt. Zusätzlich muss das im angeführten ITI-Framework des öfteren referenzierte OASIS Standard, Cross-Enterprise Security and Privacy Authorization (XSPA) Profil weitgehend berücksichtigt werden. Die drei grundlegenden Bestandteile des XSPA Profils sind wie folgt aufgelistet:

- OASIS XSPA Profile of WS-Trust for Healthcare
- OASIS XSPA Profile of XACML
- OASIS XSPA Profile of SAML for Healthcare

Die daraus resultierende Festlegung für ELGA ist, dass die Autorisierung von XDS und XCA-Zugriffen auf Basis von OASIS WS-Trust Standard Version 1.4 erfolgen muss, wobei SAML (Attributs-)Erweiterungen und Anpassungen entsprechend der angeführten XSPA Profilen entworfen und realisiert werden müssen.

Die Strukturierung der ELGA in föderierte ELGA-Bereiche, ausgehend von Konzepten gemäß XCA, XUA und WS*/WS-Trust, erfordert das Design eines verteilten Berechtigungssystems. Die im Rahmen des Berechtigungssystems eingesetzten Informations- und Kommunikationsstandards werden dabei entsprechend der aktuellen Version verwendet.

3.2. Fachliche Gesamtarchitektur (UML Klassendiagramm)

Die in der Abbildung 2 (und Abbildung 1) dargestellte Architektur von ELGA mit Berücksichtigung der angeführten Anwendungsfälle, lässt sich mit dem in der Abbildung 10 dargestellten UML Klassendiagramm weiter präzisieren. Um die Übersichtlichkeit zu bewahren, ist der Detailgrad der Abbildung absichtlich reduziert. Es sind nur jene Komponenten (Klassen) einbezogen worden, die in den erwähnten vereinfachten Abbildungen der ersten Kapitel bereits eingezeichnet sind. Das Diagramm dient primär der Übersicht auf logischer Ebene und fokussiert auf wesentliche Beziehungen zwischen den Klassen. Einzelheiten werden in weiteren Kapiteln detailliert ausgeführt.

Die in der Abbildung 10 dargestellten Klassen können wie folgt charakterisiert werden:

- Die abstrakte Klasse *ELGA-Benutzer* hat eine eindeutige ID, eine konkrete Rolle und ist über eine ELGA-Authorisation Assertion (SAML-Ticket) in ELGA föderiert. Die Klasse ist eine Generalisierung von:
  - *ELGA-Teilnehmer*
  - *ELGA-GDA*
  - *Bevollmächtigter ELGA-Teilnehmer (inklusive OBST)*
  - *Widerspruchstelle (WIST)*

- Ein *ELGA-Teilnehmer*
  - ist eindeutig identifiziert via Z-PI und besitzt eine dort geführte bPK-GH

- kann mehrere lokale Patienten ID (LPID/XAD-PID) besitzen, die in L-PIs geführt sind
- ist mit einer ELGA User I Assertion in ELGA föderiert (angemeldet)
- kann mehrere Behandlungszusammenhänge (Kontaktbestätigungen) mit GDA haben
- kann mehrere ELGA-Gesundheitsdaten (CDA) besitzen
- kann individuelle Berechtigungen (Policy) erfassen, definieren und warten
- hat immer die Rolle Bürger

- Ein *ELGA-GDA*
  - Hat eine eindeutige OID, die im GDA-Index geführt wird
  - Hat eine (oder mehrere) im GDA-I geführte ELGA-Rollen
  - ist entweder eine Organisation (z.B. Krankenhaus) oder eine physische Person (Arzt)
  - ist mit einer ELGA HCP-Assertion in ELGA föderiert (angemeldet)
  - meldet *Behandlungszusammenhänge* (Kontaktbestätigungen) von den sich in ärztlicher Behandlung befindenden Patienten (*ELGA-Teilnehmer*)
  - Ist über einen dedizierten *ELGA-Bereich* an ELGA angebunden

- Die ELGA-Ombudsstelle (OBST) ist eine Spezialisierung der Klasse *ELGA-GDA* und gleichzeitig ein bevollmächtigter ELGA-Teilnehmer (Vertreter)
  - Aufgrund der Tatsache, dass die OBST immer als bevollmächtigter Teilnehmer (siehe weiter im Kapitel 5) in ELGA angemeldet (föderiert) wird, ist es nicht vorgesehen, die OBST als selbständige Instanz ohne Vertretung in ELGA zu föderieren.

- Ein Bevollmächtigter *ELGA-Teilnehmer*
  - Vertritt einen *ELGA-Teilnehmer*
  - Ist entweder selbst ein *ELGA-Teilnehmer*, oder eine *Ombudsstelle* (*OBST*) oder eine *Widerspruchstelle* (*WIST*)
  - Ist mit einer ELGA Mandate I Assertion in ELGA föderiert (angemeldet). Eine Ausnahme ist WIST (eine detaillierte Erklärung ist im entsprechenden Kapitel 4 angeführt)

- Eine *Widerspruchstelle* (WIST)

- Durch das Anfordern einer Mandate I Assertion kann die Widerspruchsstelle zum bevollmächtigten ELGA-Teilnehmer werden
- Ist nicht im *GDA-Index* geführt
- Greift unmittelbar auf *PAP* Web-Service zu

- Ein *Behandlungszusammenhang* (Kontaktbestätigung)
  - Hat eine eindeutige ID (TRID)
  - Ist im Kontaktbestätigungsservice (*KBS*) aufgehoben (gespeichert)
  - Ist ein Akt zwischen einem ELGA-GDA und einem ELGA-Teilnehmer
  - Zugriff auf die Gesundheitsdaten eines ELGA-Teilnehmers ist für ELGA-GDA nur bei Vorhandensein einer gültigen Kontaktbestätigung möglich. Dies ist von einer *Generellen Policy* vorgeschrieben.

- *GDA-Index*
  - Ist ein zentrales Web-Service, welches aktive ELGA-GDA zu führen hat

- *KBS* (Klasse Kontaktbestätigungsservice)
  - Ist ein zentrales Web-Service, welches die von den ELGA-GDA gemeldeten *Behandlungszusammenhänge* speichert und verwaltet

- *Z-PI* (Zentraler Patientenindex)
  - Ist ein zentrales Web-Service, welches alle ELGA-Teilnehmer und mit den bPK-GH der Teilnehmer verlinkte LPIDs (Linkgruppen) führt

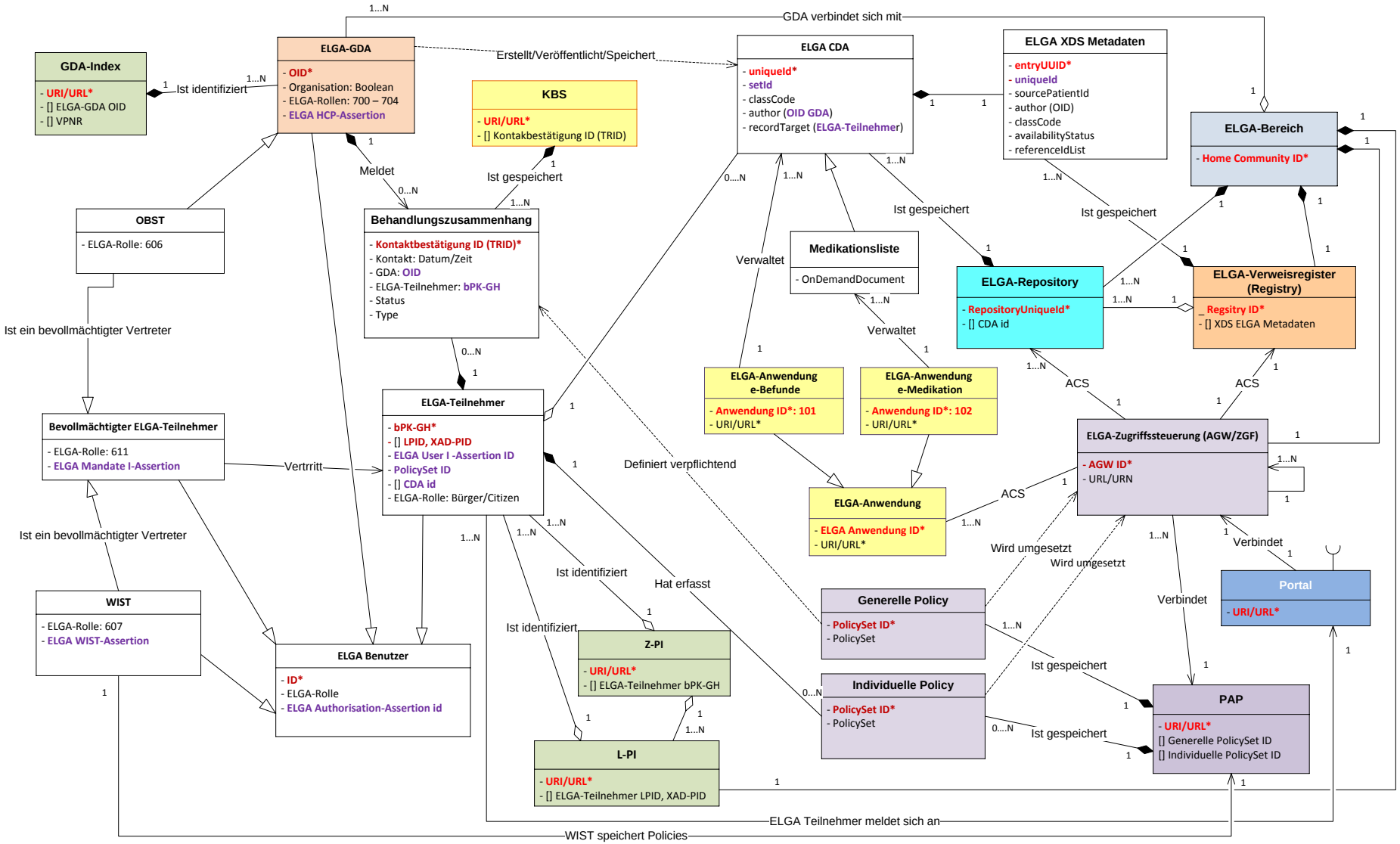

GDA-Index
- URI/URL*
- [] ELGA-GDA OID
- [] VPNR
Ist identifiziert
ELGA-GDA
- OID*
- Organisation: Boolean
- ELGA-Rollen: 700 – 704
- ELGA HCP-Assertion
GDA verbindet sich mit
Erstellt/Veröffentlicht/Speichert
ELGA CDA
- uniqueId*
- setId
- classCode
- author (OID GDA)
- recordTarget (ELGA-Teilnehmer)
ELGA XDS Metadaten
- entryUUID*
- uniqueId
- sourcePatientId
- author (OID)
- classCode
- availabilityStatus
- referenceIdList
KBS
- URI/URL*
- [] Kontakbestätigung ID (TRID)
Meldet
Ist gespeichert
ELGA-Bereich
- Home Community ID*
OBST
- ELGA-Rolle: 606
Behandlungszusammenhang
- Kontaktbestätigung ID (TRID)*
- Kontakt: Datum/Zeit
- GDA: OID
- ELGA-Teilnehmer: bPK-GH
- Status
- Type
Verwaltet
Medikationsliste
- OnDemandDocument
ELGA-Repository
- RepositoryUniqueId*
- [] CDA id
ELGA-Verweisregister (Registry)
_ Regsitry ID*
- [] XDS ELGA Metadaten
Ist ein bevollmächtigter Vertreter
ELGA-Anwendung e-Befunde
- Anwendung ID*: 101
- URI/URL*
ELGA-Anwendung e-Medikation
- Anwendung ID*: 102
- URI/URL*
ACS
Bevollmächtigter ELGA-Teilnehmer
- ELGA-Rolle: 611
- ELGA Mandate I-Assertion
Vertritt
ELGA-Teilnehmer
- bPK-GH*
- [] LPID, XAD-PID
- ELGA User I -Assertion ID
- PolicySet ID
- [] CDA id
- ELGA-Rolle: Bürger/Citizen
Definiert verpflichtend
ELGA-Zugriffssteuerung (AGW/ZGF)
- AGW ID*
- URL/URN
ELGA-Anwendung
- ELGA Anwendung ID*
- URI/URL*
Wird umgesetzt
Verbindet
Portal
- URI/URL*
Ist identifiziert
Hat erfasst
WIST
- ELGA-Rolle: 607
- ELGA WIST-Assertion
Generelle Policy
- PolicySet ID*
- PolicySet
Individuelle Policy
- PolicySet ID*
- PolicySet
Ist gespeichert
PAP
- URI/URL*
[] Generelle PolicySet ID
[] Individuelle PolicySet ID
ELGA Benutzer
- ID*
- ELGA-Rolle
- ELGA Authorisation-Assertion id
Z-PI
- URI/URL*
- [] ELGA-Teilnehmer bPK-GH
L-PI
- URI/URL*
- [] ELGA-Teilnehmer LPID, XAD-PID
ELGA Teilnehmer meldet sich an
WIST speichert Policies

Abbildung 10: ELGA UML Klassendiagramm der Gesamtarchitektur (Übersicht)

- *L-PI* (Lokaler Patientenindex, eine Instanz pro *ELGA-Bereich*)
  - Ist ein lokales Web-Service in einem *ELGA-Bereich,* welches die LPIDs (d.h. die Umsetzung des XAD-PID Konzepts in ELGA) der ELGA-Teilnehmer führt
  - Kommuniziert zwecks Datenerfassung und Abgleich mit dem Z-PI

- *ELGA CDA Dokument*
  - Hat eine weltweit eindeutige ID
  - Wird von einem ELGA-GDA (in der IHE Rolle Document Source Akteur) in ELGA veröffentlicht
  - Wird in einem ELGA-Repository gespeichert
  - ELGA-Teilnehmer haben keine oder mehrere CDA Dokumente
  - Hat abfragbare/durchsuchbare Metadaten (siehe XDS ELGA Metadaten unten)

- *XDS ELGA Metadaten*
  - Ein Satz von Metadaten beschreibt ein CDA Dokument (steht in 1:1 Relation)
  - Sind mit einer DocumentEntry.entryUUID eindeutig identifiziert
  - Sind in einem ELGA-Verweisregister gespeichert

- *Medikationsliste* (eine dynamisch, On-Demand erstellte Liste)
  - Ist eine Spezialisierung von ELGA CDA Dokument
  - Ist ein IHE On-Demand Dokument
  - Wird von der *ELGA-Anwendung e-Medikation* erstellt, verwaltet, gespeichert

- *ELGA-Anwendung* (Allgemeine Klasse)
  - Ist ein Web-Service
  - Wird von einer Instanz der *ELGA-Zugriffssteuerung* geschützt (Access Control, ACS)
  - Unterliegt dem ELGA-Berechtigungssystem

- *ELGA-Anwendung e-Medikation*
  - Ist ein zentrales Web-Service
  - Stellt die Medikationsliste eines ELGA-Teilnehmers in Form von On-Demand Dokument zur Verfügung
  - Ist eine Spezialisation der allgemeinen ELGA-Anwendungsklasse

- *ELGA-Anwendung e-Befunde*
  - Ist ein verteiltes Web-Service (eine virtuelle Einheit als Summe aller Bestandteile in den einzelnen ELGA-Bereichen)
  - Stellt verteilte Gesundheitsdaten (CDA und Bilddaten) von ELGA-Teilnehmern zur Verfügung
  - Ist eine Spezialisation der allgemeinen ELGA-Anwendungsklasse

- *ELGA-Bereich*
  - Hat eine eindeutige Home Community ID
  - Verbindet (hostet) mehrere ELGA-GDA
  - Ist von einer Instanz der *ELGA-Zugriffssteuerung* geschützt (Access Control, ACS)
  - In einem *ELGA-Bereich* liegt genau eine *L-PI* Instanz vor
  - Hat genau ein *ELGA-Verweisregister*
  - Hat ein oder mehrere *ELGA-Repositories*

- *ELGA-Zugriffssteuerung* (ZGF) eingebettet in genau ein Anbindungsgateway (AGW)
  - Steht in 1:1 Relation mit einem *ELGA-Bereich (praktisch können geclustert werden)*
  - Setzt über das Berechtigungssystem *Generelle Policies* und *Individuelle Policies* via Policy-Enforcement um
  - Schützt, weil vorgeschaltet (Access Control - ACS), das *ELGA-Verweisregister* und die *ELGA-Repositories*
  - Schützt, weil vorgeschaltet (Access Control - ACS), die *ELGA-Anwendung e-Medikation und e-Befunde*
  - Verbindet das ELGA-*Portal* mit ELGA
  - Pflegt eine direkte Verbindung mit dem PAP

- Verbindet mit anderen AGW/ZGF Instanzen von entfernten Bereichen
- Integriert ELGA-Anwendungen, wie e-Medikation (im UML nicht dargestellt)

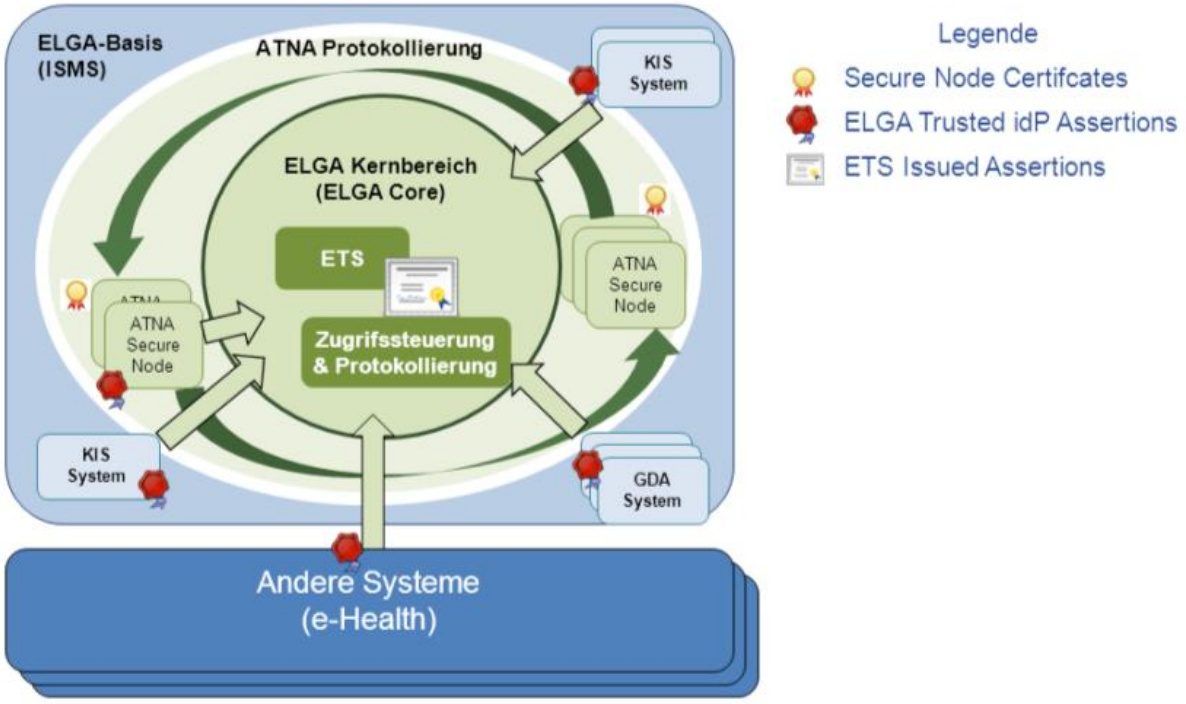
- *Portal* (ELGA Bürgerportal - EBP)
  - Ist eine Web-Applikation, die Web-Services konsumiert
  - *ELGA-Teilnehmer* greifen über das *Portal* auf ELGA zu
  - Ist via einer Instanz einer *ELGA-Zugriffssteuerung* in ELGA integriert

- *PAP* (die Klasse für die Verwaltung und Administration der Berechtigungen)
  - Ist ein zentrales Web-Service zur Verwaltung, Erstellung und Speicherung von *Generellen* und *Individuellen Policies*

Weitere Einzelheiten und ergänzende Erklärungen sind in den nachfolgenden Kapiteln enthalten.

3.3. Definition der Grenzen von ELGA

Die Grenzen von ELGA können aus unterschiedlichen Blickwinkeln (technisch, juristisch, organisatorisch, etc.) betrachtet werden. Aus Sicht der softwaretechnischen Architektur kommt der ELGA-Aspekt genau dann zum Tragen, wenn die in den ELGA-Bereichen bzw. bei den ELGA-GDA gespeicherten und registrierten Dokumente zu einem virtuellen Gesamtregister zusammengefasst werden und eine einheitliche Berechtigungssteuerung und Protokollierung für die Zugriffe erfolgt. Dies hat den Vorteil, dass ELGA etablierte Arbeitsabläufe innerhalb der einzelnen GDA bzw. Träger soweit wie möglich unverändert lässt.



727

728 *Abbildung 11: ELGA-Systemgrenzen*

729 Mit dem Begriff ELGA-Basis (hellblau in der Abbildung 11) wird ELGA im weitesten Sinne des
730 Wortes erfasst. Die ELGA-Basis beinhaltet die notwendige Infrastruktur, alle ELGA relevanten
731 Daten, Metadaten und sonstige unterstützende Komponenten, Funktionalitäten und
732 Einrichtungen inklusive des Berechtigungs- und Protokollierungssystems. Innerhalb der
733 ELGA-Basis-Grenzen sind alle Abläufe, Anforderungen und betriebliche Bedingungen strikt
734 organisatorisch via ELGA-Information Security Management System (ISMS) geregelt.

735 Jener Teil der ELGA-Basis, in dem das ELGA-Berechtigungssystem die ausschließliche und
736 komplette Hoheit über die Autorisierung und Zugriffssteuerung hat, ist der ELGA-Kernbereich
737 (ELGA-Core). Der ELGA-Core wird in Abbildung 11 grün dargestellt. Die wesentlichen
738 Komponenten des ELGA-Kernbereiches sind das ELGA-Token-Service (ETS) und die
739 Zugriffssteuerung. Diese schützen alle sensiblen Daten vor unbefugten Zugriffen.
740 Ausschließlich autorisierten ELGA-Benutzern wird Zugriff gewährt. Jeder Datenzugriff, der im
741 ELGA-Core stattfindet, wird automatisch und unwiderruflich mitprotokolliert.

742 Zwischen der ELGA-Basis und dem ELGA-Core existiert eine hellgrün dargestellte Zone, in
743 der zwar alle Zugriffe und alle sonstigen ELGA-relevanten Events einer verpflichtenden
744 Protokollierung unterliegen, jedoch das ELGA-Berechtigungssystem außer Kraft ist. Beispiel
745 hierfür ist eine IHE Kommunikation zwischen ATNA Secure Nodes (vorwiegend Automaten
746 und diagnostische Geräte). Die Teilnehmer (ATNA Secure Nodes) bauen einen abgesicherten
747 Kommunikationsweg auf (Transport Level Security), welcher auf vertrauenswürdigen
748 Zertifikaten beruht. Den Transaktionen wird, aufgrund der auf diese Weise identifizierten

Datenquelle, vertraut, wobei keine explizite Autorisierung seitens des ELGA-Berechtigungssystems stattgefunden hat.

Sonstige Systeme dürfen ohne Autorisierung durch das ELGA-Berechtigungssystem grundsätzlich ausschließlich auf interne Services und Komponenten des eigenen Bereichs zugreifen (die außerhalb von ELGA liegen). Um Zugang zum ELGA-Kernbereich zu erhalten (etwa ELGA-Verweisregister), müssen alle Transaktionen dem ELGA-Core einen Identitätsnachweis präsentieren (roter Stempel in der Abbildung 11), der von einem vertrauenswürdigen (trusted) Identity Provider (IdP) explizit für ELGA ausgestellt wurde.

Die Beschreibung der Gesamtarchitektur betrachtet im ersten Schritt die Dokumentveröffentlichung bzw. den Dokumentaustausch sowie die hierfür erforderlichen Komponenten, wie den zentralen Patientenindex (Z-PI) und die Umsetzungen der Konzepte, wie in den IHE Integrationsprofilen XDS und XCA beschrieben. Von diesen Grundlagen ausgehend werden weitere Aspekte der Gesamtarchitektur erklärt.

Die wesentliche Eigenschaft der Architektur der ELGA besteht darin, dass die Speicherung von ELGA-CDA-Dokument-Metadaten nicht in einem einzigen XDS Verweisregister, sondern verteilt in den Verweisregistern der jeweiligen ELGA-Bereiche erfolgt. Lediglich die Information, dass der ELGA-Teilnehmer in einem bestimmten Bereich registriert wurde, wird an den zentralen Patientenindex (Z-PI) übermittelt. Hierbei ist es unerheblich, ob Dokumente veröffentlicht wurden. Die an den Z-PI weitergeleitete Information (PIF) hält nur das Ereignis fest, dass dem ELGA-Teilnehmer im angegeben ELGA-Bereich eine lokale Patienten ID (L-PID) zugeordnet wurde.

Die Information über mögliche Speicherorte von medizinischen Dokumenten eines ELGA-Teilnehmers wird im Rahmen der Dokumentensuche vom Z-PI bezogen, um dadurch Such-Anfragen möglichst nur an jene ELGA-Bereiche zu übertragen, die auch tatsächlich medizinische Dokumente des ELGA-Teilnehmers beinhalten können (diesbezüglichen Details sind dem Kapitel 6.2 zu entnehmen).

Basis für die Kommunikation zwischen ELGA-Bereichen bilden Konzepte des IHE Integrationsprofils XCA.

3.4. Dokumentenaustausch auf internationalen Ebene

Dieses Kapitel erörtert Konzepte, welche auf der Annahme beruhen, dass ein Dokumentenaustausch auf europäischer Ebene aufgrund von konkreten Erkenntnissen aus Pilotierungen - beispielsweise im epSOS-Projekt - stattfinden wird. Die Inhalte basieren auf den im Rahmen dieser Pilotierungen erarbeiteten Grundlagen. Abbildung 12 zeigt die Topologie, in der die ELGA-Bereiche in Österreich zusammengeschlossen sind, im Vergleich zum EU-weiten Zusammenschluss. Für ELGA in Österreich kommt für den Zusammenschluss das oben skizzierte Modell (Abbildung 10) zur Anwendung, wobei das zentrale ELGA-Token-

Service zusammen mit dem Z-PI in gewisser Weise auch die Funktion eines „Record Locator Service“ übernimmt.

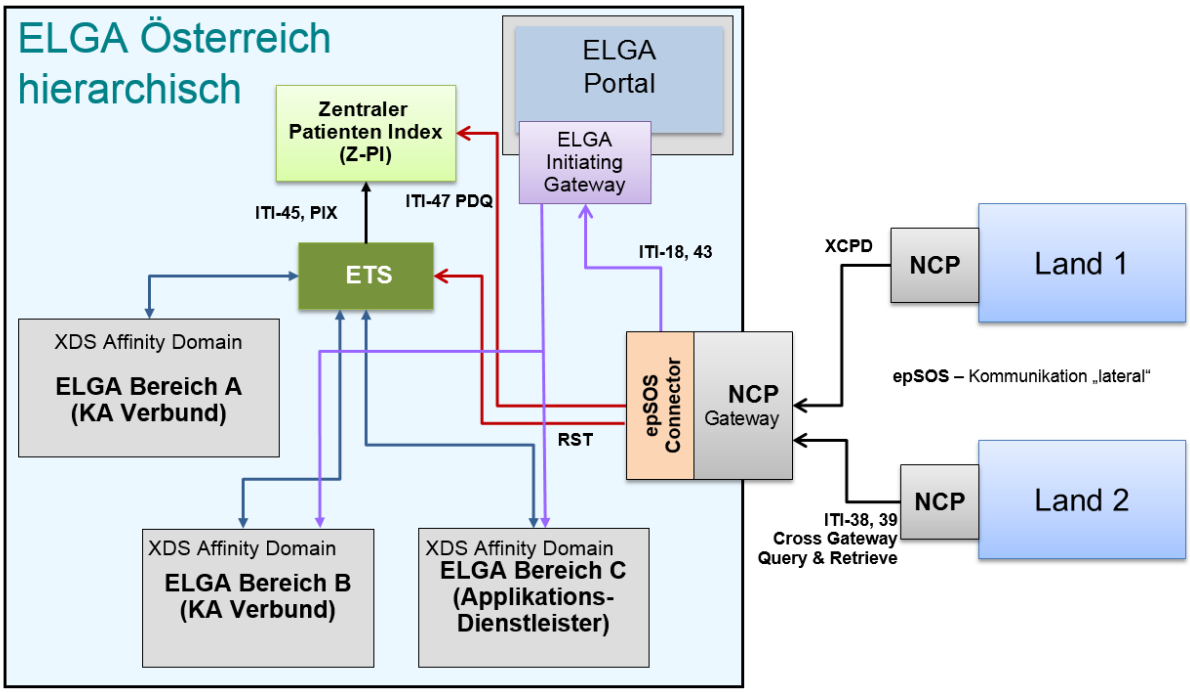


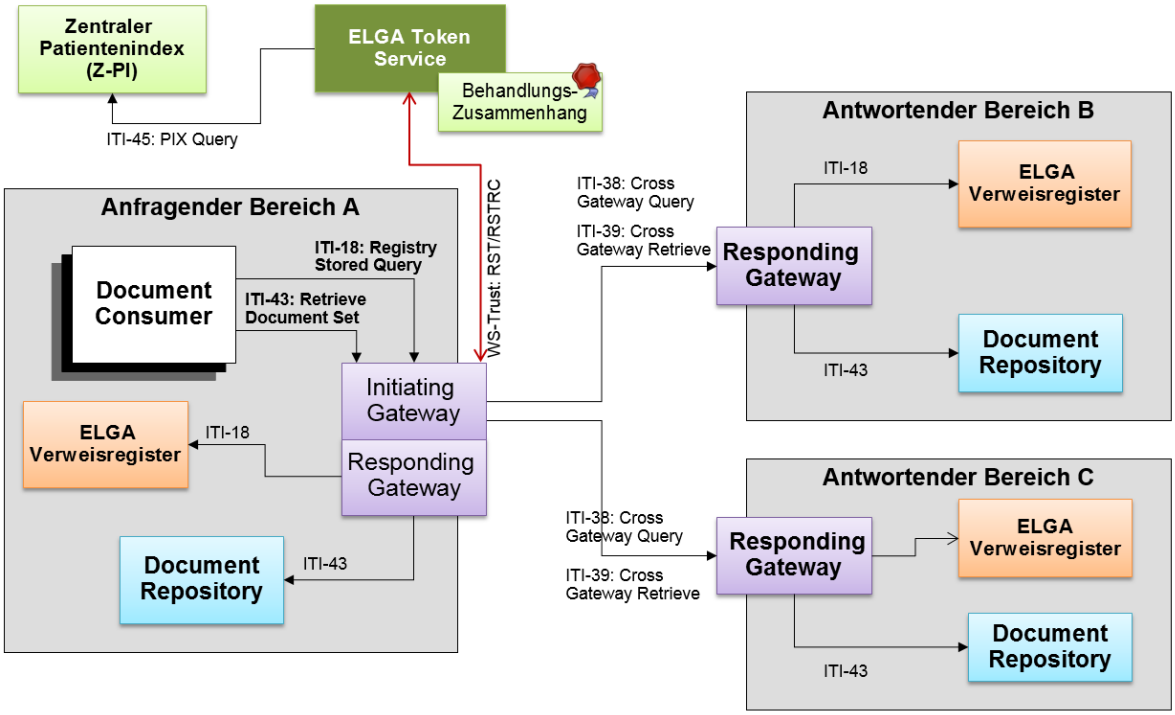
Abbildung 12: Topologie für den internationalen Informationsaustausch für ELGA

Abbildung 12 stellt die Kommunikationswege im Falle einer von außen kommenden Anfrage (Land 1 oder Land 2) dar. Der epSOS Connector übersetzt hierfür eine ankommende internationale XCPD-Anfrage auf PDQ [ITI-47] und leitet diese an den Z-PI weiter.

Basierend auf spezifischen Kriterien wird somit eine direkte Verbindung zum NCP (National Contact Point) des anzufragenden Landes aufgebaut. Diese Kriterien können z.B. die Nationalität des Patienten, die Nummer der EKVK oder von NETC@RDS gelieferte Informationen sein. Das zwischenzeitlich abgeschlossene epSOS Projekt definiert nur die länderübergreifende Kommunikation, nicht aber, wie der NCP an die Infrastruktur im jeweiligen Land (NI National Infrastructure) angebunden wird. Insofern ist der konkrete Aufbau und Realisierung eines epSOS-Connectors (Abbildung 12) Sache des jeweiligen Landes und basiert auf den Ergebnissen der Evaluierungen der epSOS Pilotierungen und muss im Fall einer konkreten Anbindung organisatorisch, rechtlich und technisch evaluiert und nachgezogen werden. Der aktuelle Stand ist über www.epsos.eu abfragbar. Länderübergreifende Abfragen dürfen nur auf Basis eines konkreten Opt-In der Betroffenen erfolgen, dessen Ausgestaltung zum gegebenen Zeitpunkt erarbeitet werden muss.

3.5. Dokumentenaustausch auf nationaler Ebene

Betrachtet man die Dokumentenabfrage in ELGA in Österreich sowie dazu erforderliche IHE Konzepte im Detail, ergibt sich folgendes Bild (siehe Abbildung 13):



808

809 *Abbildung 13: Übersicht Dokumentenabfrage in ELGA Österreich*

810 Die Darstellung in Abbildung 13 soll verdeutlichen, wie die Abfrage eines Dokuments durch
811 einen Document Consumer im Bereich A abläuft, wobei angenommen wird, dass der
812 Identifikations- und Authentifizierungsprozess bereits durchgeführt wurde und Dokumente
813 vorhanden sind. Notwendige Voraussetzungen zum Registrieren von Dokumenten und auch
814 der Zugriffschutz werden in den weiteren Kapiteln behandelt.

815 Der Abruf eines Dokuments läuft in folgenden Schritten ab:

816 ■ Der Document Consumer (GDA System) stellt mit Hilfe der Transaktion [ITI-18] *Registry*
817 *Stored Query* die Suchabfrage nach veröffentlichten Dokumenten eines Patienten. Die
818 Anfrage richtet der Document Consumer an das Initiating Gateway des eigenen ELGA-
819 Bereichs. [ITI-18] Query Parameter können hierbei XDS SubmissionSet sowie XDS
820 DocumentEntry Objekte adressieren. XDS Folder werden in ELGA nicht unterstützt
821 (siehe auch Kapitel 3.18).

822 *Anmerkung: XCA unterscheidet bezüglich des Konzepts eines Gateways im Detail die*
823 *Akteure XCA Initiating und XCA Responding Gateway. Diese wurden im Bild zu Gateway*
824 *zusammengefasst.*

825 ■ Das ELGA-Initiating Gateway nutzt das ELGA-Token-Service (ETS), um all jene ELGA-
826 Bereiche zu ermitteln, in denen der Patient registriert wurde und in denen möglicherweise
827 medizinische Dokumente des Patienten vorliegen, um eine entsprechende Autorisierung
828 (SAML Token bzw. ELGA-Assertion) anzufordern.

- Das ETS überprüft zuerst den Behandlungszusammenhang, welcher bestimmt, ob der zugreifende ELGA-GDA generell autorisiert ist, medizinische Daten für den Patienten abzufragen. Siehe hierfür auch das Kapitel Kontaktbestätigung.

- Das ETS ermittelt mit Hilfe der Transaktion [ITI-45] *PIXV3 Query* jene ELGA-Bereiche, in denen eine L-PID des Patienten vergeben wurde und folglich medizinische Dokumente vorliegen könnten.

- Das ETS (Abbildung 13) nutzt im Zuge der Autorisierung des anfragenden ELGA-Benutzers den Z-PI und strukturiert die erhaltenen Informationen in Form von mehreren ELGA-Authorisation-Assertions II (siehe unterste Klassenebene in der Abbildung 34). Die Assertion-Liste wird als Kollektion (RSTRC, WS-Trust Protokoll) dem anfragenden Initiating Gateway übermittelt. Das ELGA-Gateway kann daher die Information bezüglich der Speicherorte von medizinischen Dokumenten eines Patienten aus der so erhaltenen Liste beziehen.

- Anschließend verarbeitet das Initiating Gateway die Anfrage des XDS Document Consumer. In Abhängigkeit der Informationen der indirekten Z-PI Abfrage, werden mehrere, asynchrone Anfragen in Form von *Cross-Gateway Query* [ITI-38] an entsprechende Responding Gateways der ELGA Zielbereiche adressiert. Gleichzeitig wird eine *Registry Stored Query* [ITI-18] vom bereichsinternen Responding Gateway an das ELGA-Verweisregister im selben Bereich übermittelt.

- Nach dem Eintreffen der Antworten aller kontaktierten ELGA-Bereiche sowie des bereichsinternen ELGA-Verweisregisters erstellt das Initiating Gateway eine Sammel-Antwort an den anfragenden Document Consumer und übermittelt diese. Auf notwendige Bearbeitungen der Nachricht, Timeout-Behandlung und Aspekte des Zugriffsschutzes wird in den folgenden Kapiteln eingegangen.

- Der Abruf von konkreten Dokumenten erfolgt ebenfalls über das Initiating Gateway. Der Document Consumer entnimmt der Antwort auf die Suchanfrage die Referenz auf das gewünschte Dokument und initiiert eine [ITI-43] *Retrieve Document Set* Anfrage an das Initiating Gateway. Anhand der Referenzinformation leitet dieses die Anfrage entweder an ein bereichsinternes oder bereichsexternes Document Repository (via [ITI-39]) zum Zweck des Dokumentenabrufs weiter. Aus Sicht des anfordernden Document Consumers erfolgt die Dokumentsuche bzw. der Abruf eines Dokuments transparent mittels des bereichseigenen ELGA-Gateways.

  Hinweis: Das am Anfang dieses Dokumentes erwähnte Prinzip, wonach jede Aktion im ELGA-Core eine Authorisation-Assertion erfordert, gilt auch hier. Die Transaktion [ITI-43] Retrieve Document Set bzw. [ITI-39] Cross Gateway Retrieve enthält im SOAP Message-Body keine ELGA-Teilnehmer-bezogenen Informationen. Daher muss ein XDS

Document Consumer entweder zusätzlich entsprechende patientenbezogene Identitätsinformationen im SOAP Autorisation-Header mitsenden oder diese Information wird aus einem internen Context-Cache geholt. Weitere Details sind im BeS Pflichtenheft [18] angeführt.

3.6. Zusammenarbeit der ELGA-Bereiche

Abbildung 14 zeigt eine grobe Übersicht über das Zusammenwirken der ELGA-Bereiche. Diese wird im Wesentlichen über die standardisierten Schnittstellen definiert. In der oberen Bildhälfte werden bereichsübergreifend (logisch zentral) genutzte ELGA-Komponenten dargestellt. Diese unterstützen standardisierte Schnittstellen für ELGA-Bereiche, welche in der Mitte des Bildes dargestellt sind. Konzepte innerhalb eines ELGA-Bereichs entsprechen sogenannten Akteuren gemäß IHE IT Infrastructure Technical Frameworks.

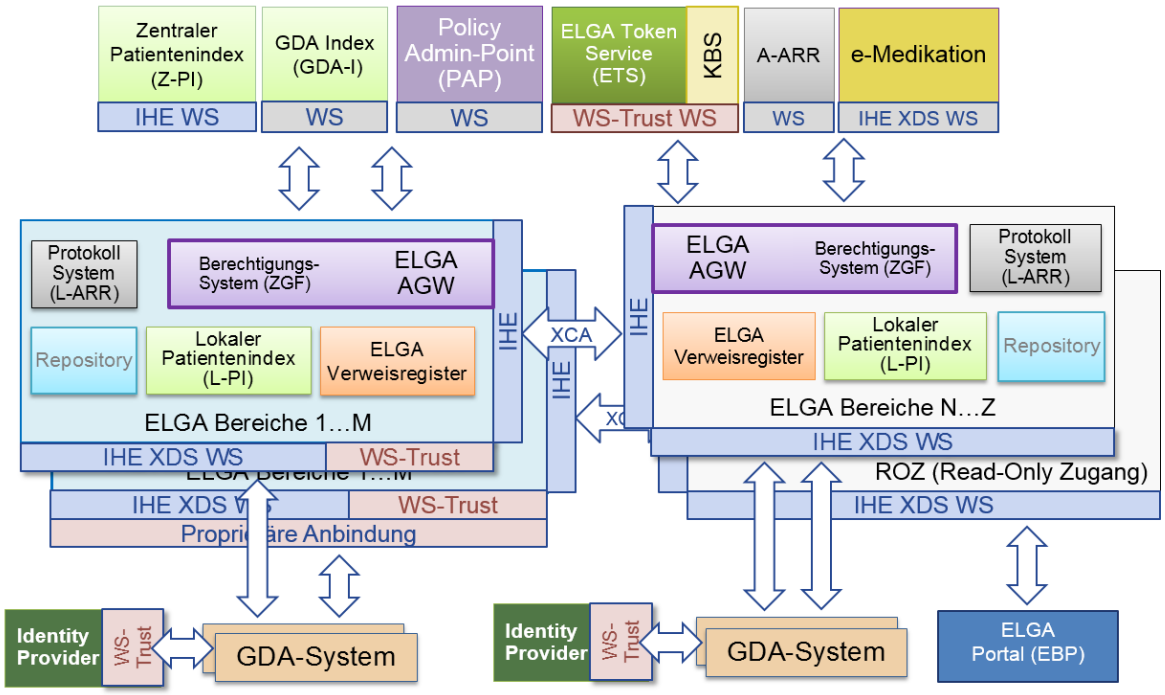


Abbildung 14: Übersicht schnittstellenrelevanter ELGA-Komponenten

Bereichsübergreifend genutzte ELGA-Komponenten sind wie folgt beschrieben:

- **Zentraler Patientenindex (Z-PI):** Der zentrale Patientenindex gewährleistet die eindeutige Identifikation von ELGA-Teilnehmern. Zusätzlich liefert er auch die Information, in welchen ELGA-Bereichen eine L-PID des ELGA-Teilnehmers vorhanden ist und somit potentiell Dokumente vorliegen. Zugriffe auf den Z-PI können über die standardisierte IHE Schnittstelle, welche die IHE Profile PIX und PDQ implementiert, stattfinden. Eine weitere Beschreibung erfolgt in Kapitel 6.

- **Gesundheitsdiensteanbieter-Index (GDA-Index):** Der GDA-Index dient der eindeutigen Identifikation von ELGA-GDA (und OBST) und ermöglicht Abfragen von rollenspezifischen Attributen in ELGA. Die Eintragung im GDA-Index stellt die Voraussetzung für die Authentifizierung des GDAs als ELGA-GDA dar. Technisch dient der GDA-Index als Basis für das ELGA-Token-Service, um *Authorisation-Assertions* auszustellen, welche die Identität und Rolle eines ELGA-GDAs unter Nutzung internationaler Informationssicherheitsstandards in verifizierter Form strukturieren. Der Zugriff auf den GDA-I erfolgt über ein vordefiniertes SOAP Web Service. Die weitere Beschreibung erfolgt in Kapitel 7.

- **Policy Administration Point mit Policy Repository (PAP):** Diese Komponente (entspricht einem **P**olicy **A**ccess **P**oint) erlaubt es, die Zugriffsberechtigungen von ELGA-Benutzern zu speichern und zu warten. In engem Zusammenspiel mit dem ETS sorgt der PAP für die Bereitstellung formalisierter Zugriffsberechtigungen, welche im Kontext der Zugriffsautorisierung verarbeitet werden.

- **ELGA-Token-Service (ETS):** Dieses stellt Authorisation-Assertions (SAML Tickets) für ELGA-Benutzer aus, die identitäts-, rollen- sowie weitere autorisierungsbezogene Attribute in einer standardisierten Form elektronisch abbilden. Authorisation-Assertions sind Teil jeder Aktion, die ein ELGA-Benutzer in ELGA-Core initiiert und werden folglich durch die Zugriffssteuerungsfassade jedes ELGA-Bereichs zum Zweck der Zugriffsautorisierung verarbeitet. Der Zugang zu den Services des ETS erfolgt über das standardisierte Kommunikationsprotokoll WS-Trust von OASIS.

  Anmerkung: Der Begriff Authorisation-Assertion wird als Synonym für Assertion gemäß dem OASIS Standard WS-Trust verwendet. Dieser spezifiziert u.a. die Ausstellung, Validierung und Erneuerung von Assertions, die gemäß des OASIS Standards Security Assertion Markup Language 2.0 (SAML) strukturiert sind.

  Beispiele:

  - Ausstellung einer *ELGA-Healthcare-Provider-Assertion* (ELGA-HCP-Assertion), mit der ein ELGA-GDA in ELGA angemeldet ist.
  - Ausstellung einer *ELGA-Treatment-Assertion* als Grundlage für die Autorisierung von Zugriffen des ELGA-GDAs auf personenbezogene medizinische Dokumente in ELGA, bedingt durch das Vorhandensein eines gültigen Behandlungszusammenhanges.

- **Kontaktbestätigungsservice (KBS):** Dieses Service speichert Kontaktbestätigungsmeldungen. Der Zugang zum Service erfolgt über das standardisierte Kommunikationsprotokoll WS-Trust (siehe hierfür auch Kapitel 3.14). Der Nachweis über einen erfolgten Kontakt zwischen GDA und Patienten kann auch mit

einem standardisierten RST an das KBS gemeldet werden bzw. von diesem abgefragt werden. Abfrageberechtigt sind nur ETS und das Portal. Darüber hinaus sind GDA berechtigt die selbst eingebrachte aktuelle Kontakte abzufragen.

- **Protokoll Aggregation (A-ARR):** Diese Komponente aggregiert die dezentral anfallenden Protokollnachrichten und stellt relevante Auszüge für die Anzeigefunktion am ELGA-Portal bereit. Die ELGA-Bereiche senden optimierte Protokollnachrichten via spezifischer Transaktionen. Das ELGA-Portal greift über vordefinierte Web Services zu.
- **ELGA-Portal (EBP):** Nutzt die zentralen Komponenten GDA-I, Z-PI, PAP, ETS, KBS, A-ARR und einen dedizierten ELGA-Document Consumer in einem EBP-Bereich (Gesundheitsdaten im EBP zu Speichern ist vorerst ist nicht vorgesehen), um die entsprechenden Inhalte für ELGA-Benutzer zu visualisieren. Die Anmeldung am ELGA-Portal für ELGA-Teilnehmer (Bürger) erfolgt grundsätzlich mit der Bürgerkarte (bzw. Handy-Signatur).
- **ELGA-Bereich und ELGA-Gateway:** ELGA-Bereiche kommunizieren miteinander ausschließlich lesend über definierte Schnittstellen entsprechend IHE XCA, welche durch ELGA-XCA-Gateways (bestehnd aus Initiating und Responding Teilen) implementiert sind. Ein XCA-Gateway ist ein IHE Konzept und in eine ZGF-Instanz eingebettet. ZGF sind wiederum in eine physische Einheit ELGA-Anbindungsgateway (AGW) inkludiert. GDA-Systeme und sonstige Dokumentenkonsumenten (Document Consumer) bzw. Dokumentenquellen (Document Source) können entweder über standardisierte IHE und OASIS Schnittstellen oder über proprietäre Schnittstellen von bestimmten Providern, die solche anbieten, angebunden werden,
  - **Standardisierte Anbindungsbausteine (zwischen einem ELGA-Bereich und jenen den Bereich nutzenden Akteuren)**: Unter Verwendung von Anbindungsbausteinen ist die direkte Anbindung an ELGA möglich und wünschenswert, falls das GDA-System die standardisierten Schnittstellen gemäß den Spezifikationen von ELGA implementiert.
  - **Proprietäre Anbindungsbausteine:** Komponenten, die die Anbindung existierender Gesundheitsinformationssysteme an ELGA ermöglichen. Eine wesentliche Funktion dieser Anbindungsbausteine ist es, die Schnittstelle, die ein GDA-System implementiert, an das von ELGA geforderte Format anzupassen (Schnittstellenkonverter). Dies umfasst z.B. bei der Kommunikation zwischen einem Krankenhausinformationssystem und dem Patientenindex die Konvertierung der Daten im HL7 Version 2 Format nach HL7 Version 3.

Anmerkung: Die heute existierenden Implementierungen des Integrationsprofils XDS nutzen Adaptoren in unterschiedlichen Ausprägungen (z.B. Adaptoren, die mit dem

Produkt gekoppelt sind, das den IHE Actor implementiert oder Enterprise Application Integration (EAI) Systeme).

Aus Architektursicht sind die lesenden Anbindungsbausteine als Teil eines *Document Consumers* zu sehen und damit mit dem GDA-System gekoppelt. Bei Bedarf sind sie daher auch durch den ELGA-GDA bereitzustellen. Lesende Anbindungsbausteine nutzen das ELGA-Core und müssen daher entsprechende Assertions anfordern und den Aufrufen beifügen.

Schreibende Anbindungsbausteine senden Dokumente mit der Transaktion *„Provide and Register Document Set –b [ITI-41]“* an ein *„Document Repository“,* welches wiederum das Dokument mit den Metadaten in dem ELGA-Verweisregister mit *„Register Document Set – b [ITI-42]”* registriert. Bei Registrieren des Dokuments muss der Wille des ELGA-Teilnehmers berücksichtigt werden. Wenn der Patient „opt-out“ erklärt hat, dürfen keine medizinischen Daten mehr in ELGA veröffentlicht werden. Daher muss die *„Document Source“* eine ELGA-*Authorisation-Assertion* anfordern und dem Aufruf beifügen, so dass die Zugriffssteuerungsfassade des ELGA-Anbindungsgateways den Zugriff autorisieren kann.

- **Protokoll Bereitstellung (Lokales Audit Record Repository, L-ARR):** Zumindest ein L-ARR existiert in jedem ELGA-Bereich und zusätzlich bei jedem Betreiber von zentralen Komponenten.
- **Dezentrale Komponente des Berechtigungssystems (Policy Enforcement):** Die Zugriffssteuerung ist eine dem ELGA-Gateway vorgeschaltete Komponente. Die Zugriffssteuerung des Berechtigungssystems setzt die einheitliche Zugriffsautorisierung in den ELGA-Bereichen um. Die mit dem jeweiligen Request an ein ELGA-Gateway gesendeten Berechtigungsregeln (Policies) werden in mehreren Schritten umgesetzt (Enforcement). Manche Richtlinien können bereits am Eingang der Zugriffsteuerung überprüft und exekutiert werden (z.B. Digitale Signaturen, Rollen, etc.). Detaillierte Policies müssen an die in der Pipeline tiefer liegenden Komponenten (PEP & PDP) weitergereicht werden.
- **ELGA-Verweisregister:** ELGA-Verweisregister samt den Schnittstellen, die der Akteur „Document Registry“ im XDS Profile anbietet (siehe Kapitel 8).
- **Patient ID Source (Patient Identity Source):** Akteur gemäß dem Integrationsprofil *Patient Identity Cross Referencing* (PIXV3). Dient dem Registrieren von Identifikationsdaten beim Zentralen Patientenindex. Ein Bereich muss sicherstellen, dass ein Patient zentral registriert ist, wenn dieser in der Gesundheitseinrichtung aufgenommen wird bzw. medizinische Dokumente dieses Patienten im bereichsinternen ELGA-Verweisregister veröffentlicht werden sollen.

- **Patient Demographics Consumer:** Akteur im Integrationsprofil PDQV3. Bietet dem XDS Document Consumer eines ELGA-Bereichs die Möglichkeit, Patienten mittels des lokalen bzw. des Zentralen Patientenindex anhand demographischer Suchanfragen eindeutig zu identifizieren. Details siehe Kapitel 6.
- **Identity Provider**
  - ist ein Secure Token Service (STS), bestätigend die elektronische Identität des authentifizierten ELGA-Anwenders der autorisiert ist, auf ELGA zuzugreifen (entweder im Namen einer GDA-Organisation oder direkt als physische Person in der entsprechenden ELGA zulässigen Rolle).
  - Identity Management basiert auf einem zielgerechten und bewussten Umgang mit Identitäten, umfassend zumindest folgende Punkte:
    - Den Identifikationsprozess, genannt Authentifizierung
    - Die Bestimmung des Autorisierungskontextes der einzelnen Identitäten
    - Die sichere Verwaltung von Identitäten
- **OID Portal** (im Bild oben nicht dargestellt) wird offline (Design-Time) verwendet. In ELGA spielen global eindeutige OID-Werte eine entscheidende Rolle. In vielen Fällen werden sie als Primärschlüssel verwendet. Darüber hinaus definieren sie Code-Listen mit ELGA-weiten eindeutigen Werten. In den nachfolgenden Kapiteln wird auf einige der wichtigsten OID auch detailliert eingegangen. Dazu zählen zum Beispiel die GDA-OID-Primärschlüssel (hinterlegt in GDA-Index) oder die OID der Code-Listen für Kontaktbestätigungen, für ELGA-Rollen, für Identifikationsmethoden. Weitere OID sind in den ELGA-Implementierungsleitfäden definiert und deklariert.
- **Terminologie-Server** (im Bild oben nicht dargestellt) wird nur offline (Design-Time) verwendet. Beispielsweise holt sich das Portal die erforderlichen Terminologien und Value Sets vom Terminologie-Server und synchronisiert diese regelmäßig (Periode sind Tage bzw. Wochen).

3.7. Fachliche Gesamtarchitektur (UML Komponentendiagramm)

In der Abbildung 15 ist die ELGA-Gesamtarchitektur auf hierarchisch und organisatorisch höchster Komponentenebene dargestellt. Angeführt sind die in den vorherigen Kapiteln bereits angesprochenen Schnittstellen und die Verbindungen zwischen den Hauptakteuren. Übersichtlichkeitshalber sind die zentralen Komponenten in eine einzige allgemeine Komponente zusammengefasst. Darüber hinaus steht der *ELGA-Bereich GDA* für jene ELGA-Bereichsinstanzen, die GDA anbinden. *ELGA-Bereich Portal* bezeichnet jene dedizierte ELGA-Bereichsinstanz, welche für die Anbindung des ELGA-Portals zuständig ist. Bereich e-

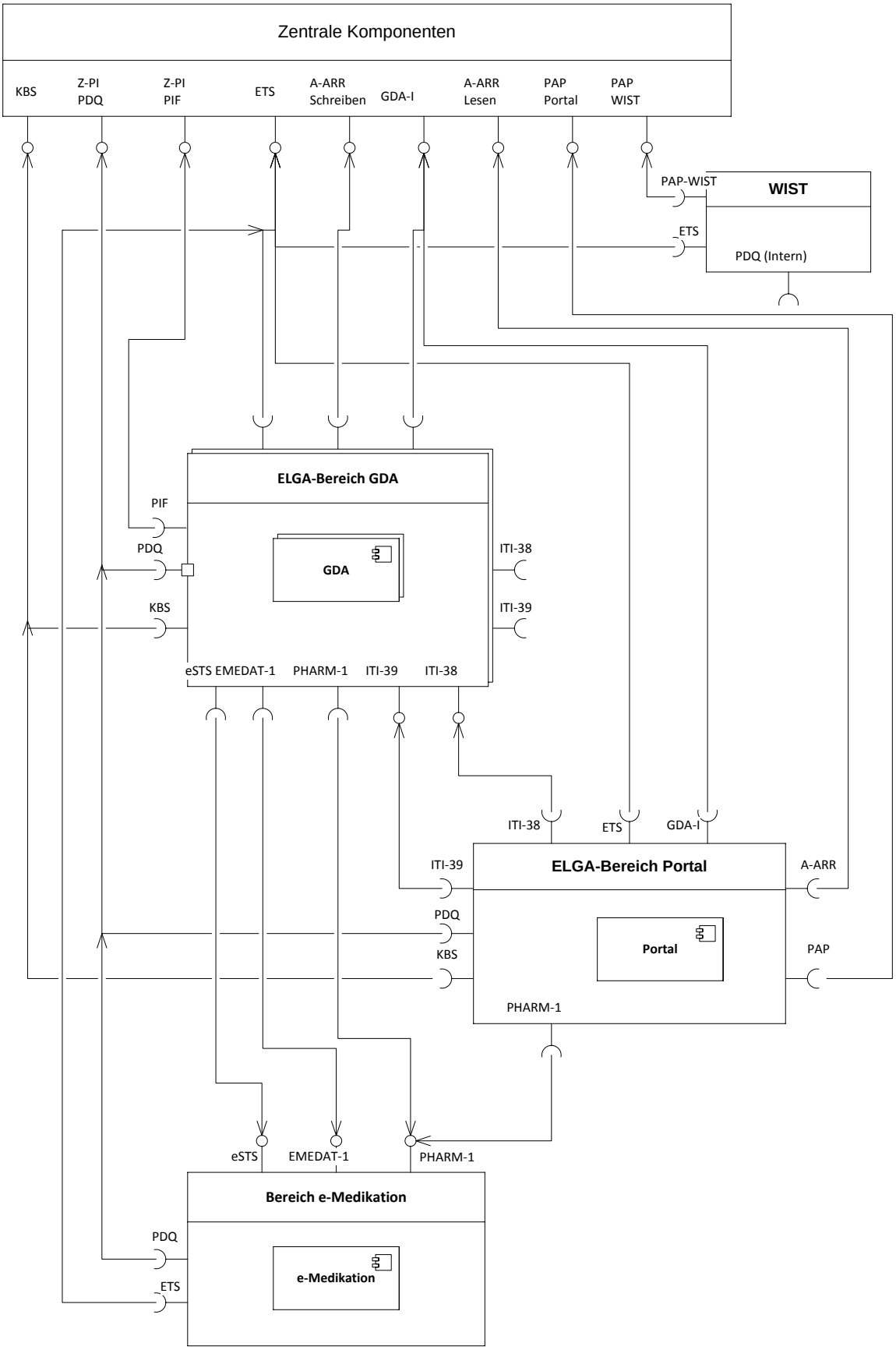
Medikation steht für die dedizierte ELGA-Bereichsinstanz, welche die ELGA-Anwendung e-Medikation anbindet. WIST steht für die dedizierte Instanz der Widerspruchstelle.

Abbildung 15 zeigt eine Übersicht mit dem Ziel, die essentiellen ELGA-weiten (sogenannten „globalen“) Schnittstellen und deren Konsumenten zu erfassen. Aus genannten Gründen sind einige Schnittstellen nur gebündelt dargestellt. Diese werden aber in der nachfolgenden Beschreibung aufgelöst.

- Schnittstellen der zentralen Komponenten
  - KBS bezeichnet die Schnittstelle des Kontaktbestätigungsservices. Diese Schnittstelle verwendet einen zweckangepassten Dialekt des WS-Trust Protokolls. Ermöglicht lesende (Portal und GDA nur die eigenen Kontakte) und schreibende (GDA) Zugriffe. Autorisierung wie folgt:
    - Lesend: ELGA HCP – Assertion, ELGA User I oder ELGA Mandate I – Assertion
    - Schreibend: ELGA HCP-Assertion
  - Z-PI/PDQ *Patient Demographics Query*. Autorisierung via ATNA Secure Node
  - Z-PI/PIF *Patient Identity Feed*. Autorisierung via ATNA Secure Node
  - Z-PI/PIX (nicht in der Abbildung 15 dargestellt). Autorisierung via ATNA Secure Node
  - ETS stellt die WS-Trust Schnittstelle des ELGA Token-Services dar. Autorisierung aufgrund vertrauenswürdigen Identity-Assertions zwecks Föderation oder Zugang über ELGA User I, Mandate I, WIST, bzw. HCP-Assertion zwecks Ausstellung von User II, Mandate II oder Treatment Assertion, inklusive Sonderfall Service Assertion.
  - A-ARR bezeichnet die Schnittstellen des Aggregierten Audit Record Repopsitory. Autorisierung wie folgt:
    - Lesend: via ELGA User I oder Mandate I – Assertion
    - Schreibend: nur ELGA Anbindungsgateway aufgrund ATNA Secure Node
  - GDA-I, ausschließlich lesende Schnittstellen. Zugang über vertrauenswürdigen ATNA Secure Nodes
  - PAP Portal stellt die lesenden und schreibenden Schnittstellen des Policy Administration Point dar. In beiden Fällen Autorisierung durch ELGA User I oder Mandate I – Assertion.
  - PAP WIST stellt die für die Widerspruchstelle dedizierte schreibende Schnittstelle dar. Zugang via ELGA WIST Mandate I Assertion.
- Schnittstellen eines GDA ELGA-Bereichs.

- ITI-38,39 Interfaces repräsentieren die antwortenden IHE Cross Community (XCA) Anbindungen (Responding Gateways). Autorisierung erfolgt mit gültiger ELGA Treatment, User II oder Mandate II – Assertion. Darüber hinaus werden die in den genannten Assertions eingebetteten XACML-Policies umgesetzt.

- Portal ELGA-Bereich bietet keine Dienste (Schnittstellen) an und besteht ausschließlich aus Service-konsumierenden Sockets
- e-Medikation ELGA-Bereich (siehe detailliert im Kapitel ELGA-Applikationen)
  - eSTS ist eine WS-Trust Schnittstelle des STS der e-Medikation
  - EMEDAT-1 generiert eine kryptografisch gesichert zufällige e-Med-ID
  - PHARM-1 repräsentiert die gebündelte Schnittstelle zur Abfrage der e-Mediaktion
- WIST Schnittstellen
  - PAP-WIST ist ein für WIST dedizierter Endpunkt, welcher nur schreibende Transaktionen erlaubt
  - ETS stellt die WS-Trust Anbindung zum ELGA Token-Service dar
  - PDQ (intern) - Aufgrund des gemeinsamen Betriebes von Z-PI und WIST durch den Dienstleister ITSV wurde eine einfachere Umsetzung der Service-Anbindung vereinbart. Die Handhabung des Services (Aufruf, Protokollierung, etc.) unterscheidet sich vom externen Zugriff nur bezüglich des Weges.



1079

1080 *Abbildung 15: ELGA-Gesamtarchitektur in Form eines UML-Komponentendiagrames*

3.8. Anforderungen an einen ELGA-Bereich

Abbildung 16 zeigt noch einmal deutlich (siehe auch Abbildung 2), dass medizinische Dokumente dezentral gespeichert und in ELGA-Bereichen veröffentlicht werden. Zentral werden nur Verweise auf die Bereiche abgelegt, in denen die Person registriert ist (aber nicht zwingend ELGA-Dokumente vorhanden sein müssen). Der Austausch medizinischer Dokumente erfolgt immer direkt zwischen einem anfragenden und einem oder mehreren antwortenden ELGA-Bereichen.

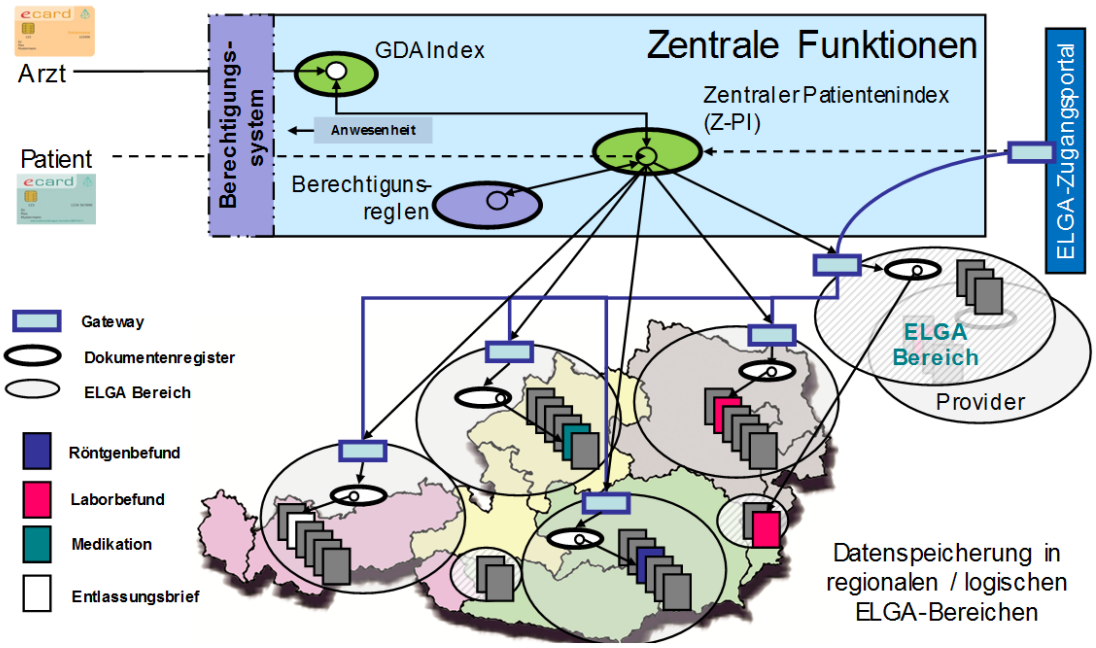


Abbildung 16: Dezentrale Verwaltung medizinischer Dokumente in ELGA-Bereichen. „Zentrale Funktionen“ beinhaltet auch alle ELGA-Anwendungen (hier nicht explizit dargestellt)

Ein ELGA-Bereich ist eine logisch-physische Einheit, die ELGA-Gesundheitsdaten veröffentlicht und abruft. Er erfüllt die für die Teilnahme an ELGA definierten funktionalen Anforderungen (Schnittstellen) und nicht-funktionalen Anforderungen (SLA, Berechtigungsprüfung). Ein ELGA-Bereich zeichnet sich durch eine Mindestmenge von implementierten Konzepten aus, die anhand der Integrationsprofile XDS und XCA definiert werden. In Anlehnung an XCA ist ein ELGA-Bereich daher als XDS-basierte Community zu betrachten.

Aufgrund des engen Zusammenhangs mit dem Integrationsprofil XDS kann ein ELGA-Bereich auch als XDS Affinity Domain gesehen werden.

Aus technischer Sicht gelten für einen ELGA-Bereich folgende Aussagen:

- Ein lesend-schreibender ELGA-GDA nutzt die Infrastruktur eines ELGA-Bereichs, um an ELGA teilzunehmen. Auch das ELGA-Portal nutzt ein ELGA-Anbindungsgateway (XCA Gateway in einer Zugriffssteuerungsfassade, eingebettet in ein AGW) um auf medizinische Dokumente in ELGA zugreifen zu können.
- Die zentralen Komponenten wie der Zentrale Patientenindex, GDA-Index und Teile des ELGA-Berechtigungssystems sind keinem ELGA-Bereich zugeordnet.
- Ein GDA-anbindender ELGA-Bereich unterstützt das IHE Profil XDS wodurch das Speichern und Modifizieren (Versionieren) bzw. das Storno von CDA ermöglicht werden muss ([ITI-41, 42, 57]). Darüber hinaus muss auch das Löschen von Dokumenten unterstützen werden.
- Ein GDA-anbindender ELGA-Bereich besitzt genau ein (eventuell im Cluster gebündeltes) AGW/ZGF, das die Transaktionen *Cross Gateway Query* [ITI-38] und *Cross Gateway Retrieve* [ITI-39] unterstützt. Für den Austausch von Bildern muss zumindest *Cross Gateway Retrieve Imaging Document Set* [RAD-75] unterstützt werden (siehe hierfür Offene Punkte im Kapitel 16.1). Das AGW stellt die erforderlichen Zugriffsteuerungsfassaden bereit und damit insbesondere unter Anwendung der im Berechtigungssystem definierten Prozesse und Schnittstellen sicher, dass
  - bei der Dokumentsuche nur jene gefilterte Treffermenge geliefert wird, auf die der anfordernde ELGA-Benutzer lesende Zugriffsrechte besitzt und dass
  - beim Dokumentenabruf nur jene Dokumente zur Verfügung gestellt werden, auf die der anfordernde ELGA-Benutzer lesende Zugriffsrechte besitzt.
- Ein GDA-anbindender ELGA-Bereich definiert für einen ELGA-Teilnehmer genau einen bereichsspezifisch eindeutigen Identifier (L-PID), der dem Zentralen Patientenindex und damit auch anderen Bereichen bekannt gegeben wird. Dieser wird bei Abfragen seitens der ELGA-Bereiche verwendet. Das Registrieren dieser L-PID beim Zentralen Patientenindex bildet die Voraussetzung für die Lokalisierung von ELGA-Bereichen, die medizinische Dokumente eines Patienten persistieren können.
- Ein ELGA-Bereich verwendet ein durch das Integrationsprofil *Audit Trail and Node Authentication* (ATNA) definiertes lokales *Audit Record Repository* (L-ARR), das die Komponenten eines ELGA-Bereichs für das Persistieren von Protokollnachrichten nutzt. Der ELGA-Bereich hat seinen Komponenten eine entsprechende Schnittstelle für das Persistieren bereitzustellen sowie für die Einhaltung der Protokollierungsvorgaben durch die Komponenten zu sorgen.
- Innerhalb des ELGA-Bereichs (ELGA-Basis) sind zumindest die im ATNA Profil definierten Sicherheitsstandards einzuhalten. Diese Sicherheitsstandards sind aber unzureichend in Bezug auf den ELGA-Kernbereich (ELGA-Core), wo eine zusätzliche

Autorisierung via SAML 2.0 Assertion vorgesehen ist (siehe auch ELGA-Berechtigungssystem).

- Jede Komponente, die ATNA-konforme Protokollierung durchführt, implementiert Konzepte gemäß des Integrationsprofils *„Consistent Time (CT)“.*
- Bereitstellung einer bereichsspezifischen Clearing- bzw. Kontaktstelle, die bei Bedarf vom Call-Center kontaktiert werden kann.
- Der interne Aufbau eines ELGA-Bereichs wird durch das ELGA-Anbindungsgateway (AGW) gekapselt. Dieses benötigt wiederum Zugriff auf das ELGA-Verweisregister und die Document Repositories des Bereichs. Dieser Zugriff ist zu ermöglichen und zumindest über „Node Authentication [ITI-19]“ abzusichern. Die Daten zum ELGA-Benutzer werden in Form einer Community Assertion weitergegeben. Die Komponenten können die Daten für Audit-Protokollierung verwenden. Sie dürfen jedoch keine Zugriffseinschränkungen festlegen, da diese einheitlich durch die Zugriffsteuerungsfassade (AGW/ZGF) erfolgen.
- Für Dokumentensuche bzw. Dokumentenabruf werden am ELGA-Gateway die geforderten SLAs [16] eingehalten. Der Bereich hat dies intern durch geeignete Vorgaben an die ihm zugeordnete ELGA-Verweisregister und Repositories sicherzustellen.
- Der ELGA-Bereich erfüllt die Anforderungen betreffend Datensicherheit aller ELGA-Gesundheitsdaten, die innerhalb des Bereichs gespeichert sind. Geeignete Vorgaben an die Komponenten des Bereiches (lokaler Patientenindex, Verweisregister, Repositories, L-ARR) sind zu definieren und zu überprüfen.
- Neben GDA anbindenden ELGA-Bereichen sind einige wenige speziell vorkonfigurierte ELGA-Bereiche zugelassen (Details sind im Kapitel 9 ausgeführt). Der Bereichscharakter dieser speziellen Bereiche ergibt sich aus Vorhandensein eines ELGA-Gateways, als Teil einer ZGF und aus der Implementierung von entsprechenden XDS oder XCA Profilen
  - Der EBP-Bereich ist ein ausschließlich initiierender Bereich, in dem nur der Initiating Gateway in der ZGF aktiviert ist. Dieser Bereich kann ankommende Anfragen nicht beantworten, da der Responding Gateway nicht aufgeschaltet ist.
  - Der Bereich der e-Medikation ist ein ausschließlich passiver (Read-Only) Bereich, in dem, im Gegensatz zum EBP-Bereich, nur ein Responding Gateway aktiviert ist. Der Initiating Gateway in der ZGF ist nicht aufgeschaltet.

3.9. Anbindung von ELGA-GDA

3.9.1. Allgemeines

Erforderliche international standardisierte Schnittstellen für die Nutzung von ELGA müssen von den ELGA-Bereichen verpflichtend bereitgestellt werden (Abbildung 17). Diese Schnittstellen können alle ELGA-GDA nutzen, wenn diese nicht durch einen eigenen Provider mit proprietären Anbindungen (Abbildung 18) versorgt sind.

Durch die ELGA-Anbindungsbausteine (Schnittstellen) müssen ELGA-GDA mit sehr unterschiedlichen IT-Systemen angebunden werden. Die Spanne reicht hierbei von Arzt-Praxen mit rudimentären IT-Systemen, in denen kein Patienten-Managementsystem vorausgesetzt werden kann, bis hin zu Krankenanstalten, die Teile einer IHE-konformen Infrastruktur installiert haben. Hierbei wird vorausgesetzt, dass IT-Systeme, die in ELGA integriert sind, bestimmte softwaretechnische Mindestvoraussetzungen erfüllen, so dass die Informationssicherheit und der Support gewährleistet werden kann. Entscheidend ist dabei die Aussage des jeweiligen Herstellers oder des Dienstleistungsanbieters (Distribution bei Open-Source) eines Betriebssystems oder einer Komponente (etwa Web-Browser) bezüglich der unterstützten Produktlebensdauer. In der Regel sind Informationen über die Produktlebensdauer (wie z.B. Ablaufdatum älterer Versionen) an öffentlich zugängigen Portalen verfügbar. Die veröffentlichten Ablaufdaten sind im Kontext des geplanten Datums der Inbetriebnahme von ELGA zu verstehen.

Die Architektur geht auch davon aus, dass anzubindende GDA (KIS-Systeme und/oder Arzt-Software) über entsprechend verfügbare und dimensionierte (im Sinne von ELGA SLA) Netzwerkverbindungen mit ELGA dauerhaft (oder etwa für die Dauer der Gültigkeit einer ELGA-Assertion) verbunden sind und Netzwerkausfälle und Bandbreitenreduktionen eher die Ausnahme als die Regel sind. Die Architektur berücksichtigt daher sog. *Occasionally Connected Clients*, also Systeme die nur sporadisch und/oder kurzfristig mit ELGA Verbindung aufnehmen nicht bzw. die Verantwortung für solche Clients gänzlich an die jeweiligen Hersteller abgegeben wird.

3.9.2. Anbindung von niedergelassenen GDA

Niedergelassene Ärzte (ausgenommen niedergelassene Radiologen und Labore) und Apotheker erzeugen (derzeit noch) keine e-Befunde und benötigen daher keinen direkten Zugang zu einem ELGA-Bereich und müssen daher auch mit keinem ELGA-Bereich eine vertragliche Beziehung eingehen. Daher gibt es für diese ELGA-GDA einen ELGA-Zugang, der lediglich den lesenden Zugriff auf e-Befunde und den Zugriff auf e-Medikation ermöglicht. Der **R**ead **O**nly **Z**ugang (ROZ) ist so ausgelegt, dass schreibenden e-Befund-Services nicht unterstützt, jedoch alle e-Medikations-Services vollumfänglich zur Verfügung gestellt werden.

Niedergelassene GDA, die Gesundheitsdaten in ELGA speichern bzw. veröffentlichen wollen (oder müssen) können zwischen zwei ELGA-Anbindungsvarianten wählen:

1. Niedergelassene GDA können einen vertraglich gesicherten Read-Write ELGA-Zugang bei einem entsprechend zugelassenen ELGA-Bereichsprovider in Anspruch nehmen
2. Niedergelassene GDA (insbesondere jene mit einem bestehenden ROZ), können über GINA und den zentral aufgestellten Vermittlungsdienst der Hauptverbandes (ELGA-Proxy, siehe [25]) an einen bestimmten ELGA-Bereich angebunden werden.

3.9.3. Schnittstellenaufbau - Varianten

Abbildung 17 zeigt zusammengefasst den Aufbau des ELGA-Bereiches und die entsprechenden international standardisierten Schnittstellen zu den zentralen Komponenten sowie zu Komponenten des ELGA-Bereiches. Die Transaktionen, als blaue Pfeile abgebildet, sind aus Gründen der Übersichtlichkeit nur exemplarisch zu betrachten. Rote Pfeile illustrieren erforderliche Kommunikation hinsichtlich der Authentifizierung durch das Berechtigungssystem (basierend auf WS-Trust).

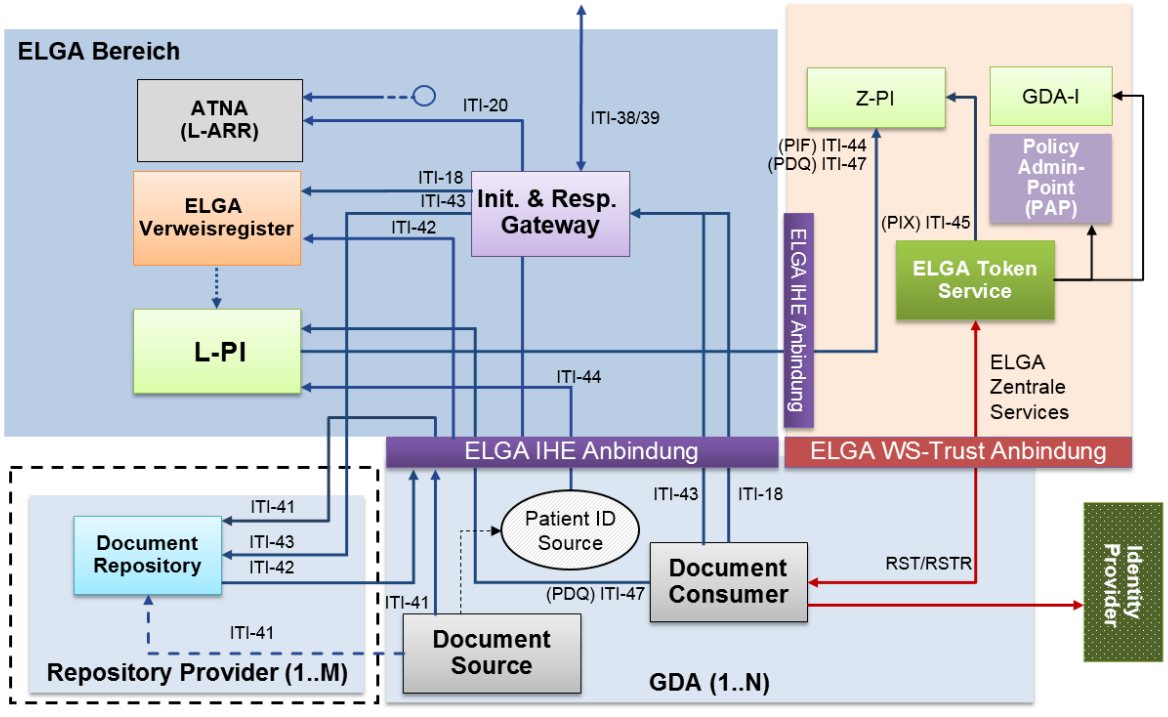


Abbildung 17: Anbindung via standardisierte Schnittstellen (Anbindungen sind auf der logisch-funktionaler Ebene. Das Konzept der Zugriffssteuerungsfassade ist hier übersichtshalber nicht eingezeichnet)

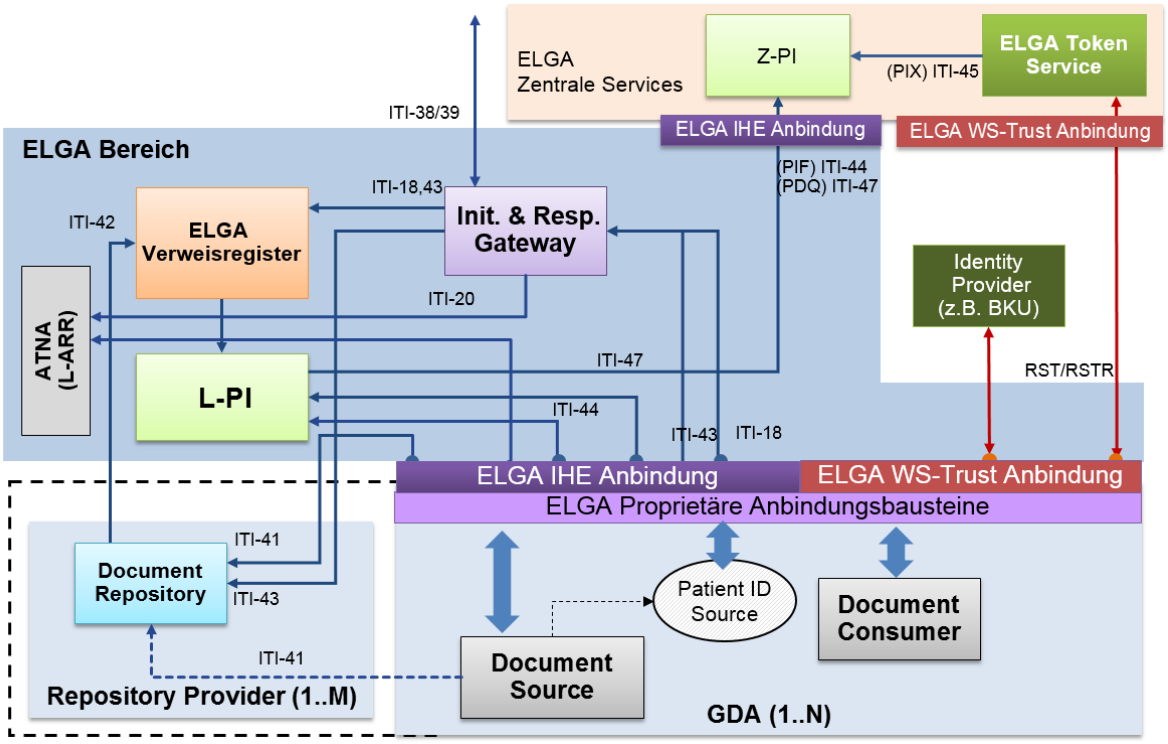


Abbildung 18: Logische Sicht der Anbindungen via spezifische (proprietäre) Bausteine. Ein Beispiel hierfür ist die ROZ-Anbindung über die GINA-Box und ELGA-Adapter bei Verwendung der spezifischen SS12-Schnittstelle

Abbildung 18 zeigt zusammengefasst den Aufbau eines ELGA-Bereiches sowie die entsprechenden proprietären Schnittstellen zur Integration von GDA-Systemen. Diese Alternative setzt die Anfragen im Hintergrund auf international standardisierte Protokolle um. (*Anmerkung: Umsetzungsdetails sind im Kapitel 9 erörtert und dargestellt*)

Im Folgenden werden die Komponenten bzw. Konzepte der Anbindung im Detail beschrieben. In beiden Fällen beinhaltet ein ELGA-Bereich einen lokalen Patientenindex (L-PI), der die demographischen Daten jener Personen enthält, für die Dokumente in der XDS Registry (ELGA-Verweisregister) veröffentlicht wurden. Für GDA-Systeme, die den jeweiligen ELGA-Bereich nutzen und das Konzept Patient Identity Source des entsprechenden IHE Integrationsprofils umsetzen (international standardisierte Schnittstelle), wird die Möglichkeit der Übermittlung von Patientendaten an den L-PI unterstützt.

Anhand des ELGA-Gateways werden alle lesenden Aktionen gemäß den Anforderungen des Integrationsprofils XCA verarbeitet. Das ELGA-Gateway ist aus Architektursicht Teil des ELGA-Berechtigungssystems und wird gemeinsam mit diesem implementiert. Die Implementierung erfolgt innerhalb der Zugriffssteuerungsfassade (ZGF). Details zur Authentifizierung, Autorisierung und Protokollierung in ELGA werden im Kapitel 9 beschrieben.

Das ELGA-Verweisregister entspricht der Umsetzung des Akteurs *Document Registry*, das im Rahmen des Integrationsprofils XDS definiert wird. Das Suchen von medizinischen

Dokumenten in ELGA (*Registry Stored Query* [ITI-18]) erfolgt ausschließlich mit Hilfe des ELGA-Gateways gemäß der in Kapitel 3.5 beschriebenen Vorgehensweise. Die Veröffentlichung von medizinischen Dokumenten in ELGA basiert auf der Registrierung von zugehörigen Dokument-Metadaten (*Register Document Set* [ITI-42]), die von *Document Repositories* gemäß dem Integrationsprofil XDS initiiert wird.

Das *Document Repository*, welches medizinische Dokumente speichert, wird in beiden Abbildungen im Verantwortungsbereich eines Repository Providers dargestellt, der dieses im Auftrag des GDAs betreibt. Bei Einhaltung der Verfügbarkeits- und Sicherheitsanforderungen kann dieses auch der ELGA-GDA selbst betreiben. Darüber hinaus und optional kann der ELGA-Bereich auch ein eigenes *Document Repository* anbieten. Zu beachten ist, dass der durch ein ELGA-Gateway initiierte Abruf eines medizinischen Dokuments unterstützt werden muss ([ITI-43] *Retrieve Document Set*).

Die Transaktion *Provide and Register Document Set* [ITI-41] erfolgt unter Einbindung von lokalen GDA-Systemen. Es liegt in der Verantwortung des ELGA-GDAs, welche technischen und organisatorischen Maßnahmen ergriffen werden, um obige IHE Transaktionen gemäß den Spezifikationen der ELGA zu unterstützen. Unter dem Fokus der technischen Interoperabilität ist es erforderlich, Schnittstellen basierend auf Transaktionen des Integrationsprofils XDS zu implementieren. Die in den beiden Abbildungen dargestellte strichlierte Linie [ITI-41] symbolisiert die theoretische Möglichkeit, die Transaktion in direkter Verbindung mit dem Repository durchzuführen.

Aus Sicht des Berechtigungssystems können beim Einbringen von Dokumenten in ELGA folgenden Bereichsvarianten betrachtet werden:

- **Variante A**: Das Dokument wird lokal gespeichert und registriert und zusätzlich eine Kopie auch für ELGA veröffentlicht. Hierfür wird eine dedizierte ELGA-Registry und ein ELGA-Repository **ausschließlich für ELGA** eingerichtet (siehe auch Kapitel 9.1). Im Fall von Opt-Out wird die Zugriffssteuerung die Dokumente in ELGA nicht übernehmen. Die eingebrachten Dokumente werden auch dann nicht in ELGA gespeichert, wenn der ELGA-Teilnehmer (Patient) über individuelle Berechtigungen dem GDA den Zugriff verwehrt hat (GDA hat 0 Tage Zugriff).
- **Variante C (C**ustom**)**: Das Dokument wird nur lokal gespeichert und lokal registriert und zusätzlich für ELGA markiert. Die Markierung erfolgt mit einem explizit für ELGA definierten booleschen Metadaten-Flag im lokalen Verweisregister (Details sind im Kapitel 9 ausführlich erklärt). Im Fall von Opt-Out wird die Zugriffssteuerung die Dokumente für ELGA nicht markieren. Die Dokumente werden auch dann nicht für ELGA gekennzeichnet werden, wenn der ELGA-Teilnehmer (Patient) über individuelle Berechtigungen dem GDA den Zugriff verwehrt hat (GDA hat 0 Tage Zugriff).

Eine detaillierte Beschreibung der diesbezüglichen Konfigurationen der ELGA-Bereiche und der ZGF ist im Kapitel 9.1.4. nachzulesen.

Für die erfolgreiche Integration von GDA-Systemen in ELGA können sogenannte Anbindungsbausteine, wie in den Abbildungen grob dargestellt, zum Einsatz kommen.

Die Schnittstellen in Abbildung 17 und Abbildung 18, welche in ELGA zur Nutzung durch ein GDA-System zur Verfügung gestellt werden, ergeben sich im Wesentlichen aus allen Transaktionen. Diese sind:

- *Provide and Register Document Set-b* [ITI-41] (XDS)
- *Register Document Set-b* [ITI-42] (XDS)
- *Registry Stored Query* [ITI-18] (XDS)
- *Retrieve Document Set* [ITI-43] (XDS)
- *Patient Demographics Query* [ITI-47] (PDQV3)
- *Patient Identity Feed* [ITI-44]; nur nach spezieller Vereinbarung
- Web Services Schnittstelle zum ETS des Berechtigungssystems [WS-Trust Protokolle]
  - Request Security Token (RST)
  - Request Security Token Response Collection (RSTRC)
- *Record Audit Event* [ITI-20] in der vom Protokollierungssystem spezifizierten Form

Zusätzliche Transaktionen bzw. Schnittstellen, die in den Abbildungen nicht explizit eingezeichnet sind:

- *Maintain Time* [ITI-1]
- *PIX V3 Query* [ITI-45]
- *Update/Delete Document Set* [ITI-57/62] (XDS Metadata Update/Delete Document Set)
- Web Services Schnittstelle zum jeweiligen Kontaktbestätigungsservice
- Widerrufsliste für Zertifikate via OSCP (Server-, Token- und Anwendungs-Zertifikate)
- HL7v2 Schnittstellen sind abhängig von der Implementierung der GDA-Anbindung bzw. des Anbindungsbausteins genauso möglich.

3.9.4. Patienten Management

Ein wesentlicher Einflussfaktor für ELGA ist das Patienten Management bzw. das zugehörige Identifier Management. Hier legt IHE IT TF Vol. 1 in Kapitel 10.4.9 „Patient Identification Management“ fest, dass eine Document Registry mit einer sogenannten XDS Affinity Domain Patient ID (XAD-PID), einer eindeutigen PID für den Bereich, arbeitet (Details siehe Kapitel 6.3).

Ein ELGA-GDA, der ein Dokument registrieren will, muss zuvor sicherstellen, dass der betroffene ELGA-Teilnehmer im L-PI registriert ist (Anforderung des IHE Profils). Der L-PI muss den ELGA-Teilnehmer spätestens zu diesem Zeitpunkt auch an den Z-PI melden, damit das Dokument in ELGA gefunden werden kann. Darüber hinaus bzw. alternativ muss es für einen ELGA-GDA ermöglicht sein einen Patienten auch über globalen Identifier (wie SV-Nummer oder bPK-GH) zu identifizieren (vorwiegendes Szenario im niedergelassenen Bereich).

Welche Schnittstellen der drei möglichen (PIF, PDQ, PIX) zwischen GDA-System und lokalem Patientenindex (L-PI) implementiert werden, ist bilateral zwischen Auftraggebern beider Systeme abzustimmen. Es wird empfohlen, auf die Transaktionen der IHE-Profile PIX und PDQ zu setzen.

Das Patienten Management bedarf zwischen den einzelnen GDA-Systemen und dem übergeordnetem L-PI, unabhängig von der einzelnen Systemgröße und der Anzahl an gespeicherten Patienten in einem System, eines permanent etablierten Clearing-Prozesses, welcher im Anlassfall zur Auflösung von Dateninkonsistenzen durchlaufen werden kann. Wie dieser Prozess aufzusetzen ist, muss zwischen den Auftraggebern der GDA-Systeme bzw. dem L-PI, analog zu den Abstimmungen zwischen den Auftraggebern der einzelnen L-PI und dem Z-PI, abgestimmt werden.

Dokumentenabfragen können vom GDA, bei Vorliegen der anderen Zugriffsvoraussetzungen, auch unter Angabe eines Fachschlüssels (zurzeit VSNR, bPK, EKVK-Nummer) durchgeführt werden, ohne den Patienten vorher registrieren zu müssen.

3.9.5. Teilnahmeanforderungen

Innerhalb eines ELGA-Bereichs werden Teilnahmeanforderungen für ELGA-Verweisregister bzw. für GDA-Systeme, die die Akteure Document Consumer, Patient Demographics Consumer bzw. XDS Repository umsetzen, festgelegt. Für GDA-Systeme gelten folgende Anforderungen:

- Existierender Eintrag des ELGA-GDAs in der Komponente GDA-Index.
- Verwendung eines in ELGA zulässigen Authentisierungsverfahrens (Bürgerkarte, Vertragspartnerauthentifizierung des e-card Systems oder von der ELGA Sicherheitskommission (E-SIKO) zugelassener IdP. Die Basiskriterien eines ELGA-konformen Identity Provider sind:
  - Bestätigt die elektronische Identität der im Subjekt der ausgestellten Tokens angeführten Organisation oder physischen Person und zwar:
    - Die angeführte Organisation ist ein ELGA-GDA
    - Die Authentizität der angeführten Person wird durch ein zugelassenes Authentifizierungsverfahren überprüft
    - Die bestätigte elektronische Identität (Person) ist ein für den Zugriff auf ELGA berechtigter Anwender (oder Akteur)
  - Die Bestätigung ist in Form eines SAML 2 Tokens auszustellen und mit einem vertrauenswürdigen Zertifikat zu signieren
  - Der IdP bürgt für die Richtigkeit der im signierten Token angeführten Angaben
- Implementierung der Schnittstellen zur Anbindung an ELGA. Dies kann im Fall von IHE-konformen Systemen reinen Konfigurationsaufwand bedeuten bzw. auch den Einsatz von Anbindungsbausteinen (Schnittstellenkonvertierungen etc.) erforderlich machen. Alternativ bzw. ergänzend kann dies auch durch ein Software-Upgrade des GDA-Systems erfolgen.
- Falls ein *Patient Identity Feed* [ITI-44] aus einem lokalen GDA-System in den L-PI erfolgen soll:
  - Nutzung eines Patienten Management Systems, mit korrekter Identifier Vergabe (d.h. keine Wiederverwendung und keine Synonyme) und vorhandenen Clearing-Funktionen.
  - Verpflichtender Nachweis der IHE-Konformität für die Funktion *Patient Identity Feed* [ITI-44].
  - Implementierung hoher Datensicherheitsanforderungen.
  - Die Durchführung notwendiger Clearing-Maßnahmen ist sicherzustellen. Es muss eine Ansprechstelle für Support eingerichtet werden, die zumindest zur normalen Bürozeit Anfragen beantwortet und Clearingaufgaben durchführt.

3.9.6. Beispiel für die Strukturierung eines ELGA-Bereichs

Im Folgenden werden am Beispiel eines KA-Verbundes auch mögliche Alternativszenarien für den Aufbau diskutiert, insbesondere unter dem Aspekt, wie die Integration vorhandener XDS Infrastruktur in ELGA unter möglichst geringem Adaptierungsaufwand erfolgen kann. Diesbezüglichen Konfigurationsdetails sind im Kapitel 9.1.4 detailliert erörtert.

Abbildung 19 zeigt einen möglichen Aufbau eines ELGA-Bereichs (entspricht **Variante A**, gemäß im Kapitel Berechtigungs- und Protokollierungssystem eingeführter und zugelassener Varianten, siehe auch Abbildung 45), grau dargestellt, bestehend aus einem lokalen Patientenindex (L-PI), Protokollierungskomponente (*L-Audit Record Repository*), ELGA-Verweisregister, ELGA-Repository und dem ELGA-Anbindungsgateway als Virtuelle Maschine (VM) mit dem ELGA-Gateway der Zugriffsteuerungsfassade (Berechtigung). Mit Ausnahme des L-PI befinden sich die Komponenten des ELGA-Bereiches in der Trusted Perimeter Zone. Diese Architektur lässt sich mit dem erhöhten externen Zugriffs-Bedarf seitens anderer ELGA-Bereiche und seitens Internet (EBP) begründen. Wenn die internen Datenspeicher weiterhin geschützt und nur für interne Zugriffe erhalten bleiben sollten, müssen entsprechende Instanzen mit Kopien der für ELGA bestimmten Daten im abgeschotteten Perimeter-Netzwerk eingerichtet werden.

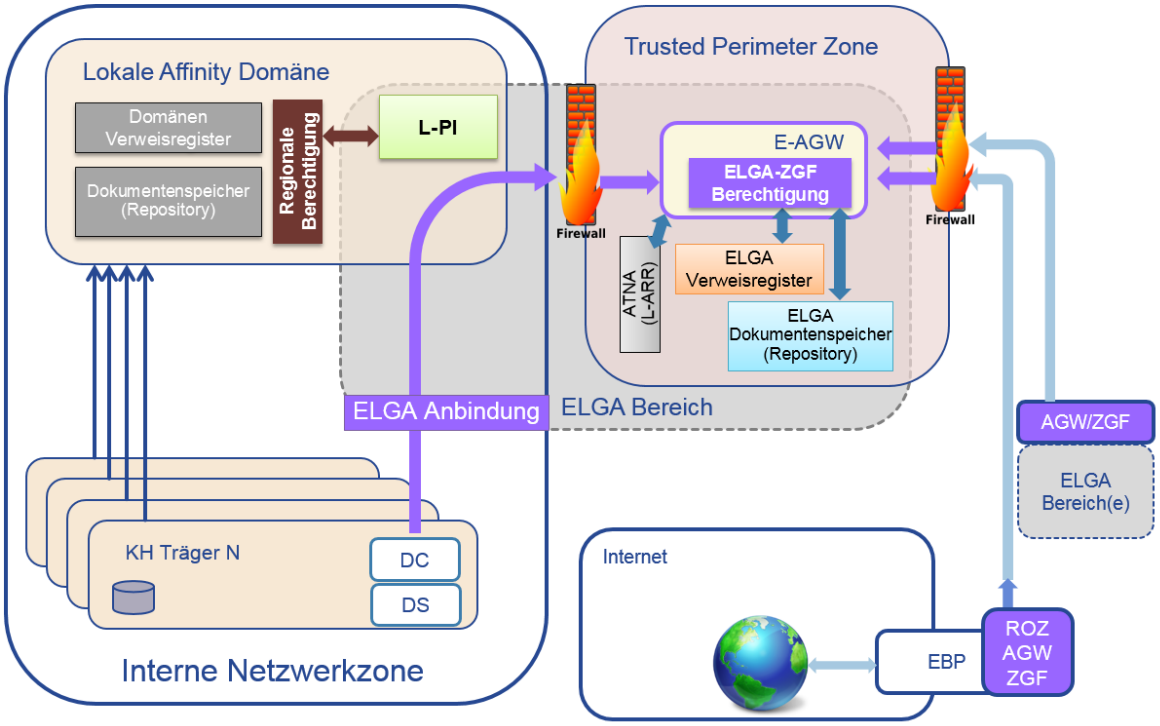


Abbildung 19: Alternativbeispiel für den Aufbau eines ELGA-Bereichs

Der L-PI dient der KIS-übergreifenden Patientenverwaltung. Er setzt somit das Konzept *Patient Demographics Supplier* des Integrationsprofils PDQ um und benutzt den zentralen Patientenindex in der Rolle eines *Patient Demographics Consumer*, um auch zentral

gespeicherte Daten verfügbar zu machen. Es wird angenommen, dass der L-PI auch als PIX-Manager des ELGA-Bereichs fungiert und damit für die Patienten des Bereichs einen eindeutigen Identifier, die L-PID, vergibt.

Der L-PI fungiert auch als Patient Identity Source für den Zentralen Patientenindex und führt den [ITI-44] *Patient Identity Feed* durch. Ein solcher Feed wird spätestens unmittelbar vor der Veröffentlichung des ersten medizinischen Dokuments für diesen Teilnehmer ausgelöst. Wie der Anstoß genau erfolgt wird intern vom Bereich festgelegt. Jedenfalls muss der ELGA-Bereich vor dem Feed an den L-PI für die lokale Speicherung sorgen, sodass keine „Phantom-Patienten“ im Z-PI entstehen können.

In der Abbildung ist ein Dokumentenspeicher (XDS Document Repository) innerhalb der Affinity Domäne (AD) dargestellt und zusätzlich gibt es auch einen ELGA-Dokumentenspeicher im ELGA-Bereich. ELGA-GDA greifen über die vordefinierten ELGA-Schnittstellen auf den ELGA-Dokumentenspeicher zu. Es sind ausschließlich der ELGA-Architektur entsprechend autorisierte Zugriffe zugelassen.

Die ELGA-Zugriffssteuerung/Gateway-Funktionalität (integriert in eine Virtuelle Maschine des AGW) implementiert sowohl das XCA Profil für den Dokumentenaustausch auf Basis von XDS.b als auch das XCA-I Profil für den Austausch von Radiologie-Dokumenten auf Basis XDS-I (siehe hierfür auch Abbildung 29 bzw. Kapitel 8.5. bezüglich XDS-I). Es ist anzumerken, dass Imaging-Profile erst zu einem späteren Zeitpunkt in die Funktionspalette von AGW/ZGF integriert werden. Siehe hierfür Kapitel 16.1, Offene Punkte Liste.

Das AGW charakterisiert sich in dieser Konfiguration wie folgt:

- Implementierung des Integrationsprofils XCA mit den Akteuren *Initiating Gateway* und *Responding Gateway*. Zur Lokalisierung der anzufragenden ELGA-Bereiche werden die durch das ELGA-Token-Service (ETS) ausgestellten *Authorisation-Assertions* ausgewertet, wodurch das ETS die Funktion eines PIX Consumer übernimmt.
- Integraler Bestandteil des ELGA-Berechtigungssystems. Die Zugriffssteuerungsfassade ermöglicht die Autorisierung von Zugriffen auf die ELGA-Verweisregister bzw. die XDS und XDS-I Repositories. Auch der lokale Document Consumer greift auf ELGA ausschließlich mittels des ELGA-Anbindungsgateways zu. Der interne Zugriff aus dem lokalen GDA-System auf lokale (interne) Ressourcen bleibt vom ELGA-Zugriffschutz unberührt. Hierfür gelten unabhängig von ELGA andere gesetzliche Rahmenbedingungen.
- Das XCA ELGA *Imaging Gateway* ermöglicht bereichsübergreifenden Zugriff auf Bilddaten wie dies das IHE Radiology Technical Framework Integrationsprofil XCA-I vorsieht. Die Zugriffe unterliegen ähnlicher Autorisierung wie beim XCA ELGA-Gateway. Das ETS muss kontaktiert werden, um die entsprechenden Berechtigungen in Form einer SAML-Assertion

abzuholen und diese beim Responding XCA-I Gateway zu präsentieren. Policy Enforcement für ankommende Anfragen ist genauso vorgesehen, wobei auch eine verteilte PEP/PDP-Architektur vorstellbar ist (PEP kann direkt mit der Imaging Source integriert werden).

Grundsätzlich werden alle Aktionen in ELGA durch alle an einer Aktion beteiligten Komponenten protokolliert. Protokollnachrichten werden gemäß des Integrationsprofils ATNA in einem bereichsspezifischen *Audit Record Repository* (L-ARR) persistiert.

Die Initiierung der Authentifizierung in ELGA (Login oder Sign-On) kann durch eine spezielle Komponente erfolgen (Beispiel: *Identity Providing Gateway*, nicht in der Abbildung). Diese kann sich eines (nur in speziell geschützten Umgebungen zugelassenen) SW-Zertifikats bedienen, um sich gegenüber dem ETS zu authentisieren. Anschließend übernimmt diese Komponente die Aufgabe, die vom lokalen IdP (etwa ein Authentication Server in Kombination mit Active Directory oder Novell Directory) ausgestellte Identity Assertion (z.B. in Form eines Kerberos Tokens) in eine für ELGA bestimmte SAML 2.0 Assertion umzuwandeln und diese dem ETS zu präsentieren um folglich eine Identitätsföderation zu ermöglichen.

3.10. ELGA-Web Services

ELGA wird im Wesentlichen gemäß dem Integrationsprofil XDS mittels SOAP-basierender Web Services umgesetzt. Dieser Ansatz unterstützt die einheitliche Nutzung der WS-* Standards für die Kommunikation von Softwarekomponenten und die einheitliche Strukturierung von Zusatzinformationen wie z.B. autorisierungsrelevante Attribute.

3.10.1. Transaktionsklammer

Zusätzlich muss bei allen ELGA-Transaktionen zur Nachverfolgbarkeit eine eindeutige Transaktionsnummer vergeben und in den Nachrichtenkopf aufgenommen werden. Sie muss auch in alle Web Service Aufrufe bzw. Folgeaufrufe übernommen werden. Grundsätzlich muss jedes System eines ELGA-Benutzers, das IHE basierte Konzepte implementiert und eine Aktion in ELGA initiiert, eine Transaktionsnummer vergeben, wobei diese sowohl in die L-ARR, Z-L-ARR wie auch in die A-ARR Protokollierung zu übernehmen ist (d.h. z.B. ein Document Consumer sowohl bei Registry Stored Query [ITI-18] und jedem Retrieve Document Set [ITI-43]).

Technisch soll die „Transaktionsnummer“ eine OID sein. Die OID soll als URN gemäß RFC 3061 (A URN Namespace of Object Identifiers) codiert sein. Diese soll im SOAP Header unter Nutzung des WS-Context Standards im Element <context-identifier> transportiert werden. Der Standard wird hier ohne „activity model“ genutzt.

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
  <soap:Envelope xmlns:soap="http://www.w3.org/2002/06/soap-envelope">
    <soap:Header>
      <elga:context
        xmlns="http://docs.oasis-open.org/ws-caf/2005/10/wsctx"
        xmlns:elga="http://elga.at/context/"
        soap:mustUnderstand="1">
      <context-identifier>
        urn:oid:1.3.6.1.2.1.27.47114711
      </context-identifier>
    </elga:context>
.....
```

Alternativ zur OID wird die Verwendung eines Universally Unique Identifier (UUID) zugelassen. Die UUID soll in Form eines URN gemäß RFC 4122 codiert werden. Beispiel: `urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6`.

Zu beachten ist, dass dies eine implementierungsspezifische Erweiterung darstellt, die alle durch ELGA integrierten Systeme (Akteure) unterstützen müssen, da ansonsten die Ziele der Protokollierung nicht erreichbar sind. Die Rede ist hierbei von GDA/KIS-Systemen sowie Registry und Repository Akteuren.

3.10.2. ELGA Release-Richtlinien

Die in [24] beschriebene **ELGA Produktrelease-Richtlinie** basiert prinzipiell auf Abwärtskomptabilität der mit der jeweiligen Herbst-Release (ER2) freigegebenen Schnittstellen. Die Abwärtskompatibilität wird im nächsten Kapitel auf einzelne Bestandteile heruntergebrochen analysiert und der verpflichtende Ablauf definiert (siehe Kapitel 3.10.4.2). Frühjahrs-Releases (ER1) beinhalten dementsprechend ausschließlich Fehlerkorrekturen und Hotfixes. So gesehen ist bei einer ER1 keine Änderung an den bereits existierenden Schnittstellen und Endpunkten zu erwarten (siehe Kapitel 3.10.4.1). Um alle möglichen Szenarien abzudecken, werden im nächsten Kapitel (siehe 3.10.4.3) aber auch Maßnahmen für jenen unerwünschten Fall definiert, wenn bei einer künftigen ER2 keine Abwärtskompatibilität mehr gewährleistet werden kann.

3.10.3. ELGA Service Information Manager (SIM)

Client Akteure müssen in der Lage sein, die aktuelle Version der zur Verfügung stehenden Komponenten und die Liste der ansprechbaren Service-Provider Endpunkte (URL) vom

System abzufragen. Hierfür wird das Konzept eines Service Information Managers (SIM) eingeführt, der die notwendigen Informationen an einen autorisierten Klienten (z.B. GDA/KIS System) liefert.

Es muss zwischen einem zentralen und dezentralen, sowie XCA SIM unterschieden werden, wie dies in der Abbildung 20 verdeutlicht wird.

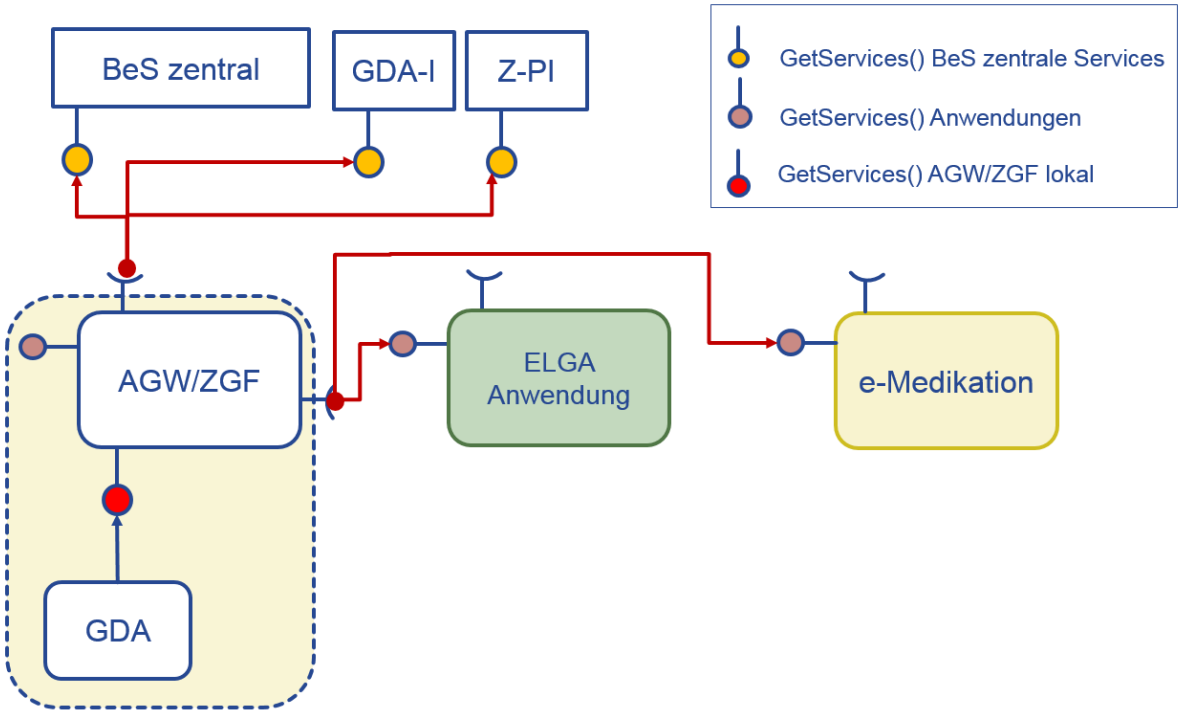


Abbildung 20: Service Information Manager Schnittstellen und deren Zusammenspiel

Grundsätzlich wird die in der obigen Abbildung 20 dargestellte Informations-Kette mit dem Ansprechen des lokalen SIM-Endpunktes gestartet. Dieser Endpunkt (*GetServices*) liefert *per default* nur die Versionsnummer der AGW/ZGF und die **lokalen** XDS URL-Endpunkte zurück. Dadurch wird die lokale Anfrage schnell und performant erledigt, weil für die Beantwortung der Anfrage keine Remote-Verbindung hergestellt werden muss.

Durch eine erweiterte Anfrage an den SIM-Endpunkt (*GetServicesAll*) liefert diese Schnittstelle zusätzlich auch die Versionsnummer und URL-Endpunkte der zentralen Services sowie die Versionsnummer der zugänglichen ELGA-Anwendungen. Die Anfrage löst mehrere entfernte Anfragen aus. Es werden die SIM der verfügbaren zentralen Komponenten und die SIM der ELGA-Anwendungen kontaktiert.

Details bezüglich verwendeter Protokolle und Spezifikation der SIM-Schnittstelle sind in einem eigenen Pflichtenheft auszuarbeiten. Als Ausgangsbasis muss die Struktur der Anfrage des

entsprechenden e-Card Service Managers herangezogen werden. Siehe beispielhaft das XSD-Schema per Service:

```
<xs:complexType name="GetServicesResponse">
      <xs:sequence>
        <xs:element name="return" type="Service" maxOccurs="unbounded" minOccurs="0" />
      </xs:sequence>
 </xs:complexType>

<xs:complexType name="Service">
      <xs:sequence>
        <xs:element name="description" type="xs:string" minOccurs="0" />
        <xs:element name="endPointURL" type="xs:string" minOccurs="1" />
        <xs:element name="name" type="xs:string" minOccurs="1" />
        <xs:element name="type" type="xs:string" minOccurs="0" />
        <xs:element name="version" type="xs:string" minOccurs="1" />
        <xs:element name="configuration" type="xs:string" minOccurs="1" />
      </xs:sequence>
</xs:complexType>
```

Tabelle 9: Grundlegende Struktur der Antwort des ELGA-SIM

Service		
Attribute	**Typ/Länge**	**Bedeutung**
name (R)	String/16	Name des Service (z.B. ETS, Z-PI, GDA-I, …usw.)
type (O)	String/32	Deployment Typ des Service (z.B. SOAP wrapped/literal, HTTPS-POST, oder REST, FHIR-DSTU2 usw.
version (R)	String/64	Major & Minor Version (und evtl. Build) des Service
configuration (O)	String/64	Zusätzliche Angaben zum Deployment/Config-Package
description (O)	String/256	Beschreibung des Service
endPointUrl (R)	String/256	Relative URL des Endpunktes für diesen Service

Tabelle *10*: Bedeutung der XSD-Elemente; O-Optional, R-Required

3.10.4. Versionierung

Die ELGA-Geschäftslogik und ELGA-Dienste werden durch ELGA Web-Services angeboten und von dafür autorisierten Akteuren konsumiert. ELGA Softwarekomponenten und insbesondere Web-Services sind zu versionieren, wobei das allgemein verbreitete Muster „*Major.Minor.Build“* zu verwenden ist. Darüber hinaus ist zwischen den einzelnen Teilen und Ausprägungen der zu versionierenden Dienste und der Versionsnummer selbst wie folgt zu unterscheiden:

1. **Service Endpunkt Adresse**: ist eine echte URL. Wird in SOAP via http/POST angesprochen. Endpunkte müssen in den Pfadnamen (den Hostnamen folgend) bei Erhöhung der Major-Version zumindest diese Major-Version abgebildet haben. Beispiele: https://elga-online.at/ETS/V2 oder https://elga-online.at/ETS/V3

2. **SOAPAction**: ist für SOAP V1.2 ein optionales http-Header Element mit einem Wert im URI-Format. Es dient dazu, den http-Request an die entsprechenden SOAP-Layer/Bindings zu senden. Meistens führt eine SOAPAction zu einer konkreten Methode. SOAPActions sollten in ELGA Web-Services zwar versioniert werden, jedoch können wegen der Vielfältigkeit von URI hierfür keine fest vorgeschriebenen Regeln aufgestellt werden. Beispiel für eine SOAPAction ist: „http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue“

3. **Schnittstelle**: ist eine via WSDL/XSD Repräsentation freigegebene Ansammlung von unterstützten SOAPActions, Methoden und Datentypen sowie von dazugehörigen Parametern. Schnittstellen sind durch entsprechende Namespaces (*targetNamespace*-Attribut) zu versionieren. Das hier verwendete Muster ist optional, jedoch muss bei inkompatiblen Änderungen zumindest die Major-Version enthalten sein. Beispiele: *targetNamespace* = „http://kbs.spirit.com/V3“ oder *targetNamespace* = "http://ets.spirit.com/V3"

4. **Software Instanz**: ist einer oder mehreren Service-Exe und/oder Dlls gleichzusetzen, die eine oder mehrere Schnittstellen anbietet. Hierfür ist eine strikte Versionierung via *„Major.Minor.Build“* vorgegeben, die als entsprechende Datei-Attribute und/oder Teile von Dateinamen im gegebenen Betriebssystem abzubilden sind.

5. **Deployment Paket**: ist ein aus mehreren Teilen zusammengestelltes Produkt, welches Endpunkte, Schnittstellen und Software Instanzen (etwa Apache & ZGF) bereitstellt. Ein typisches Beispiel ist das AGW, ausgeliefert als virtuelle Maschine. Solche Pakete sind mit zumindest zwei kompletten, zusammengefügten Versionsnummern zu versehen. Konkret gilt für das Einheitspaket ZGF und AGW: *„ZGF_Major.ZGF_Minor.ZGF_Build.ZGF_Konfig.AGW_Konfig“*

6. Bei der **Versionierung** von oben angeführten Endpunkten, Schnittstellen, Software Instanzen etc. ergeben sich zwangsläufig Abhängigkeiten, die organisatorisch zu verwalten sind. Die Hebung einer Versionsnummer einer bestimmten Komponente (z.B. des Endpunktes) muss nicht unbedingt das gesamte System betreffen. Es muss ermöglicht werden bei Bedarf auch Teilkomponenten, einzelne Schnittstellen und einzelne Endpunkte auf eine höhere Version zu heben, ohne dabei die Version von anderen Teilkomponenten oder des Gesamtsystems ändern zu müssen.

3.10.4.1. Build-Nummer Änderung (betrifft ER1)

Eine Änderung der ***Build***-Nummer bezieht sich auf vollkompatible Versionen innerhalb des gleichen *Major.Minor* Versionskreises. Eine Erhöhung der Build-Nummer ist bei Fehlerbehebungen und/oder Patching erforderlich. Hierbei bleibt der Funktionsumfang der Software unangetastet (keine Erweiterungen).

Ändert sich etwa wegen Fehlerbehebung nur die Build-Nummer, so können die betroffenen Komponenten in beliebiger Reihenfolge in Betrieb genommen werden. Es gibt keine Schnittstellenänderung. Es muss eine 100% Kompatibilität zur niedrigeren Build-Nummern aufrechterhalten bleiben. Hierfür muss in einem geplanten (oder temporär angekündigten) Wartungsfenster die alte Komponente von Netz genommen und die neue gestartet werden.

3.10.4.2. Minor-Version Erhöhung (Abwärtskompatibilität, betreffend ER2)

Eine Änderung (Erhöhung) der **Minor**-Nummer signalisiert eine abwärtskompatible Änderung mit geänderten (erweiterten) Funktionalitäten. Die Software mit erhöhter Minor-Nummer bleibt jedoch immer abwärtskompatibel.

- URL-**Endpunkte** von Web-Services bleiben unangetastet
- Bezüglich neuer oder geänderter **SOAPActions** sind keine verpflichtenden Regeln einzuhalten, nur die Abwärtskompatibilität muss verpflichtend garantiert werden (keine willkürliche Änderung der kompatiblen Methoden-Namen)
- Die **Schnittstelle** bleibt abwärtskompatibel (ältere Minor-Versionen können die neueren Minor-Version garantiert benutzen). Die Änderungen sollten (optional) jedoch in Form der ***targetNamespace***-Benennung abgebildet werden
- Für die **Instanz/Komponente** gilt die verpflichtende Erhöhung der Minor-Nummer

Ändert sich etwa wegen Funktionserweiterung die Minor-Nummer, dann müssen die betroffenen Komponenten in der hier angeführten Reihenfolge in Betrieb genommen werden:

1. In einem dafür vorgesehenen Server-Wartungsfenster sind zuerst die neuen (betroffenen) zentralen Serverkomponenten mit höherer Minor-Nummer in Betrieb zu nehmen.
2. Ist das Server-Wartungsfenster beendet, müssen alte Client-Komponenten die Services der neu aufgesetzten Server-Komponenten problemlos (da Abwärtskompatibilität gewährleistet) konsumieren können. Während des serverseitigen Wartungsfensters ist kein Client-Betrieb möglich. Da alte Clients technisch gesehen die neuen Services beliebig lang konsumieren können, sind die Zugriffe alter Client-Komponenten organisatorisch auf maximal 1 Jahr zu beschränken.

3. Wenn alte Client-Komponenten (eines Bereiches) die Services der neuen Server-Komponenten nachweislich konsumieren können, kann das Aufsetzen der neuen Client-Komponenten mit höherer Minor-Nummer beginnen.

4. In einem dafür vorgesehenen Wartungsfenster müssen in den Bereichen neue Client-Komponenten mit höherer Minor-Nummer ausgerollt werden.

3.10.4.3. Major-Version Erhöhung (Inkompatible Änderungen)

Eine Änderung der **Major**-Version ist bei inkompatiblen Änderungen (sog. *Breaking Changes*) notwendig, da Abwärtskompatibilität nicht mehr garantiert werden kann. Die Schnittstelle ändert sich massiv. Eine Major-Nummer Erhöhung muss durch die Änderung der entsprechenden URL-Endpunkte mitgetragen werden. Dadurch ist zu verhindern, dass sich ältere Clients der neuen inkompatiblen Version bedienen.

Inbetriebnahme von *Breaking-Changes* Versionen mit erhöhter Major-Versionsnummer muss nach folgendem Schema ablaufen:

1. Es wird angenommen die aktuelle Server-Version ist 2.2.10. Eine neue Version 3.0.0 muss nun aufgesetzt werden. Am Beispiel von ETS wird angenommen, dass der aktuelle V2.2.10 Endpunkt unter **https://elga-online.at/ETS** erreichbar ist.

2. Während der Betrieb mit V2.2.10 Komponenten unangetastet läuft, müssen neue Endpunkte für die zentralen Serverkomponenten errichtet werden. Am obigen Beispiel von ETS, wird der neue Endpunkt unter **https://elga-online.at/ETS/V300** eingerichtet (für KBS wäre dies z.B. **https://elga-online.at/KBS/V300**). Zu diesem Zeitpunkt sind parallel zwei Endpunkte für ETS aktiv (ähnlich für KBS, PAP, A-ARR etc.). Die Last läuft aber noch zu 100% über die alten V2.2.10 Endpunkte.

3. Sobald die neuen Server-Endpunkt erreichbar und aktiv sind, können in den ELGA-Bereichen zusätzlich zu den alten V2.2.10 Komponenten neue AGW/ZGF Komponenten der erhöhten Major-Version ausgerollt/aufgesetzt/eingerichtet werden. Die neuen Client Major-Version Komponenten greifen auf die entsprechenden neuen V3.0.0 Major-Version-Serverendpunkte zu.

4. Damit entsteht ein Zustand mit zwei parallel laufenden vollwertigen, aber unterschiedlichen Versionen, wobei die volle Last noch immer die alte Version V2.2.10 trägt.

5. Ab einem von Administratoren abgestimmten Zeitpunkt werden in den einzelnen ELGA-Bereichen die zwangsläufig aktualisierten GDA/KIS Software-Anfragen auf V3.0.0 AGW/ZGF umgeleitet. Damit entsteht ein Zustand, in dem die alten GDA/KIS-Systeme noch über V2.2.10 laufen, aber die neu aufgesetzten GDA/KIS-Systeme

bereits über die V3.0.0 ELGA-Komponenten angebunden sind. Es laufen parallel zwei voneinander unabhängige Major-Versionen.

6. Die alten V2.2.10 gebundenen GDA/KIS-Systeme können noch eine bestimmte Zeit die alten Komponenten ansprechen. Sobald das Deployment von neuen GDA/KIS-Systemen abgeschlossen ist, können zuerst die in den ELGA-Bereichen installierten alten AGW/ZGF Komponenten abgeschaltet werden.
7. Erfolgt die Umstellung in allen ELGA-Bereichen, können zuletzt auch die alten V2.2.10 Server-Endpunkte vom Netz genommen werden. Dadurch bleiben nur mehr die neuen V3.0.0 Endpunkte und Schnittstellen erreichbar und das Rollout gilt als abgeschlossen.

3.11. Verfügbarkeit

3.11.1. Verfügbarkeit logisch zentraler Komponenten

Verfügbarkeit definiert sich allgemein (oberflächlich) durch sogenannte Verfügbarkeitsklassen, die im Prinzip anhand der „9er“ in der prozentuell ausgedrückten Verfügbarkeits-Wahrscheinlichkeitszahl klassifiziert sind. Für ELGA muss zumindest eine Verfügbarkeit in einem Ausmaß, wie dies in [16] ELGA Service Levels definiert ist, garantiert werden.

Anmerkung: Bei einer Klasse 3 (99,9%) Verfügbarkeit ist die monatliche ungeplante Nicht-Erreichbarkeit mit 44 Minuten limitiert. Bei der Gesamtbewertung der Verfügbarkeitsklassen sind nicht nur die serverseitige Infrastruktur, sondern auch die für das Aufrechterhalten der Verbindungen verantwortlichen Komponenten (Kabelleitungen, Stromversorgung, etc.) miteinzubeziehen.

Grundsätzlich wird davon ausgegangen (Annahme), dass für die Nutzung von ELGA folgende zentrale Komponenten hochverfügbar sind:

- Externer vertrauenswürdiger Identity Provider (sofern ein zentrales System wie das e-card System zur Authentisierung verwendet wird)
- ELGA-Token-Service (ETS)
- Für den Abruf der XACML Regeln vorgesehener Service, der Policy Administration Point (PAP)
- Kontaktbestätigungs-Service (KBS)
- Zentraler Patientenindex (Z-PI)
- GDA-Index (GDA-I)
- Aggregierte Audit Record Repository (A-ARR)
- Lokale Audit Record Repository (L-ARR) für die zentralen Komponenten

- e-Medikation (ELGA-Anwendung)

Die Verfügbarkeitsdefinitionen sonstiger Komponenten in ELGA sind [16] zu entnehmen. Darüber hinaus ist zu vermerken, dass die Hochverfügbarkeit logisch zentraler ELGA-Komponenten (da diese von allen ELGA-Systemen benutzt werden) die der dezentralen Systeme übersteigen muss.

3.11.2. Verfügbarkeit der ELGA-Verweisregister

Aus Sicht der Architektur müssen auch die Verweisregister und die Verbindung zwischen diesen (ELGA-Anbindungsgateway bzw. Netzwerkinfrastruktur) eine hohe Verfügbarkeit aufweisen. Dies begründet sich darin, dass das Ergebnis einer Dokumentensuche beim Ausfall von nur einem angefragten Verweisregister als unvollständig gekennzeichnet werden muss und damit für den anfragenden GDA im Allgemeinen nur geringen Nutzen aufweist. Hingegen könnte für den Zugriff auf ein konkretes Dokument eine geringe Verfügbarkeit akzeptiert werden, weil hier klar ist, welches Dokument fehlt und damit zumindest eine sichere Beurteilung des Sachverhalts durch den GDA möglich ist.

Anmerkung: Vollständigkeitshalber wird aus Architektursicht darauf hingewiesen, dass natürlich auch die Möglichkeit eines zentralen hochverfügbaren Verweisregisters bestünde. Diese wurde jedoch bewusst zugunsten der Regionalisierung nicht aufgegriffen.

Für den dezentralen Betrieb des ELGA-Anbindungsgateways und des ELGA-Verweisregisters bedeutet dies folgende Empfehlungen:

1. Redundanter Netzanschluss und redundante Netzwerk-Infrastruktur
2. Beschränkung der Wartungszeiten auf die ELGA-weit vordefinierten Wartungsfenster
3. Redundante Hardware und Stromversorgung (Storage, Hosts)
4. Wenn möglich Implementierung von Lastverteilung oder Hot-Standby mit automatisiertem Fail-Over für die ELGA-relevanten Services
5. Wenn möglich die Umsetzung einer Rufbereitschaft wenn kein bedienter Betrieb möglich ist.

3.11.3. Offline Betrieb der ELGA-Bereiche

Unter offline Betrieb eines ELGA-Bereichs werden Szenarien zusammengefasst, die bei Nichterreichbarkeit von zentralen oder dezentralen Services entstehen. Unter dem Begriff Nichterreichbarkeit werden alle Störungen bzw. SLA-Verletzungen zusammengefasst, die aus Sicht des lokalen ELGA-Anbindungsgateways entstehen. Folgende Ausfallszenarien sind zu betrachten:

- **Ausfall von zentralen Services**. Sind zentrale Services, egal aufgrund welcher Betriebseinschränkungen, nicht erreichbar, so sind ohne weitere Maßnahmen keine Zugriffe auf ELGA möglich, da sich das Berechtigungssystem auf diese Services stützt.

  Konsequenz: Ein Ausfall bzw. die Nicht-Erreichbarkeit der zentralen Dienste muss beim Aufruf der Methoden der ELGA Service-Schnittstellen klar und eindeutig feststellbar sein.

- **Ausfall von entfernten (remote) ELGA-Bereichen**. Dieser Betriebszustand tritt bei Nichterreichbarkeit der Dienste anderer ELGA-Bereiche auf und führt jedenfalls zu fachlichen Einschränkungen, da Suchergebnisse teilweise unvollständig sind bzw. sein könnten. Die Verfügbarkeit kann somit nur durch zusätzliche technische Maßnahmen bei der Vernetzung bzw. in den einzelnen ELGA-Bereichen erhöht werden.

  Konsequenz: Die Service-Schnittstellen von ELGA (z.B. *Registry Stored Query*) müssen den initiierenden Akteuren ein unvollständiges Resultat wegen Unerreichbarkeit (z.B. Timeout) eines ELGA-Bereichs erkennbar retournieren.

3.12. Altdatenübernahme

Grundsätzlich startet ELGA mit dem Einschaltzeitpunkt, eine „Vorbefüllung“ der ELGA ist aus rechtlichen Gründen nicht erlaubt.

ELGA-relevante Gesundheitsdaten (die nach dem Einschaltzeitpunkt von ELGA entstanden sind) können in ELGA über die Zugriffssteuerungsfassade übernommen werden, indem sie entweder:

1. im ELGA-Verweisregister explizit registriert werden oder
2. existierende Verweise im lokalen XDS-Registry mit einem ELGA-Flag für ELGA markiert werden (die Markierung muss über das zuständige AGW erledigt werden)

Bei der Einbindung von bereits existierenden ELGA-Bereichen müssen die im lokalen Patientenindex (L-PI) vorhandenen demografischen Daten in einem Ersterfassungsschritt beim zentralen Patientenindex (Z-PI) angemeldet werden. Für die Altdatenübernahme beim Z-PI sind keine proprietären Funktionen notwendig, die Funktionalität kann durch die regulären Schnittstellen ausreichend bedient werden.

3.13. Vertrauensverhältnisse und Zertifikatsdienste

Vertrauensverhältnisse basieren ausschließlich auf X.509 Zertifikaten. Das Management der notwendigen Zertifikate wird auf Basis einheitlicher ELGA-PKI Richtlinien aufgebaut. Zertifikate sind zumindest für folgende Zwecke notwendig:

1. ATNA Secure Node Zertifikate je Akteur (Server- und Clientzertifikate bzw. Applikationszertifikate). Diesbezügliche kryptographische Einschränkungen (bezüglich TLS-Version) sind im Kapitel 9.3 explizit angeführt.

2. Zertifikate für das Signieren von SAML 2.0 Token (nur vom ETS)

Grundsätzlich werden alle ELGA-Akteure in drei Sicherheitszonen (Ebenen) eingeordnet.

1. Zentrale-Ebene mit den zentralen Komponenten, inklusive Z-PI, GDA-I, ETS, PAP, A-ARR
2. Ebene der ELGA-Bereiche, welche durch die Zugriffssteuerungsfassaden und entsprechend konfigurierte Registries und Repositories vertreten wird
3. GDA-Ebene oder Client Ebene, beinhaltet die einzelnen KIS-Systeme bzw. Arztsoftware, Document Consumer und Document Source Akteure (inkl. ELGA-Portal).

Die Akteure der zentralen Ebene und der ELGA-Bereichsebene beziehen ELGA-relevante Zertifikate von einer dafür eingerichteten zentralen ELGA-Core PKI. Registry- und Repository-Akteure der ELGA-Bereiche beziehen die Zertifikate von der Bereichs-PKI. Akteure der dritten Ebene beziehen im Regelfall Zertifikate von der PKI des jeweils vertraglich gebundenen ELGA-Bereiches. Darüber hinaus ist es möglich sog. *peer-to-peer* Vertrauensverhältnisse einzeln, aufgrund von externen CAs ausgestellten Zertifikaten, aufzubauen.

Laut Beschluss der Arbeitsgruppe Netzwerk & Zertifikate dürfen Akteure der dritten Ebene nicht direkt auf die zentralen Komponenten zugreifen. Der Zugriff erfolgt immer über die zweite Ebene. Die Anfragen (Requests) der dritten Ebene werden auf der zweiten Ebene ausnahmslos terminiert und falls es die ursprüngliche Endpunktadresse verlangt, Richtung zentrale Komponenten neu aufgesetzt. Diesbezügliche Performanceeinbußen müssen entsprechend berücksichtigt werden. Ausnahmen von dieser Regelung sind denkbar, soweit ein Akteur der dritten Ebene ein entsprechendes vertrauenswürdiges Zertifikat besitzt, und sich als vertrauenswürdiger *ATNA Secure Node* präsentiert.

Alle betroffenen PKI müssen diesbezüglich folgende Richtlinien erarbeiten und der ELGA-SIKO vorlegen:

- **Generelle Sicherheitsrichtlinien** (Security Policy - SP) in denen alle im jeweiligen ELGA-Bereich vorliegenden ELGA-relevanten Services und Komponenten aufgelistet werden müssen, deren Betrieb und Zugang mit Zertifikaten geregelt und gesichert ist.
- **Zertifikatsrichtlinien** (Certificate Policy - CP). Hier muss das allgemeine Regelwerk bezüglich des Umgangs mit Zertifikaten festgehalten werden. Es wird festgelegt, wer die Verantwortung bei kompromittierten Zertifikaten tragen muss und wie mit solchen Situationen im Allgemeinen umgegangen wird. Es wird beschrieben, wie und wo private und öffentliche Schlüssel abgelegt, gesichert und verwaltet werden sowie von wem und wie diese exportiert und migriert werden dürfen.

- **Certificate Practice Statements** (CPS) wodurch der konkrete und verpflichtend vordefinierte Umgang mit Zertifikaten geregelt wird. Es wird etwa die Liste jener in ELGA zugelassenen CAs aufgelistet (Namen, DNS, Adressen), die Zertifikate für ELGA ausstellen dürfen. Es müssen die Prozesse beschrieben werden, die das Verhalten beim Ausrollen und Erneuern der Zertifikate regeln. Es müssen Zeiträume definiert werden, innerhalb derer das Erneuern der Zertifikate stattfinden muss. Die verwendeten Schlüssellängen und kryptografischen Algorithmen werden hier ebenso aufgelistet, wie die verpflichtenden technischen und organisatorischen Maßnahmen bei Feststellung einer Kompromittierung.

3.13.1. Vertrauensverhältnisse zwischen ELGA und externen Identity Providern

3.13.1.1. TLS-Ebene

Zwischen ELGA und externen Identity-Providern gibt es keine direkte Kommunikation. Ein IdP macht weder Anfragen an ELGA, noch wendet sich ein Akteur der zentralen und/oder Bereichsebenen an einen IdP.

3.13.1.2. SAML-Token-Ebene

Die Authentifizierung der Benutzer in ELGA ist externalisiert. ELGA vertraut bestimmten externen Identity Providern, die für ELGA-Benutzer eine elektronische Identität in Form einer SAML 2.0 Assertion ausstellen. Hierfür müssen Vertrauensverhältnisse mit den jeweiligen vertrauenswürdigen IdP aufgebaut und verwaltet werden. Die Vertrauensverhältnisse basieren auf einer expliziten Trust-Liste, die beim zentralen ELGA-Token-Service geführt und verwaltet wird. Darüber hinaus muss gewährleistet werden, dass das zur IdP-Token-Signatur verwendete Zertifikat dem IdP eindeutig zuordenbar ist. Eine Zulassung von externen IdP in ELGA ist die Aufgabe der ELGA-Sicherheitskommission (E-SIKO). Jeder IdP wird einzeln überprüft und beurteilt.

3.13.2. Vertrauensverhältnisse zwischen ELGA-Bereichen

3.13.2.1. TLS-Ebene

ELGA-Bereiche kommunizieren ausschließlich über vorgeschaltete AGW miteinander. Ein AGW enthält eine ZGF-Komponente, welche eine Initiating- und einen Responding-Gateway Komponente integriert. Ein Initiating-Gateway (I-GW) ist in der Regel ein Client und ein Responding Gateway (R-GW) ein Server. Hierfür muss ein I-GW mit einem Client-Zertifikat vom ELGA Core-PKI ausgestattet werden und die R-GW-Komponente mit einem entsprechenden Server-Zertifikat. Die Root CA der ELGA Core-PKI ist auf den einzelnen AGW in der Liste vertrauenswürdiger CAs eingetragen. Darüber hinaus müssen die bekannten AGW Instanzen (R-GW) bei den I-GW als zugelassen vorkonfiguriert werden.

3.13.2.2. SAML-Token-Ebene

Beim zu errichtenden zentralen ELGA-Token-Service müssen die Vertrauensverhältnisse zwischen den Service-Providern der ELGA-Bereiche (AGW) und dem zentralen ETS bilateral aufgebaut werden. Hierfür sind alle AGW Instanzen (die R-GW Komponenten) so zu konfigurieren, dass der Signatur des zentralen ETS vertraut wird. Wenn ein ZGF/I-GW als Client eine ELGA-Assertion (Treatment, User II bzw. Mandate II) vom ETS bezieht, dann wird dieser Token mit dem vertrauenswürdigen ETS-Zertifikat signiert. Nachdem alle AGW/ZGF-Instanzen dem zentralen ETS vertrauen, ergibt sich das Vertrauensverhältnis zwischen den einzelnen AGW/ZGF Instanzen automatisch.

3.13.3. Vertrauensverhältnisse zwischen GDA und dem ELGA-Bereich

3.13.3.1. TLS-Ebene

Laut IHE ATNA Secure Node Vorgaben müssen alle Akteure (GDA-Systeme), die unmittelbar mit dem AGW kommunizieren, authentifiziert sein und entsprechend eine TLS-Verbindung aufbauen. Hierfür beziehen Client (das GDA-System) und Server (WAF/Apache Server integriert in AGW) entsprechende Client- bzw. Server-Zertifikate der PKI des jeweiligen ELGA-Bereichs. Die PKI des ELGA-Bereiches ist unabhängig von der ELGA Core-PKI. In einem ELGA-Bereich können GDA-Systeme von unterschiedlichen PKI die eigenen Client-Zertifikate beziehen. Dies hat aber zur Konsequenz, dass der AGW Server all jenen Root-CA vertrauen muss, deren Zertifikate im Bereich Verwendung finden. Ein GDA-Client (Akteur) muss zumindest dem eigenen Root CA und dem Root CA des AGW Servers vertrauen. Im Optimalfall sind die beiden PKI identisch. Darüber hinaus muss das AGW den einzelnen Akteur-Instanzen (GDA-Systeme) explizit vertrauen.

Wenn ein GDA-Akteur eine Anfrage an ein zentrales Services stellen will, dann muss dies über die entsprechenden Endpunkte der AGW via TLS-Verbindung erfolgen. AGW terminiert die TLS-Verbindung, und baut Richtung zentraler Dienste eine neue TLS-Verbindung auf. Diese zweite TLS-Verbindung basiert auf dem ELGA-Core PKI Client-Zertifikat des AGW. Somit bürgt eine AGW für alle anfragenden Akteure der dritten (GDA-) Sicherheitszone.

3.13.3.2. SAML-Token-Ebene

Auf dieser Ebene müssen keine Vertrauensverhältnisse vorkonfiguriert werden. Ein GDA-Akteur bezieht eine Identity Assertion (IDA) von seinem IdP. Mit dieser IDA holt er über das AGW beim ETS eine ELGA HCP-Assertion ab (ELGA-Login). Die ELGA HCP-Assertion ist vom ETS signiert (integritätsgeschützt). Der Akteur muss die Signatur nicht verifizieren, nur bei sich aufheben (max. 4 Stunden ab Ausstellung). Die Verifikation des Tokens erfolgt vom Berechtigungssystem beim Initiieren von Transaktionen über das AGW.

3.13.4. Vertrauensverhältnisse zwischen Komponenten der zentralen Services

3.13.4.1. TLS-Ebene

Zentrale Komponenten kommunizieren miteinander direkt. Die gegenseitige Authentifizierung der Komponenten erfolgt aufgrund Secure Node TLS-Zertifikaten von Core-PKI.

3.13.4.2. SAML-Token-Ebene

Zwischen zentralen Komponenten werden SAML-Token nicht gefordert.

3.14. Kontaktbestätigungsservice

3.14.1. Allgemeines

Bereits in der Abbildung 2 sind zwei Ausprägungen von Kontaktbestätigungsservices dargestellt (detaillierte Erklärung und Verwendung siehe weiter im nächsten Kapitel 3.14.4). Das zentrale ELGA-Kontaktbestätigungsservice hat die führende Rolle und dient als einzige Quelle für das ETS, um existierende Kontakte zwischen GDA und Patienten abzufragen. Die dafür bereitgestellte Schnittstelle basiert auf dem von OASIS standardisierten WS-Trust Protokoll (RST/RSTR) und ist im Pflichtenheft des Berechtigungssystems detailliert zu beschreiben.

Kontaktbestätigungen (OID: 1.2.40.0.34.5.161) werden in stationäre und ambulante Aufenthalte unterschieden. Daraus ergeben sich vier GDA-Kontakte, die gemeldet werden

können (in Klammern sind die gültigen Werte des oben angeführten OID-Codesystems gelistet):

1. Stationärer Kontakt (K101)
2. Ambulanter Kontakt (K102)
3. Entlassungskontakt (K103)
4. Delegierter Kontakt (K104)

3.14.2. Regeln für den Umgang mit Kontaktbestätigungsmeldungen

Unten angeführte Regeln sind mit R1 bis R14 durchnummeriert. Referenzen werden in der Form KBS-Rx angeführt, wobei x die Nummer der Regel repräsentiert.

- R1) Stationärer Kontakt

  Bei stationären Kontakten hat der zuständige GDA uneingeschränkten, im Rahmen seiner durch die individuellen Policies des ELGA-Teilnehmers gesetzten Rechte, Zugang zu den Gesundheitsdaten des Patienten.

  - R1.1) Die gesetzlich zulässige Zugriffszeit von 28 Tagen gilt ab einer Entlassungsmeldung via Entlassungskontakt.

- R2) Ambulanter Kontakt

  Bei ambulanten Kontakten hat der zuständige GDA im Zeitraum der gesetzlich zulässigen Zugriffszeit von 28 Tagen, im Rahmen seiner durch die individuellen Policies des ELGA-Teilnehmers gesetzten Rechte, Zugang zu den Gesundheitsdaten des Patienten.

- R3) Wahlfreiheit für KH und PH

  ELGA-GDA in der ELGA-Rolle Krankenhaus oder Pflegeeinrichtung dürfen sowohl ambulante wie auch stationäre Kontakte melden. Zulässige Qualitäten der Patientenidentifikation sind die Nutzung des L-PI, des e-card Systems mit und ohne Stecken der e-card sowie das Stecken der Bürgerkarte.

  - R3.1) Bei stationärer Aufnahme eines Patienten besteht die Wahlfreiheit zwischen einem stationären Kontakt und einem ambulanten Kontakt.
  - R3.2) Bei einem ambulanten Aufenthalt des Patienten besteht obige Wahlmöglichkeit nicht.
  - R3.3) Die Default Zugriffszeiten für diese GDA dürfen über die gesetzlichen 28 Tage hinaus nicht verlängert werden. Die Verkürzung der Zugriffszeiten via individuellen Zugriffsberechtigungen ist aber möglich.

- R3.4) Ambulante Kontakte können in stationäre Kontakte mit dem gleichen Kontakt-Zeitstempel umgewandelt werden.

- R4) Kontaktqualität für Arzt / Zahnarzt und Apotheker

  ELAG-GDA in der ELGA-Rolle (niedergelassener) Arzt, Zahnarzt oder Apotheker dürfen nur ambulante Kontakte melden. Zulässige Qualität der Patientenidentifikation ist ausschließlich die Nutzung des e-card Systems mit Stecken der eCard.

- R5) Beendigung einer stationären Aufnahme

  Ein stationärer Aufenthalt ist ausnahmslos mit einem Entlassungskontakt zu beenden.

  - R5.1) Die Einbringung eines Entlassungskontaktes ist ausschließlich nach, bezogen auch den Zeitstempel, einer, mit ihm in Verbindungstehender, stationären Aufnahme möglich.

  - R5.2) Eine Entlassungsmeldung ohne einer stationären Aufnahme muss zur Fehlermeldung führen und wird vom KBS nicht gespeichert.

- R6) Singulärer stationärer Kontakt pro GDA/Patient

  Pro GDA und pro Patient (bPK-GH) darf nur ein stationärer Kontakt aktiv sein. Weitere stationäre Meldungen müssen zu einer Fehlermeldung führen und werden vom KBS nicht gespeichert.

  - R6.1) Es können pro Patient (bPK-GH) mehrere aktive stationäre Kontakte von unterschiedlichen GDA existieren. Beispiel: Pflegeheim meldet einen stationären Aufenthalt. Patient wird zur Operation vom Pflegeheim ins Krankenhaus überstellt, GDA meldet auch einen stationären Kontakt. Es gibt zwei aktive stationäre Kontakte für den einen Patienten (bPK-GH).

- R7) Gültiger ambulanter Kontakt

  Pro GDA zählt immer nur der chronologisch jüngste, bezogen auf den Zeitstempel, ambulante Kontakt. Vorherige ambulante Kontakte mit älterem Zeitstempel werden gespeichert, sind aber automatisch wirkungslos.

- R8) Stornierung von Kontakten

  Sämtliche Kontakte können auch storniert werden. Nach dem stornieren des jüngsten Kontaktes wird der zweitjüngste Kontakt zur Zugriffsprüfung herangezogen.

  - R8.1) Das stornieren einer stationären Aufnahme ohne vorangegangener Stornierung der damit in Verbindung stehenden Entlassung ist nicht zulässig.

- R9) Priorität stationärer Kontakte

Stationäre Kontakte gehen immer vor ambulanten Kontakten. Ambulante Kontakte mit jüngerem Zeitstempel werden aufgezeichnet, beenden die Gültigkeit eines stationären Kontaktes nicht.

- R10) Delegation von Kontakten

  Gültige stationäre und ambulante Kontakte können an jene GDA delegiert werden, die in die Behandlung des Patienten explizit einbezogen werden/wurden. Delegierte Kontakte sind grundsätzlich wie ambulante Kontakte. Die Gültigkeit der delegierten Kontakte stützt sich auf die Gültigkeit der zugrundeliegenden Kontakte.

  - R10.1) Ambulante Kontakte „vererben“ dem delegierten Kontakt ihren Startzeitpunkt
  - R10.2) Stationäre Kontakte erhalten als Startzeitpunkt den Delegationszeitpunkt.
  - R10.3) Wenn der einem delegierten Kontakt zugrundeliegende Kontakt storniert wird, muss auch der delegierte Kontakt für ungültig erklärt werden, sprich dieser muss ebenfalls automatisiert storniert werden.
  - R10.4) Delegierte Kontakte dürfen nicht weiterdelegiert werden.

- R11) Update ohne gültigen Kontakt

  Wenn das ETS keine Kontaktbestätigung für einen identifizierten ELGA-Teilnehmer (L-PID bzw. bPK-GH) im zentralen ELGA-Kontaktbestätigungsservice finden kann, werden dem GDA sämtliche Zugriffsversuche auf die angeforderten Gesundheitsdaten des jeweiligen Patienten untersagt. Ausnahme ist das Updaten (Richtigstellen) von Gesundheitsdaten gemäß Datenschutzgesetz 2000, Artikel 1, § 1 Absatz 3 Punkt 2. Hierfür wird seitens des Berechtigungssystems ermöglicht, dass auch bei einer abgelaufenen Kontaktbestätigung bereits eingebrachte CDA richtiggestellt werden können (inklusive Statusänderung auf *Deprecated*, storniert).

- R12) Variable zeitliche Einbringung von Kontaktbestätigungen

  Kontakte können grundsätzlich bis zu 28 Tage in der Vergangenheit und bis zu 24 Stunden in der Zukunft eingebracht werden.

  - R12.1) Es ist nicht zulässig zeitsynchrone Kontakte (identischer Zeitstempel) einzubringen. Sollte ein Kontakt mit einem bereits im KBS existierenden Zeitstempel eingebracht werden, dann muss dies in einer Fehlermeldung resultieren.
  - R12.2) Der aktuelle Kontaktstatus ermittelt sich aus der aufsteigendem Reihenfolge der Zeitstempel und nicht aus der Reihenfolge der Einbringung.

- R13) Historisierung

  Die primäre Aufgabe des KBS ist es den aktuellen Behandlungszusammenhang (Kontakt-Zeitstempel) zwischen dem Patienten und dem GDA festzuhalten. Eine Historisierung für

betriebstechnische Unterstützung soll mit entsprechenden Methoden (z.B. Trigger welcher den tatsächlichen Einmeldezeitpunkt festhält „CreationTime“) im Backend realisiert werden.

- R14) ELGA-GDA kann die selbst eingebrachten und gerade aktiven Kontakte zu einem, mit ihm im Behandlungskontakt stehenden, Patienten abfragen.

3.14.3. Löschen von eingebrachten Kontakten

Kontakte sind nach einem Jahr ab Einmeldung vom KBS zu löschen und zwar nachfolgend aufgelisteten Regeln beachtend:

1. Löschen von allen ambulanten Kontakten die älter als 1 Jahr sind
2. Löschen von allen delegierten Kontakten die älter als 1 Jahr sind
3. Löschen von allen Entlassungs-Kontakten die älter als 1 Jahr sind
4. Löschen von jenen stationären Kontakten, zu denen der entsprechende Entlassungskontakt soeben gelöscht wurde.

Anmerkung: Nach dem Löschen eines Entlassungskontaktes und vor dem Löschen des dazugehörigen stationären Kontaktes darf der stationäre Kontakt nicht aktiv werden.

5. NICHT gelöscht werden dürfen jene stationäre Kontakte die älter als Jahr sind, für die aber noch keine entsprechende Entlassung gemeldet wurde.

3.14.4. Kontaktbestätigungsservice Varianten

Grundsätzlich existiert in ELGA ein zentrales Kontaktbestätigungsservice (KBS). Das zentrale ELGA-Kontaktbestätigungsservice arbeitet darüber hinaus nahtlos mit dem Security Token Service (STS) des e-card Systems (Abbildung 21) zusammen. Letzteres ist für den niedergelassenen GDA-Bereich mit direkter Anbindung an das e-card System der Sozialversicherung vorgesehen. Es wird davon ausgegangen, dass die GDA-Software beim Stecken der e-card den dadurch entstandenen und vom STS des e-card Systems signierten Kontakt (Schritt 3) über die GINA-Box erhält und an das zentrale ELGA-Kontaktbestätigungsservice weiterleitet. Die gültige Kontaktbestätigung muss in der Folge im Rahmen einer WS-Trust RST-Transaktion mit einer ELGA HCP-Assertion im SOAP Security Header an das zentrale ELGA-KBS gemeldet werden (siehe Schritt 4). Somit werden nur jene Kontakte anerkannt, die mit einer gültigen ELGA HCP-Assertion eingebracht werden. Nur ELGA-GDA können eine ELGA HCP-Assertion besitzen. ELGA-GDA in der Rolle Arzt oder Apotheker dürfen Kontakte ausschließlich aufgrund obigen Verfahrens (Stecken der e-Card) an KBS melden.

ELGA-GDA aus dem Krankenhaus- oder Pflegebereich ohne e-card Anbindung müssen Kontakte selbst ausstellen (etwa über eine Aufnahmekanzlei oder ein Patientenmanagementsystem, siehe Schritt 3) und den so entstandenen Kontakt an das zentrale ELGA-KBS melden (Schritt 4), wobei die Rolle „Krankenanstalt“ bzw. Pflegeheim“ vom Berechtigungssystem zu überprüfen ist. Siehe hierfür auch die entsprechende Berechtigungsmatrix (Spalte KBS) in der Tabelle 18.

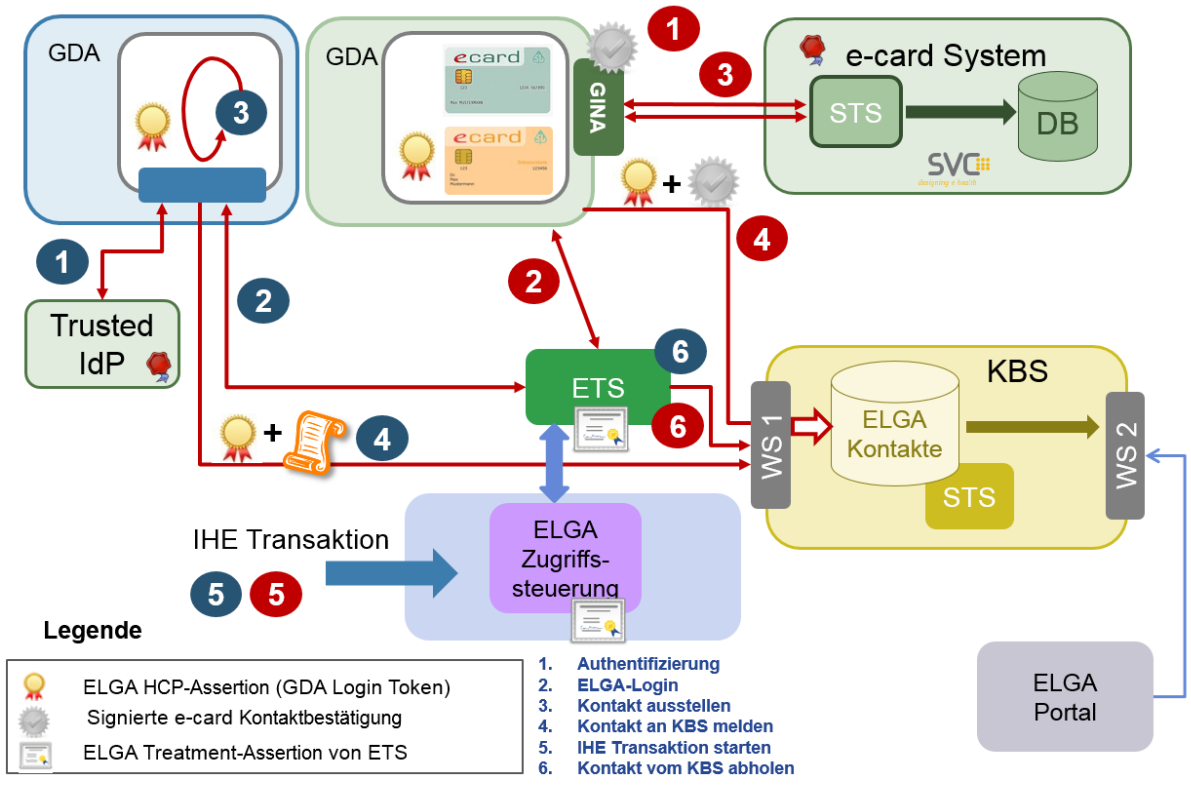


Abbildung 21: Zusammenarbeit der Kontaktbestätigungsservices (siehe e-card System). Blaue Nummern bezeichnen die Schritte eines GDA ohne e-card, rot ist GDA mit e-card Anbindung.

3.14.5. Kontaktbestätigungsservice Fallbeispiele

Das ELGA-Berechtigungssystem nutzt die Einträge des zentralen Kontaktbestätigungsservices, um die resultierende Zugangsberechtigung der ELGA-GDA zu ermitteln. Beispiele in Abbildung 22 illustrieren, wie das ELGA-Token-Service (ETS) anhand der im *Policy Administration Point* (PAP) gespeicherten Regeln des betroffenen ELGA-Teilnehmers die resultierenden Zugriffsberechtigungen des ELGA-GDAs ermittelt.

Wenn der Patient, ein ELGA-Teilnehmer, („Ich“ in Abbildung 22) am 01.01.2016 die e-card beim Dr. Hausarzt steckt (A1 – ambulanter Kontakt), dann hat Dr. Hausarzt ohne weiteres

Zutun des Patienten, laut Gesetzesvorgabe, 28 Tage lang Zugriff auf die ELGA-Gesundheitsdaten des entsprechenden ELGA-Teilnehmers. Wenn der ELGA-Teilnehmer via EBP Dr. Hausarzt vertraut und individuell den Zugriff dieses Arztes auf 365 Tage (1 Jahr) verlängert, dann hat Dr. Hausarzt in Folge Zugriff bis 01.01.2017.

Der so erweiterte Zeitraum auf 1 Jahr gilt weiterhin automatisch bei jedem Stecken der e-card. Somit wird die Richtlinie (1 Jahr Zugriff) des ELGA-Teilnehmers bei jedem Neustecken der e-card dynamisch neu initiiert. Hierfür muss der Patient nicht erneut den Zugriffszeitraum des Hausarztes erweitern. Ein Widerruf kann mit Hilfe des ELGA-Portals jederzeit deklariert werden.

Ein weiteres Beispiel (Abbildung 22) zeigt das dauerhafte Einschränken des Zugriffes des Dr. Urlaubsvertreters auf 2 Tage, immer berechnet vom Datum des Steckens der e-card (A5 und A6 ambulante Kontakte).

Kontaktbestätigungsservice				ETS & Enforcement
GDA	**Datum**	**Kontakt**	**Patient**	**Gültig bis**
Dr. Hausarzt	01.01.2016	A1(e-card)	Ich GDA 365 Tage	A1 => 01.01.2017
Dr. Hausarzt	01.02.2016	A2(e-card)	Ich	A1 => archiviert A2 => 01.02.2017
Dr. Hausarzt	23.12.2016	A3(e-card)	Ich	A2 => archiviert A3 => 23.12.2017
Dr. Urlaubsvertreter	12.02.2017	A4(e-card)	Ich GDA 2 Tage	A4 => 14.03.2017
Dr. Urlaubsvertreter	01.07.2017	A5(e-card)	Ich	A5 => 03.07.2017
Dr. Vienna	03.07.2017	A6(e-card)	Ich GDA 0 Tage	A6 => kein Zugriff
Dr. Vienna	12.07.2017	A7(e-card)	Ich	A7 => kein Zugriff
KH-Spital	03.08.2017	S1 Stationär	Ich	S1 => Zugriff erlaubt
KH-Spital	14.08.2017	E1 Entlassung	Ich	S1 => Archiviert E1 => 11.09.2017
KH-Spital delegiert an Labor	16.08.2015	E1 >> D1 Delegiert	Ich	D1 => 11.09.2017

Abbildung 22: Beispieleinträge eines Kontaktbestätigungsservices und Umsetzung des Willens des ELGA-Teilnehmers (Kontakte: A – Ambulant, S – Stationär, E – Entlassung)

Das dritte Beispiel (Dr. Vienna) dient dazu zu zeigen, dass das Verweigern der Zugriffe auf die eigenen ELGA-Gesundheitsdaten am ELGA-Portal ausgesprochen werden kann. In späterer

Folge kann der ELGA-GDA auf die Gesundheitsdaten des Patienten nicht zugreifen (A6 und A7 ambulante Kontakte).

Das vierte Beispiel (KH-Spital) dient zur Erklärung, dass eine bestätigte Spitalsaufnahme den behandelnden GDA ermächtigt, auf die Gesundheitsdaten des Patienten unbeschränkt zuzugreifen (S1 stationärer Kontakt), wobei die gesetzliche Ablauffrist von 28 Tagen erst ab einem bestätigten Entlassungsdatum zu laufen beginnt (E1 Entlassungskontakt).

Das letzte Beispiel zeigt die Möglichkeit einen gültigen Kontakt an einen ELGA-GDA, etwa ein Labor, zu delegieren (E1 >> D1). Der so delegierte Kontakt (D1) erbt die Gültigkeit vom zugrundeliegenden Entlassungskontakt (E1).

Zusätzliche Fallbeispiele sind in der Abbildung 23 angeführt. Mit Hilfe einer hypothetischen Kette aufeinander folgender Kontaktmeldungen wird die Wechselwirkung der einzelnen Kontaktmeldungen beispielhaft erklärt.

1. Der GDA meldet bei meinem ersten Besuch am 10.06.2015 einen ambulanten Kontakt (A1), welcher standardmäßig 28 Tage gültig ist.
2. Am 12.06.2014 wird ein externer GDA (z.B. Labor) in meine Behandlung einbezogen und der aktuelle Kontakt wird an den ausgewählten GDA delegiert (D1).
3. Am 14.06.2015 setze ich über das Portal die Zugriffsdauer meines GDA auf 0 Tage. Dadurch wird Kontakt A1 vom Berechtigungssystem außer Kraft gesetzt.
4. Am nächsten Tag muss ich beim selben GDA stationär aufgenommen werden. Hierfür wird ein stationärer Kontakt (S1) am 15.06.2015 gemeldet. Der vorherige Kontakt A1 wird archiviert, aber wegen meiner Zugangseinschränkung ist S1 ungültig und der GDA kann nicht auf meine Gesundheitsdaten zugreifen.
5. Am 16.06.2014 im Spital liegend steige ich am Portal ein und ziehe die vorherigen Zugriffseinschränkungen zurück. Dadurch wird der stationäre Kontakt S1 aktiv und mein GDA kann uneingeschränkt auf meine Gesundheitsdaten zugreifen.
6. Am 18.06.2015 meldet mein GDA meine Entlassung (E1). Dies stellt sich aber als voreiliger Administrationsfehler heraus und wird prompt am 19.06.2015 storniert. Es gilt nach wie vor der Kontakt S1.
7. Ich werde am 24.06.2015 tatsächlich entlassen (E2).
8. Mein GDA meldet am 25.06.2015 (irrtümlich) noch einmal meine Entlassung E3. KBS antwortet mit einem Fehler „*Patient bPK-GH wurde bereits entlassen*“. Es gilt die Entlassung E2 wodurch mein GDA noch bis 22.07.2015 (28 Tage) auf meine Befunde zugreifen kann bzw. neue Befunde in ELGA registrieren kann.

9. Am 28.06.2014 delegiert mein GDA den Entlassungskontakt an einen weiteren GDA (D2). Dieser GDA darf anhand der zugrundeliegenden Kontaktbestätigung (E2) auch nur bis 22.07.2015 auf meine ELGA Gesundheitsdaten zugreifen.

Kontaktbestätigungsservice				ETS & Enforcement
GDA meldet	**Datum**	**Kontakt**	**Patient**	**Gültig bis**
Ambulanter Kontakt	10.06.2015	A1	Ich	A1 => 08.07.2015
Kontakt delegieren	12.06.2015	A1 >> D1	Ich	D1 => 08.07.2015
	14.06.2015		Ich: GDA 0 Tage	A1 => ungültig Zugriff verweigert
Stationärer Kontakt	15.06.2015	S1	Ich	A1 => archiviert S1 => ungültig
	16.06.2015		Ich: GDA 28 Tage	A1 => archiviert S1 => uneingeschränkt
Entlassungskontakt	18.06.2015	E1	Ich	A1, S1 => archiviert E1 => 16.07.2015
E1 stornieren	19.06.2015	E1	Ich	E1 => gelöscht S1 => uneingeschränkt
Entlassungskontakt	24.06.2015	E2	Ich	S1 => archiviert E2 => 22.07.2015
Entlassungskontakt	25.06.2015	E3	Ich	E3 => Fehler! E2 => 22.07.2015
Kontakt delegieren	28.06.2015	E2 >> D2	Ich	D2 => 22.07.2015

Abbildung 23: Wechselwirkungsfallbeispiele von gemeldeten stationären, ambulanten und delegierten Kontakten

3.14.6. Datenerfassung

Die Aufzeichnung eines stattgefundenen Kontaktes benötigt zumindest die unten angeführten Daten. Diese Daten werden für die Periode eines Jahres (ab Speicherung) aufgehoben und müssen danach gelöscht werden. Ausnahmen sind auch über ein Jahr gültige stationäre Kontakte.

- Eindeutige Identifikation des Ausstellers des Kontaktes (GDA OID)
- Datum und Zeitpunkt des Behandlungskontaktes (UTC-Format)
- Qualifikation des Behandlungskontaktes (Codesystem OID: 1.2.40.0.34.5.161)
  - Ambulanter Kontakt

- Aufnahme in eine stationäre Einrichtung oder permanente Betreuung. Berechtigt den GDA zum zeitlich uneingeschränkten Zugang zu Patientendaten. Dies wird durch eine Entlassungs-Qualifikation aufgehoben.
- Entlassung aus einer stationären Einrichtung oder aus permanenter Betreuung
- Delegierter Kontakt, wenn ein GDA im Besitz einer gültigen Kontaktbestätigung einen anderen GDA (z.B. Labor, Radiologe, etc.) in die Behandlung einbezieht.

- Eindeutige ID des Patienten (bPK-GH)
  - Ein ELGA-GDA kann auch die L-PID des Patienten angeben. Das KBS muss dann den lokalen Identifier via Z-PI auflösen
- Qualität der Identifikation (Codesystem OID: 1.2.40.0.34.5.162, in Klammern sind die gültigen Werte des Codesystems angeführt)
  - Stecken der e-card (PIM101)
  - Stecken der Bürgerkarte (PIM102)
  - Identifikation des Patienten über den L-PI, z.B. via Aufnahmekanzlei (PIM103)
  - Identifikation des Patienten über e-card System ohne stecken der e-card (PIM104)
- Status des Ereignisses (gültig oder zu stornieren)

3.15. ELGA Dokumenten- und Datenmodell

Für die erste Umsetzungsphase von ELGA wurden die Dokumentenklassen Entlassungsbrief (Ärztlich, Pflegerisch), Laborbefund und Befunde der bildgebenden Diagnostik („Radiologiebefunde“) sowie die Daten der e-Medikation ausgewählt. Zur Verwendung in ELGA werden diese Dokumente in standardisierte XML-Dateien im Format HL7 CDA umgesetzt. Nur Dokumentenklassen gemäß generellen Policies können in ELGA verarbeitet werden. Die Vorgaben für die Erstellung der CDA-Dokumente sind die "ELGA CDA-Implementierungsleitfäden", die in mehreren Phasen von Arbeitsgruppen unter Beteiligung von Vertretern der österreichischen Ärzteschaft, Pflege, Krankenanstalten, Forschung, Softwarehersteller für Spitäler, Institute und Ordinationen und unter fachlicher Begleitung von Standardisierungsorganisationen erstellt wurden.

Die eigentlich schützenswerten Daten (sog. *Assets*) in ELGA sind die oben genannten Gesundheitsdokumente und e-Medikationsdaten, die in den dafür bestimmten Repositories gespeichert und aufbewahrt werden. Die Aufgabe des ELGA-Berechtigungssystems ist es, diese Dokumente nur für in ELGA autorisierte Benutzer zugänglich zu machen. Das Lifecycle-Management von diesen Dokumenten zählt nicht zur dedizierten Aufgabe von ELGA, auch wenn hier über die ELGA-Zugriffsteuerungsfassade unterstützende Funktionen angeboten werden, wie das Speichern, Veröffentlichen, Versionieren (Replacement via [ITI-41,42]) sowie

das Storno ([ITI-57]) von ELGA-Dokumenten und das Löschen ([ITI-62]) bzw. Unzugänglich machen von ELGA-Metadaten und Dokumenten. Die Abbildung zusätzlicher administrativer Informationen zu ELGA-Dokumenten mittels XDS Folder wird in ELGA nicht unterstützt. Eine Strukturierung (Zusammenfassung bzw. Beziehungsaufbau) von Dokumenten ist Aufgabe des zur Anzeige genutzten GDA-Systems.

Das ELGA-Berechtigungssystem liefert in erster Linie immer nur jene CDA-Dokumente, die im Status „*approved*“ sind. Um Dokumente, die in den Status „*deprecated*“ gesetzt worden sind zu lesen, müssen spezifische Anfragen (z.B. zeige alle Versionen eines bestimmten Dokumentes) von dafür berechtigten Document Consumern gestellt werden.

Gemäß dem XDS Document-Lifecycle sind neu veröffentlichte Dokument-Metadaten mit dem Status „*approved“* zu versehen. Diese ersetzen die entsprechenden Vorversionen. Technisch wird dabei ein neues Dokument, das in Beziehung vom Typ *„replace“* (RPLC) zur Vorversion steht, erstellt. Auch Ergänzungen zu einem bestehenden Dokument müssen direkt im betroffenen Dokument durchgeführt und anschließend als Folgeversion über die Dokumentenbeziehung *„replace“* (RPLC) abgebildet werden. Ein bereitstellen von eigenständigen Dokumentanhängen bei eBefunden mittels „*append"* (APND) ist nicht erlaubt. Es dürfen ausschließlich Dokumente derselben Dokumentklasse ersetzt werden, d.h. Entlassungsbrief ärztlich durch Entlassungsbrief ärztlich, Laborbefund durch Laborbefund etc. Dementsprechend muss das Metadaten-Attribut XDSDocumentEntry.classCode von ersetztem und ersetzenden Dokument ident sein. Bei der Veröffentlichung der Dokument-Metadaten erhalten die Metadaten der Vorversion den Status „*deprecated“*. Folgeversionen zu Originaldokumenten dürfen aus Gründen der rechtlichen Autorenschaft ausschließlich von jenem GDA (Organisation) registriert werden, der auch das entsprechende Originaldokument in ELGA veröffentlich hat. Weiters müssen Mechanismen der Versionierung von Dokumenten und Dokument-Metadaten entsprechend den Vorgaben des *Allgemeinen Implementierungsleitfaden für ELGA CDA Dokumente*, „6.2.12. Versionierung des Dokuments“ und *ELGA XDS Metadaten,* „1.3.1.2. Ersetzen eines Dokuments durch eine neue Version („Updaten“), 2.2.17. referenceIdList“ verpflichtend eingesetzt werden. Diese Methodik wird unabhängig von Erstellungszeitpunkt des Dokuments angewandt, d.h. ein Dokument darf auch durch ein Dokument ersetzt werden, das älter als das ersetzte Dokument ist.

Den Umsetzungsoptionen des IHE Integration Profiles XDS folgend existieren grundsätzlich weitere Möglichkeiten der Dokumententransformation (XFRM- und XFRM_RPLC-Beziehungen). Als einzig zulässiges Format für eBefunde in ELGA wurde HL7 CDA v2 (als Teil von HL7 v3 Product Suite) festgelegt um semantische Interoperabilität sicherzustellen. Daher existiert keine Notwendigkeit für weitere Formattransformationen. XFRM- und XFRM_RPLC-Beziehungen sind daher nicht erlaubt.

Standardmäßig beziehen sich individuelle Zugriffsberechtigungen immer auf eine SetID, welche die aktuellen und künftigen Versionen eines Dokuments zusammenfasst, und nicht nur auf eine bestimmte Version eines „*approved*“ CDA Dokumentes. Wird dieses Dokument mit einer neuen Version ersetzt und der Status wechselt auf „*deprecated*“, werden die vorher gesetzten individuellen Berechtigungen aber erst dann auf die neue Version übertragen, wenn die SetID gemäß IHE ITI TF [11] in der *referenceIdList* (Metadaten) gespeichert ist. Siehe hierfür in Kapitel 8. die Erläuterung ELGA-Verweisregister und Dokumentenaustausch.

Die Versionierung von Dokumenten bzw. das Richtigstellen von bereits veröffentlichten CDA-Dokumenten ist bei Vorhandensein einer gültigen Kontaktbestätigung zwischen GDA und Patienten immer möglich. Darüber hinaus laut Datenschutzgesetz 2000 Artikel 1, § 1 Absatz 3 Punkt 2 (im Verfassungsrang) der Patient hat das Recht auf Richtigstellung unrichtiger Daten und zwar auch dann, wenn eine Kontaktbestätigung abgelaufen ist. Eine Richtigstellung ist erst dann verhindert, wenn der ELGA-Teilnehmer das Dokument in ELGA gelöscht, den GDA gesperrt oder Opt-Out erklärt hat.

Grundsätzlich müssen alle über ELGA verfügbaren Dokumente unabhängig von deren Größe uneingeschränkt abrufbar bleiben. Für CDA-Dokumente sind entsprechende Empfehlungen zur Größenbeschränkung in den Implementierungsleitfäden definiert. Für Bilder, die im Rahmen der bildgebenden Diagnostik in ELGA relevant werden, muss dies betrieblich erst erarbeitet werden.

3.16. Netzwerkarchitektur

3.16.1. Allgemeines

Die Netzwerkarchitektur definiert die Voraussetzungen und Bedingungen für die Vernetzung der notwendigen physischen Geräte (Server, Router, Switches, etc.), die zur Aufrechterhaltung des Betriebes von ELGA notwendig sind. Im TCP/IP Schichtenmodell betreffen diese Überlegungen die IP-Protokollebene.

3.16.2. Zugelassene Netze und Netzwerkverbindungen

Beim Aufbau des für ELGA zuständigen Netzwerkes wird auf die in Österreich bereits etablierten Gesundheitsnetzwerke *eHI-net* und *Healix* gesetzt. ELGA-Bereiche und zentrale Services sind ausschließlich über diese Gesundheitsnetzwerke anzubinden.

Es sind Provider unabhängige IPv4 Adressen zu verwenden. Die notwendigen Netzwerkadressen müssen (soweit möglich) in zusammenhängenden Blöcken reserviert/bezogen werden. Dabei sind Abhängigkeiten und Anzahl der IT-Umgebungen, die Anzahl der Redundanzen sowie die Anzahl der Anschlüsse zum AGW zu berücksichtigen.

Die Netze werden untereinander verbunden, sodass Einrichtungen, welche im jeweils anderen Gesundheitsnetzwerk stehen, erreichbar sind (siehe Abbildung 24: Netzaufbau für ELGA Punkt f). Dies geschieht unabhängig von den derzeitigen Betreibern der Netze Healix und eHI-net.

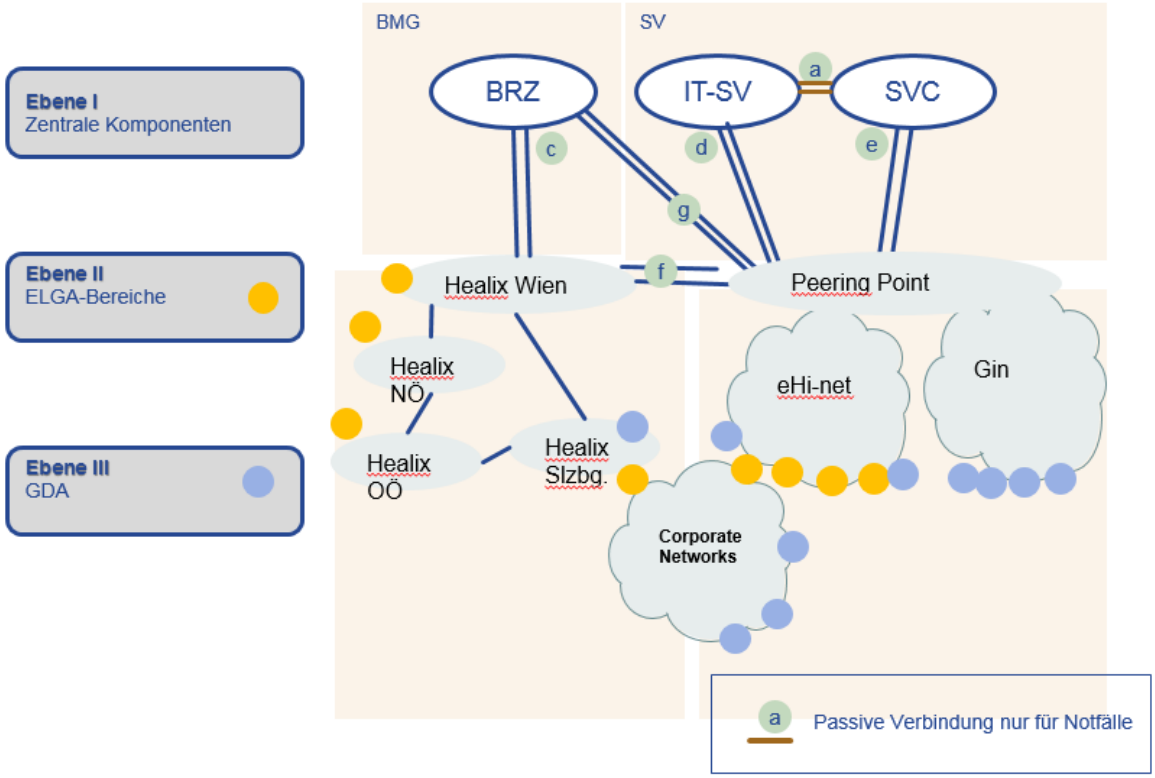


Abbildung 24: Netzaufbau für ELGA

Die Netzwerkanbindung der zentralen Services auf Ebene I (ETS, Z-PI, GDA-I, KBS, PAP, A-ARR) ist redundant mit physischer und örtlicher Trennung (separate Linienführung) der Leitungen vorzusehen. Diese Anforderung ist aus der Mindestverfügbarkeitsdefinition der zentralen Services abgeleitet, die via ELGA Service Levels [16] festgelegt sind. Innerhalb der Ebene II sind die ELGA-Bereiche angesiedelt. Auf der Ebene II sind ausschließlich die Netze Healix und eHi-Net zugelassen und welche mit den zentralen Komponenten wie oben abgebildet verbunden sind (Leitungen c, d, e g). Innerhalb der Ebene III befinden sich die GDA-Systeme. Diese können über die Netze Healix, eHi-Net, GIN oder eigene Corporate Networks an die Ebene II angebunden werden.

Zentrale Komponenten sind zusätzlich mit CNSV-Netz (siehe Leitungen a und b) verbunden. Damit wird die Kommunikation zwischen den einzelnen zentralen Komponenten bzw. Betreibern der zentralen Komponenten über ein Corporate Network (CNSV-Netz) verschlüsselt und physisch direkt geleitet.

Anmerkung: Ebenso dürfen sich ELGA-Bereiche Corporate Netzwerke bedienen, solange diese in ihrer Hoheit liegen und den gesetzlichen Bedingungen entsprechen.

3.16.3. Netzwerkbandbreiten

Die erforderlichen Netzwerkgeschwindigkeiten wurden auf drei Stufen definiert.

1. Die Stufe 1 ist mit der bestehenden Netzwerkinfrastruktur zu realisieren und muss zumindest eine Bandbreite von 2x10 Mbit/sec garantieren. Diese Stufe ist ausschließlich für Tests zu verwenden.
2. Stufe 2 soll zumindest mit 2x100 Mbit/sec operieren können. Aufgrund des Mengengerüstes (Kapitel 13) wird davon ausgegangen, dass diese Stufe für den regulären ELGA-Betrieb zumindest in den ersten Monaten/Jahren und für den Transport von CDA ausreichen wird. Bildmaterial kann nur in sehr beschränktem Ausmaß transportiert werden.
3. Die Stufe 3 (zumindest 2x1 Gbit/sec) muss spätestens bei Inbetriebnahme von Bilddaten-Übertragung bzw. dann eingesetzt werden, wenn die Grenzen der Stufe 2 ausgeschöpft sind. Die Aufschaltung wird terminlich situativ gemäß Betriebsüberwachung und nach betriebswirtschaftlichen Kriterien gesteuert.

3.16.4. Namensauflösung und Namenskonventionen

Für den Betrieb des zentralen ELGA Domain Name Systems (DNS) mit einer Mindestverfügbarkeit laut ELGA Service Levels [16] ist das BRZ vorgesehen. Darüber hinaus muss der AGW Domänennamen der zentralen Komponenten (Ebene I) aufgelöst werden können; bei sonstigen Domänennamen wird auf eine Weiterleitung (*forwarding*) in Richtung der jeweiligen DNS-Instanz des eigenen ELGA-Bereiches gesetzt. Die Domänennamen der zentralen Dienste/Komponenten (Ebene I) sowie der Dienste der Ebene II werden beim zentralen DNS eingetragen und gewartet. Grundsätzlich ist von der anbei liegenden Namenskonvention der Domänennamen auszugehen (siehe Tabelle 11 und Tabelle 12)

Umgebung	Kürzel (Zahl / Symbol)	Domäne
Referenz	10 / R	.10.elga-core.at
Labor 1	20 / L1	.20.elga-core.at
Labor 2	30 / L2	.30.elga-core.at
Integration	40 / I	.40.elga-core.at
GDA- Softwarehersteller	50 / I2	.50.elga-core.at
Vorproduktion	60 / V	.60.elga-core.at
Produktion	80 / P	.80.elga-core.at

Tabelle 11: Namenskonvention der zentralen Ebene I

Kürzel	ELGA-Bereich	Domäne

10	Oberösterreich	umgebung.elga-x10.at
11	KAV-Wien	umgebung.elga-x11.at
12	A1	umgebung.elga-x12.at
13	Steiermark	umgebung.elga-x13.at
14	AUVA	umgebung.elga-x14.at
15	Tirol	umgebung.elga-x15.at
16	Kärnten	umgebung.elga-x16.at
17	SVC-RO	umgebung.elga-x17.at
18	NÖ	umgebung.elga-x18.at
19	Burgenland	umgebung.elga-x19.at
20	Salzburg	umgebung.elga-x20.at
21	Vinzenzgruppe	umgebung.elga-x21.at
22	Vorarlberg	umgebung.elga-x22.at
23	AURA	umgebung.elga-x23.at
24	Health-net GmbH	umgebung.elga-x24.at
81	Portal inkl. OBST	umgebung.elga-x81.at
82	WIST	umgebung.elga-x82.at
91	ITH	umgebung.elga-x91.at
92	x-tention	umgebung.elga-x92.at
93	Testcenter x-tention	umgebung.elga-x93.at
95	Testcenter WIST	umgebung.elga-x95.at
96	Testcenter eMed	umgebung.elga-x96.at
97	Testcenter Portal	umgebung.elga-x97.at
98	Testcenter ROZ	umgebung.elga-x98.at
99	Test-Team	umgebung.elga-x99.at

Tabelle 12: Namenskonvention der Ebene II

Es wird davon ausgegangen, dass sich ein GDA ausschließlich mit einem ELGA-Bereich (Ebene II) verbindet.

Network Time Protocol (NTP): Es muss ein zentraler Secure NTP-Dienst verwendet werden. Dieser Dienst ist für jeden ELGA-Bereich verbindlich zu verwenden.

GDA können zusätzlich zu den angeführten Gesundheitsnetzwerken (eHI-net, Healix) auch via GIN an ELGA angebunden werden. Sollten GDA nur über das Internet anbindbar sein, so sind zusätzliche kryptografische Maßnahmen zu treffen, etwa in Form von verpflichtenden VPN-Verbindungen.

3.17. ELGA-Assets

ELGA-Assets sind all jene Ressourcen, die aufgrund von gesetzlichen Bestimmungen besonders schützenswerte Informationen beinhalten und welche zum Austausch zwischen explizit autorisierten Akteuren zur Verarbeitung oder Einsichtnahme angeboten werden

können. Hierfür wird in primäre, sekundäre und tertiäre Assets unterschieden. All diese Assets sind ausschließlich über kryptografisch abgesicherte Transportwege (TLS) zu übertragen. Ausnahmen (wenn vorhanden) müssen einzeln begründet und zur Genehmigung bei der Sicherheitskommission vorgelegt werden. Zugriff auf Assets ist ausschließlich über explizite Autorisierung gestattet, wobei dies zumindest auf Ebene von ATNA Secure Nodes erfolgen muss.

Primäre Assets sind alle Gesundheitsdaten inklusive CDA und Multimediadaten, die in den einzelnen ELGA-Bereichen in XDS Verweisregistern und Repositories sowie in Bildarchiven gespeichert sind und noch werden. Primäre Assets sind in der Hoheit der einzelnen ELGA-Bereiche und den vertraglich und technisch an diese Bereiche gebundenen GDA sowie in der Hoheit der Betreibern der ELGA-Anwendungen (z.B. e-Medikation), die solche Daten (Assets) persistieren.

Primäre ELGA-Assets sind

- CDA Dateien in Repositories
- Daten der Bildgebenden Diagnostik (überwiegend in PACS)
- Metadaten in den Verweisregistern
- Daten der e-Medikation, Medikationslisten

Sekundäre Assets sind jene Daten, die vom ELGA-Berechtigungssystem für die Autorisierung der Zugriffe auf die primären Assets angelegt, gebraucht, ausgegeben, verwaltet und herangezogen werden.

Sekundäre ELGA-Assets sind

- Generelle XACML-Policies gespeichert in PAP
- Individuelle XACML-Policies und signierte Willenserklärungen gespeichert in PAP
- Kontaktbestätigungen gespeichert im KBS
- Datenbestände des GDA-I
- Patientendaten im Z-PI
- SAML 2 Assertions (Authorisation Assertion), die vom ETS ausgegeben werden
- Community Assertions, die von der ZGF ausgestellt werden

Tertiäre Assets sind die laufend anfallenden Protokolldaten, welche der lückenlosen Nachvollziehbarkeit aller Zugriffe auf die primären und sekundären Assets dienen.

Tertiäre ELGA-Assets sind

- Protokolle in den einzelnen L-ARR der ELGA-Bereiche

- Protokolle im zentralen L-ARR sowie die Protokolle von GDA-I und Z-PI
- Protokolle im A-ARR
- Logdaten (Traces) des Berechtigungssystems

3.18. Profilierung der IHE-Transaktionen

Die offiziellen IHE-Profile [11] definieren eine weite Palette an Umsetzungsmöglichkeiten, die von IHE-Konformen Akteuren (z.B. Verweisregistern und Repositories) implementiert werden können. Aus der Sicht der im Kapitel 2.7 aufgelisteten ELGA-Anwendungsfälle ist jedoch die Unterstützung aller möglichen Umsetzungsoptionen nicht notwendig und wäre kontraproduktiv, da auch Profile getestet werden müssten, die seitens ELGA keine Relevanz haben und in den Sicherheitsbetrachtungen nicht entsprechend berücksichtig sind. Die Verwendung nicht getesteter Profile birgt hohe (auch sicherheitstechnische) Risiken und kann zu unvorhersehbaren inkonsistenten System-Zuständen führen. Die Umsetzungsoptionen der IHE Integrationsprofile sind daher entsprechend der zu realisierenden Anwendungsfälle einzuschränken und deren korrekte Implementierung im Rahmen der Tests zu verifizieren.

Es ist wichtig zu vermerken, dass die hier genannten Einschränkungen ausschließlich seitens aktiv zugreifender IHE-Akteure (Clients) gelten, also seitens GDA/KIS (z.B. XDS Document Source & Consumer, Anbindungsbausteine) bzw. der Komponenten, welche die Anfragen von ELGA-Teilnehmern umsetzen. Nachdem diese Zugriffe immer und ausschließlich über die ZGF geführt sind, müssen ZGFs die in diesem Kapitel aufgezählten Einschränkungen aktiv umsetzen. Clients, welche gegen diese Regeln verstoßen, sind durch entsprechend dokumentierte Fehlercodes zu informieren.

Die Profilierungen von Transaktionen des Z-PI (und L-PI) sind entsprechender Schnittstellendokumentation [22] zu entnehmen (betrifft PIX, PUN, PIF und PDQ).

Darüber hinaus sind Zugriffe auf die in der folgenden Tabelle aufgelisteten Transaktionen einzuschränken und vom ELGA-Berechtigungssystem zu autorisieren. Die Semantik der Requests/Responses folgt der jeweiligen IHE-Dokumentation. Die Unterstützung von synchronen Web Service Zugriffen ist verpflichtend. Asynchrone Web Services sind für eine spätere Ausbauphase verpflichtend vorgesehen jedoch in der Anlaufphase von ELGA werden diese noch nicht eingesetzt. Die Dokumentensuche und deren Abruf beschränkt sich hierbei auf XDS Objekte SubmissionSet sowie DocumentEntry. XDS Folder werden nicht unterstützt und bei Verwendung eine Fehlermeldung „XDSRegistryMetadataError“ bei [ITI-18, ITI-42] bzw. „XDSRepositoryMetadataError“ bei [ITI-41] an den Aufrufer retourniert. Der Ablauf der Zugriffsautorisierung bleibt unabhängig von der Aktion ident.

2292

Transaktion	Titel	Anmerkungen / Einschränkungen
ITI-18	Registry Stored Query	Suche ist auf hier aufgelisteten Query ID eingeschränkt • *FindDocuments* • *GetAll* Darüber hinaus werden XDS Folder in ELGA nicht unterstützt. Einschränkungen sind im Kapitel 11.2 e-Befunde ausführlich erläutert.
ITI-20	Record Audit Event	Ohne Einschränkungen wie IHE_ITI_TF_Vol2a Kapitel 3.20 definiert
ITI-38	Cross Gateway Query	Entsprechend IHE_ITI_TF_Vol2b, Kapitel 3.38 unter Berücksichtigung der oben explizit genannten Einschränkungen von ITI-18
ITI-39	Cross Gateway Retrieve	Entsprechend des unterstützten ITI-43 Profiles Entsprechend IHE_ITI_TF_Vol2b, Kapitel 3.39
ITI-40	Provide X-User Assertion	Verpflichtende Unterstützung von autorisierungs-relevanten SAML2-Token, so wie in Kapitel 9 definiert
ITI-41	Provide and Register Document Set-b	• Wie IHE_ITI_TF_Vol2b Kapitel 3.41 definiert. In ELGA werden ausschließlich XDS Submission Set und XDS Document Entry unterstützt. • Die Verwendung von XDS Folder ist nicht erlaubt. • Im Kontext der Versionierung ist ausschließlich die Dokument-Metadatenbeziehung „RPLC“ zulässig. Darüber hinaus sind SubmissionSets mit „APND“ strikt abzulehnen. Dasselbe gilt für „XFRM“ Beziehungen. • Die Größe der eingebrachten CDA ist auf 20 MB einzuschränken. Größere Dokumente sind abzulehnen. • Bei „RPLC“ muss gewährleistet werden, dass die Metadaten AuthorInstitution und ClassCode des neu eingebrachten Dokumentes übereinstimmen.
ITI-42	Register Document Set-b	Wie IHE_ITI_TF_Vol2b Kapitel 3.42 definiert. In ELGA werden ausschließlich XDS Submission Set und XDS Document Entry unterstützt. Die Verwendung von XDS Folder ist nicht erlaubt. Darüber hinaus gelten die Punkte, die bei ITI-41 bereits definiert sind
ITI-43	Retrieve Document Set-b	Wie IHE_ITI_TF_Vol2b Kapitel 3.43 definiert
ITI-44	Patient Identity Feed HL7 V3	Wie in [22] definiert

ITI-45	PIXV3 Query	Wie in [22] definiert eingeschränkt auf zentrale Akteure wie ETS, KBS und Lösch-Service/Daemon bzw. L-PI
ITI-46	PIXV3 Update Notification	Wie in [22] definiert
ITI-47	Patient Demographics Query HL7 V3	Wie in [22] definiert
ITI-57	Update Document Set	• Ausschließlich „*NonVersioningUpdate“ (proprietär) und „UpdateAvailabilityStatus“* (Dokument Storno) entsprechend IHE ITI TF Supplement XDS Metadata Update, Kapitel 3.57.4.1.3.3.5 werden unterstützt. Es darf kein DocumentEntry (*ExtrinsicObject*) in der Nachricht enthalten sein. Mittels „*UpdateAvailabilityStatus“* stornierte Dokumente dürfen nicht reaktiviert werden, d.h. nach einmaligem UpdateDocumentSet dürfen keine weiteren Statusänderungen erfolgen. • Die Größe der eingebrachten CDA ist auf 20 MB einzuschränken. Größere Dokumente sind abzulehnen. • Es muss gewährleistet werden, dass die Metadaten AuthorInstitution und ClassCode des neu eingebrachten Dokumentes übereinstimmen.
ITI-62	Delete Document Set	Entsprechend IHE ITI TF Supplement XDS Metadata Update, Kapitel 3.62
ITI-63	Cross Gateway Fetch	geplant
ITI-64	Notify XAD-PID Link Change	Sonderfall. Diese native HL7-Nachricht darf in Falle eines Clearings direkt an eine ELGA-Registry (in Varianten A und C) gesendet werden. Anschließend muss eine entsprechende proprietäre [ELGA-1] Reparaturtransaktion ausgelöst werden. Details siehe im Weiteren (Kapitel 9.7 über Clearing in ELGA).
[ELGA-1]	XAD-PID Link Change Repair	ELGA-Hash Reparaturfunktion entsprechend Schnittstellenbeschreibung und/oder Beschreibung im Pflichtenheft des Berechtigungssystems [18]
[PHARM-1]	Query Pharmacy Documents	Suche ist auf hier aufgelisteten Query ID eingeschränkt. Die Details bezüglich Einschränkungen auf Aufrufparameter sind im [15] nachzulesen • *FindPrescriptionsForDispense* • *FindMedicationList* • *FindDispenses*

		• *FindPrescriptions*
[EMEDAT-1]	e-Med spezifische Zusatzfunktionen	• *GenerateDocumentID* (laut Dokumentation in [15]) • *RequestSecurityToken* (entsprechend WS-Trust Standard bzw. [15])

Tabelle 13: Profilierung/Einschränkung der ELGA-Transaktionen

Bei der Veröffentlichung von CDA in ELGA muss das BeS rigoros eine Gültigkeits- und Formatprüfung der von IHE vorgeschriebenen Metadaten durchführen. Siehe entsprechend [7]. Es ist die explizite Aufgabe der ZGF ELGA-Submissions bzw. Veröffentlichungen in ELGA abzulehnen, sobald die von Document Source Akteur zur Verfügung gestellten Metadaten gegen die ELGA-Leitfäden und der hier angeführten Profilierung verstoßen.

4. ELGA-Widerspruchstelle (WIST)

Laut gesetzlichen Vorgaben ist zumindest eine Widerspruchstelle einzurichten, die schriftlich und/oder nicht elektronisch ausgesprochene Opt-Out (bzw. Opt-Out Widerruf) Erklärungen von ELGA-Teilnehmern entgegennehmen und diese über eine vordefinierte Schnittstelle an den zentralen Policy Administration Point (PAP) weiterleiten kann. Der PAP speichert in der Folge den so erklärten Patientenwillen in Form einer XACML-Policy. Die WIST ist gesetzlich berechtigt folgende individuelle Berechtigungen für einen ELGA-Teilnehmer in den PAP zu speichern:

1. Generelles Opt-Out bzw. Widerruf des generellen Opt-Outs
2. Partielles Opt-Out betreffend einer oder mehrerer bestimmter ELGA-Anwendungen bzw. Widerruf eines oder mehrerer partiellen Opt-Outs wie:
    a. e-Befunde
    b. e-Medikation
    c. weitere zukünftig vorhandene ELGA-Anwendungen

Hierfür gilt die Regelung, dass bei einem generellen Opt-Out der ELGA-Teilnehmer von allen existierenden ELGA-Anwendungen (dzt. e-Befunde, e-Medikation) wie auch von künftigen ELGA-Anwendungen abgemeldet ist. Ein partielles Opt-Out hingegen betrifft immer nur eine oder mehrere explizit ausgewählte ELGA-Anwendung/en und hat weder Einfluss auf die implizite Teilnahme an weiteren vorhandenen noch künftigen ELGA-Anwendungen.

4.1. WIST-Authentifizierung

Es ist nicht davon auszugehen, dass ein WIST-Mitarbeiter (Code: 607 in der ELGA Codeliste ELGA_Funktionsrollen) im interaktiven Modus (ohne Batch-Job) auf ELGA zugreifen wird. Die von den einzelnen WIST-Mitarbeitern erfassten ELGA-relevanten Dokumente und

Einstellungen werden im Batch-Verarbeitungsmodus von einem Service-Prozess/Daemon in ELGA eingebracht (siehe Abbildung 25). Hierfür authentifiziert sich der WIST-Prozess beim lokalen Identity Provider (IdP) wie ein interaktiver Anwender. Der zuständige IdP, der ein Vertrauensverhältnis mit dem ETS eingerichtet hat, stellt eine SAML 2 Assertion aus, welche, neben dem WIST-Subject (Organisation) und Lang-Text betreffend den konkreten Anwender (Automat/Account), auch die OID der WIST beinhaltet (1.2.40.0.34.3.1.4). Diese OID ist nicht im GDA-I geführt. Dem ELGA-Berechtigungssystem (ETS) ist diese OID daher etwa in Form einer geschützten Konfigurationsdatei bekanntzugeben. Das ETS föderiert WIST aufgrund vertrauenswürdiger Signatur und OID. Der Account ist dann föderiert wenn eine ELGA-WIST-Assertion ausgestellt wird. Durch das Erhalten einer ELGA-WIST-Assertion ist der WIST-Prozess in ELGA angemeldet.

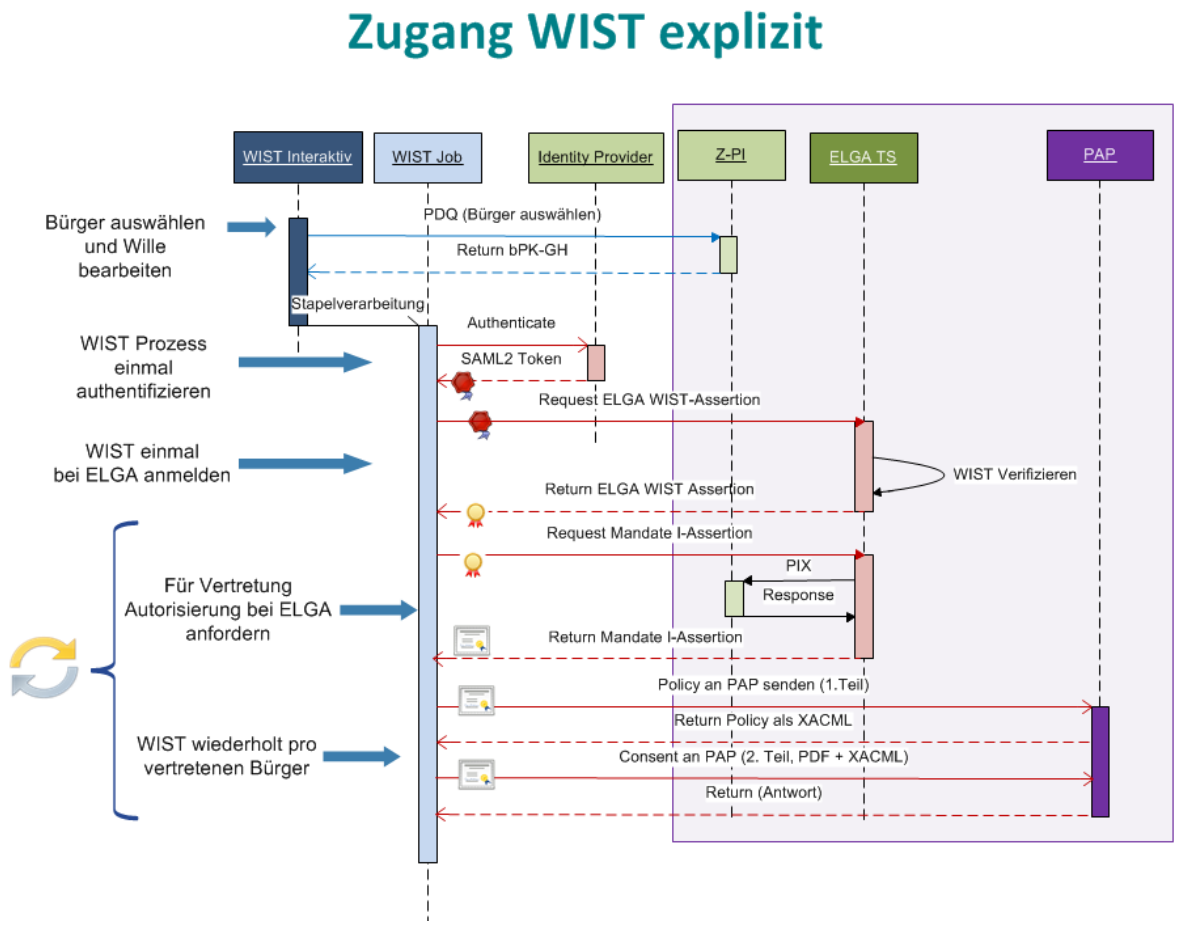


Abbildung 25: Sequenzdiagramm für WIST-Zugang

4.2. WIST-Autorisierung, Vertretungen

Ein ordentlich angemeldeter (föderierter) WIST-Account ist berechtigt, beim ETS eine Vertreter Vollmacht für einen vorher identifizierten Bürger (ELGA-Teilnehmer) anzufordern. Hierfür muss WIST die ELGA-WIST-Assertion im Header der Anfrage (RST) präsentieren, sowie in

der Nachricht den Vertretenen via bPK-GH anführen. Bei berechtigten Anfragen antwortet das ETS mit dem Ausstellen einer ELGA-Mandate I Assertion. Diese Assertion berechtigt (autorisiert) WIST zum Speichern von oben definierten, individuellen Berechtigungen des Vertretenen (Opt-Out bzw. Opt-Out Widerruf).

Die WIST ist nicht berechtigt, bereits vorhandene individuelle Berechtigung von Vertretenen zu erfahren. Die WIST darf individuelle Berechtigungen nur in einer sog. „*Write-Only Manner*" speichern. Die Willenserklärungen sind in Form von amtssignierten PDF-Dokumenten sowie in Form ihrer technischen Repräsentation im PAP zu speichern. Hierfür ist die entsprechende PAP-Schnittstellendokumentation zu konsultieren.

4.3. WIST-Instanziierung

Eine Widerspruchstelle wird bei der ITSV GmbH eingerichtet. Einzelne Mitarbeiter bearbeiten die eingetroffenen Anfragen von Bürgern ohne explizite ELGA-Anmeldung. Die Authentisierung, Autorisierung und Protokollierung erfolgt durch das Dokumentenmanagementsystem der ITSV. Für Zwecke der Patientenidentifikation bedienen sich WIST-Mitarbeiter einer internen PDQ-Schnittstelle.

Die Aufträge werden für eine spätere Stapelverarbeitung gesammelt. Die Stapelverarbeitung wird durch einen Batch-Job (automatischer Prozess) angestoßen und durchgeführt. Der Prozess muss sich beim IdP authentifizieren und in der Folge beim ETS eine ELGA-WIST-Assertion anfordern. Im ausgestellten Ticket steht die Beschreibung/Text des Accounts unter welchem der Prozess läuft. Diese Information wird auch für die ELGA-Protokollierung herangezogen. Die verantwortlichen WIST-Mitarbeiter werden von ELGA nicht protokolliert, müssen aber intern von der WIST (ITSV) selbst protokolliert werden.

Die WIST-Verarbeitung muss über einen speziell geschützten und getrusteten ATNA-Secure-Node in der höchsten Sicherheitszone abgewickelt werden, der zusätzliche Einsatz eines vollwertigen client AGW kann beim WIST-Betreiber (ITSV) daher entfallen. Serverseitig müssen jedoch einem AGW entsprechende Schutzmaßnahmen (wie WAF) implementiert werden.

4.4. Zusammenführen von individuellen Berechtigungen im PAP

Wie oben erklärt, arbeitet WIST in einem sog. *Fire & Forget* Modus. Über WIST eingebrachte individuelle Berechtigungen werden ohne vorherige Abfrage bereits vorhandener Policies direkt dem PAP zum Speichern gesendet. Der PAP muss daher in der Lage sein, die Summe aller eingepflegten XACML-Policies zu verwalten und zu einem einzigen gültigen PolicySet zusammenzuführen. Diese Merge-Operation muss nicht nur die von der WIST eingebrachten Berechtigungen berücksichtigen, sondern auch jene vom ELGA-Portal. Theoretisch ist es möglich, dass Bürger im interaktiven Modus bestimmte individuelle Berechtigungen setzen

und diese später über die WIST ergänzen oder annullieren. Das Berechtigungssystem stützt sich somit ausschließlich auf den unmittelbar nach dem Speichern zusammengeführten Satz an Berechtigungen.

Wenn der Bürger am Portal einsteigt, muss das zusammengeführte PolicySet dargestellt werden. Darüber hinaus sind dem Bürger alle signierten Willenserklärungen (PDF-Dokumente) zur Verfügung zu stellen.

5. ELGA-Ombudsstelle (OBST)

Laut gesetzlichen Vorgaben sind Ombudsstellen (OBST) zu errichten, die in allen Belangen einen Bürger (ELGA-Teilnehmer) in ELGA vertreten können und via explizit angeforderter Vollmachten im Namen des Vertretenen in ELGA agieren dürfen, und zwar:

1. Befunde des Vertretenen lesen
2. Medikationsdaten des Vertretenen lesen
3. Zugriffsprotokolle des Vertretenen einsehen
4. Alle GDA-Kontakte des Vertretenen einsehen
5. Individuelle Berechtigungen des Vertretenen laut dessen Vorgaben ohne Einschränkungen zu verwalten

5.1. OBST-Authentifizierung und Autorisierung

Es wird davon ausgegangen [20], dass OBST-Mitarbeiter als berufsmäßig bevollmächtigte Vertreter im Namen der vertretenen ELGA-Teilnehmer interaktiv auf ELGA zugreifen werden. Hierfür muss jeder OBST-Mitarbeiter ein entsprechend digital signiertes Mandat vom e-Government einholen. Die vom e-Government ausgestellte SAML2 Assertion entspricht dem PVP-Profil und enthält:

- Im Subject (NameID) die OID der OBST-Organisation. Die OID ist im GDA-Index geführt und vom ETS validierbar
- Eindeutige Identität (bPK-GH) der zugreifenden Person (OBST-Mitarbeiter). Muss vom ETS via Z-PI validiert werden.
- Die namentliche Bezeichnung der zugreifenden Person.
- Eindeutige Identität (bPK-GH) des Vertretenen ELGA-Teilnehmers. Muss vom ETS via Z-PI validiert werden.
- Die namentliche Bezeichnung des Vertretenen

Nach Überprüfung der präsentierten e-Government Mandate-Assertion ist vom ETS eine entsprechende ELGA Mandate I Assertion mit der Rolle ELGA-Ombudsstelle (Code: 706 in

der ELGA Codeliste ELGA_GDA_Aggregatrollen) auszustellen. Dadurch wird die elektronische Identität des bevollmächtigten Vertreters und des Vertretenen in ELGA föderiert und für die Benutzung von ELGA autorisiert. Diese Assertion berechtigt (autorisiert) OBST zum uneingeschränkten Zugang zu den Gesundheitsdaten und individuellen Berechtigungen, sowie Zugriffsprotokollen des Vertretenen.

5.2. ELGA-Zugang von OBST-Portal

Funktionstechnisch unterscheidet sich der OBST-Zugang vom Zugang eines vom e-Government bevollmächtigten Vertreters kaum. Das bedeutet, dass dem berufsmäßigen (OBST) Vertreter die identischen Funktionen wie einem durch das Mandate Issuing Service des e-Government gewillkürten Vertreter zur Verfügung stehen. Darüber hinaus ist zu vermerken, dass wegen der Mächtigkeit eines OBST-Accounts dieser mit zusätzlichen Maßnahmen zu schützen ist. Die Mächtigkeit des Accounts ergibt sich aus der Tatsache, dass - während bei gewillkürten bevollmächtigten Vertretern eine vorherige elektronische Zustimmung des Vertretenen für das Ausstellen eines e-Government Vertretermandates erforderlich ist - im Falle der OBST zur Ausstellung eines Vertretermandates allein das Bestandsgeberzertifikat auf der Chipkarte ausreicht. Eine explizite technische Zustimmung des Vertretenen ist für einen Vollzugriff durch OBST nicht notwendig.

Somit unterscheidet sich grundsätzlich der physische (primäre) Zugang eines OBST-Mitarbeiters zum ELGA-Portal dadurch, dass aus Sicherheitsgründen zusätzliche Zugangseinschränkungen erfüllt werden müssen. Das Wesentliche der zusätzlichen Maßnahmen ist, dass nicht nur die Authentizität der OBST-Mitarbeiter und der OBST bestätigt werden muss, sondern auch die Authentizität des Zugangsgerätes sowie die Einschränkung hinsichtlich der zulässigen IP-Adressen des Zugangsgerätes. Es gibt eine Reihe von Maßnahmen um diese Bedingungen zu erfüllen. Dazu zählt die Authentifizierung der Zugangsgeräte über entsprechend ausgestellte und an den Geräten installierte ELGA Core-PKI Zertifikate, sowie der Zugang über eHiNet/Healix/GovIX.

Weitere diesbezüglichen Details sind in der entsprechenden OBST-Dokumentation [20] nachzulesen.

6. Patientenindex

6.1. Allgemeines

ELGA arbeitet bei der Identifikation von ELGA-Teilnehmern mit einem hierarchischen Konzept. Die ELGA-Bereiche definieren eine, für den Bereich gültige, *Patient Identity Source*, den lokalen Patientenindex (L-PI). Die Patienten Management Systeme der ELGA-GDA melden ihre Daten an den L-PI. Dieser übermittelt wiederum die im Bereich konsolidierten

Identifikationsdaten über „Patient Identity Feed“ an den Zentralen Patientenindex (Z-PI). Die Einmeldung in den Z-PI ist eine Voraussetzung für das Auffinden von ELGA-Dokumenten und muss damit schon vor dem ersten Registrieren eines ELGA-Dokuments erfolgen, da dies eine Voraussetzung für die Ausstellung der Authorization Assertion durch das ETS ist.

Der zentrale Patientenindex stellt wiederum dem ELGA-GDA qualitätsgesicherte demografische Daten aus externen Registern für die Identifikation von ELGA-Teilnehmern (Patienten) bereit. Zu diesem Zweck werden die Daten aus der Zentralen Partner Verwaltung der Sozialversicherung (ZPV) laufend übernommen. Die ZPV erhält ihrerseits wiederum Meldungen der Personenstandsbehörden über Änderungen. Weiters wird im Rahmen der Ausstattung mit bPK (gemäß ELGA-Gesetz §4 Abs. 6) diesen Personen das bPK-GH zugeordnet, sofern ein Matching der Daten erfolgreich ist. Darüber hinaus steht den Benutzern der ZPV Zugriff auf das Stammzahlregister der Republik Österreich (nicht jedoch auf das Ergänzungsregister natürlicher Personen) zur Verfügung, womit im Einzelfall Klärungen bei Abweichungen vorgenommen werden können.

Im zentralen Patientenindex sind somit alle Personen, die von der österreichischen Sozialversicherung erfasst sind, mit ihrer eindeutigen Sozialversicherungsnummer, dem aktuell bekannten Personenstand und dem aktuell bekannten (und damit ggf. unversorgten) bPK vorhanden.

Abbildung 26 zeigt den hierarchischen Aufbau der Z-PI relevanten IHE Transaktionen. Hauptanwendungsfälle sind:

- Die Einmeldung neuer bzw. das Update von vorhandenen ELGA-Teilnehmern mittels *Patient Identity Feed* [ITI-44]-Transaktionen (Secure Node über direkte TLS-Verbindung).
- Die Abfrage von demografischen Daten (*Patient Demographics Query* – PDQ [ITI-47])
  - durch die GDA-Software (nur mit HCP-Assertion) die den *Patient Demographics Consumer* Akteur umsetzt
  - durch L-PI (Secure Node über eine direkte TLS-Verbindung)
- Die PIX-Query [ITI45], die das ELGA-Token-Service zur Lokalisierung der Bereiche benutzt, in denen nach Dokumenten zum Patienten gesucht wird (Secure Node über eine direkte TLS-Verbindung).
  - KBS und PAP sind auch PIX-Consumer, ähnlich wie ETS (KSB wegen Umwandlung L-PID/bPK-GH; PAP wegen Lösch-Aufträge bei Opt-Out Policy)

Zugang und Autorisierung von Z-PI Zugriffen erfolgt ausschließlich über Secure Nodes, die mittels entsprechend ausgestellten Zertifikaten authentifiziert sind. ELGA-Tokens sind nicht erforderlich. Der PIX-Zugang ist ausschließlich zentralen Services (ETS, KBS und PAP)

gestattet. Der PIF-Zugang ist auf den lokalen Patientenindices (L-PI) beschränkt. Ein PIF ist explizit nicht über ELGA-Anbindungsgateway zu führen, da der Z-PI jeden L-PI anhand von ATNA Zertifikaten identifizieren muss. Zu diesem Zweck wird eine Sub-CA in der ELGA Core-PKI eingerichtet.

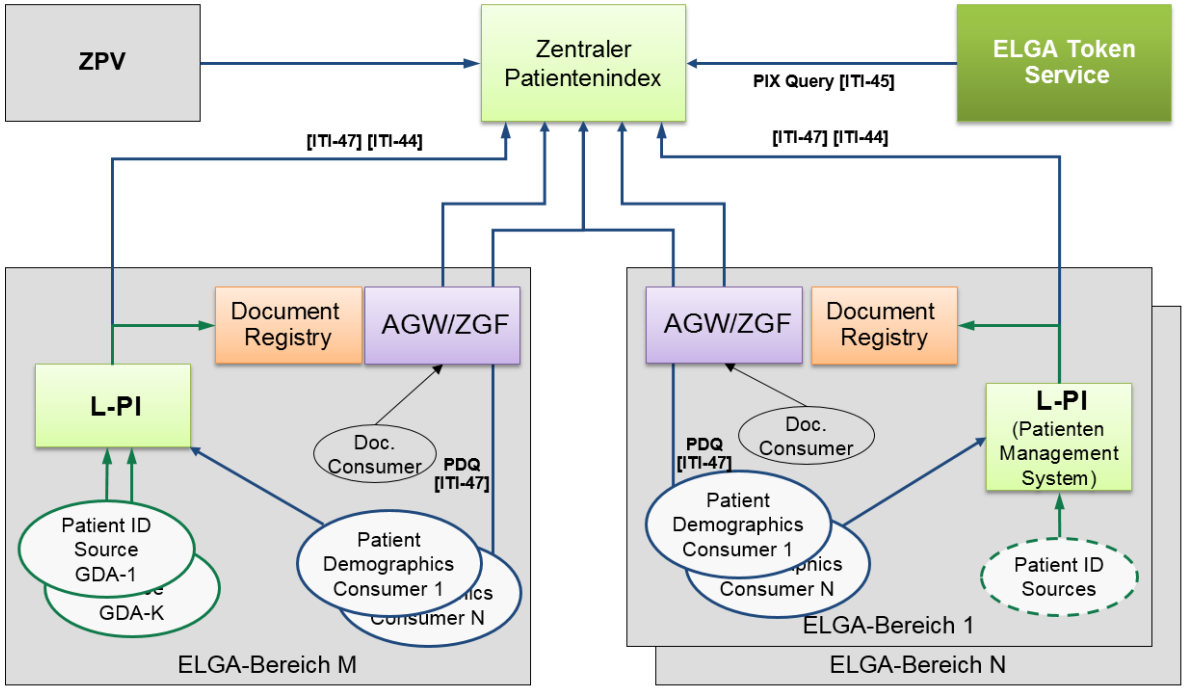


Abbildung 26: Schnittstellenübersicht Patientenindex

6.2. Zentraler Patientenindex

Abbildung 27 zeigt eine Übersicht über den Zentralen Patientenindex (Z-PI) mit seinen Schnittstellen und Daten.

Die schon oben beschriebene Schnittstelle zur ZPV nutzt auf technischer Ebene soweit wie möglich die Business Logik der IHE-Transaktionen. Für bestimmte Operationen, wie z.B. stornieren, werden spezifische Erweiterungen genutzt. Die Erstbefüllung erfolgt aufgrund der großen Datenmenge durch einen Batch-Job, der direkt mit SQL arbeitet.

Der Z-PI speichert alle gemeldeten Daten in einer sender- bzw. bereichsspezifischen Ablage. Es sind somit die zuletzt gemeldeten Daten von jeder Quelle bekannt. Verwendung finden diese für Matching- und Clearing-Mechanismen. Alle Sender, die Daten an den Z-PI melden, müssen ihre ELGA-Teilnehmer mit einem eindeutigen Identifikationsschlüssel, der sogenannten L-PID (local patient identifier, spezifisch je ELGA-Bereich) an den Z-PI melden. Die Einmeldung ist Voraussetzung für das spätere Lokalisieren und Zuordnen von ELGA-

Gesundheitsdaten zu ELGA-Teilnehmern. Personen können auch ohne nachfolgende Registrierung eines ELGA-CDA-Dokuments vom L-PI an den Z-PI gemeldet werden. Dies kann z.B. der effizienten Workflowunterstützung der Patientenadministration im Krankenhaus dienen. Von einer a-priori Meldung von Personen ohne existierenden Behandlungszusammenhang ist jedoch aus Performancegründen abzusehen.

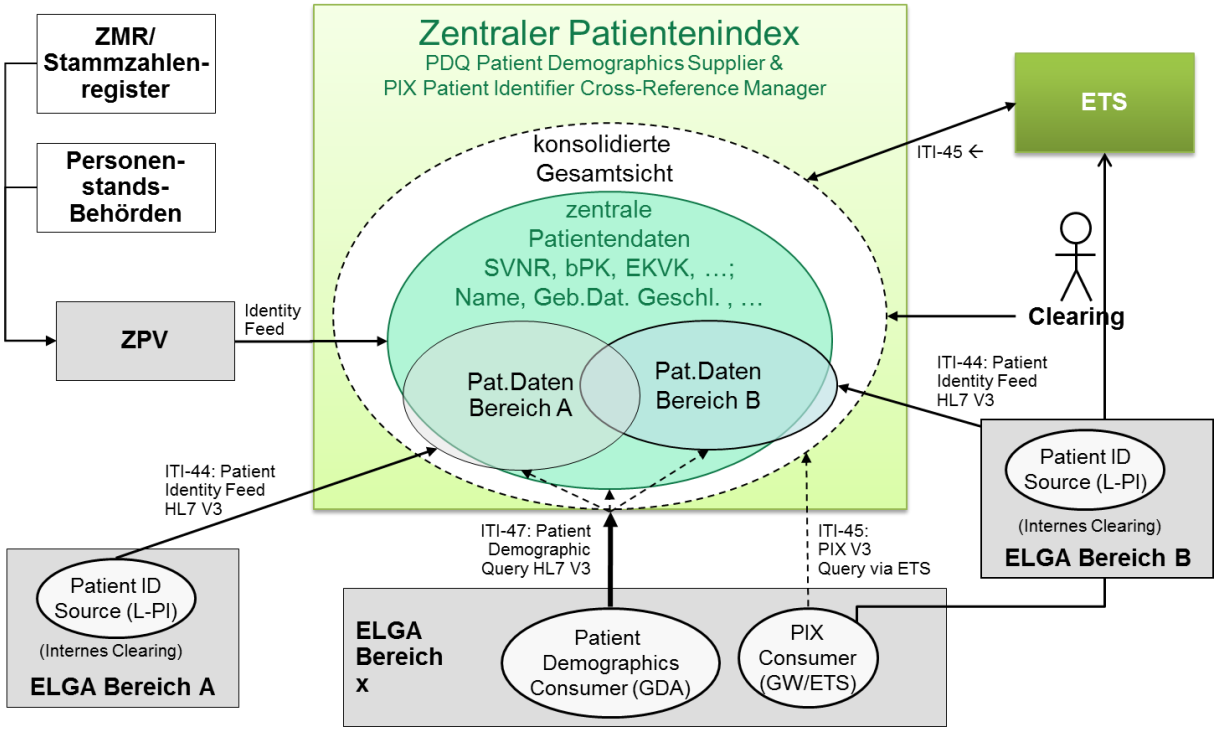


Abbildung 27: Übersicht zentraler Patientenindex

Bei der Einmeldung in den Z-PI müssen neben dem Vorhandensein der L-PID gewisse Mindestkriterien erfüllt sein, um die Qualität der Daten sicherzustellen. Diese umfassen das Vorhandensein von Vorname (außer Neugeborene), Familienname, Geburtsdatum, Geschlecht und eines Fachschlüssels (zurzeit Versicherungsnummer, bPK-GH oder EKVK-Nummer).

Mit Hilfe der *Patient Demographics Query* kann ein ELGA-GDA zu betreuende ELGA-Teilnehmer (via L-PI) im Z-PI suchen und eindeutig identifizieren. Er sucht dabei die Daten in der „konsolidierten Gesamtsicht“ und erhält im Standardfall je Patient einen Datensatz mit den „führenden“ Daten. Die führenden Daten sind jene der ZPV, sofern diese vorhanden sind, und sonst die zuletzt eingemeldeten Daten aus beliebiger Quelle. Das Suchergebnis kann durch Parametrierung der Suche angepasst werden.

Ein ELGA-GDA soll grundsätzlich bei der Aufnahme die PDQ nutzen, wenn der Patient anhand des L-PI nicht identifiziert werden kann oder wenn er im Fall der erfolgreichen Identifikation

anlassbezogen einen Abgleich mit den zentralen Daten durchführen möchte um z.B. zu prüfen, ob die Person als verstorben gekennzeichnet ist.

Um die Patienten-IDs aus unterschiedlichen ELGA-Bereichen einer Person zuordnen zu können, wird bei jedem *Identity Feed* immer ein Identitätsabgleich (Matching) durchgeführt. In eindeutigen Fällen werden die Identifier aus den unterschiedlichen Domänen verlinkt. In Zweifelsfällen erfolgt keine Verlinkung wobei die betroffenen Daten ggf. online oder durch einen Batch Job für ein späteres Clearing markiert werden. Durch Steuerung der Breite des „Graubereichs“ werden Qualität / Aufwand des zentralen Clearings gesteuert.

Die Abfrage, in welchen ELGA-Bereichen medizinische Dokumente eines ELGA-Teilnehmers gesucht werden sollen, erfolgt anhand der bekannten L-PIDs beim Z-PI. Diese beinhaltet die *Assigning Authority,* der ein *Service Endpoint* am Gateway (URL) zugeordnet ist. Die Zuordnung erfolgt durch Konfigurationsdaten im Berechtigungssystem.

Wie im XCA Profil festgelegt, benutzt das *Initiating Gateway* je anzufragender Domain die L-PID der Ziel-Domain zur Identifikation des Patienten im Rahmen der *Cross Gateway Query*. Es erhält diese nicht mit einer direkten PIX-Abfrage sondern in Form der Liste der vom ETS zurückgesendeten (via RSTRC) *ELGA-Treatment-Assertions*. Die PIX-Query wird somit vom ETS initiiert. Diesbezügliche Details (Sequenzdiagramme) sind dem Anhang *Beschreibung der Anwendungsfälle* zu entnehmen bzw. in den nachfolgenden Kapiteln nachzulesen.

Der Z-PI implementiert HL7 V3 Schnittstellen. Dies ist im Einklang mit der generellen serviceorientierten Architektur basierend auf SOAP Web Services. Da zum jetzigen Zeitpunkt die Mehrzahl der von ELGA-GDAs genutzten Systeme jedoch nur HL7 V2 bzw. 2.5 unterstützen, ist eine entsprechende Umsetzung seitens der ELGA-GDA/Systemanbieter vorzunehmen. Dabei müssen die im Integrationsprofil PIXV3 definierten Kompatibilitätsregeln zwischen HL7 V2 und V3 Berücksichtigung finden.

Bezüglich des Aufbaus von Identifikatoren (HL7 Data Type CX / V3) sind in ITI TF Vol. 2a, Appendix N.1 „CX Datatype“ bzw. im Integrationsprofil PIXV3, Kap. 2.5 und Appendix R Details beschrieben. In HL7 V3 hat die PID den Datentyp *Instance Identifier.* Sie besteht aus den Komponenten *root* und *extension* wobei *root* eine *OID* für die *Assigning Authority* ist und die *extension* der eigentliche Identifikator.

Fachliche Identifikatoren, wie z.B. eine Sozialversicherungsnummer oder die Nummer der Europäischen Krankenversicherungskarte werden ebenfalls als Identifikatoren im Z-PI gespeichert und gemäß PIX Profil an Service Consumer übermittelt. Die fachlichen Identifikatoren müssen bei einem Feed mitgegeben werden um ein eindeutiges Matching zu unterstützen.

Das bPK-GH wird vom Z-PI im Wesentlichen zur Unterstützung des Logins am Portal geführt. Eine dezentrale Verwendung ist nicht zwingend erforderlich. Damit können berechtigte Benutzer jedenfalls eine Abfrage mit dem bPK-GH durchführen.

Anmerkung: Die aktuelle Version des Z-PI/PDQ liefert das bPK-GH nur an das ELGA Portal, die uneingeschränkte Verwendungsmöglichkeit für Berechtigte wird bis zum Go Live von ELGA beabsichtigt.

Das Bild sieht auch eine Komponente vor, die das im Zentralen Patientenindex erforderliche Clearing durchführt. Für diese wird eine adäquate Benutzerschnittstelle (Web-GUI) bereitgestellt. Die Clearingaufgabe im Z-PI beschränkt sich auf das Feststellen von Clearingfällen und die Einleitung von Korrekturmaßnahmen. Die Korrektur von Daten erfolgt immer durch die zuständigen Quellen (d.h. ELGA-Bereiche bzw. ZPV), da der Z-PI nicht die Aufgabe bzw. das Recht hat, die gemeldeten Daten zu verändern.

Weiters beinhaltet der Z-PI Mechanismen zur Fehlererkennung und Fehlerbehandlung. So wird z.B. erkannt, wenn ein ELGA-Bereich unterschiedliche L-PIDs mit der gleichen SV-Nummer speichern möchte oder wenn eine Transaktion zentral Patienten zusammenführen würde, denen unterschiedliche SV-Nummern zugeordnet sind. Der Algorithmus ist so gestaltet, dass dieser bei korrekter dezentraler Dateneingabe ohne manuelle Eingriffe von zentraler Seite für Konsistenz sorgt. Folgende Vorgangsweise ist implementiert:

- Eine *Identity Feed* Transaktion führt zu einem neuen Matching-Vorgang sofern relevante Daten geändert wurden.
- Die Verlinkung der Identifier wird so angepasst, dass sie dem Ergebnis des letzten Matching-Vorgangs entspricht.
- Der Matching-Algorithmus ist so konzipiert, dass erkennbare Inkonsistenzen jedenfalls dazu führen, dass keine Verlinkung erfolgt bzw. der Feed abgewiesen wird.

6.3. Patientenindex der ELGA-Bereiche

Für die ELGA-Bereiche stellt der lokale Patientenindex (L-PI) die Quelle für den eindeutigen Identifikator eines Patienten in der XDS Affinity Domain dar. Dieser wird im IHE-Profil mit „Domain Patient ID“ der XDS Affinity Domain (XAD-PID) bezeichnet, während im vorliegenden Papier die Umsetzung der XAD-PID in ELGA mit L-PID bezeichnet wird.

Laut IHE Patient Identification Management darf die XDS Registry nur Dokumente annehmen, die einer bekannten XAD-PID zugeordnet sind. Es ist daher die Aufgabe des L-PI, diese XAD-PID, d.h. L-PID, zu vergeben.

Die lokalen Systeme der ELGA-GDA bedienen sich des lokalen Patientenindex (L-PI), um die XAD-PID zu ermitteln. Dabei wird von der Registry eines ELGA-Bereichs die lokale PID (auch GDA-PID) in den L-PI eingemeldet [ITI-44] bzw. die zugehörige XAD-PID mit einer PIX-Query

[ITI-45] abgefragt. Das ELGA-CDA-Dokument für diesen Patienten wird mit der zuvor abgefragten XAD-PID registriert [ITI-41]. Zusätzlich wird in den Metadaten die GDA-PID im Attribut „sourcePatientId“ mitgegeben.

Die obigen Absätze erläutern die Beschreibungen in den IHE-Profilen zum Management der Patienten Identifier. Sie stellen jedoch keine Festlegung für die interne Arbeitsweise von ELGA-Bereichen dar. Wesentlich ist nur, dass sich die Software des ELGA-Bereichs an den Schnittstellen wie gefordert verhält. Insbesondere wird der ELGA-Bereich nicht gezwungen, eine permanent gültige L-PID zu pflegen. Die L-PID wird von der Architektur nur temporär verwendet. D.h. im Rahmen einer Dokumenten-Abfrage werden die L-PIDs eines Patienten am Z-PI erneut abgefragt. Durch Clearing-Fälle geänderte L-PIDs müssen daher aber grundsätzlich dem Z-PI kommuniziert werden. Auch die Möglichkeit der Stornierung von Patienten-Identitäten ist im Z-PI implementiert.

L-PI in jenen ELGA-Bereichen, die auch niedergelassene GDA anzubinden beabsichtigen, müssen dem Z-PI idente IHE konforme Schnittstellen für die Kommunikation mit den angebundenen GDA anbieten. Die Autorisierung erfolgt via ELGA-HCP-Assertion und wird über die AGW/ZGF geführt.

6.4. Zugriffsautorisierung und Zugangseinschränkungen

Ein direkter Zugang zu Z-PI Schnittstellen wird ausschließlich aufgrund ATNA Secure Nodes gewährt. Zertifikate für berechtigte Akteure sind ausschließlich vom ELGA Core-PKI zu beziehen. Darüber hinaus ist es netzwerktechnisch nicht erforderlich, Anfragen der Akteure über einen ELGA-Anbindungsgateway zu führen (auch wenn dies in manchen Fällen nicht verboten ist – siehe weiter unten). Zusätzliche Zugangseinschränkungen hinsichtlich der einzelnen Z-PI relevanten IHE-Transaktionen sind wie folgt definiert:

6.4.1. Patient Demographics Query

Laut Gesetzesvorgabe sind alle GDA, also auch nicht-ELGA-GDA, berechtigt, demographische Suchanfragen (PDQ) an den Z-PI zu stellen. Zugriffsberechtigte Akteure müssen über vorkonfigurierte ATNA Secure Node Zertifikate authentifiziert werden. Zugriffe für ELGA-GDA sind grundsätzlich nur über ELGA-Anbindungsgateways erlaubt. Hierfür sind zwei Anwendungsfälle zu unterscheiden:

- Zugriffe auf den Z-PI durch ELGA-GDA, die in ELGA angemeldet sind. Diese Zugriffe sind verpflichtet eine gültige HCP-Assertion der Anfrage beizufügen. Der Z-PI prüft die HCP-Assertion, protokolliert den Zugriff einschließlich zugreifenden GDA im IHE Audit-Trail und erzeugt daraus bei Bedarf eine Auskunft gemäß DSG 2000.
- GDA, die nicht im GDA-Index geführt werden (diese sind keine ELGA-GDA). Diese Akteure sind verpflichtet den Zugang mit dem Z-PI Betreiber auszumachen.

Für beide Zugriffe sieht der Z-PI eine standardisierte Basislösung aufgrund ATNA Secure-Nodes vor. Alle berechtigten Systeme müssen gemäß den Vorgaben des Integrationsprofils ATNA entsprechende Zertifikate vorweisen. Der Z-PI führt eine oder mehrere Listen der vertrauenswürdigen und zugelassenen Secure-Nodes. Aufbauend auf Secure-Nodes kann Z-PI zusätzliche Anforderungen (wie HCP-Assertion, siehe oben) stellen.

Die Antwort auf eine PDQ-Anfrage liefert primär qualitätsgesicherte demographische Informationen über ELGA-Teilnehmern. Das IHE-Profil sieht vor, dass auch die Identifikatoren der Patienten in der PDQ-Antwort übermittelt werden, wobei in der Anfrage festgelegt werden kann, welche Domänen der Consumer benötigt. Sind keine Domänen festgelegt, so sollen laut IHE-Profil alle bekannten Identifier übermittelt werden.

Da das Vorhandensein einer L-PID zumindest einen Hinweis darstellt, dass der ELGA-Teilnehmer mit dem ELGA-Bereich „in Berührung“ gekommen ist, muss aus Sicht der Architektur die PDQ-Antwort speziell für die Anwendung in ELGA so eingeschränkt werden, dass keine L-PIDs übergeben werden.

6.4.2. Patient Identity Feed - PIF

PIF-Zugriffe sind ausschließlich den L-PI Akteuren in den einzelnen ELGA-Bereichen gestattet, welche durch vorkonfigurierte ATNA Secure Node Zertifikate authentifiziert werden. PIF-Zugriffe (an Z-PI) sind nicht über ELGA-Anbindungsgateways zu führen. Das ELGA-Berechtigungssystem kommt hierbei nicht zum Einsatz und die Transaktion findet nicht im ELGA-Core statt. Entsprechende Bedrohungs-Szenarien sind aus Perspektive der allgemeinen Sicherheit zu betrachten. Beispiel: Wenn einem Server auf Basis eines vorgelegten Server-Zertifikates vertraut wird, müssen mögliche Kompromittierungsszenarien eines System-Administrators, der sich an diesem Server anmeldet und den Computer als Backdoor für gerichtete Attacken nutzen möchte (etwa um den Z-PI zu kompromittieren), identifiziert und bewertet werden.

6.4.3. Patient Identifier Cross Reference Query – PIX-Query

PIX wird ausschließlich dem ETS aufgrund vorkonfiguriertem ATNA Secure Node Zertifikate erlaubt. PIX-Zugriffe sind nicht über ELGA-Anbindungsgateways zu führen. Es ist nicht vorgesehen, dass GDA-Systeme bzw. ELGA-Benutzer innerhalb von ELGA direkt PIX-Anfragen an den Z-PI initiieren, da dies datenschutzrechtlichen Vorgaben widerspricht. Ohne die vom Patienten definierten individuellen Berechtigungen abzufragen, dürfen keinerlei Hinweise betreffend der Existenz von ELGA-Gesundheitsdaten eines Patienten an den ELGA-GDA übermittelt werden. PIX-Anfragen werden nur von ELGA-Token Service (ETS) zugelassen.

Das ETS erstellt PIX-Anfragen im Rahmen der Zugriffsautorisierung. Das Resultat der PIX-Anfrage wird in Form von *ELGA-Authorisation-Assertions* strukturiert und lediglich an

Komponenten des Berechtigungssystems retourniert. Das Wissen über ELGA-Bereiche, die zumindest Identifikatoren eines ELGA-Teilnehmers nutzen und potentiell ELGA-Gesundheitsdaten zur Verfügung stellen, verbleibt somit innerhalb des ELGA-Berechtigungssystems und wird zu keinem Zeitpunkt an GDA-Systeme übermittelt.

7. GDA-Index

7.1. Allgemeines

Der Gesundheitsdiensteanbieter-Index (GDA-I) führt die an ELGA teilnehmenden GDA mit deren Organisationseinheiten und Rollen auf. Jeder ELGA-GDA ist im GDA-I eingetragen. Weiterführende Informationen sind dem Servicehandbuch des GDA-I [17] zu entnehmen.

Für den GDA-Index gelten folgende Aussagen:

- Ein GDA kann nur dann an ELGA als ELGA-GDA teilnehmen, wenn er im GDA-I eingetragen ist.
- Der GDA-I ist aus Sicht von ELGA die verbindliche zentrale Quelle der Rollen, die flexibel erweiterbar ist.
- Der GDA-I bietet historisierte Informationen auch über GDA, die nicht mehr im aktiven Status sind. Aufbewahrung dauerhaft inaktiver GDAs erfolgt max. drei Jahre.

Für einen ELGA-GDA liefert der GDA-I im Wesentlichen folgende Daten:

- Eine eindeutige Identifikation der ELGA-GDA entweder als öffentliche OID vom entsprechenden OID-Zweig.
- Die ELGA-Rolle des ELGA-GDAs. Anhand dieser Information wird die Berechtigung zum Datenzugriff geprüft bzw. ein Datenzugriff autorisiert.
- Die Angabe ob der gegebene ELGA-GDA eine Organisation ist.
- Name bzw. Bezeichnung (Freitext).
- Standorts- (bzw. Ordinations-) Adresse
- Wenn der gegebene ELGA-GDA eine physische Person ist
  - muss die GDA Organisation angeführt werden.
  - muss die entsprechende Fachrichtung des ELGA-GDA angeführt werden (unterstützend für Suchanfragen am ELGA-Portal)

Es wird zwischen amtlich bestätigten Daten (Zulassungsaufgabe) und informativen Daten unterschieden. Bestätigt sind Identifier, Rollen und Name.

Der GDA-I ist für ELGA die verbindliche Quelle für den Zusammenschluss der verwendeten Identitäten (*Identity Federation*). So wird z.B. die Verbindung der OID zur Vertragspartnernummer, die durch die Sozialversicherung vergeben wird, dort abgebildet. Dies gilt für alle in ELGA zugelassenen Identity Provider.

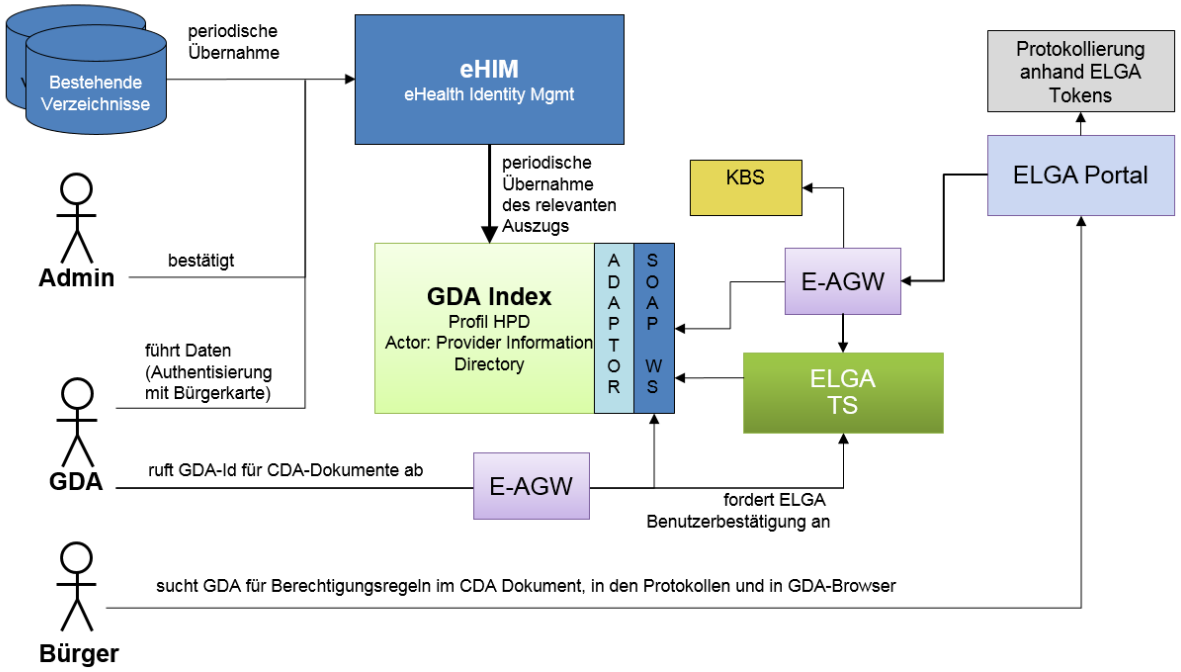


Abbildung 28: Übersicht GDA-Index

Abbildung 28 zeigt die Einbindung des GDA-I in ELGA mit den wesentlichen Datenflüssen zwischen den Komponenten. Die Bestandgeber liefern die Daten aus bestehenden Verzeichnissen an das sogenannte eHealth Identity Management (eHIM). Dieses übernimmt die Daten, prüft diese und überführt sie in den GDA-I.

Es ist nicht vorgesehen, dass der GDA-I die IHE Transaktion *Provider Information Query* [ITI-58] implementiert. Diese IHE Query ist nicht SOA-freundlich (*Service Oriented Architecture*) weil sie voraussetzt, dass alle abfragenden Consumer die Details der internen Struktur des Directorys kennen, welche durch das HPD-Schema vorgegeben wird (Healthcare Provider Directory). Nachdem Schema-Abweichungen zwischen IHE Vorgaben und tatsächlichen Implementierung nicht komplett ausgeschlossen werden konnten, mussten HPD-Schema basierende Aufrufe ausgeschlossen werden. Um eine möglichst hohe Unabhängigkeit von HPD-Schema und internen GDA-I Implementierungsdetails zu erreichen, wurde eine ELGA-spezifische WS-Schnittstelle (Kontrakt) ausgearbeitet.

7.2. GDA-Index Web Service Schnittstelle

Die primäre Aufgabe der Schnittstelle ist es im OID-Baum gelistete GDA Organisationen (OID:1.2.40.0.34.3.1) und GDA Personen (OID:1.2.40.0.34.3.2) als ELGA-Zulässige zu qualifizieren. Mit Aufruf von `GetGdaDescriptors()` antwortet der GDA-Index mit einer `GdaDescriptor` Struktur, welche Einzelheiten zum abgefragten GDA enthält (siehe Tabelle 14). Es wird zwischen Organisationen und physischen Personen (Ärzte) via booleschen `IsOrganisation` Feld unterschieden. Darüber hinaus ist der Datenbestand im GDA-I historisiert. Aktive und für ELGA zugelassene GDA sind explizit via `IsActive` vermerkt. Wenn hier FALSE angeführt ist, dann ist der GDA für ELGA-Zugriffe nicht autorisiert. Solche GDA sind bloß aus historischen Gründen geführt, um das Auflösen von etwaigen Identifier (z.B. in der Kontaktbestätigung) zu ermöglichen.

Die sekundäre Aufgabe der Schnittstelle ist es, diverses Suchen im GDA-I zu ermöglichen. Das Suchen ist in einem KIS notwendig, um Kontakt-Delegation durchführen zu können.

```
// für ETS
GDAIndexResponse GetGdaDescriptors(InstanceIdentifier)

// für GDA und KIS-Systeme (Suche Zwecks Kontakt-Delegation)
GDAIndexResponse GdaIndexSuche (GdaDescriptor)

// für das Portal (EBP Zwecks Auflösung von OID)
List GDAIndexResponse GdaIndexListenSuche (List InstanceIdentifier)


Class InstanceIdentifier
{
      String   IssuingAuthority;  // Wertvergebende Instanz (O)
      String   Id;                // Wert/Identifier (R)
      String   Description;          // Beschreibung im Klartext (O)
}

Class GdaDescriptor
{
      InstanceIdentifier GdaId          // GDA-ID (R)
      String             DisplayName    // Bezeichnung oder Name (R)
      String             SureName       // Nachname wenn Person (O)
      String             Title          // Titel wenn Person (O)
      GdaAddress         Address           // Adresse/Strukturiert (O)
      Bool               IsOrganisation; // Wenn Person „FALSE“ (R)
      Bool               IsActive;         // GDA ist aktiv „TRUE“ (R)
      List<InstanceIdentifier> ElgaRoles; // ELGA_GDA_Aggregatrollen (R)
      List<InstanceIdentifier> Disciplines;  // Fachrichtung (R)

}

Class GDAIndexResponse

{
      GdaDescriptor           Gda           // GDA Beschreibung (R)
      List<GdaDescriptor>     LinkedGda;    // Verlinkte GDA (O)
}
```

Tabelle 14: GDA-I Web Service Definition. Die tatsächliche Schnittstelle kann von diesem Originalentwurf aufgrund diverser Optimierungen abweichen und ist dem GDA-Index Servicehandbuch [17] zu entnehmen. O == optional, R == required/verpflichtend

Eine interne Variante des SOAP-Requests `GetGdaDescriptors_Active()` wird nur vom ETS verwendet (liefert nur aktive GDA mit Status IsActive=TRUE), um auf dessen Basis der im GDA-I strukturierten Identitäts- und Rolleninformationen von **ELGA**-GDA abzufragen. Die allgemeine `GetGdaDescriptors()` Anfrage steht hingegen auch für sonstige Konsumenten (GDA, KIS-Systeme) zur Verfügung. Damit werden berechtigte ELGA-GDA identifiziert und die für die identifizierten ELGA-GDA erlaubten ELGA-Rollen abgeholt.

Der SOAP-Request `GdaIndexSuche()` ist für GDA/KIS-Systeme bestimmt. Mit dieser Schnittstelle werden nach Such- und Filterkriterien bestimmte ELGA-GDA gezielt gesucht. Beispielsweise können Name und/oder Adresse und/oder Rolle bzw. Fachrichtung (entsprechend der Codelisten *ELGA_GDA_Aggregatrollen*, bzw. künftig auch *ELGA_Fachärzte* oder *ELGA_GTelVoGDARollen*) des gesuchten GDA angegeben werden. Die Antwort des GDA-I enthält eine Liste der zutreffenden GDA. Der Aufruf ist von KIS und diverser Arztsoftware zu verwenden um jenen GDA zu identifizieren, an den eine Kontaktbestätigung weitergereicht (delegiert) werden soll.

Der SOAP-Request `GdaIndexListenSuche()` ist für das Portal bestimmt. Damit werden Informationen (z.B. Identifier in Kontaktbestätigungen) dem ELGA-Teilnehmer aufgelöst.

Die Klasse `GdaDescriptor` beinhaltet eine Ansammlung von möglichen Informationen die der GDA-I für einen bestimmten GDA liefern kann. Die Schnittstellen antworten entweder mit einer Instanz der `GDAIndexResponse` Struktur oder mit einer Liste bestehend aus mehreren `GDAIndexResponse` Instanzen. Die geschachtelte Liste (`LinkedGda`) ist für GDA-Personen von Bedeutung (Authentifiziert via Bürgerkarte und bPK-GH) und kann die Liste von verlinkten GDA-Organisationen (OID) enthalten.

7.3. Zugriffsautorisierung und Zugangseinschränkungen

Ein direkter Zugang zu GDA-I Schnittstellen wird ausschließlich aufgrund ATNA Secure Nodes gewährt. Zertifikate für berechtigte Akteure sind ausschließlich von der ELGA Core-PKI zu beziehen. Dieses Web-Service verlangt keine Autorisierung über ELGA-Tokens. Zusätzliche Zugangseinschränkungen hinsichtlich der einzelnen GDA-I relevante Schnittstellenaufrufe sind wie folgt definiert

- *GetGdaDescriptors()* Aufrufe sind ausschließlich dem ETS erlaubt. Hierfür authentifiziert sich das ETS gegenüber GDA-I via ATNA Secure Node Zertifikat. Diese Schnittstelle liefert ausschließlich aktive ELGA-GDA
- *GdaIndexListenSuche()* Aufrufe sind ausschließlich dem Portal erlaubt. Hierfür authentifiziert sich das entsprechende AGW des Portals gegenüber dem GDA-I via ATNA

Secure Node Zertifikat. Diese Schnittstelle liefert sowohl aktive wie auch inaktive ELGA-GDA

- *GdaIndexPersonenSuche()* Aufrufe sind dem GDA (für das Delegieren von Kontakte an ausgewählte GDA) erlaubt. Hierfür authentifizieren sich die entsprechenden AGW der ELGA-Bereiche gegenüber dem GDA-I via ATNA Secure Node Zertifikate. Diese Schnittstelle liefert sowohl aktive wie auch inaktive ELGA-GDA

8. ELGA-Verweisregister und Dokumentenaustausch

8.1. Allgemeines

Dieses Kapitel beschreibt die Veröffentlichung bzw. Registrierung, Suche und Abruf von ELGA-Gesundheitsdaten in Form von ELGA-CDA-Dokumenten, ohne dabei auf die exakte Funktionalität des Berechtigungssystems einzugehen, auch wenn dieses nicht komplett außer Acht gelassen werden kann. Prinzipiell werden Konzepte der Integrationsprofile XDS, XDS-I und XCA bzw. XCA-I genutzt. Es werden folgende Konzepte betrachtet:

- XDS: Document Source, Document Repository, Document Registry, XDS SubmissionSet, XDS DocumentEntry und Document Consumer
- XCA: Initiating Gateway, Responding Gateway
- XDS-I: zusätzlich zu XDS: Imaging Document Source, Imaging Document Consumer
- XCA-I: Initiating Imaging Gateway, Responding Imaging Gateway

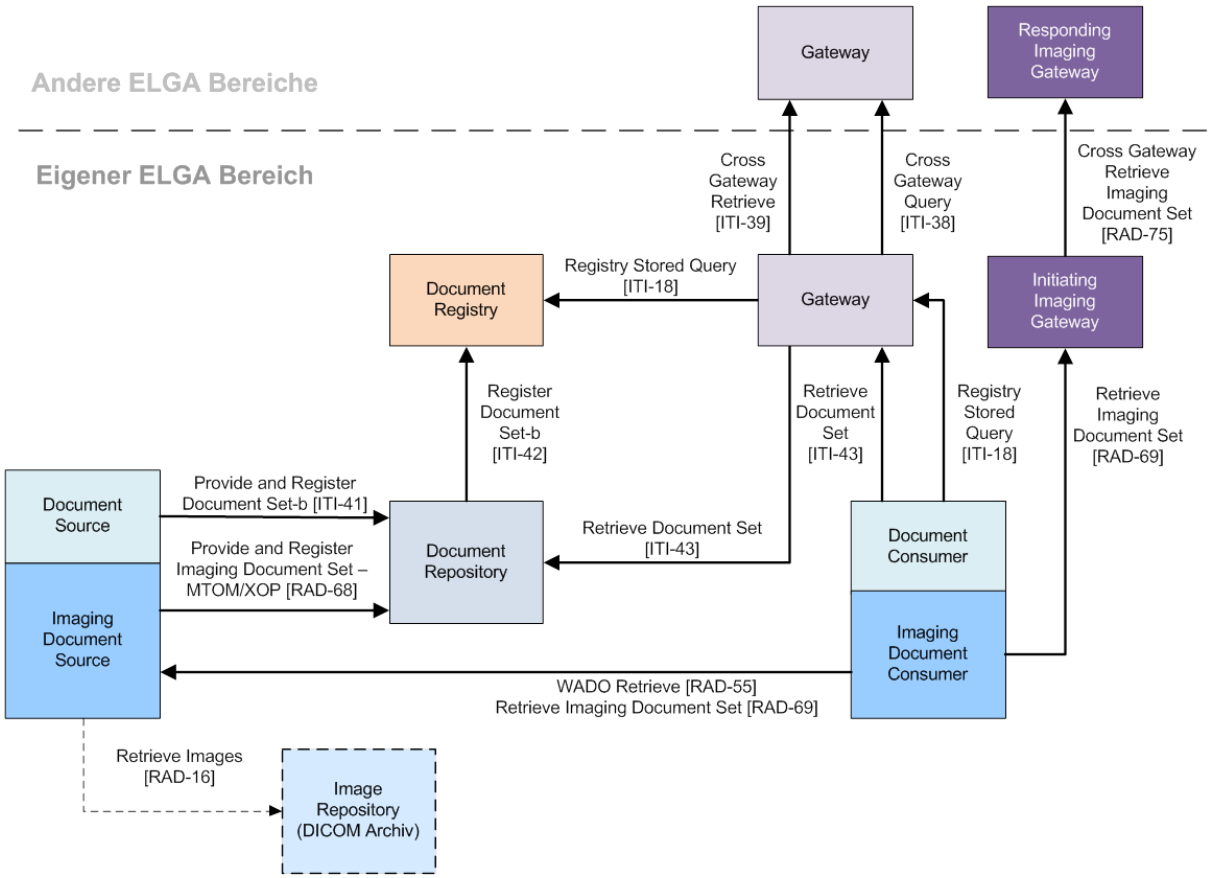


Abbildung 29: Übersicht Dokumentenaustausch (für Variante A, ITI-57 nicht eingezeichnet, bezüglich XDS-I & XCA-I siehe auch die Liste der offenen Punkte im Kapitel 16.1)

Die Abbildung 29 zeigt die im Rahmen von ELGA genutzten IHE Transaktionen ohne Autorisierung.

Hinsichtlich der in ELGA zu verwendenden Dokumentenformate gilt folgendes:

- CDA Level 1: mit eingebetteten PDF oder Text Dateien (XML-Tag: <nonXmlBody>).
- CDA Level 2 und 3: ggf. mit beigelegten, referenzierten Multimediadateien (XML-Tag: <renderMultiMedia>)
- DICOM. Hier wird im Rahmen des XDS-I Profils die Option *Set of DICOM Instances* unterstützt. Im Rahmen der Transaktion [RAD-68] *Provide and Register Imaging Document Set* wird ein *Key Object Selection* (KOS-) Objekt im Repository hinterlegt und registriert. Der Abruf der eigentlichen DICOM-Objekte muss zumindest über [RAD-69] *Retrieve Imaging Document Set* ermöglicht/unterstützt werden. Weitere Zugriffsmöglichkeiten wie WADO-URL oder WADO-RS sind in [23] detailliert dargestellt.
- Das Dokument *Allgemeiner Implementierungsleitfaden für ELGA-CDA-Dokumente* [8] beschreibt detailliert die allgemeinen Regeln für die Verwendung des CDA-Standards im Rahmen der ELGA-CDA-Dokumente.

- Das Dokument *XDS-Metadaten zur Registrierung der CDA-Dokumente* [7] spezifiziert das XDS DocumentEntry (Metadaten des Dokuments) für die Registrierung eines CDA Dokuments in der ELGA-Infrastruktur. Bezüglich XDS DocumentEntry erfolgt die Festlegung, dass diese großteils aus dem CDA-Dokument abzuleiten sind. Weiters werden Details betreffend die unterschiedlichen unterstützen Dokumentenformate erläutert. Die Strukturierung weiterer (administrativer) Informationen mittels XDS Folder ist nicht vorgesehen und wird daher nicht unterstützt.

Im Folgenden werden Festlegungen mit Implikationen auf die ELGA-Architektur hervorgehoben:

- Eindeutige Identifier (bestehend aus *Root* bzw. *Root* + *Extension*) für Dokumente (CDA Element ClinicalDocument/id. XDS DocumentEntry: uniqueId) sind wesentlich, um konsistente Referenzen zu erzeugen, z.B. innerhalb von Berechtigungsregeln. Der *Root*-Identifier für Dokumente ist eine OID, die von der Document Source vergeben werden muss. Hierfür bietet sich der OID des GDA oder des eigenen Bereiches an (sog. Home-Community ID). Zu beachten ist, dass beim Ersetzen von Dokumenten (XDS Option: „Document Replacement“) ein neuer Identifier vergeben wird.

- Die *setId* bezeichnet das Set aller Versionen eines Dokumentes. Sie bleibt über alle Versionen der Dokumente konstant (initialer Wert bleibt erhalten). Um eine eindeutige Identifikation aller Dokumente eines Dokumentenstammes (vorhergehende und auch zukünftige Versionen) innerhalb der XDS DocumentEntry Objekte zu ermöglichen, ist die Verwendung eines gemeinsamen Identifikators in den Metadaten notwendig. Das *referenceIdList* Element stellt eine solche Liste von internen oder externen Identifiern dar. Im Rahmen von ELGA ist die ClinicalDocument/SetId als ein Eintrag in der *referenceIdList* in den XDS DocumentEntry Objekten einzubringen. Weitere andere Einträge in der *referenceIdList* sind möglich aber derzeit nicht Bestandteil der ELGA Vorgaben.

- Durch die Verwendung von XCA ist in allen Referenzen auf ein Dokument auch die homeCommunityId, also der eindeutige Identifier eines ELGA-Bereichs in dem das Dokument registriert ist, enthalten.

- Die XDS-Registry stellt sicher, dass neue Versionen eines medizinischen Dokuments ausschließlich von jenem ELGA-GDA veröffentlich werden dürfen, der das ursprüngliche Dokument registriert hat.

8.2. Erweiterung von Metadaten im ELGA-Verweisregister (XDS-Registry)

Eine XDS-Registry kann grundsätzlich sowohl ELGA relevante als auch sonstige Metadaten enthalten. Um ELGA relevante Dokumente zu kennzeichnen, muss die Registry zwei proprietäre ELGA-Metadaten implementieren:

- **ELGA-Flag** ist ein boolescher Wert. Auf TRUE gesetzt, kennzeichnet dieser ein in ELGA veröffentlichtes Dokument
- **ELGA-Hash** (siehe auch Kapitel 9.1.4) auch als Prüfsumme genannt, ist ein einfacher Hashwert über ausgewählte Metadaten, welche das Berechtigungssystem (BeS) berechnet. Der Hashwert dient dazu **versehentliche** Manipulationen von ELGA relevanten Daten klar zu erkennen.

Folgende Metadaten werden in die Prüfsumme (ELGA-Hashwert) einbezogen. Die Reihenfolge, sowie der verwendete Hash-Algorithmus werden vom Berechtigungssystem (BeS) bestimmt:

1. Patienten-ID
2. Document Unique ID
3. Document Creation Date
4. Document-Hash
5. Document Class-Code
6. Document Status (approved, deprecated)
7. referenceIdList (von der Liste nur Document-setId heranzuziehen)
8. ELGA-Flag (in der Standardvariante immer TRUE)

Der ELGA-Hashwert ist in der ersten Ausbauphase nicht als kryptografischer Schutz gegenüber bewusstem Missbrauch bzw. Attacken zu verstehen, sondern als Hilfsmittel unbeabsichtigten oder unrechtmäßigen Änderungen vorzubeugen. Solche unbeabsichtigten Änderungen könnten etwa durch eigene interne Geschäftslogik von nicht koordiniert eingesetzten e-Health-Applikationen entstehen. In einer späteren Ausbauphase muss jedoch in Betracht gezogen werden diesen Hashwert auch entsprechend kryptografisch zu sichern. Die Entscheidung, ob und wann diese Maßnahme zu ergreifen ist, liegt bei den Betriebsführungsgremien und den Sicherheitsadministratoren.

8.3. Verwendung interner Repositories in ELGA

Die ELGA GmbH empfiehlt, einen ELGA-Bereich als eine logisch/physisch getrennte Infrastruktur/ Instanz zu betreiben (siehe Kapitel 3.9.6, entspricht Variante A). Insbesondere

muss entweder ein logisch (Flagging, Variante C) oder ein physisch getrenntes, eigenes ELGA-Verweisregisters für ELGA-CDA-Dokumente zum Einsatz kommen (realisiert via Variante A), weil erst dadurch die Trennung zwischen ELGA- und non-ELGA-CDA-Dokumenten deutlich und nachvollziehbar wird. Weitere diesbezüglichen Konfigurationsdetails werden im Kapitel 9.1.4 ausführlich beschrieben.

Unabhängig vom Aufbau eines ELGA-Bereichs ist jedenfalls sicherzustellen, dass bei einem Zugriff im Kontext von ELGA ausschließlich jene Dokumente übermittelt werden, für die der ELGA-Benutzer durch das ELGA-Berechtigungssystem autorisiert wurde. Für den internen Zugriff (z.B. innerhalb eines KA-Verbundes) muss ebenfalls sichergestellt werden, dass genau jene Dokumente sichtbar sind, die aufgrund des internen Zugriffsschutzes sichtbar sein dürfen.

Abbildung 30 zeigt ein Beispiel für die Trennung des lesenden Zugriffs auf ELGA-CDA-Dokumente vom Zugriff auf interne Dokumente. Diese Abbildung geht davon aus, dass im ELGA-Bereich eine selbständige ELGA-Registry und ein selbständiges ELGA-Repository errichtet wurden (entspricht Variante A, siehe Kapitel 9.1.4). Die Pfade für den Zugriff im Kontext von ELGA sind schwarz dargestellt. ELGA liefert die gewünschte Auswahl aus der bereichsübergreifenden Gesamtsicht entsprechend den Zugriffsberechtigungen des anfragenden ELGA-GDAs, d.h. die Zugriffsautorisierung erfolgt durch die Zugriffssteuerungsfassade des ELGA-Berechtigungssystems. Der interne Zugriff ist getrennt davon zu betrachten und bezieht sich ausschließlich auf Dokumente innerhalb des Trägers. Soll im XDS Document Consumer eine Gesamtsicht auf interne und ELGA-Dokumente dargestellt werden, so müssen 2 Abfragen durchgeführt und die Treffermengen vereinigt werden.

Der *Policy Enforcement Point* (PEP) ist für die Durchsetzung der Berechtigungsregeln verantwortlich. Für den ELGA-Zugriff ist er Teil der Zugriffssteuerungsfassade. Für den internen Zugriff ist ein eigener PEP zu verwenden.

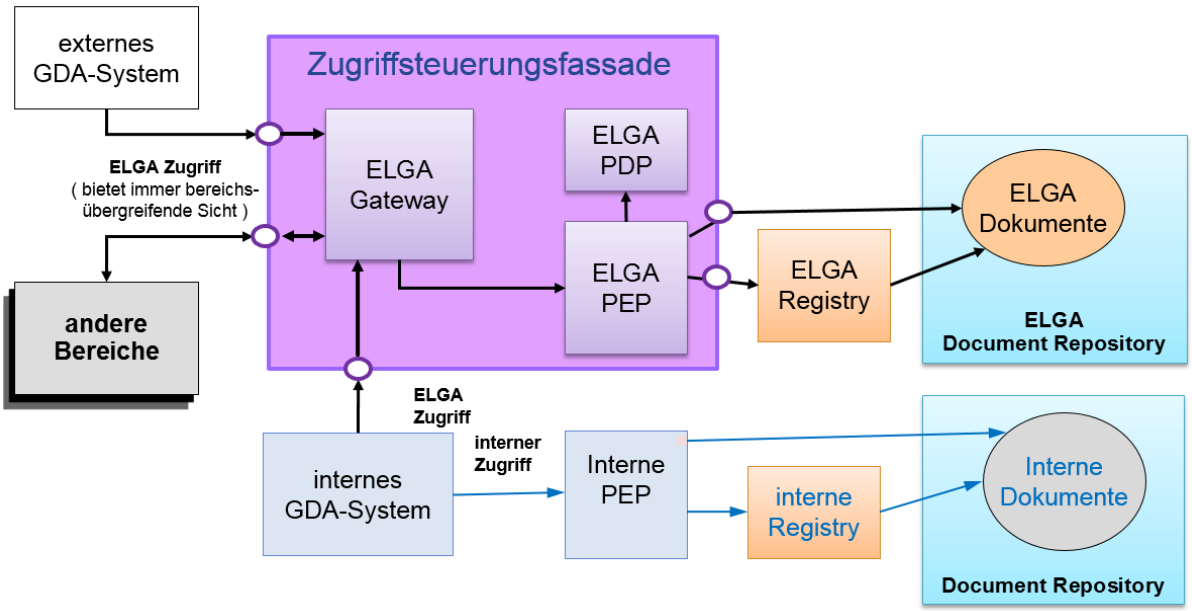


Abbildung 30: Trennung von Zugriff auf ELGA von interner PEP

8.4. Anforderungen an ein ELGA-Anbindungsgateway und ELGA XCA-Gateway

In ELGA wird das Konzept eines IHE XCA Gateways als ELGA-XCA-Gateway realisiert. Ein ELGA-XCA-Gateway stellt eine entscheidende Komponente für die Performanz und Qualität der Kommunikation in ELGA dar. Ein ELGA-XCA-Gateway ist immer in Verbindung mit einer vorgeschalteten Zugriffsteuerung zu betrachten (Abbildung 31). Diese beiden Komponenten werden in Form einer ZGF vereint und ausgeliefert.

Vor allem sind ELGA-XCA-Gateways im Sinne von WS-Trust sowohl als *Relying Parties* (*X-Service Provider*) als auch Requestors (*X-Service User*) anzusehen, wobei der in diesem Kontext erforderliche, vertrauenswürdige *Security Token Service (X-Assertion Provider)* durch das ETS repräsentiert wird. Folglich ist ein *ELGA-Initiating-Gateway* immer ein Requestor und ein *ELGA-Responding-Gateway* eine *Relying Party*. Die Autorisierung erfolgt ausschließlich aufgrund gültiger ELGA-*Authorisation-Assertions*. Die notwendige *Authorisation-Assertion* muss vom ETS angefordert werden (Abbildung 31).

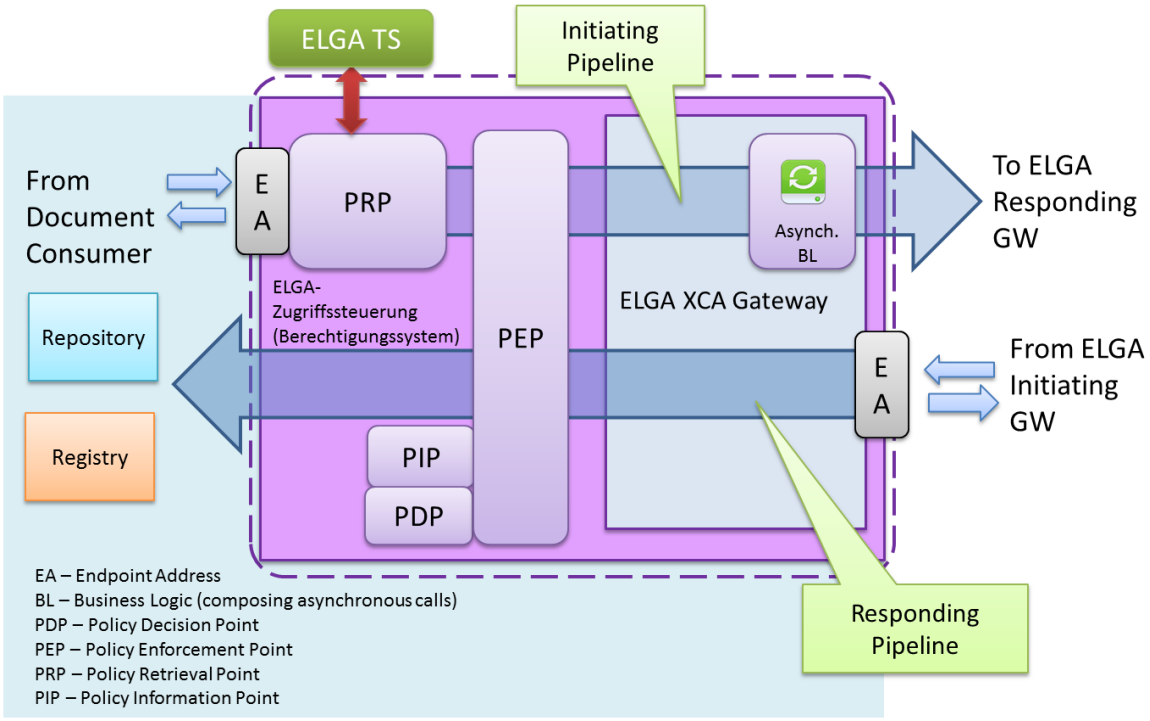


Abbildung 31: ELGA-Berechtigungssystem mit den ELGA-Gateway Pipelines und den dazugehörigen logischen Komponenten

Initiiert ein Document Consumer eine Transaktion an ein ELGA-Initiating-Gateway (siehe Initiating Pipeline in Abbildung 31), muss diese eine gültige ELGA-Authorisation-Assertion umfassen. Gültige Ausprägungen der Assertion-Klassen sind im Kapitel 9 beschrieben und in der Abbildung 35 dargestellt.

Die Anfrage eines Document Consumers übernimmt der Policy Retrieval Point (PRP) der vorgeschalteten ELGA-Zugriffsteuerungsfassade. Die präsentierte *Authorisation-Assertion* wird analysiert und dem ETS übermittelt. Das ETS kann in der Folge eine oder mehrere neue *Authorisation-Assertions* ausstellen, die in Verbindung mit weitergeleiteten Cross-Community (XCA) Zugriffen verwendet werden.

Der PEP der Zugriffssteuerungsfassade des ELGA-Berechtigungssystems filtert basierend auf *Authorisation-Assertions*, die verifizierte Autorisierungsattribute enthalten, unzulässige Zugriffe. Autorisierte Dokumentanfragen werden an die Business-Logik Komponente des ELGA-Gateways weitergeleitet (unterstützt neben synchrone auch asynchrone Anfragen). Diese Business-Logik verarbeitet die der Dokumentenanfrage beigefügten *Authorisation-Assertions* und nutzt die darin enthaltenen URI-Adressen (SAML-Element *<AudienceRestriction>),* um entsprechende ELGA-Gateways zu kontaktieren. Die Business-Logik Komponente leitet die Dokumentenanfrage nun an alle betroffenen ELGA Zielbereiche parallel weiter und retourniert die Antworten konsolidiert an den anfragenden XDS Consumer.

Zusätzlich zur Implementierung des XCA, werden an das hier logisch abgebildete Zugriffssteuerungsfassade–Gateway Pärchen folgende Anforderungen gestellt:

- Unterstützung zentraler PIDs. Für eine Abfrage muss auch ein zentraler Identifier des Patienten (PID), wie z.B. bPK-GH, akzeptiert werden. Damit ist eine Abfrage in ELGA auch für einen Patienten möglich, wenn dieser nicht im lokalen Patientenindex geführt ist. Diese Anforderung gilt für alle ELGA-Bereiche, um aus Sicht des Consumers ein einheitliches Verhalten anzubieten.
- ELGA-Treatment Assertion, User II-Assertion sowie Mandate II-Assertion werden in der aktuellen Release des Berechtigungssystems zur einmaligen Verwendung vom ETS ausgestellt. Eine mehrmalige Verwendung (innerhalb des Gültigkeitszeitraumes – wenige Minuten) ist für künftigen Release-Versionen vorgesehen.
- *Anmerkung: Um dieses Prinzip umzusetzen muss jede ELGA-Assertion eine eindeutige ID führen. Responding-Gateways sind verpflichtet die Liste aller gesehenen Assertion-IDs bis zur deren Gültigkeitsdauer (einige wenige Minuten) aufzuheben. Wird die empfangene Assertion-ID in der Liste gefunden, muss sie als wiederverwendet eingestuft und abgelehnt werden.*
- Die Unterstützung asynchroner Web Services kann aufgrund gewonnener Betriebserfahrung später realisiert werden.
- XCA-Anfragen zu anderen ELGA-Bereichen müssen parallel durchgeführt werden.
- Für die Durchführung von XCA-Anfragen muss ein konfigurierbares User-Timeout implementiert werden. Darunter wird ein Zeitintervall verstanden, nach dem der Request jedenfalls in Richtung Aufrufer beantwortet wird, auch dann, wenn noch nicht alle Antworten verfügbar sind. Die Antwort an den Aufrufer muss die Ergebnisse der bis zum Timeout abgeschlossenen Unterabfragen in aggregierter Form enthalten und im Return-Code ist ein „partieller Fehler“ mit Kennzeichnung der fehlenden Bereiche anzugeben. Das User-Timeout muss dynamisch (im laufenden Betrieb) konfigurierbar sein.
- Verletzungen der Zugriffsberechtigungen (Access Violation) müssen ein SOAP-Fault triggern. Siehe hierfür auch das Kapitel 9.5, Das Verhalten des Berechtigungssystems
- Für neu initiierte Anfragen muss eine Transaktionsnummer (vgl. Kapitel 3.10) vergeben werden, sofern diese nicht schon vom Aufrufer vergeben wurde.
- Antwortzeiten müssen vermessen und protokolliert werden. Diese Protokollierung dient dem Zweck des Performance-Tunings, Monitorings und SLA-Reporting. Diese Funktion muss dynamisch ein- bzw. ausgeschalten werden können. Details sind dem Kapitel 14 zu entnehmen.
- Unterstützung schreibender Zugriffe durch die ZGF des ELGA-Anbindungsgateways.
- Abbildung 32 zeigt die Unterstützung von schreibenden IHE Transaktionen (*Provide and Register Document Set*) durch das ELGA-Berechtigungssystem. Damit kann der ELGA-

Bereich in einfacher Weise den von ELGA geforderten Zugriffschutz beim Veröffentlichen eines Dokumentes implementieren. Kapitel 9 enthält die Details zum Berechtigungssystem.

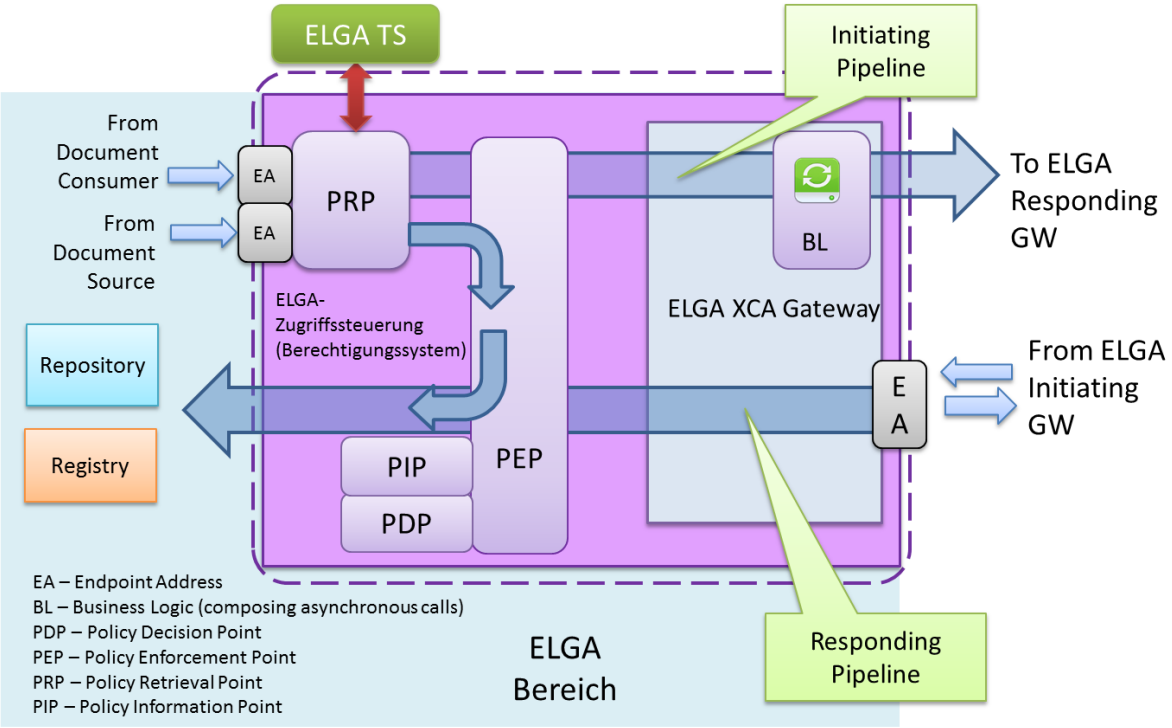


Abbildung 32: ELGA-Berechtigungssystem mit Schreiben in Registry & Repository

8.5. Bilddaten Austausch (XDS-I / XCA-I)

Der Austausch von Bilddaten in ELGA wird in einem eigenen Architekturpapier (siehe [23]) mit dem Hersteller des Berechtigungssystems erarbeitet. Die so erstellte Architektur wird danach zur Begutachtung und Annahme der Expertengruppe Bilddaten sowie den Systempartnern vorgelegt. Dieses Kapitel erörtert das Problem nur übersichtshalber und bezieht sich auf Konzepte, die in den IHE Dokumenten *Radiology Technical Framework Volume 1 Integration Profiles* [9] und *Radiology Technical Framework Supplement XCA-I* [10] beschrieben sind. Detaillierte Vorgaben und Richtlinien hierfür sind in [23] und später im Pflichtenheft zu definieren. Folgende Punkte sind jedoch in Betracht zu ziehen:

- Die Kombination von XDS-I.b und XDS.b in eine bereits vorhandene XDS.b ELGA-Infrastruktur (AGW/ZGF) sollte ermöglicht werden.
- DICOM-Protokolle/Zugriffe müssen von ELGA-Transaktionen verborgen bleiben und über eine dafür dedizierte Komponente (Adapter) ansprechbar sein.
- Clientseitige WADO (RAD-55) Zugriffe müssen unterstützt werden.

- Es ist zu bedenken, das ELGA ein Service- und nicht GUI (User Interface) – orientiertes System ist. WADO wurde aber dediziert für visualisierende Web-Browser basierende Anwendungen eingeführt.
- Bei WADO (RAD-55) Zugriffen ist Autorisierung über SOAP-XUA nicht vorgesehen, und SAML-Tokens können ohne entsprechende Anpassung (z.B. in Form von JWT Verwendung) nicht transportiert werden. Das IHE Internet User Assertion Profile (IUA) muss herangezogen werden.

- Es muss in [23] geprüft werden, inwieweit sowohl WADO-RS wie auch WADO-WS Protokolle (Zugriffe) angeboten werden können.

- Der Bilddatenaustausch ist jedenfalls im ELGA-Core zu sehen. Zur Autorisierung wird hierfür auch ein entsprechendes Token des ELGA-Berechtigungssystems (ausgestellt vom ETS) verwendet. Grundlegendes Policy Enforcement muss direkt im XDS-I / XCA-I Gateway umgesetzt werden.
  - Community-übergreifende (XCA-I) Bilddaten-Zugriffe sind primär über [RAD-75] (Cross Gateway Retrieve) abzuwickeln. Die Transaktion ist geeignet XUA/SAML2 zu transportieren und den Sicherheitsbedingungen des ELGA-Berechtigungssystems zu genügen.
  - Erhöhte Anforderungen an das Netzwerk (Bandbreite) sind zu berücksichtigen.
  - Community-intern (XDS-I) ist zumindest auf [RAD-69] (Retrieve Imaging Document Set) zu setzen. Die Transaktion ist geeignet XUA/SAML2 zu transportieren und den Sicherheitsbedingungen des ELGA-Berechtigungssystems zu genügen. Darüber hinaus sind die Möglichkeiten von WADO-Zugriffen zu eruieren (siehe oben).

9. Berechtigungs- und Protokollierungssystem

Für die Implementierung der österreichischen elektronischen Gesundheitsakte (ELGA) ist zusätzlich zu den lokalen Berechtigungs- und Protokollierungssystemen der durch ELGA integrierten GDA-Systeme ein nationales bereichsübergreifendes Berechtigungs- und Protokollierungssystem notwendig. Dieses regelt generell den ELGA-GDA-übergreifenden Zugriff auf patientenbezogene Informationen und führt Protokoll über erfolgte Zugriffe.

Das ELGA-Berechtigungs- und Protokollierungssystem repräsentiert die technische Umsetzung der legistischen und datenschutzrechtlichen Anforderungen, die sich aus dem Elektronische Gesundheitsakte-Gesetze ergeben (wer darf wann, aufgrund welcher Voraussetzungen, auf welche Daten zugreifen und in welche Dokumente Einsicht nehmen). Das Gesetz legt strikte Vorgaben für den Zugriff auf die in ELGA gespeicherten Daten und für die lückenlose Protokollierung fest.

Hierfür werden Lösungsmethoden definiert, die folgende Aspekte umfassen:

- Föderierung von extern authentifizierten elektronischen Identitäten der ELGA-Benutzer basierend auf elektronischen Zertifikaten (Beispiel Bürgerkarte)
- Autorisierung aller Zugriffe in ELGA über ein Standard-basiertes Zugangskontrollsystem
- Protokollierung aller Aktionen in ELGA über ein Protokollierungssystem

Die Protokollierung spielt für die Umsetzung der datenschutzrechtlichen Anforderungen eine entscheidende Rolle. Insbesondere stellt die Natur der durch ELGA verarbeiteten Daten hohe Ansprüche an die zum Einsatz kommenden Protokollierungsverfahren. Jeder ELGA Akteur speichert Protokolle im bereichseigenen lokalen Audit Record Repository (L-ARR). Logisch zentrale ELGA Akteure persistieren Protokolle in entsprechenden zentralen lokalen ARRs (Z-L-ARR). Die konkrete Zahl der L-ARRs im Bereich der logisch zentralen Akteure, entscheidet sich durch den jeweiligen Betreiber der betroffenen Services und Komponenten. Es sind hier drei Betreiber zu betrachten. Ein Betreiber (ITSV) für den Z-PI mit einem entsprechenden L-ARR, ein Betreiber (SVC) für e-Medikation und Portal und ein Betreiber (BRZ) für die restlichen Services mit zumindest einem weiteren Z-L-ARR.

Darüber hinaus wird ein aggregiertes ARR (A-ARR) für das ELGA-Portal eingerichtet. Das A-ARR persistiert einerseits ATNA-Protokolle die von GDA-Akteuren auf Gesundheitsdaten der Patienten ausgelöst worden sind (lesend und schreibend) und andererseits Protokolle die verändernde Zugriffe auf das zentrale PAP belegen. Weitere Quellen für die Protokollierung im A-ARR sind zu ermöglichen (EBP-Login von Bürgern und Ombudsstellen). Diese Protokolle dienen als Quellinformation für die von ELGA-Teilnehmern über das ELGA-Portal angeforderten Zugriffsprotokolle.

Neben den angeführten Grundlagen, auf denen das Konzept des Berechtigungssystems beruht, repräsentieren die folgenden funktionalen Anforderungen in Anlehnung an die Gesamtarchitektur wichtige Entscheidungsgrundlagen für den gewählten Lösungsansatz:

- Flexible, auf internationale Standards zurückgreifende service-orientierte Lösung, die ohne weitreichende proprietäre Eingriffe in die Festlegungen für die ELGA-Bereiche in einfacher Weise erweiterbar ist.
- Sicherstellung, dass Zugriffe sowohl auf logisch zentrale als auch auf dezentral geschützte ELGA-Objekte und Ressourcen (Zugriffsberechtigungen, Protokollspeicher, Dokumente, Befunde, Bilder, Verweise auf diese Informationsobjekte usw.) einer einheitlichen Konzeption der Autorisierung durch das ELGA-Berechtigungssystem unterliegen.
- Sicherstellung einer einheitlichen Zugriffsentscheidung in allen ELGA-Bereichen innerhalb eines zu definierenden Zeitraums nach der Änderung von Zugriffsberechtigungen.

- Unterstützung der IHE Integrationsprofile *Audit Trail and Node Authentication* (ATNA), *Cross Enterprise User Assertion* (XUA) und *Attribute Extension*, *Cross Community Access* (XCA).

- Unterstützung der aktuellen OASIS Standards *eXtensible Access Control Markup Language* (XACML), *Security Assertion Markup Language* 2.0 (SAML), *Web Services Security SAML Token Profile* und *Web Services Security: SOAP Message Security 1.1*, *WS-Trust*

- *Basic Patient Privacy Consent* (BPPC) wird in ELGA nicht umgesetzt. Eine ähnliche, dem ELGA-Gesetz entsprechende Funktionalität wird in Form eines signierten Consent-Dokuments eingeführt. In ELGA werden Zugriffsberechtigungen durch den ELGA-Teilnehmer mit Hilfe des ELGA-Portals gewartet werden können. Das am Portal erzeugte Consent-Dokument enthält die textuelle Übersetzungen der erstellten XACML-Policies bzw. die technischen Referenzen auf diese Policies (nicht aber die Berechtigungen selbst).

9.1. Architektur des ELGA-Berechtigungssystems

Das ELGA-Berechtigungssystem wurde so konzipiert, dass Änderungen der Vorgaben des ELGA-Gesetzes bzw. von entsprechenden Verordnungen hierzu, die einer bestimmten Dynamik unterliegen werden, ohne grundlegende technische Änderungen an der Systemarchitektur durchgeführt werden können und dahingehend entsprechende Flexibilität besteht.

Grundsätzlich basiert das ELGA-Berechtigungssystem auf den in OASIS WS-Trust beschriebenen Sicherheitskonzepten und darüber hinaus auf Prinzipien und Anwendungsfällen, welche im IHE White Paper Access Control [4] erläutert werden. Insbesondere wird die in diesem Dokument präsentierte Kommunikationstechnik *Policy Push* durch das ELGA-Berechtigungssystem für den elektronischen Austausch von Zugriffsberechtigungen realisiert.

Die Vertraulichkeit und Sicherheit auszutauschender medizinischer Daten unter Nutzung von Web Browsern innerhalb ELGA wird, entsprechend den Festlegungen der aktuellen Versionen der OASIS Standards SAML-Core sichergestellt.

In Abbildung 33 sind die Grundlagen des ELGA-Berechtigungssystems betreffend die Authentifizierung und Autorisierung von ELGA-Benutzern und deren Zugriffe vereinfacht dargestellt.

1. Ein ELGA-Benutzer muss sich im ersten Schritt immer gegenüber einem in ELGA zulässigen Identity Provider authentisieren, um dadurch eine Identity-Assertion zu erhalten.

2. Anschließend erfolgt, basierend auf dieser Identity-Assertion, die Autorisierung durch das ELGA-Token-Service, welches resultierend *ELGA-Authorisation-Assertions* als eigentliche Grundlage für Zugriffsentscheidungen innerhalb ELGA ausstellt (siehe Abbildung 34). Somit entsteht eine virtuelle (bzw. föderierte) Identität des Benutzers in ELGA.

3. Die durch das ELGA-Token-Service ausgestellten *Authorisation-Assertions* müssen durch ELGA-Benutzer (bzw. durch deren Informationssysteme) allen ihren Operationen in ELGA zum Zweck der Zulässigkeitsevaluierung durch das Berechtigungssystem beigefügt werden.

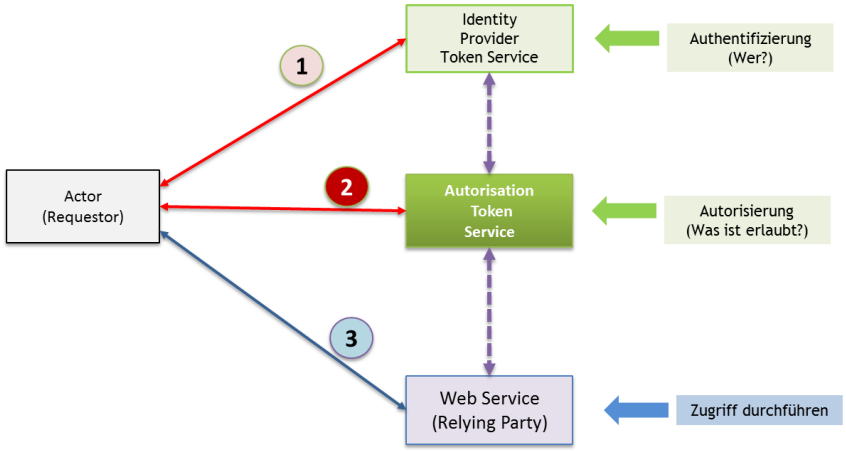


Abbildung 33: ELGA-Authentifizierungs- und Autorisierungsübersicht

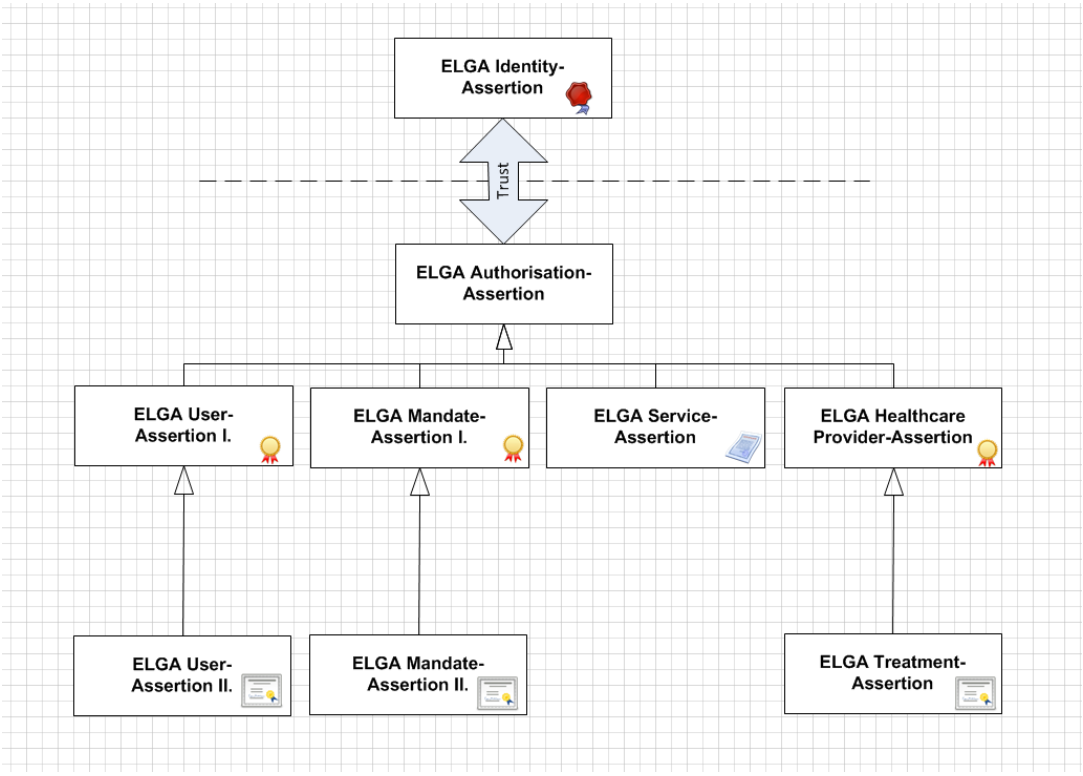


Abbildung 34: ELGA-Authorisation-Assertion Klassenhierarchie (vereinfachter Darstellung)

9.1.1. Prinzipien der Authentifizierung und Autorisierung in ELGA

9.1.1.1. Allgemeines

Authentifizierung der einzelnen Akteure in ELGA erfolgt auf zwei Ebenen.

- Auf der Transport-Ebene (https) dürfen nur sich gegenseitig bekannte und vertrauende Knoten (Akteure) miteinander reden. Hierfür sind alle Akteure ATNA Secure Nodes und das gegenseitige Vertrauen basiert auf X.509 Zertifikaten. Jeder Akteur (Server oder Anwendung) muss sich gegenüber seinem Kommunikationspartner ausweisen und entsprechend eine TLS-Verbindung zur Kommunikation aufbauen. Diesbezügliche Einzelheiten sind im Kapitel 9.1.4 erläutert.

- Auf der SOAP-Nachrichten-Ebene ist es für alle Aktionen in ELGA notwendig, dass die elektronische Identität und Rolle des konkreten ELGA-Benutzers in verifizierter Form vorliegen. Diese elektronische Identität des ELGA-Benutzers in den einzelnen Aktionen durch eine Identity-Assertion (spezifiziert mittels *Security Assertion Markup Language 2.0*) bestätigt werden muss. Die initiale elektronische Identität (Identity Assertion) muss der ELGA-Benutzer zuvor bei einem externen *Identity Provider* (IdP) angefordert haben, welcher die eigentliche Authentifizierung durchgeführt hat. Alle weiteren *ELGA-Authorisation Assertion* sind aufgrund der initialen elektronischen Identität vom ETS auszustellen. Eine detaillierte Abbildung der diesbezüglichen Beziehungen zwischen den einzelnen Assertions (UML-Klassen) ist in der Abbildung 35 dargestellt.

Die initiale Identity-Assertion ist explizit für ELGA bzw. das ELGA-Token-Service als *Relying Party* auszustellen (SAML-Element <AudienceRestriction>). In der Abhängigkeit des eigentlichen Subjektes, bestätigt ein externer IdP:

1. Bei ELGA-Teilnehmern die Identität des Bürgers (aufgrund Bürgerkarte) für ELGA.
2. Bei GDA wird primär die Identität der Organisation (z.B. Krankenhaus, Pflegeheim, Ordination) bestätigt. Zusätzlich (sekundär) muss aber die in Vertretung der Organisation agierende physische Person namentlich angeführt werden. Der GDA haftet für die korrekten Angaben.
3. Bei der WIST wird die Identität der Organisation bestätigt. Die IDA muss die OID 1.2.40.0.34.3.1.4 (ELGA-Widerspruchstelle) enthalten.
4. Bei der OBST wird die Identität der Organisation OID 1.2.40.0.34.3.1.3 (ELGA-ombudsstelle) und die Identität der natürlichen Person via bPK-GH bestätigt.

5. Bei Sicherheits- oder Regelwerkadministrator die autorisierte Identität der natürlichen Person

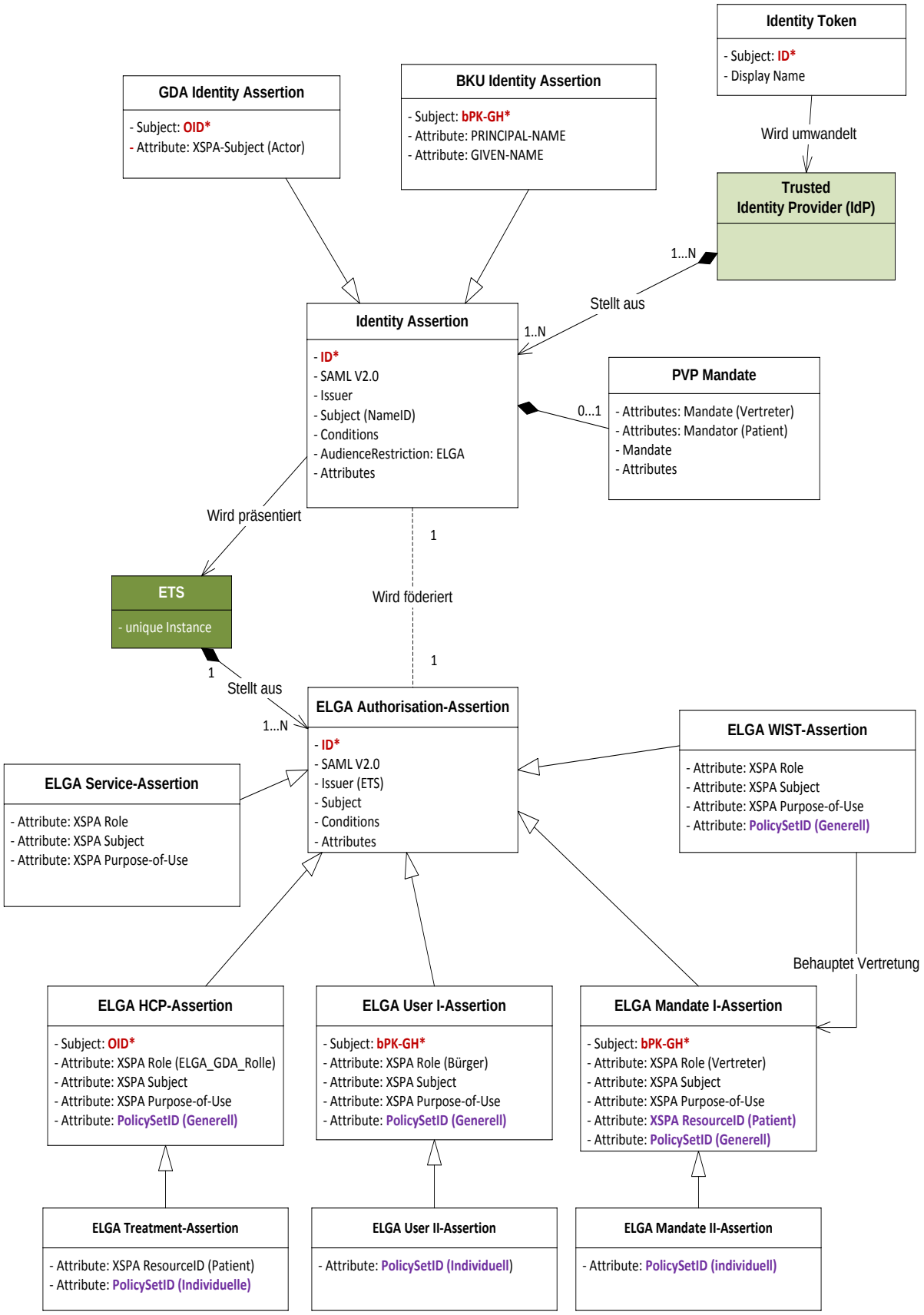
Die Identity Assertion enthält verpflichtend das Subjekt (Organisation), den das Subjekt beschreibenden Namen, einen tatsächlichen Akteur (physische Person oder Service). Die exakte Liste der beizufügenden Angaben ist wie folgt:

- Subjekt (Name-ID)
  - Bei ELGA-Teilnehmer ein bPK-GH (Bürger gemäß OID 1.2.40.0.10.2.1.1.149)
  - Bei GDA ein OID (z.B. gemäß 1.2.40.0.34.3.1 oder 1.2.40.0.34.3.2 eHealth-Austria; Organisations bzw. Persons). Darüber hinaus ist es erlaubt eine Vertragspartnernummer gemäß 1.2.40.0.10.1.4.3.2 (Verwaltung; hvb; vpnr-eHealth) anzuführen.
- Display-Name der Organisation. Wenn eine GDA-Organisation zugreift, ist der aufgelöste Name der Institution anzugeben. Dies wird vom ETS im Attribut XSPA-Organisation erwartet und eingebettet.
- Alias, im Klartext der Name der zugreifenden physischen Person. Diese Angabe wird vom ETS (sowohl bei GDA wie auch bei ELGA-Teilnehmer) im SAML2-Attribut *XSPA-Subject* erwartet und in das gleichnamige Attribut der neu ausgestellten *ELGA Authorisation-Assertion* geschrieben.
  - Greift hier ein Service (Automat) zu, dann ist die klare Bestimmung und Name des Services bzw. des Auftraggebers anzuführen
- Issuer, eine eindeutige Kennung der vertrauenswürdigen ausstellenden Instanz (IdP), welche die Assertion ausgegeben hat. Diese Angabe ist anhand der entsprechenden vertrauenswürdigen Zertifikate der jeweiligen IdP zu verifizieren.
- Home-Community ID (optional), die ELGA-weite eindeutige Identifikation des jeweiligen ELGA-Bereichs, in der die Identity Provider (und die GDA) beheimatet sind.

Der Identity Provider hat die *Identity Issuance Policies* für ELGA offenzulegen. Die ELGA-SIKO überprüft die vorgelegte Policy sowie die technische und organisatorische Gegebenheiten vor Ort und entscheidet über die Vergabe des Trust-Verhältnisses.

Wenn der Zugriff des ELGA-Benutzers durch ein unsicheres (nicht vertrauenswürdiges) offenes Netzwerk erfolgt, muss die Signatur der Identity Assertion dem Signaturgesetz (qualifiziertes Zertifikat) entsprechen. Wenn der ELGA-Benutzer aus einem physisch abgesicherten (vertrauenswürdigen) Netzwerk kommt, können auch andere Qualitäten in Betracht gezogen werden. Diese sind von der ELGA-Sicherheitskommission explizit zu bestimmen.

Die ELGA-Identity-Assertion wird vom ELGA-Benutzer zum Zweck der Authentisierung gegenüber dem ELGA-Berechtigungssystem verwendet. In Abhängigkeit des konkreten ELGA-Benutzers resultiert die erfolgreiche Authentifizierung in der Ausstellung einer ELGA-*Authorisation-Assertion*, welche neben der in ELGA zulässigen Identität und Rolle des ELGA-Benutzers auch weitere Attribute betreffend der Zugriffsautorisierung strukturiert abbildet. Mögliche Ausprägungen der ELGA-Auth*orisation-Assertion* Klassen werden in der Abbildung 35 detailliert (und in der Abbildung 34 vereinfacht) veranschaulicht. Die dargestellten *Authorisation-Assertion*-Klassen sind grundsätzlich anhand des Inhalts des Attributs *„Purpose-of-Use“* identifizierbar (siehe Tabelle 15). Das Value-Set des Attributes ist ELGA-spezifisch in Anlehnung auf das XSPA Purpose-of-Use Profiles.


Identity Token
- Subject: ID*
- Display Name
Wird umwandelt
GDA Identity Assertion
- Subject: OID*
- Attribute: XSPA-Subject (Actor)
BKU Identity Assertion
- Subject: bPK-GH*
- Attribute: PRINCIPAL-NAME
- Attribute: GIVEN-NAME
Trusted
Identity Provider (IdP)
1...N
Stellt aus
1..N
Identity Assertion
- ID*
- SAML V2.0
- Issuer
- Subject (NameID)
- Conditions
- AudienceRestriction: ELGA
- Attributes
PVP Mandate
- Attributes: Mandate (Vertreter)
- Attributes: Mandator (Patient)
- Mandate
- Attributes
0...1
Wird präsentiert
1
Wird föderiert
ETS
- unique Instance
1
Stellt aus
1...N
1
ELGA Authorisation-Assertion
- ID*
- SAML V2.0
- Issuer (ETS)
- Subject
- Conditions
- Attributes
ELGA WIST-Assertion
- Attribute: XSPA Role
- Attribute: XSPA Subject
- Attribute: XSPA Purpose-of-Use
- Attribute: PolicySetID (Generell)
ELGA Service-Assertion
- Attribute: XSPA Role
- Attribute: XSPA Subject
- Attribute: XSPA Purpose-of-Use
Behauptet Vertretung
ELGA HCP-Assertion
- Subject: OID*
- Attribute: XSPA Role (ELGA_GDA_Rolle)
- Attribute: XSPA Subject
- Attribute: XSPA Purpose-of-Use
- Attribute: PolicySetID (Generell)
ELGA User I-Assertion
- Subject: bPK-GH*
- Attribute: XSPA Role (Bürger)
- Attribute: XSPA Subject
- Attribute: XSPA Purpose-of-Use
- Attribute: PolicySetID (Generell)
ELGA Mandate I-Assertion
- Subject: bPK-GH*
- Attribute: XSPA Role (Vertreter)
- Attribute: XSPA Subject
- Attribute: XSPA Purpose-of-Use
- Attribute: XSPA ResourceID (Patient)
- Attribute: PolicySetID (Generell)
ELGA Treatment-Assertion
- Attribute: XSPA ResourceID (Patient)
- Attribute: PolicySetID (Individuelle)
ELGA User II-Assertion
- Attribute: PolicySetID (Individuell)
ELGA Mandate II-Assertion
- Attribute: PolicySetID (individuell)

3165

3166

Abbildung 35: UML-Klassendiagramme der ELGA Identity- und ELGA Authorisation-Assertion Klassen. Rot gekennzeichnet sind die Primärschlüssel, lila die Fremdschlüssel.

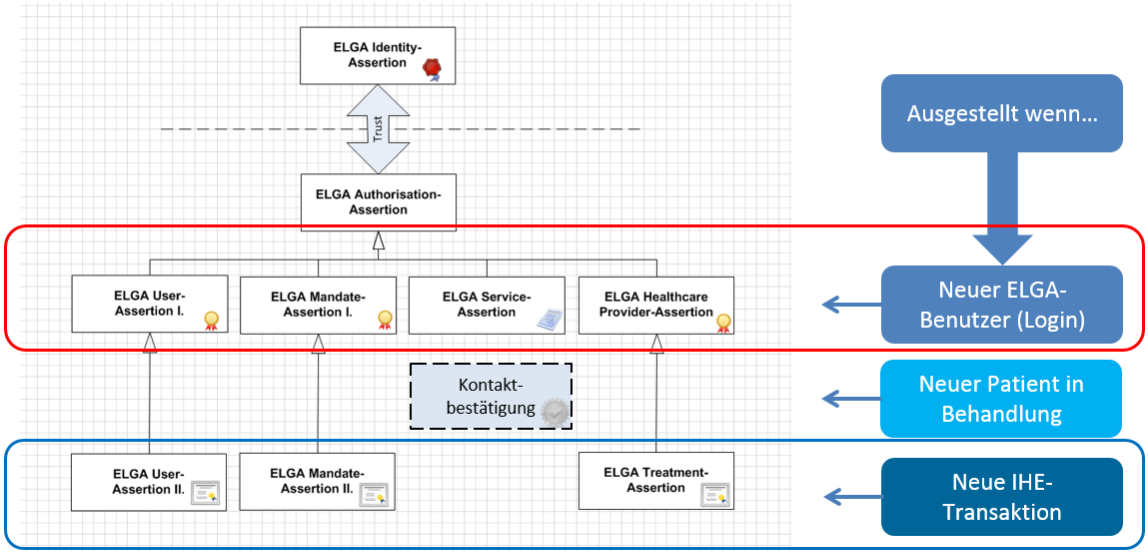
Beim Akt des Föderierens von GDA muss der anfragende Akteur die angeforderte ELGA-Rolle vom dafür bestimmten Codesystem OID: 1.2.40.0.34.5.3 im entsprechenden RST Request für eine *ELGA Authorisation Assertion* explizit als *Claim* anführen (z.B. 700 – Arzt, 704 - Apotheker). Diese Angabe wird durch die Komponente GDA-Index verifiziert

ELGA-*Authorisation-Assertions* der ersten Ebene (siehe Abbildung 36) repräsentieren sogenannte föderierte Identitäten in ELGA. Eine föderierte Identität ist ein zugelassener ELGA-Benutzer im angemeldeten (Log-in) Zustand, dem anhand der präsentierten ELGA-Identity-Assertion und zugeordneten ELGA-Rolle (verifiziert via GDA-Index) vertraut wird.

Mit Ausnahme der ELGA-Service-Assertion ist die Existenz einer föderierten Identität die Voraussetzung für die Ausstellung weiterer spezialisierter *Authorisation-Assertions*.

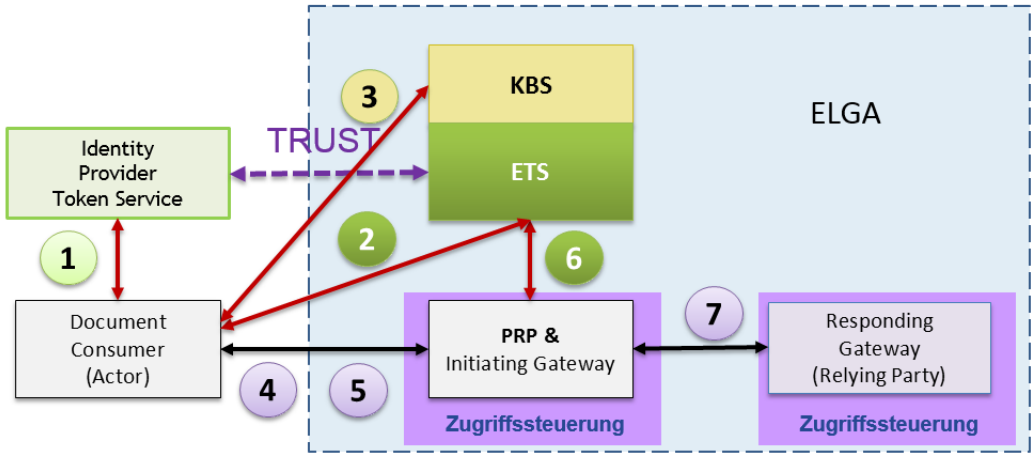
ELGA-*Authorisation-Assertions* der zweiten (untersten) Ebene repräsentieren delegierte *Authorisation-Assertion* Klassen. Diese *Authorisation-Assertions* bilden neben identitäts- und rollenbezogenen Informationen auch generelle und individuelle Zugriffsberechtigungen strukturiert ab und werden ausschließlich für ELGA-Zugriffssteuerungsfassaden ausgestellt, die im Namen von erfolgreich Angemeldeten und föderierten Identitäten agieren.

Die Struktur von ELGA-*Authorisation-Assertions* folgt im Allgemeinen dem Informationsmodell des OASIS Sicherheitsstandards SAML 2.0 und im Speziellen den Constraints bzw. Einschränkungen gemäß dem Integrationsprofil XUA. Tabelle 15 listet beispielhaft eine mögliche Instanz des Informationsmodells einer ELGA-*Authorisation-Assertion* sowie allgemeine Hinweise. Die Ziffern in der ersten Spalte der Tabelle repräsentieren die Hierarchieebenen der beschriebenen XML-Elemente.



3190

3191 *Abbildung 36: Autorisations-Klassen je nach Ereignis der Ausstellung*



1. Authentifizierung, Request Identity-Assertion
2. ELGA-Login, Request HCP-Assertion
3. Kontaktbestätigung initiieren
4. Document Consumer: IHE Transaction auslösen
5. Zugriffssteuerungsfassade: Anfrage abfangen
6. PRP: „*ActAs*“ Document Consumer, Request Treatment-Assertion
7. Gateway: IHE XCA Transaction

3192

3193 *Abbildung 37: Authentifizierung und Autorisierungsschritte eines GDA in ELGA*

	Assertion Element	Attribute/Value	Beschreibung	Beispiel, Anmerkung
1	Assertion	@Version	SAML 2.0	2.0
		@ID	Unique Identifier	UUID der Assertion
		@IssueInstant	UTC	Assertion wurde ausgestellt
2	Issuer		Eindeutige Bezeichnung des Ausstellers des Tokens	Beispiel: urn:elga:ets
2	Signature		Digital signature	
2	Subject		Parent element	
3	NameID		Eindeutige Bezeichnung der mit diesem Token autorisierten Identität	Identity-Assertion: bPK-GH oder L-PID; bei GDA ist hier der OID erwartet
		@Format	X509SubjectName	
		@SPProvidedID	Display Name	Beispiele: Dr. Max Musterdoktor Franz Mustermann AKH, KAV Wien (Organisation)
3	SubjectConfirmation	@Method	Passive Clients (Web-Browser) „bearer“; Aktive Clients “sender-vouches” odewr „holder-of-key“	urn:oasis:names:tc:SAML:2.0:cm: holder-of-key sender-vouches bearer
2	Conditions	@NotBefore	Vor dieser UTC-Zeit…	Subject kann nicht bestätigt werden
		@NotOnOrAfter	Nach dieser UTC-Zeit…	Subject kann nicht bestätigt werden
3	AudienceRestriction			
4	Audience		URI: URN/URL der Relying Party (X-Service Provider) für den die Assertion bestimmt ist	Kardinalität 1 bis N; Beispiele: https://elga-online.at/KBS https://elga-online.at/ETS
2	AuthnStatement	@AuthnInstant	UTC-Zeit der Autorisierung	
3	AuthnContext			
4	AuthnContextClassRef		Für ELGA derzeit ausschließlich X509 Zertifikat	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
2	AttributeStatement			
3	Attribute@Name	subject:npi	Optional	
3	Attribute@Name	XSPA-Subject	(Freitext) im Namen der Organisation handelnde konkrete Person	Beispiele: • Dr. Max Mayer (Urologie) • Max.Meyer@uniwien.at • ID123456-Max-Meyer-Dr
3	Attribute@Name	XSPA-Organisation	Subjects Display Name aus GDA-I, für physische Personen nicht vergeben	Beispiel: Wiener KAV, Donauspital
3	Attribute@Name	XSPA-Role	Subjects ELGA-Rolle aus GDA-I, ein CE Wert	Beispiel (nur der Text): Arzt, Apotheker, Bürger, Krankenanstalt
3	Attribute@Name	Purpose-of-Use	TREATMENT EMEDIDTREATMENT REQUEST SYSADMIN MANDATE PUBLICHEALTH LOCAL_REQUEST	Treatment-Assertion Treatment-Assertion für e-Med User-Assertion Service-Assertion Mandate-Assertion HCP-Assertion Community-Assertion
3	Attribute@Name	XSPA-ResourceID	L-PID oder bPK-GH des Patienten in CX Format	Der Wert enthält eine Referenz auf die „Ressource“. Bei Treatment Assertion und User-Assertion den ID des Patienten. Bei Mandate-Assertion des Auftraggebers (Vertretener).
3	Weitere Attribute		für einzelne XACML-Policies	Individuelle Berechtigungen

3194 *Tabelle 15: Beispiel einer grundlegenden ELGA-Authorisation-Assertion Struktur*

3195

Der Nachweis der Identität z.B. bei Nutzung einer Public Key Infrastructure (PKI) (Fall Bürgerkarte und a/o-card) basiert darauf, dass der ELGA-Benutzer vom IdP gesendete Authentisierungsdaten mit dem privaten Schlüssel seiner Karte signiert. Der IdP kann die Signatur anhand des im Zertifikat enthaltenen und von einer Zertifizierungsstelle bestätigten, öffentlichen Schlüssels prüfen (=Authentifizierung). Die Identitätsbestätigung ist für eine festzulegende Zeitdauer gültig. Zum Freischalten der Signaturfunktion der Karte ist wiederum die Eingabe eines PINs erforderlich. Zum Nachweis der Identität ist also in diesem Fall Besitz und Wissen notwendig. Neben Bürgerkarte und a/o-card sind weitere alternative Verfahren zur Authentisierung basierend auf der Nutzung qualifizierter Zertifikate möglich.

In ELGA werden unterschiedliche IdP zugelassen. Das Berechtigungssystem muss so konzipiert werden, dass neue IdP und Authentifizierungsverfahren in einfacher Weise ergänzt werden können. Durch ELGA unterstützte IdP sind:

- Die Österreichische Bürgerkartenumgebung sowie Handy-Signatur innerhalb des ELGA-Berechtigungssystems.
- Das e-card System auf Basis der Vertragspartner-Authentisierung. Diese kann unter Benutzung der a/o-card (welche denselben Mechanismus nützen) bzw. eines SW-Zertifikats für Krankenanstalten erfolgen.
- Portalverbund (e-Government) mit dem PVP Protokoll in der Version 2.1.2 oder höher
- Durch die ELGA-Sicherheitskommission (SIKO) für ELGA zugelassene und in ELGA eingebundene IdP, insbesondere zur Unterstützung von Krankenanstalten und Verbünden.

Eine typische Authentifizierungs- und Autorisierungs-Reihenfolge bzw. die notwendigen (und optionalen) Schritte bei der Ausstellung der einzelnen *ELGA-Authorisation-Assertions* sind in der Abbildung 37 dargestellt. In der Abbildung 35 sind folgende ELGA Assertion-Klassen dargestellt:

9.1.1.2. ELGA-Identity-Assertion

- Ausstellung durch vertrauenswürdige Identity Provider für ELGA-Benutzer
  - Zulassung durch Entscheidung der ELGA-Sicherheitskommission (SIKO)
  - Vertrauensverhältnis zwischen Identity Provider und ETS erforderlich
- Subject\NameID enthält die Identität des ELGA-Benutzers:
  - Wenn ELGA-Teilnehmer, dann bPK-GH
  - Wenn ELGA-GDA Organisation oder OBST, dann OID (oder VPNR)
  - Wenn ELGA-GDA physische Person, dann eine interne ID
  - Wenn WIST dann OID

- Subject\SPProvidedID (optional): Display-Name von Subject\NameID
- Subject Confirmation Method: bearer
- AudienceRestriction\Audience: ELGA bzw. ETS
- Attributes
  - XSPA Subject: Name der tatsächlich zugreifenden Person, wird in A-ARR mitgeführt
  - XSPA Organisation ID: OID der GDA welcher via GDA-I verifiziert wird
  - ELGA OID Issuing Authority: ID der Stelle welche Organisation ID vergeben hat

9.1.1.3. ELGA-Authorisation-Assertion

Eine ELGA-Authorisation Assertion dient primär dem Zweck der Identitätsföderation. Eine elektronische Identität, welche von einem externen vertrauenswürdigen Identity Provider ausgestellt wurde, kann damit in ELGA föderiert werden. Der Akt der Föderation ist auf harte Bedingungen gebunden, die erfüllt werden müssen um für den Akteur eine neue föderierte ELGA-Identität auszustellen.

- Ausstellung durch ELGA Token Service (ETS)
- Superklasse, abstrakt, fasst gemeinsame Eigenschaften zusammen
- Identitätsattribute, Rollenattribute, Zugriffsart

9.1.1.4. ELGA-User I Assertion

- Subject\NameID: ELGA-Teilnehmer (bPK-GH)
- Bedingung: ELGA-Teilnehmer ist via Z-PI identifizierbar (hat eine bPK-GH)
- Subject Confirmation Method: sender-vouches
- AudienceRestriction\Audience: ETS, KBS, PAP, A-ARR
- Attributes: ELGA-Teilnehmer-spezifische Identitätsattribute, Rollenattribute (implizit Bürger) und Zugriffsart (regulär)
- Gültigkeitsdauer 20 Minuten (konfigurierbar bis zu 30 Minuten)
- Purpose of use: REQUEST
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar
- Token ist mindestens zweimal erneuerbar (ohne erneute Authentifizierung)

9.1.1.5. ELGA-User II Assertion

- Subject\NameID: ID oder URI der initiierenden Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA User I Assertion
- AudienceRestriction\Audience: URI des betroffenen ELGA-Bereiches
  - Ausgestellt einzeln für jeden zu adressierenden ELGA-Bereich
- Attributes: ELGA-Teilnehmer-spezifische Zugriffsberechtigungen

- Gültigkeitsdauer: 5 Minuten
- Purpose of use: REQUEST2
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.6. ELGA User Community-Assertion

- Subject\NameID: ID oder URI der antwortenden (Reponding) Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via ActAs)
  - Referenzierte Identität in ELGA User-Assertion II
- AudienceRestriction: URI der direkt adressierten Ressourcen
  - Ressourcen sind Registry, Repository oder eine ELGA-Anwendung
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: COMMUNITY
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.7. ELGA-Mandate I Assertion

- Subject\NameID: bevollmächtigter ELGA-Teilnehmer (Vertreter, bPK-GH)
- Bedingung: Sowohl der bevollmächtigter Teilnehmer wie auch der/die vertretene ELGA-Teilnehmer sind via Z-PI identifizierbar (beide haben eine gültige bPK-GH)
- Subject Confirmation Method: sender-vouches
- AudienceRestriction\Audience: ETS, KBS, PAP, A-ARR
- Attributes:
  - Identitätsattribute, Rollenattribute und Zugriffsart des bevollmächtigten ELGA-Teilnehmers
  - Identitätsattribute des vollmachtgebenden ELGA-Teilnehmers
- Purpose of use: MANDATE
- Wenn für OBST-Mandate ausgestellt wird, dann muss der OID der Ombudsstelle angeführt werden
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar
- Token ist mindestens zweimal erneuerbar (ohne erneute Authentifizierung)

9.1.1.8. ELGA-Mandate II Assertion

- Subject\NameID: Initiierende Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA Mandate I Assertion
- AudienceRestriction\Audience: URI des betroffenen ELGA-Bereiches
- Attributes:
  - generelle und individuelle Zugriffsberechtigungen des vollmachtgebenden ELGA-Teilnehmers

- generelle Zugriffsberechtigungen des bevollmächtigten ELGA-Benutzers
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: MANDATE2
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.9. ELGA Mandate Community-Assertion

- Subject\NameID: Antwortende (Reponding) Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA Mandate-Assertion II
- AudienceRestriction\Audience: URI der direkt adressierten Ressourcen
  - Ressourcen sind Registry, Repository oder eine ELGA-Anwendung
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: COMMUNITY
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.10. ELGA-Service-Assertion

- Subject\NameID: ID von ELGA-Service
- Bedingung: Akteur/Service ist authetifiziert bzw. über die dafür dienende lokale Sicherheitsgruppe autorisiert
- Subject Confirmation Method: bearer
- AudienceRestriction\Audience: URN der entsprechenden Service-Endpoints
- Attributes:
  - ELGA-Service spezifische Identitätsattribute, Rollenattribute
- Gültigkeitsdauer: bis zu 1 Stunde
- Purpose of use: SERVICE
- Berechtigt NICHT lesend auf ELGA Gesundheitsdaten zuzugreifen
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.11. ELGA-Healthcare Provider-Assertion

- Subject\NameID: ELGA-GDA, auch Ombudsstellen (OID)
- Bedingung: GDA ist im GDA-Index als aktiver ELGA-GDA geführt
- Subject Confirmation Method: bearer
- AudienceRestriction\Audience: ETS, KBS, URN des ZGF/AGW
- Attributes:
  - ELGA-GDA-spezifische Identitätsattribute, Rollenattribute
  - ELGA-GDA-spezifische generelle Zugriffsberechtigungen
  - Home Community-ID (optional)
- Gültigkeitsdauer: bis zu 4 Stunden (parametrierbar)
- Purpose of use: PUBLICHEALTH

- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar
- Token ist einmal erneuerbar (ohne erneute Authentifizierung)

9.1.1.12. ELGA-WIST-Assertion

- Subject\NameID: ELGA-Widerspruchstelle, wobei die Object-ID von berechtigten WIST nicht im GDA-I gelistet, sondern im Berechtigungssystem vorkonfiguriert ist.
- Bedingung: In der Identity Assertion behauptete OID der WIST ist dem Berechtigungssystem (ETS) bekannt
- Subject Confirmation Method: bearer
- AudienceRestriction\Audience: PAP
- Attributes: ELGA-spezifische Identitätsattribute, Rollenattribute
- Gültigkeitsdauer: bis zu 4 Stunden (parametrierbar)
- Purpose of use: WIDERSPRUCHSTELLE
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar
- Token ist nicht erneuerbar (laut Anforderungen des Betreibers ITSV)

9.1.1.13. ELGA-Treatment-Assertion

- Subject\NameID: Initiierende Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA HCP-Assertion
- AudienceRestriction\Audience: URI des betroffenen ELGA-Bereiches
- Attributes:
  - ELGA-Teilnehmer-spezifische Informationen und individuelle Zugriffsberechtigungen
  - Generelle Zugriffsentscheidungen
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: TREATMENT
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.14. ELGA e-Med-ID Treatment Assertion

- Subject\NameID: Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA HCP-Assertion
  - Präsentiert zusätzlich: e-Med-ID Token, ausgestellt vom STS der ELGA Anwendung e-Medikation
- AudienceRestriction\Audience: URI der ELGA-Anwendung e-Medikation
- Attributes:
  - ELGA-Teilnehmer-spezifische individuelle Zugriffsberechtigungen
  - Generelle Zugriffsentscheidungen

- Wird ohne Überprüfung einer gültigen Kontaktbestätigung zwischen GDA und ELGA-Teilnehmer ausgestellt
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: EMED_ID
- Token ist für einmalige Transaktion und daher nicht wiederverwendbar

9.1.1.15. ELGA HCP Community-Assertion

- Subject\NameID: Antwortende (Reponding) Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via *ActAs*)
  - Referenzierte Identität in ELGA Treatment-Assertion
- AudienceRestriction\Audience: URI des direkt adressierten Ressourcen
  - Ressourcen sind Registry, Repository oder eine ELGA-Anwendung
- Attribute: Optional betroffener ELGA-Teilnehmer (soweit patID vorhanden/bekannt)
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: COMMUNITY
- Token ist im Zeitraum der angeführten Gültigkeit wiederverwendbar

9.1.1.16. ELGA Generic Community-Assertion

Diese Klasse ist in der Abbildung 35 nicht dargestellt. Wird von einer ELGA-ZGF ohne ETS Beteiligung für XDS-Zwecke (für sich selbst) in folgenden Fällen ausgestellt:

1. Aufgrund einer gültigen vertrauenswürdigen bereichsspezifischen Assertion, wenn die initiierte Transaktion nicht ELGA-relevant ist. Eine nicht ELGA-relevante Transaktion ist insbesondere in der ELGA-Bereich Variante C von Bedeutung, und zwar wenn der ELGA-Flag bewusst auf FALSE (nicht ELGA relevant) gesetzt ist. Siehe hierfür Kapitel über die Konfiguration des ELGA-Anbindungsgateways.
2. Darüber hinaus kann die ZGF eine generische Community-Assertion für den eigenen lokalen Lösch-Dienst ausstellen um die vom Bürger (ELGA-Teilnehmer) beauftragten und vom PAP freigegeben CDA in einem Batch-Job zu löschen.
3. Beim Update von CDA Dokumenten, wenn keine gültige (oder eine abgelaufene) Kontaktbestätigung bzw. eine vom ELGA-Teilnehmer gesetzte individuelle Policy das Updaten (Richtigstellen) des Dokumentes verhindern würde.

- Subject: Antwortende (Reponding) Zugriffssteuerungsfassade
- Subject Confirmation Method: sender-vouches
- Delegierte Assertion (via OnBehalfOf)
  - Referenzierte Identität in bereichsspezifischen (nicht ELGA) Assertion
- Audience Restriction: URI der direkt adressierten Ressource

- Erlaubte Ressourcen sind Registry oder Repository
- Attribute: ELGA-Teilnehmer (L-PID oder bPK-GH) deren Gesundheitsdaten vom GDA-Zugriff betroffen sind
- Gültigkeitsdauer: bis zu 5 Minuten
- Purpose of use: COMMUNITY

9.1.1.17. Erneuern von ELGA-Assertions

Prinzipiell werden Identity Assertions, die von vertrauenswürdigen IdP ausgestellt worden sind, in ELGA einmalig föderiert. Läuft die Gültigkeit einer ELGA-Assertion ab, muss gemäß WS-Trust mit einem entsprechenden neuen (oder noch gültigen) Identity Assertion erneuert werden (Token Renewal). Die Erneuerung von Tickets benötigt jedoch in den meisten Fällen eine erneute Authentifizierung des Subjektes (ELGA-Benutzer). Um den Aufbau eines „non intrusive“ Systems zu unterstützen bzw. um die Benutzerfreundlichkeit zu erhöhen, muss das ELGA Berechtigungssystem bestimmte ELGA-Assertions ohne wiederholte Aufforderung zur Authentifizierung limitiert erneuern können. Die Bedingung dafür ist eine noch gültige ELGA-Login-Assertion der gleichen Klasse.

ELGA-Login-Assertions, die für wenige Minuten (bis zu 30 Minuten) ausgestellt worden sind, können auf diese Weise höchstens zweimal erneuert werden. Für die Erneuerung muss eine noch gültige ELGA-Assertion der gleichen Klasse präsentiert werden. Typischerweise betrifft dies vor allem die ELGA-User-Assertion I (ausgestellt für 20 bis max. 30 Minuten). Für ELGA-Assertions, die für mehrere Stunden ausgestellt worden sind, kann die Erneuerung ohne explizite Authentifizierung nur einmal stattfinden. Typischerweise betrifft diese Maßnahme die ELGA-HCP-Assertions (ausgestellt für 2 bis max. 4 Stunden).

9.1.2. Anforderungen an ELGA Token Service (ETS)

Die in der Abbildung 34 dargestellte ETS-Klasse spielt eine zentrale Rolle bei der Ausstellung von allen *ELGA Authorisation Assertion* Instanzen. Hierfür muss dem Schutz von ETS eine außerordentlich hohe Aufmerksamkeit gewidmet werden. Der Dienst muss mit allen möglichen und bekannten Mitteln geschützt werden.

Die kryptografische Tätigkeit des ETS muss mit einem HSM (Hardware Security Module) effektiv unterstützt und abgesichert werden. Der private Schlüssel muss für das Signieren der selbst ausgestellten ELGA-Authorisation Assertion im HSM aufgehoben werden.

Das ETS kommuniziert ausschließlich über das OASIS WS-Trust Version 1.4 Protokoll.

Das ETS muss darüber hinaus die Liste der vertrauenswürdigen Identity Provider führen, indem die Zertifikate, den öffentlichen Schlüssel der zugelassenen und daher vertrauenswürdigen IdP beinhaltend, dem ETS bekanntgegeben werden. Das ETS muss periodisch (jedoch nicht seltener als einmal je 12 Stunden) den entsprechenden OCSP oder

Revocation List kontaktieren, bevor über die Vertrauenswürdigkeit der präsentierten Signatur entschieden wird. Das ETS muss bei Verifikation der digitalen Signatur überprüfen, ob das verwendete Zertifikat dem behaupteten Identity Provider entspricht.

Das ETS muss so konfiguriert werden, dass bei Gefahr in Verzug, einem Identity Provider die zugesprochene Vertrauenswürdigkeit auch sofort entzogen werden kann.

Beim ETS muss die Liste aller ELGA-Bereichs URL/URN geführt werden, welche mit entsprechenden Community ID der ELGA-Bereiche tabellarisch zu verknüpfen sind. Die Liste muss bei der Ausstellung von ELGA Treatment-Assertion, sowie beim Ausstellen von ELGA User II und Mandate II Assertion herangezogen werden um den URL/URN der angesprochenen ELGA-Bereiche in das SAML-Element <AudienceRestriction> eingefügt werden kann.

Das ETS stellt pro ELGA-Bereich einen für den jeweiligen Bereich dedizierten ELGA Treatment Assertion oder User II bzw. Mandate II Assertion aus. Die Anzahl der *pro Registry Stored Query* ([ITI-18]) ausgestellten Token leitet sich von der PIX-Antwort der Z-PI ab. Nur ein ZGF-Akteur kann beim ETS eine ELGA Treatment Assertion, User II oder Mandate II Assertion anfordern, und zwar als RST via „*ActAs*“-Delegation.

Das ETS protokolliert die eigene Tätigkeit einerseits in Z-L-ARR und andererseits in das A-ARR. Die Z-L-ARR Protokollierung hat lückenlos zu erfolgen, die Ausstellung, Validierung und Stornierung von allen *ELGA Authorisation Assertion* muss aufgezeichnet werden. Im A-ARR hingegen ist nur das Ausstellen von ELGA Treatment Assertion, User II und Mandate II zu protokollieren (siehe diesbezüglichen Details im entsprechenden Protokollierungskapitel). Das ETS greift auf Z-L-ARR und A-ARR als Secure Node via TLS zu.

Dem ETS ist es erlaubt sowohl auf die KBS-Datenbank als auch auf die PAP-Datenbank direkt zuzugreifen. Dies ist in einer wesentlich höheren Performanz begründet.

Das ETS greift als Secure Node via TLS auf die Akteure Z-PI und GDA-I zu.

Das ETS muss hoch performant und hochskalierbar aufgebaut und konfiguriert werden, mit genügend Ressourcen für das Abfangen von eventuellen unvorhersehbaren Spitzenlasten. Bei der Schätzung der Last von ETS im Vollbetrieb sind die im Kapitel 13 (Mengengerüst) angeführte Werte heranzuziehen. Darüber hinaus ist die bereits bekannte Lastenverteilung existierender STS-Lösungen im Gesundheitswesen zu berücksichtigen. Dazu zählt das e-Card System der Sozialversicherung. Demnach muss ETS im Normalbetrieb eine Last von 50 bis 120 Anfragen pro Sekunde verarbeiten können. Kurzfristige Spitzen (0,15% der Gesamtjahreslast welche in einer einzigen Stunde anfällt) sind mit bis zu 500 Anfragen pro Sekunde vorstellbar.

9.1.3. Richtlinien für Umsetzung der Zugriffsberechtigungen

9.1.3.1. Allgemeines

Die Autorisierung in ELGA erfolgt per *default deny*-orientiert, d.h. ein Zugang muss explizit erlaubt werden, ansonsten wird er automatisch abgelehnt. Zugriffsberechtigungen in ELGA werden grundsätzlich auf drei Protokollebenen umgesetzt:

1. Alle miteinander kommunizierenden Akteure müssen sich auf Transport-Level (TLS) als ATNA Secure Nodes ausweisen (authentifizieren). Diese Regelung gilt ausnahmslos und verpflichtend.
2. Darüber hinaus wird für Akteure im ELGA-Kernbereich WS-Trust implementiert. Der Zugriff basiert auf *ELGA-Authorisation Assertions*, bzw. an diese *Assertions* geknüpfte Rollen und Attribute (sog. Claims). Grundsätzlich geht es auf dieser Ebene um ein System, das rollenbasierend Zugangseinschränkung umsetzt (*Role Based Access Control)*
3. Zugriffsautorisierungen auf **Gesundheitsdaten von Patienten** sind zusätzlich auch mit deklarativ kodierten Zugriffsrichtlinien (*XACML-Policies*) verbunden.

In der Tabelle 16 sind alle gemeinsam verwendeten Services aufgelistet und die entsprechenden Voraussetzungen für einen Zugang auf Ebene 2 (WS-Trust) und 3 (XACML-Policy) angeführt.

Tabelle 17 fasst in einer höheren Granularität in Matrix-Form die Zugangsbeschränkungen und Voraussetzungen auf allen drei Protokollebenen zusammen. Hierbei ist zu vermerken, dass ein ELGA-Anbindungsgateway Proxy (AGW) in Form eines Apache-Servers umgesetzt wird, welcher weder XACML-Richtlinien noch ELGA-Assertions verlangt. Diese Sicherheitsnachweise werden durch das AGW jedoch an die jeweiligen Targets weitergeleitet, wo die Prüfungen verbindlich stattfinden.

Tabelle 18 konkretisiert die Zugangseinschränkungen aufgrund der in den einzelnen ELGA-Assertions präsentierten ELGA-Rollen.

No.	Services	*Zugang, Authorisation via*	*XACML Policy-Enforcement*
1	ETS	HCP-Assertion User I Assertion Mandate I Assertion WIST-Assertion Trusted Identity Assertion	Nein
2	PAP (individuelle Berechtigungen)	User I Assertion (R/W) Mandate I Assertion (R/W) WIST-Assertion (W)	Nein
3	PAP (generelle Berechtigungen)	ELGA-Service Assertion (R/W)	Nein
4	A-ARR	User I Assertion (R) Mandate I Assertion (R) ETS-Service via Secure Node (W) ZGF-Service via Secure Node (W) PAP-Service via Secure Node (W)	Nein
5	KBS	HCP-Assertion (R*/W) User I Assertion (R) Mandate I Assertion (R)	Nein
6	AGW Proxy	Ohne Assertion, Secure Node	Nein
7	ZGF	HCP-Assertion User I Assertion Mandate I Assertion	Nein
8	Registry Repository (XDS/XCA)	Treatment-Assertion (R/W) User II Assertion (R) Mandate II Assertion (R)	Ja via PEP/PDP in ZGF
9	eMed-STS	HCP-Assertion	Nein
10	EMEDAT-1	HCP-Assertion (R)	Nein
11	PHARM-1	e-Med Treatment-Assertion (R/W) User II Assertion (R) Mandate II Assertion (R)	Ja via PEP/PDP in ZGF
12	Zentrale L-ARR	ELGA-Service Assertion (R)	Nein
13	GDA-I	Ohne Assertion, Secure Node (R)	Nein
14	Z-PI	• Grundsätzlich Secure Node (R/W) für PIF und PIX • HCP-Assertion für PDQ	Nein

Tabelle 16: ACS-Übersicht auf ELGA Service Provider. R – Nur lesend, W – nur schreibend, R/W – lesend und modifizierend, R - GDA darf die selbst eingebrachten Kontakte abfragen*

SAML	RGY RPY	PAP	KBS	A-ARR	ETS	e-Med	Portal	ZGF Init.	ZGF Resp.	AGW Proxy
IDA	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	SAML Nicht BENÖTIGT
HCP	Nein	Nein	R*/W	Nein	Ja	Nein	Nein	R/W + f(Role)	Nein	
TA	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	R+ f(Pol)	
TA e-Med	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	R/W+ f(Pol) + EIA	
U1A	Nein	R/W	R	R	Ja	Nein	R/W	R/W	Nein	
U2A	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	R+ f(Pol)	
M1A	Nein	R/W	R	R	Ja	Nein	R/W	R/W	Nein	
M2A	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	R+ f(Pol)	
WIST	Nein	W	Nein	Nein	Ja	Nein	Nein	Nein	Nein	
CYA	R/W	Nein	Nein	Nein	Nein	R/W	Nein	Nein	Nein	
ZGFSA	R/W	R/W	Nein	W	Nein	Nein	Nein	Nein	Nein	
Akteur										
ZGF I	Ja	Nein	Nein	W	Ja	Nein	Nein		Ja	
ZGF R	Ja	Nein	Nein	Nein	Ja	Ja	Nein	Nein		
ETS	Nein	R	R	Ja		Nein	Nein	Nein	Nein	Nein
Portal	Nein	Nein	Nein	Nein	Nein	Nein		Ja	Nein	Ja
AGW Proxy	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Nein	
D.C.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja

*Tabelle 17: ELGA-Zugangsmatrix für die Kombinationen „**Assertions** versus **Services**“ und „**Akteure** (im Besitz einer entsprechenden Assertion) versus **Services**“, R* - lesen nur die eigenen Kontakte*

Legende zur obigen Tabelle 17 allgemein:

- Farben
  - Grün markiert erlaubten Zugang durch Assertion Validierung (weitere Abhängigkeiten sind vermerkt)
  - Rot markiert direkten Zugriff auf Datenbankebene
  - Grau markiert physisch unmögliche Zugriffe oder Zugriff auf sich selbst
  - Orange markiert Zugang aufgrund TLS/Secure Node Authentication
  - Gelb markiert direkten Zugang vom Apache auf ZGF innerhalb des AGW
  - Schwarz sind grundsätzlich blockierte (Deny) Zugänge

- R – Read; lesender Zugriff mit angeführten Assertion erlaubt
- W – Write; schreibender Zugriff mit angeführten Assertion erlaubt
- f(Role) – Rollenabhängige Funktion entsprechend der im Codesystem OID 1.2.40.0.34.5.3 oder OID 1.2.40.0.34.158 erfassten Rollen
- f(Pol) – XACML-Policy gesteuerte Funktion, welche via PEP/PDP umgesetzt wird
- Nein – Zugriff ist grundsätzlich verweigert
- Ja – Zugriff ist grundsätzlich erlaubt (in der weiteren Verarbeitung wird über R oder W eine Entscheidung getroffen). Bei ETS bezeichnet dies die Berechtigung auf Issue bzw. Cancel RST.

Legende zur Tabelle 17 (Fortsetzung), SAML- und Akteur-spezifische Abkürzungen:

- **RGY** – XDS Registry
- **RPY** – XDS Repository
- **IDA** – Identity Assertion berechtigt über EAGW Proxy
  - auf ETS zuzugreifen um eine föderierte Identität anzufordern
- **HCP** – ELGA HCP Assertion berechtigt über EAGW-Proxy
  - Lesend und schreibend auf KBS zuzugreifen
  - auf der initiierenden ZGF Transaktionen anzustoßen
  - beim ETS TA anzufordern
  - beim eMED-STS eine e-Med-ID Assertion anzufordern
- **TA** – Treatment Assertion berechtigt
  - auf XDS-Registry oder Repository lesend und schreibend zuzugreifen soweit eine Community Assertion von der antwortenden ZGF ausgestellt wurde
  - auf e-Medikation lesend und schreibend zuzugreifen soweit eine Community Assertion von der antwortenden ZGF ausgestellt wurde. Wenn der Zugriff aufgrund e-Med-ID erfolgt, dann muss eine e-Med-ID Assertion zusätzlich dem ETS präsentiert werden. Das ETS erstellt anschließend eine eMed Treatment-Assertion.
  - auf eine antwortende ZGF zuzugreifen, welche XACML-Policy Beschränkungen berücksichtigt und umsetzt (Repsonding Policy)
- **ZGFSA** – Service Assertion angefordert von einem Service (Daemon) in ZGF
- **U1A** – User I Assertion berechtigt über EAGW-Proxy
  - auf PAP lesend und schreibend zuzugreifen
  - KBS lesen
  - A-ARR lesen
  - beim ETS U2A anfordern
  - am Portal angemeldet sein und arbeiten
  - bei zuständigen initiierenden ZGF Transaktionen zu starten
- **U2A** – User II Assertion berechtigt

- auf XDS-Registry oder Repository lesend zuzugreifen soweit eine Community Assertion ausgestellt wurde
- auf e-Medikation lesend zuzugreifen soweit eine Community Assertion ausgestellt wurde
- auf eine antwortende ZGF zuzugreifen, welche XACML-Policy Beschränkungen berücksichtigt und umsetzt (Repsonding Policy)

- **M1A** – Mandate I Assertion (wie U1A) jedoch für bevollmächtigte Vertreter
- **M2A** – Mandate II Assertion (wie U2A) jedoch für bevollmächtigte Vertreter
- **WIST** – WIST Assertion berechtigt
  - schreibend auf PAP zuzugreifen wobei rollenabhängige Einschränkungen gelten
  - beim ETS eine Mandate I Assertion anzufordern
- **CYA** – Community Assertion
  - auf XDS Registry, Repository oder auf e-Medikation (bzw. ELGA-Anwendungen) schreibend und lesend zuzugreifen
- **ZGF I** – initiierende (initiating) Zugriffssteuerungsfassade (BeS) ist als Secure Node konfiguriert für den Zugriff auf
  - ETS
  - XCA Akteur **ZGF R**
- **ZGF R** – antwortende (responding) Zugriffssteuerungsfassade (BeS) ist als Secure Node konfiguriert für den Zugriff auf
  - XDS Registry/Repository Akteure
  - E-Befunde (XDS-Registry, Repository)
  - E-Medikation (bzw. weitere ELGA-Anwendungen, soweit neu eingeführt)
- **ETS** – ELGA Token Service ist als Secure Node konfiguriert für den Zugriff auf
  - PAP
  - KBS
- **AGW** – ELGA Anbindungs-Gateway (Proxy) führt keine Assertion-Validierung durch. Zugriff aufgrund vertrauenswürdigen Secure Nodes (orange Markierung). Zugang zu
  - PAP
  - KBS
  - ETS
  - A-ARR
  - GDA-I
  - Z-PI (PDQ)
  - ZGF-I
- **EIA** – e-Med-ID Assertion (gilt nur für die ELGA-Anwendung e-Medikation)
- **D.C.** – Document Consumer (etwa ein GDA/KIS-System)

ELGA Rolle	PAP		e-Bef. CDA	e-Med	A-ARR	L-ARR	Z-L-ARR	KBS				Z-PI
	Indiv. Policy	Gener Policy						Amb	Stat	Entl	Del.	
GDA Arzt	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓
GDA Apotheke	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✓
GDA KH	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
GDA PH	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
Bürger Teilnehmer	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗
Regelwerk-Administrator	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Sicherheits-Administrator	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗
WIST	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
OBST	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓

✓ Schreiben aufgrund e-Card Kontaktbestätigung
✓ Schreiben, beliebige (auch e-Card) Kontaktbestätigung
✓ Nur lesen
✓ Nur Opt-out bzw. Re-Opt-In
✓ Lesen und schreiben
✗ Kein Zugriff

Tabelle 18: Zugriffsberechtigungsmatrix in Abhängigkeit von ELGA-Rollen. KH = Krankenhaus, PH = Pflegeheim, Amb = Ambulanter Kontakt, Stat = Stationärer Kontakt, Entl = Entlassung, Del = Kontakt Delegieren

Obige Tabelle ist wie folgt zu lesen. Beispiel erste Zeile (GDA Arzt) definiert die Berechtigungen eines ELGA-GDA in der Rolle Arzt (Code: 700 von OID 1.2.40.0.34.5.3). Demnach kann der GDA

- auf die Dienste des PAP überhaupt nicht zugreifen ✗.
- e-Befunde (CDA) kann lesen, erstellen und modifizieren (inklusive stornieren) ✓.
- e-Medikationsdaten können lesend und schreibend bearbeiten ✓.
- Hat kein Zugriff auf A-ARR ✗
- Kann Protokolldaten bezüglich der eigenen Tätigkeit aus dem lokalen ARR (L-ARR) anfordern und lesen ✓
- Hat keinen Zugriff auf die zentrale L-ARR ✗
- Bezüglich KBS/Kontaktbestätigungen
  - Einen ambulanten Kontakt kann er nur aufgrund einer e-Card Kontaktbestätigung melden ✓
  - In dieser Rolle darf er keinen stationären Kontakt melden ✗

- Entlassungsmeldung ist nicht erlaubt
- ambulante Kontakte können an ELGA-GDA delegiert werden

- Auf Z-PI darf lesend zugreifen (nur PDQ ist erlaubt, in der Tabelle nicht angeführt)

9.1.3.2. Zugriffsberechtigungen auf ELGA-Gesundheitsdaten

Jeder Zugriff auf ELGA-Gesundheitsdaten (siehe Positionen 7 und 10 in der Tabelle 16) wird basierend auf einer Kombination von generellen und individuellen Zugriffsberechtigungen geprüft, welche zum einen an die Rolle des ELGA-Benutzers geknüpft und zum anderen durch ELGA-Teilnehmer selbst in Bezug auf ihre medizinischen Daten individuell definiert werden. Wenn keine expliziten Berechtigungen eine konkrete Aktion betreffend existieren, darf diese nicht durchgeführt werden. Das System unterstützt das *Policy Based Access Control* Modell. Ziel des Berechtigungssystems ist es daher sowohl die Identität und Rolle des ELGA-Benutzers eindeutig zu verifizieren (Arzt, Apotheke etc.), als auch darauf basierende generelle und relevante individuelle, durch den ELGA-Teilnehmer festgelegte, Zugriffsberechtigungen umzusetzen.

In Anlehnung an Abbildung 17 wird der darin dargestellte ELGA-Bereich mit der soeben erklärten Autorisierungsfunktion des ELGA-Berechtigungssystems erweitert. Daraus resultiert das in der Abbildung 38 illustrierte Bild eines ELGA-Bereichs inklusive Berechtigungssystem (siehe BeS) welches in Form von zwischengeschalteten Komponenten (*Design Pattern Interceptor*) realisiert ist.

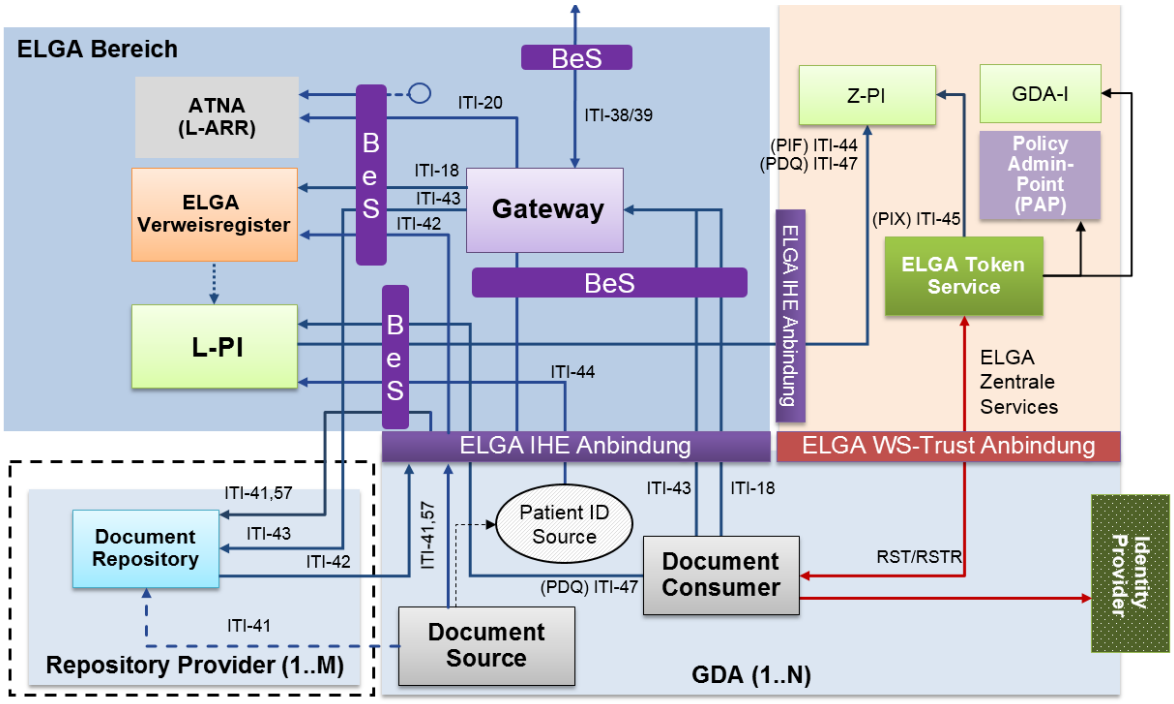


Abbildung 38: Zusammenspiel ELGA-Anbindung und ELGA-Berechtigungssystem (BeS)

Zugriffe auf personenbezogene medizinische Dokumente in ELGA werden durch eine Reihe von generellen und individuellen Zugriffsberechtigungen gesteuert. Durch Verordnung des Bundesministers für Gesundheit werden die generellen Zugriffsberechtigungen definiert, die festlegen, in welchen Rollen ELGA-GDA welche ELGA-Gesundheitsdaten verwenden dürfen.

ELGA-Teilnehmer steuern durch die Einräumung individueller Zugriffsberechtigungen die Zugriffe der einzelnen ELGA-GDA auf einzelne ELGA-Gesundheitsdaten.

Die ELGA eines ELGA-Teilnehmers enthält Verweise auf ELGA-Gesundheitsdaten, die in diversen Speichermedien bei ELGA-GDA elektronisch abgelegt sind. Der Zugriff auf die einzelnen Dokumente erfolgt mithilfe dieser Verweise.

ELGA-Teilnehmer besitzen folgende individuelle Steuerungsmöglichkeiten:

- Verweise auf ein Dokument ein- oder ausblenden
- Dokumente zum dauerhaften und unwiderruflichen Löschen freigeben
- Die Zugriffsdauer von ELGA-GDA ändern und zwar
  - nach einem bestätigten GDA-Besuch (Kontaktbestätigung liegt vor)

Die individuellen Zugriffsberechtigungen haben höhere Priorität als die generellen Zugriffsberechtigungen. Die formale Strukturierung von Zugriffsberechtigungen erfolgt entsprechend dem Standard *eXtensible Access Control Markup Language* (XACML) entwickelt durch die *Organization for the Advancement of Structured Information Standards* (OASIS).

Das ELGA-Berechtigungssystem setzt im Wesentlichen die generellen und individuellen Zugriffsberechtigungen um (Autorisierung) wie in Abbildung 38 vermerkt (siehe Komponenten markiert mit BeS = Berechtigungssystem). Abbildung 38 ist auf eine funktionale Darstellung beschränkt. Dem gegenüber verdeutlicht Abbildung 39 das ELGA-Berechtigungssystem als kompakte, einheitliche, logische (eventuell auch physische) Komponente, welche im unteren Teil des Bildes (siehe Inputs) die einzelnen IHE-Transaktionen unterstützt, diese in der Folge autorisiert und anschließend im oberen Teil an die entsprechenden Akteure weiterleitet.

9.1.3.3. Änderung der Zugriffsberechtigungen bei Opt-Out

Bei Opt-Out bzw. partiellem Opt-Out werden individuelle Berechtigungen im PAP nach folgendem Schema angepasst (wofür die Geschäftslogik vom PAP garantieren muss):

a. **Generelles Opt-Out**. Individuelle Berechtigungen des betroffenen ELGA-Teilnehmers werden ausnahmslos entfernt, und zwar

- Ausgeblendete Verweise auf einzelne Dokumente (CDA)
- Löschaufträge von einzelnen Dokumenten (CDA)
- GDA-zugriffeinschränkende Policies

- Partielle Opt-Out-Erklärungen

b. **Partielles Opt-Out nur von e-Befund**. Entsprechende individuelle Berechtigungen des betroffenen ELGA-Teilnehmers werden entfernt, und zwar:

- Ausgeblendete Verweise auf einzelne Dokumente (CDA) außer Medikationsliste
- Löschaufträge von einzelnen Dokumenten (CDA), außer Medikationsliste

c. **Partielles Opt-Out nur von e-Medikation**. Entsprechende individuelle Berechtigungen des betroffenen ELGA-Teilnehmers werden entfernt, und zwar:

- Ausgeblendeter Verweis auf die Medikationsliste
- Löschauftrag auf die Medikationsliste

d. **Gleichzeitiges partielles Opt-Out von e-Befund und e-Medikation**. Aus der Sicht der individuellen Berechtigungen ist dies derzeit wie ein generelles Opt-Out zu verstehen mit einer wichtigen Ausnahme. Beim Aufschalten einer neuen ELGA-Anwendung nimmt der ELGA-Teilnehmer automatisch daran teil (ohne jegliche individuelle Berechtigungen).

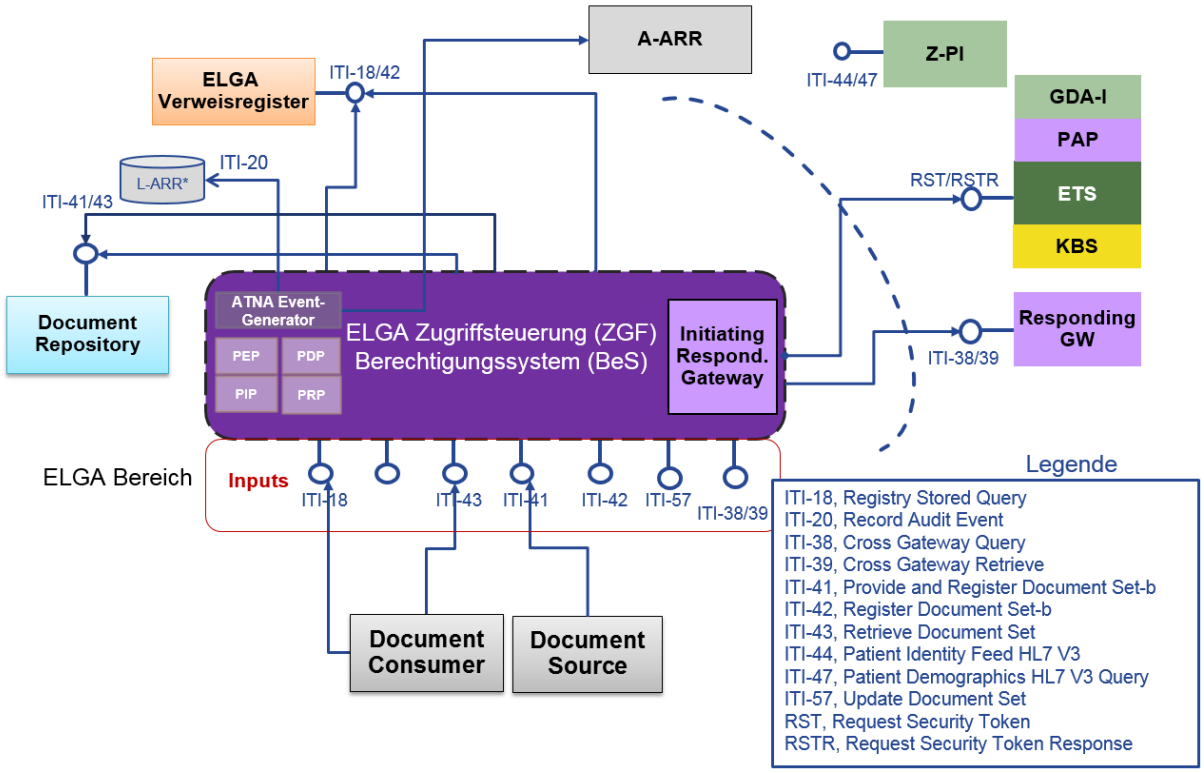


Abbildung 39: Das ELGA-Zugriffssteuerungsfassade als kompakte Komponente

Bezüglich der Zugriffsart wird zwischen regulärem Zugriff und Zugriff in Vertretung differenziert. Im Rahmen der vom e-Government bereitgestellten Services sind

Authentifizierungen Bevollmächtigter möglich. Folglich unterstützt das Berechtigungssystem Zugriffe solcher Bevollmächtigter. Die Ausstellung von *Authorisation-Assertions* in diesem Zugriffskontext erfordert die Identitätsverifikation des Bevollmächtigten (Person bzw. Organisation) und des Vollmachtgebers durch das ELGA-Berechtigungssystem.

Abbildung 40 stellt klar, dass die Zugriffssteuerungsfassade zweigeteilt ist. Es besteht grundsätzlich aus einem anfragenden (Initiating) Teil und aus einem antwortenden (Responding) Teil.

- Der antwortende Teil spielt ausschließlich bei XCA Transaktionen eine Rolle, indem er die Autorisierung der einkommenden Anfragen prüft und Policy Enforcement durchführt.
- Der anfragende Teil übernimmt aus dem angebundenen ELGA-Bereich alle Anfragen und leitet entsprechende XDS- oder XCA-Transaktionen ein (oder beides parallel). Darüber hinaus müssen XDS-Antworten auch entsprechend gefiltert werden.

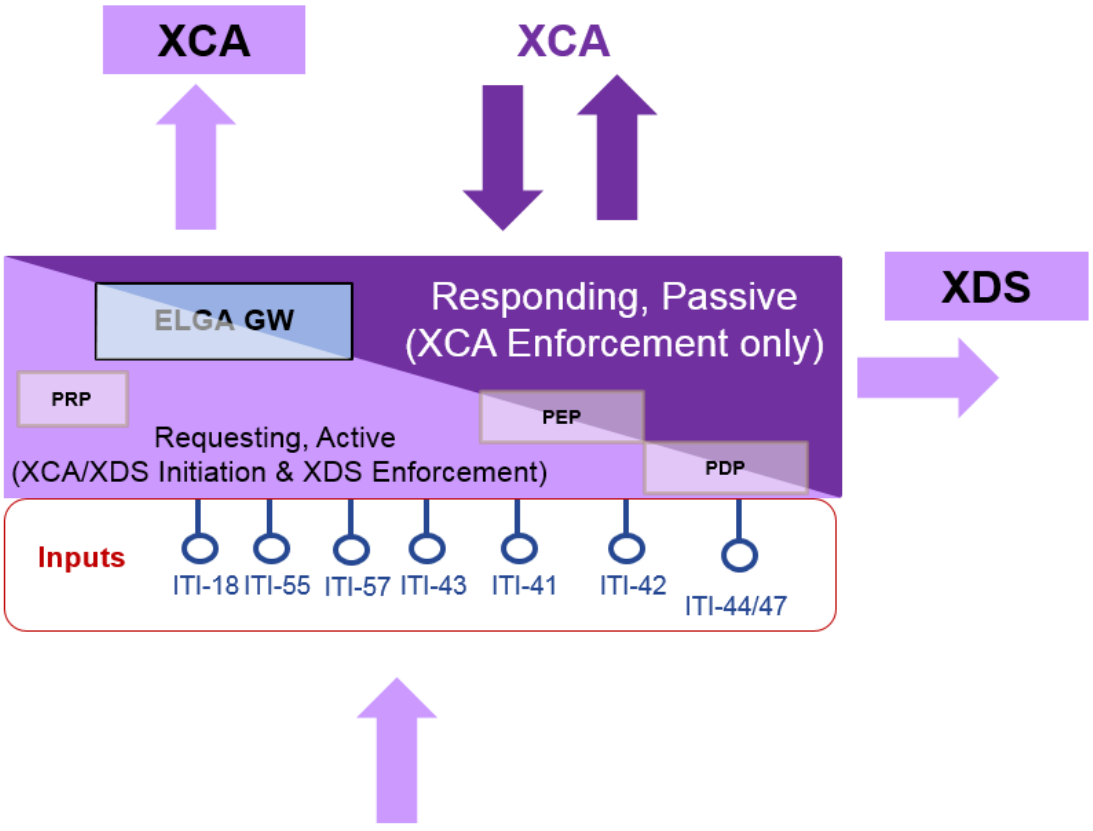
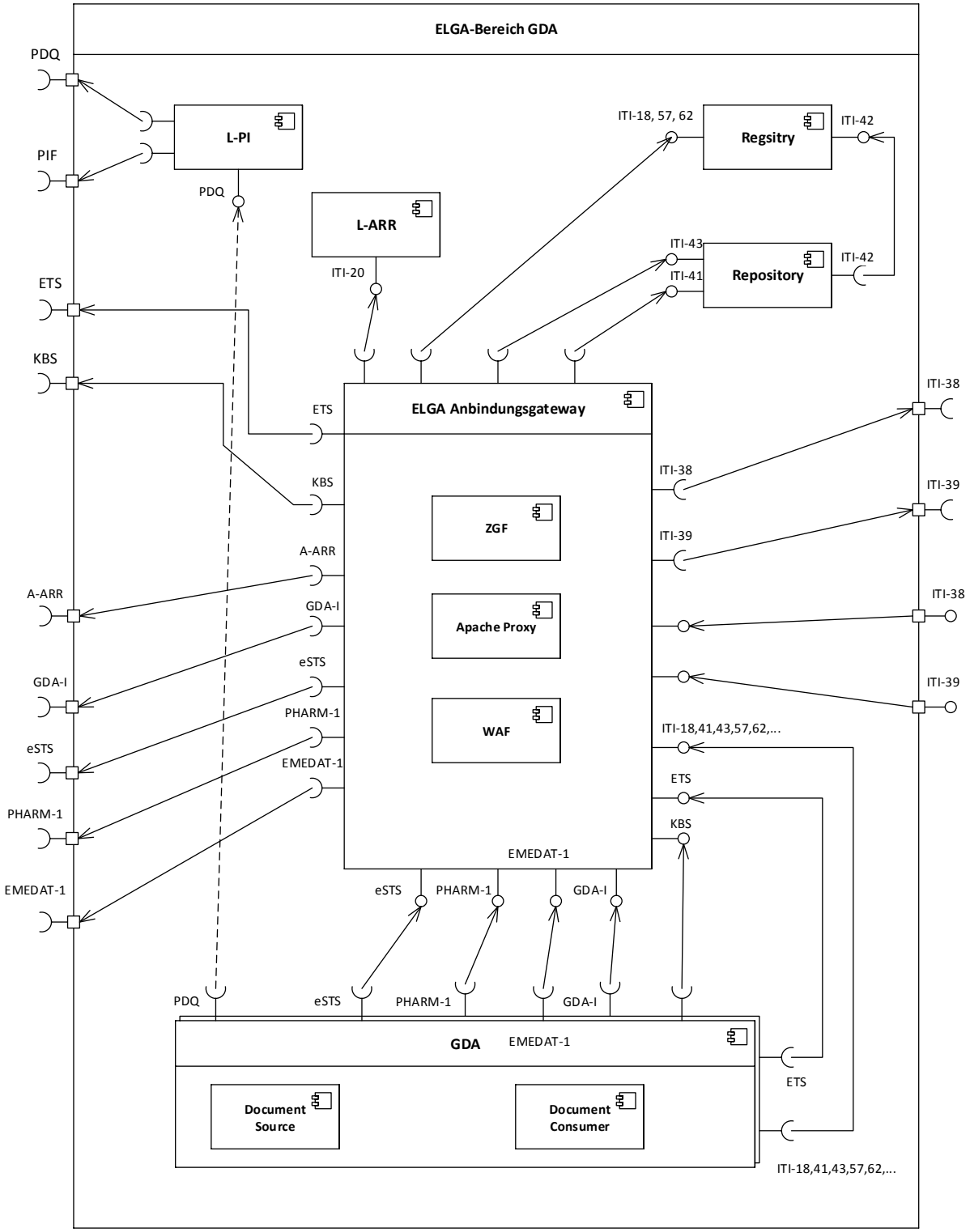


Abbildung 40: Berechtigungssystem bestehend aus anfragenden und antwortenden Teilen (ELGA-Zugriffssteuerungsfassade)

Eine Zugriffssteuerungsfassade (ZGF) ist in Form einer Virtuellen Maschine (VM) zu realisieren und auszuliefern. Diese VM bindet die einzelnen ELGA-Bereiche an die gemeinsame ELGA-Infrastruktur an. Die VM wird im Weiteren als ELGA-Anbindungsgateway (AGW) bezeichnet. Die AGW enthält grundsätzlich eine ZGF Instanz und weitere sicherheitstechnisch relevante Komponenten.

9.1.3.4. UML Komponentendiagramm eines ELGA-Bereiches

Die Abbildung 41 konkretisiert die Architektur eines ELGA-Bereiches, der über ein AGW in die gesamte ELGA-Infrastruktur eingebunden wird. Es wird damit verdeutlicht, dass die Anbindung der ELGA-GDA ausschließlich über eine Instanz der AGW realisiert ist. Das AGW ist das bereichsübergreifende Bindeglied zwischen den einzelnen ELGA-Bereichen (siehe ITI-38, 39) sowie der Proxy eines ELGA-Bereiches zu den zentralen Services. Ausnahme ist der lokale Patientenindex (L-PI), der laut Beschluss der Projektsteuerung auch direkt mit den entsprechenden zentralen Services des Z-PI verbunden werden kann, da die Client-Authentifizierung aufgrund ATNA Secure Nodes gewährleistet wird.



3718

3719

3720 *Abbildung 41: UML Komponentendiagramm eines ELGA-Bereichs*

9.1.3.5. UML Komponentendiagramm eines AGW

Das Innenleben des in der Abbildung 41 zentral dargestellten AGW ist in der Abbildung 42 aufgelöst. Es wird verdeutlichen, dass alle Inputs ausnahmslos über die Web Application Firewall (WAF) Komponente geleitet sind.

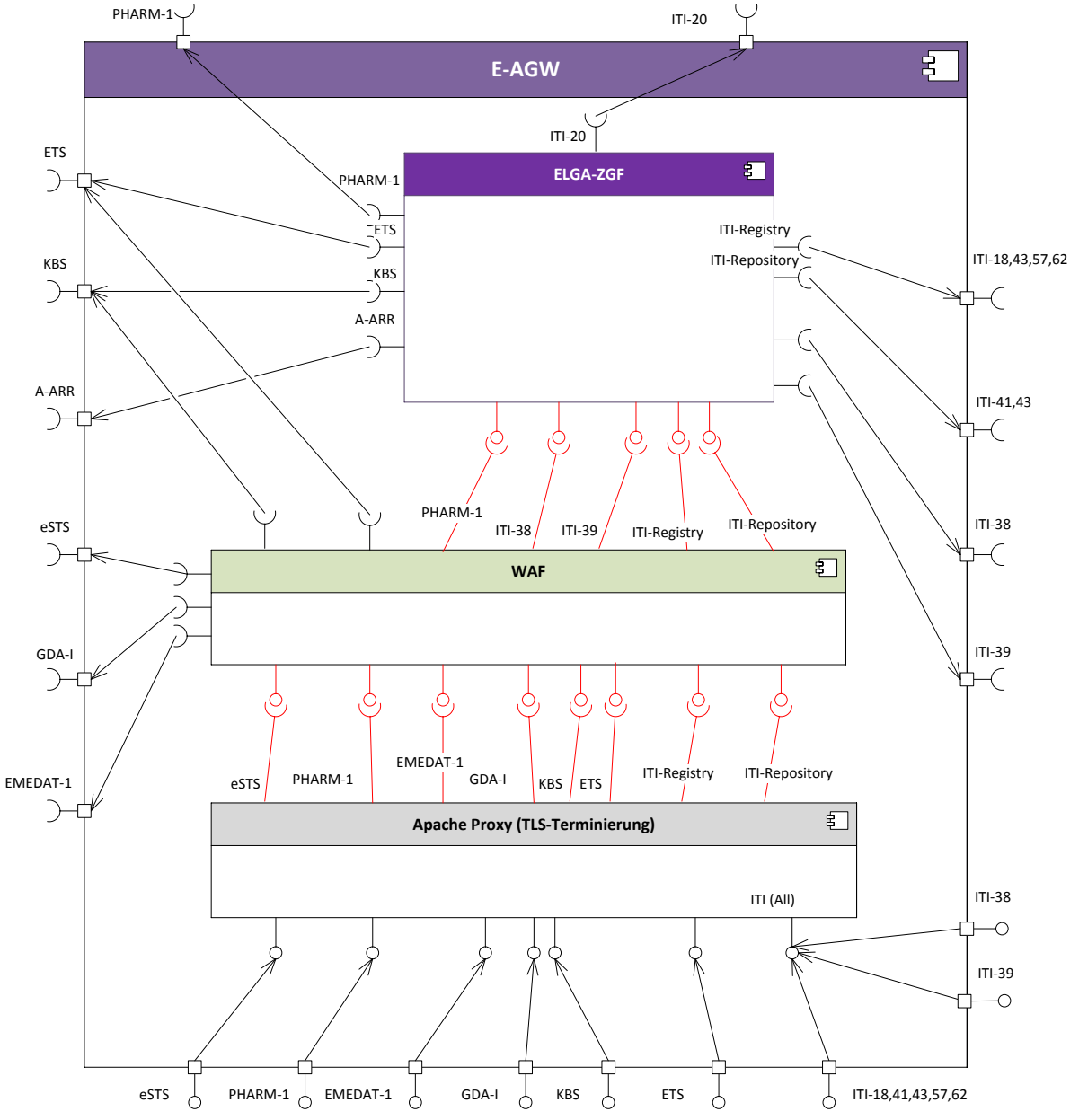


Abbildung 42: UML-Komponentendiagramm eines AGW. Rote Verbindungen sind unverschlüsselt, schwarze Verbindungen sind TLS.

Die Apache-Komponente terminiert die eingehenden TLS-Verbindungen und leitet die Anfragen an die WAF-Komponente weiter. Diese Proxy-Komponente ist so konfiguriert, dass

IHE-Anfragen für Gesundheitsdaten an die ZGF zur Verarbeitung weitergereicht werden. Sonstige Anfragen werden an die entsprechenden zentralen Services weitergeleitet. Hierfür wird für jeden Request eine neue TLS-Verbindung mit dem entsprechenden ELGA-Core Secure Node Zertifikat erzeugt. Damit wird garantiert, dass zentrale Komponenten ausschließlich über vertrauenswürdigen Quellen angesprochen werden. Die E-ZGF setzt laut Definition das vorgegebene Enforcement der Berechtigungen (XACML-Policies) durch und leitet die Anfragen intern (XDS) oder community-übergreifend (XCA) weiter. Diesbezüglich siehe näheres im nachfolgenden Kapitel über Autorisierung.

Anmerkung: Das AGW in der obigen UML-Abbildung repräsentiert die für die GDA-Bereiche typische Komponente. Darüber hinaus gibt es auch speziell vorkonfigurierte AGWs etwa für die Anbindung des Portals oder der e-Medikation. In der Portal-Konfiguration müsste die Zeichnung um die Schnittstellen für das Erreichen der PAP/A-ARR-Services erweitert werden.

Es muss darauf hingewiesen werden, dass die Validierungslast zwischen WAF und ZGF bzw. WAF und zentralen Komponenten abgestimmt und koordiniert werden muss, um drohende Performanceverluste durch unnötige Doppelgleisigkeiten zu vermeiden. Wenn WAF etwas per Definition geprüft hat, sollte die dahinter stehende Komponente (ZGF oder eine zentrale Komponente) dies nicht mehr wiederholen müssen.

9.1.3.6. XDS/XCA Zugriffsautorisierung

Der Zugriffskontrollmechanismus des ELGA-Berechtigungssystems wurde unabhängig von der Art des ELGA-Benutzers (u.a. ELGA-Teilnehmer, ELGA-GDA) konzipiert. Als Basis für dezentrale Zugriffsentscheidungen dienen Zugriffsberechtigungen, welche logisch zentral gespeichert und verwaltet werden. Diese Zugriffsberechtigungen werden einheitlich als Teil einer ELGA-*Authorisation-Assertion* strukturiert. Hierbei wird zwischen ELGA-*User-Assertion II* (im Fall des Zugriffs durch ELGA-Teilnehmer), ELGA-*Mandate-Assertion II* (im Fall des Zugriffs durch Bevollmächtigte) und ELGA-*Treatment-Assertion* (im Fall des Zugriffs durch ELGA-GDA) differenziert. Im Rahmen der Zugriffskontrolle kommen daher Berechtigungen, welche in Form von ELGA-User-/Mandate II bzw. Treatment-Assertion abgebildet sind, zum Einsatz.

Das primäre Ziel der Autorisierung ist es, Zugriff auf schützenswerte Ressourcen nur auf dafür berechtigte ELGA-Anwender (und Akteure) einzuschränken (Access Control – ACS). Mit schützenswerten Ressourcen sind im Allgemeinen folgende Kategorien und Akteure gemeint:

- XDS Registry
- XDS Repository
- ELGA-Anwendungen

Die oben aufgelisteten Ressourcen werden zwar vom ELGA-Berechtigungssystem in Form der ELGA-Zugriffssteuerung geschützt, es kann aber nicht ausgeschlossen werden, dass einzelne Instanzen zusätzliche Autorisierung verlangen, sei es wegen Protokollführung oder weil die angesprochenen Ressourcen in einer anderen, externen Sicherheitsdomäne (nicht ELGA) beheimatet sind. Letzteres ist der Fall für Registry und Repositories bei ELGA-Bereichen in der Konfigurationsvariante C (siehe hierfür die Erläuterung im nächsten Kapitel).

Die ELGA-Zugriffssteuerung (Access Control) stellt aus obigen Gründen bei unmittelbaren Zugriffen auf die genannten Ressourcen ein sog. *Community Assertion* (siehe vorheriges Kapitel) aus. Diese Assertion wird im Security Header der SOAP-Anfrage eingebettet. Die *Community Assertion* wird von einer internen STS-Komponente der ZGF ausgestellt und signiert. Zwischen ZGF-STS und der angesprochenen Ressource muss ein gültiges Vertrauensverhältnis aufgebaut werden können (öffentliche Schlüssel des Zertifikates für die Signatur muss bei der Ressource hinterlegt werden). Das Zertifikat ist ein ELGA-Bereichsspezifisches Zertifikat.

Die unten angeführte Auflistung gibt einen Überblick über die wesentlichen logischen Einheiten der Zugriffssteuerung:

- *Policy Enforcement Point* (PEP) ist im OASIS Standard XACML definiert. Er empfängt die an eine ELGA-Komponente (Verweisregister bzw. Repository) adressierte Anfrage eines *Document Consumers* und extrahiert daraus im Hinblick auf die Zugriffsautorisierung die für die Umsetzung der Zugriffsentscheidung notwendigen Attribute. Als nächstes werden alle Autorisierungsattribute durch den PEP zum Zweck der Entscheidungsfindung gesammelt an den PDP übergeben. Abschließend wird die durch den PDP übermittelte Zugriffsentscheidung durchgesetzt (d.h. zulassen, verweigern bzw. filtern).

- *Policy Information Point* (PIP) ist im OASIS Standard XACML definiert. Er liefert auf Anfrage des PEP optional weitere Attribute, die hinsichtlich einer Entscheidungsfindung durch den *Policy Decision Point* (PDP) benötigt werden.

- *Policy Decision Point* (PDP) ist im OASIS Standard XACML definiert. Er trifft die Entscheidung, ob der Zugriff auf eine Ressource gestattet wird oder nicht. Für die Evaluierung einer Zugriffsentscheidung werden die durch den PEP bereitgestellten Autorisierungsattribute herangezogen. Die resultierende Zugriffsentscheidung (zulassen bzw. verweigern) wird dem PEP als Antwort retourniert.

- *Policy Retrieval Point* (PRP). Der PRP (siehe RFC 2904; AAA Authorization Framework) ist eine funktionale Komponente des Berechtigungssystems und wird als Teil der Zugriffssteuerungsfassade logisch gemeinsam mit dem Konzept eines XCA Gateways als ELGA-Gateway umgesetzt. Die Notwendigkeit PRP zu definieren ergibt sich aus WS-Trust. Der PRP ist ein aktiver Client/Requestor, wie dies WS-Trust vorsieht. Er fordert

daher für alle bereichsübergreifenden und ggf. bereichsinternen IHE Transaktionen ELGA-*Treatment-Assertions* (Zugriff durch ELGA-GDA), ELGA-User-*Assertions II* (Zugriff durch ELGA-Teilnehmer) oder ELGA-Man*date-Assertions II* (Zugriff durch Bevollmächtigte) vom ETS an. Die jeweils ausgestellte *Authorisation-Assertion* repräsentiert die bereichsübergreifend föderierte Identität des ELGA-Benutzers und bildet darüber hinaus die Grundlage für die Zugriffsautorisierung aller Aktionen in ELGA. Der PRP empfängt initiierte Aktionen der ELGA-Benutzer und generiert ausgehend von beigefügten ELGA-*Authorisation-Assertions* Ausstellungs-Anfragen bezüglich darauf aufzubauender Treatment-Assertions bzw. *User-/Mandate-Assertions II*, um resultierend föderierte Identitätsbeziehungen zu schaffen (z.B. zwischen HCP-Assertion und *Treatment-Assertion*, zwischen *User-Assertion I & II*).

- *Policy Administration Point* (PAP) repräsentiert die Komponente, die in Verbindung mit dem ELGA-Portal als GUI dem ELGA-Teilnehmer die Möglichkeit sicherstellt, individuelle Zugriffsberechtigungen in ELGA zu definieren und zu verwalten. Über die vom PAP freigegebene Schnittstelle (Web-Service) können auch andere berechtigte Akteure (z.B. Widerspruchstelle) PAP-Funktionalität direkt ansprechen.

- *Facade-STS* ist ein von den angesprochenen bereichsinternen Ressourcen trusted Service (Komponente), welches Community Assertions ausstellt.

Das ELGA-Berechtigungssystem setzt sich somit einerseits aus dezentralen Zugriffssteuerungsfassaden mit integrierten ELGA-Gateways (eingebettet in ein ELGA-AGW), die in den ELGA-Bereichen umgesetzt sind, und andererseits aus dem zentralen ELGA-Token-Service (ETS) und dazugehörigen Komponenten und Services zusammen. Die oben beschriebenen Komponenten *Policy Enforcement Point*, *Policy Information Point, Policy Retrieval Point* sowie *Policy Decision Point* bilden die dezentrale Zugriffssteuerungsfassade eines ELGA-Bereichs. Diese Zugriffssteuerungsfassade stellt die einheitliche Autorisierung von Zugriffen authentifizierter ELGA-Benutzer auf medizinische Dokumente in ELGA gemäß den Vorgaben individueller und genereller Zugriffsberechtigungen ELGA-bereichsübergreifend sicher.

9.1.3.7. Autorisierte Dokumentensuche

Die autorisierte Dokumentensuche (siehe Abbildung 43) bzw. ein darauf folgender Abruf eines medizinischen Dokuments in ELGA gestaltet sich aus der Perspektive eines niedergelassenen ELGA-GDAs am Beispiel Vertragspartner und unter Nutzung der ELGA-Schnittstellen wie folgt (siehe detailliert weiter unten):

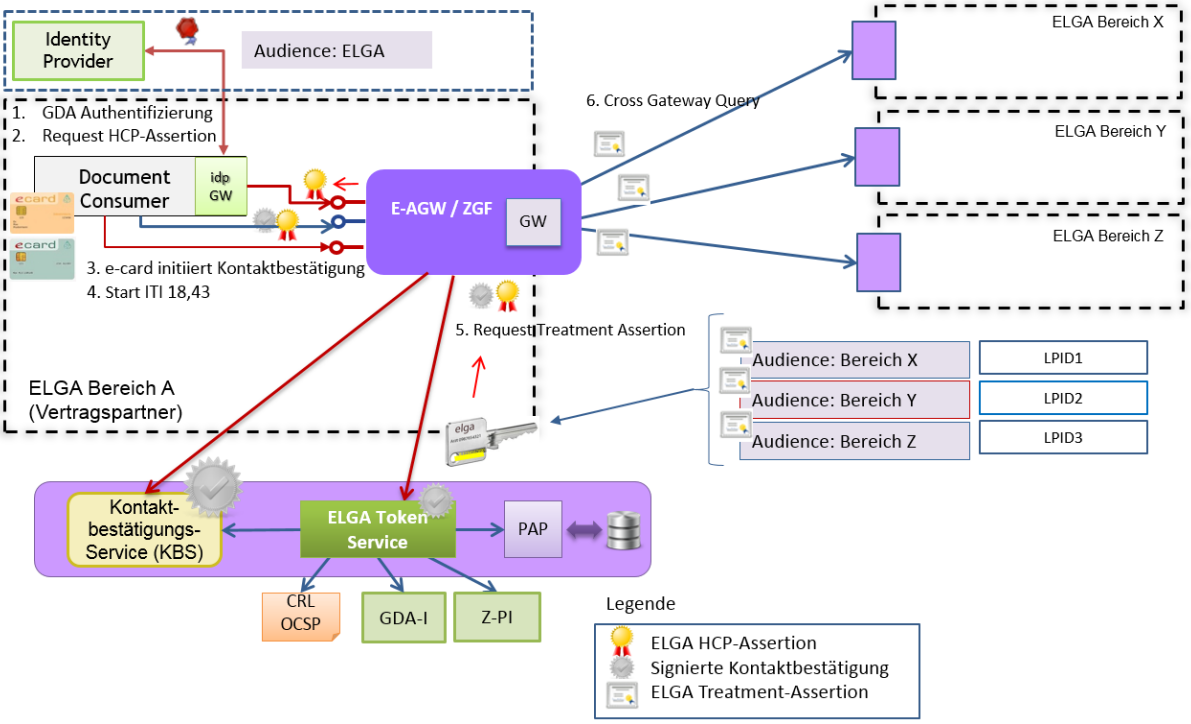


Abbildung 43: Autorisierung von GDA-Zugriffen in ELGA (Szenario für Vertragspartner). Schritt 1, GDA-Authentifizierung, Schritt 2 HCP-Assertion anfordern, Schritt 3 Kontaktbestätigung melden, Schritt 4 Registry Stored Query Transaktion starten, Schritt 5 Treatment Assertion anfordern, Schritt 6 Anfrage an entfernten ELGA-Bereiche senden.

Eine detailliertere Beschreibung der obigen Schritte:

1. Der ELGA-GDA fordert mit Hilfe der benutzten Software (eventuell via Identity Providing Gateway) im ersten Schritt eine ELGA-Identity-Assertion an. Er erhält diese nach Durchführung des entsprechenden Authentifizierungsverfahrens von seinem zuständigen (externen) IdP.

2. Die vom ELGA-GDA verwendete Software fordert im Hintergrund eine ELGA-*Healthcare Provider-Assertion* (HCP-Assertion) beim ELGA-Token-Service des Berechtigungssystems an (siehe IdP GW, Identity Providing Gateway). Dem ETS wird die vorher ausgestellte ELGA-Identity-Assertion übermittelt, die als Grundlage für die Ausstellung der HCP-Assertion dient. Die Kommunikation läuft über das im AGW eingebettete Proxy.

3. Das ETS validiert die ELGA-Identity-Assertion und verifiziert die Zulässigkeit (Vertrauensverhältnis und Signatur) des IdP. Es wird überprüft, ob der ELGA-GDA mit der angeforderten Rolle im GDA-Index registriert und für ELGA zugelassen ist. Zusätzlich wird die vom IdP verwendete ID des ELGA-GDAs (z.B. VPNR) durch die in ELGA zulässige OID des ELGA-GDAs ersetzt.

4. Resultierend wird eine ELGA-HCP-Assertion durch das ETS erstellt und an die anfordernde Software retourniert (via RSTR).

5. Der ELGA-GDA ist nun in ELGA angemeldet.

6. Ein Patient erscheint in der Ordination des obigen Vertragspartners und steckt seine e-card, wodurch eine Kontaktbestätigung beim e-Card System initiiert wird. Die vom e-card System signiert zurückgesendete Kontaktbestätigung wird vom GDA-System (Arztsoftware) dem zentralen KBS (Kontaktbestätigungsservice) via AGW prompt weitergeleitet.

7. Der behandelte Patient ist nun identifiziert und ein Arzt-Patient Behandlungszusammenhang bestätigt. Der ELGA-GDA startet eine patientenbezogene Dokumentensuche. Der Document Consumer Akteur übermittelt hierbei immer seine lokal aufgehobenen ELGA HCP-Assertion.

8. Die ZGF fängt die gesendete Nachricht ab, extrahiert daraus die HCP-Assertion und generiert anschließend die Anfrage einer Treatment-Assertion (*Request Security Token* RST), um diese an das ETS zu übermitteln.

9. Das ETS validiert die ELGA-HCP-Assertion.

10. Die Gültigkeit des Behandlungszusammenhangs (Kontakt) zwischen aufrufendem ELGA-GDA und betroffenen ELGA-Teilnehmer wird überprüft. ETS fragt hierfür beim KBS nach einer entsprechenden Kontaktbestätigung.

11. Im nächsten Schritt werden die ELGA-Bereiche, in denen der ELGA-Teilnehmer registriert wurde und die potentiell seine medizinischen Dokumente speichern, identifiziert (PIX-Query an Z-PI).

12. Basierend auf der Rolle des anfordernden ELGA-GDAs werden dessen generelle Zugriffsberechtigungen, sowie die durch den betroffenen ELGA-Teilnehmer festgelegten individuellen Zugriffsberechtigungen vom *Policy Administration Point* (PAP) abgefragt.

13. Abschließend werden die Identitätsinformation des Patienten, Identitäts- und Rolleninformationen des ELGA-GDAs, generelle und individuelle Zugriffsberechtigungen sowie generelle Zugriffsentscheidungen in Form von ELGA-bereichsspezifischen *Treatment-Assertions* (siehe Tabelle 15) einheitlich strukturiert und an die aufrufende ZGF retourniert (eine Assertion je ELGA-Bereich, in dem möglicherweise medizinische Dokumente des Patienten persistiert werden). Anhand der bekanntgewordenen Zugriffsberechtigungen (eingebettet in die Treatment-Assertions) kann die aufrufende ZGF bereits eine Vorentscheidung treffen und die Anfrage verweigern oder

weiterverarbeiten (ist z.B. der GDA vom ELGA-Teilnehmer gesperrt, kann die Anfrage mangels Zugriffsberechtigungen seitens GDA abgebrochen werden).

14. Als Nächstes wird die Anfrage des ELGA-GDAs bereichsintern (XDS) bzw. bereichsübergreifend (XCA) weiterverarbeitet.

15. Die ZGF des antwortenden ELGA-Bereichs nimmt die Anfrage entgegen, prüft auf Vorhandensein, Vertrauenswürdigkeit und Gültigkeit der ELGA-*Treatment-Assertion*.

16. Die ZGF extrahiert aus der Anfrage sowie der ihr beigefügten ELGA-*Treatment-Assertion* für den autorisierten Zugang relevante Teile, die sogenannten Claims (z.B. Identität des anfordernden ELGA-GDA, dessen Rolle, Identität des Patienten, Art des Zugriffs, Dokumentenklasse sowie individuelle Berechtigungen).

17. Bevor die Anfrage an ein ELGA-Verweisregister (bzw. Repository) weitergeleitet wird, erfolgt die Ausstellung und Einbettung einer Community Assertion durch die ZGF mit Hilfe des internen STS.

18. Das ELGA-Verweisregister (bzw. Repository) empfängt und verarbeitet die Anfrage. Im Security-Header der Anfrage ist eine Community Assertion eingebettet, die für Protokollierungszwecke verwendet werden kann. Die resultierende Antwort wird an das ELGA Responding-Gateway übertragen.

19. Die Steuerung wird nun an den *Policy Enforcement Point* PEP weitergeleitet, der eine Anfrage betreffend Zugriffsentscheidungen an den *Policy Decision Point* (PDP) sendet. Die Antwort wird auf, für das Zugangskontrollsystem relevante Teile mit den Autorisierungsattributen, überprüft.

20. Der PDP trifft basierend auf den durch den PEP übermittelten Autorisierungsinformationen und Zugriffsberechtigungen die Zugriffsentscheidung (z.B. Autorisierung von Zugriff auf ein konkretes Dokument) und teilt diese dem PEP mit.

21. Der PEP setzt die Zugriffsentscheidung um, indem die Antwort des ELGA-Verweisregisters entsprechend geblockt bzw. gefiltert oder ungefiltert an den anfragenden ELGA-Bereich (Initiating Gateway) weitergeleitet wird.

22. Die ZGF des anfragenden ELGA-Bereichs empfängt die Antwort und leitet diese an den anfragenden ELGA-GDA weiter. Das Ergebnis der ITI-18 Abfrage (insbesondere der Anwender-Kontext & gültige Berechtigungsregeln) wird für einen konfigurierbaren Zeitraum (z.B. Gültigkeitsdauer der entsprechenden HCP-Assertion) gepuffert, um für nachfolgende IHE ITI-43 (Retrieve Document Set) Transaktionen zu dienen

23. Der anfragende ELGA-GDA empfängt die zulässige Antwort auf die von ihm initiierte Anfrage.

24. Der ELGA-GDA hat nun ein beschränktes Zeitintervall (je nach ZGF-Konfiguration bis zu 30 Minuten) aus der in der ZGF gepufferten ITI-18 Ergebnisliste einen oder mehreren CDA auszuwählen und diese via ITI-43 anzufordern. Sollte der vorkonfigurierte Zeitraum überschritten werden, muss die vorher abgesetzte *Registry Stored Query* ([ITI-18]) wiederholt werden (entsprechende Fehlermeldung auf abgelaufenen Kontext-Puffer ist zu beachten).

***Anmerkung**: Zugriffsverletzungen (Access Violations) führen grundsätzlich auf den Schnittstellen des ELGA-Berechtigungssystems zu SOAP-Faults. Sonstige Fehler werden mit vorabgestimmten Returncodes (siehe die öffentliche IHE ITI Framework Unterlage Volume 3) den aufrufenden Akteuren signalisiert. Es ist die Aufgabe des jeweiligen GUI diese Transaktionsresultate entsprechend benutzerfreundlich an den interaktiven Anwender (GDA, Bürger, etc.) zu vermitteln. Individuelle Berechtigungen (Opt-Out, GDA wurde gesperrt, etc.) dürfen nicht an Dritte (GDA) weitergegeben werden! Der wahre Grund, warum ein GDA in ELGA keine Dokumente für den Patienten findet, darf nicht preisgegeben werden (außer Fehler aufgrund von technischen Defekten). Auch aus Sicherheitsgründen dürfen eventuelle Angreifer keine Fault-Details erfahren.*

Es ist zu vermerken, dass sich das obige Szenario leicht von einem Krankenhausszenario unterscheidet, wo die Aufnahme eines Patienten über die entsprechende administrative Stelle erfolgt. Siehe diesbezügliche Sequenzdiagramme in Abbildung 62 und Abbildung 63.

9.1.3.8. Autorisiertes Dokumentenupdate

Laut Datenschutzgesetz 2000, Artikel 1, §1 Absatz 3 Punkt 2 im Verfassungsrang, hat der ELGA-Teilnehmer das Recht auf Richtigstellung unrichtiger Daten. Dadurch muss das Berechtigungssystem erlauben, CDA Dokumente durch Berechtigte auch dann zu ändern, wenn keine gültige Kontaktbestätigung vorliegt, und/oder wenn das Dokument vom ELGA-Teilnehmer ausgeblendet bzw. der GDA-Zugriff beschränkt wurde. Eine Änderung (Update) des Dokumentes muss nur in folgenden Fällen untersagt werden:

- Dokument wurde vom ELGA-Teilnehmer gelöscht
- ELGA-Teilnehmer hat generelles Opt-Out erklärt
- ELGA-Teilnehmer hat partielles Opt-Out betreffend des Dokumentes erklärt

Eine Änderung des Dokumentes ist technisch über die ZGF wie folgt durchzuführen

- Storno des Dokumentes via ITI-57 (Metadata Update availability Status). Status des Dokumentes wird in der Registry auf "*deprecated*" gesetzt.
- Ersetzen (Replace - RPLC) von existierenden Dokumenten via ITI-41/42 *Provide and Register DocumentSet*. Damit wird eine neue Version des Dokumentes geschrieben und die vorherige Version des Dokumentes auf „*deprecated*" gesetzt.

Obige Transaktionen können im Besitz eines gültigen Schlüssels gestartet werden, welcher das zu stornierende bzw. zu ersetzende Dokument eindeutig identifiziert. Es werden zwei Möglichkeiten betrachtet. Änderung im Besitz der *entryUUID* oder der *setId* (vermerkt in *referenceIdList*) des Dokumentes. Seitens Registry- oder Repository-Akteure gibt es keinen Unterschied zwischen einem regulären Update (mit gültigem Kontakt) oder einem irregulären ohne gültigen Kontakt. In beiden Fällen erfolgt ein Zugriff seitens ZGF mit einer ELGA Community-Assertion. Somit ist die ZGF in der Lage, bei Update (Storno oder RPLC) die ETS-Entscheidung zu revidieren und übersteuern. Die ZGF lässt sich regulär (im Besitz einer gültigen Treatment-Assertion) oder außerordentlich (ETS hat keine Treatment-Assertion erlassen) eine Community-Assertion ausstellen, mit der dann der eigentliche Zugriff auf das Backendsystem erfolgt.

Beim Update von Dokumenten in der Registry & Repository ist darauf zu achten, dass der ELGA-Hashwert in der Registry ungebrochen bleiben muss. Um dieses Kriterium zu erfüllen, müssen zusätzliche sogenannte Kompensationstransaktion seitens ZGF durchgeführt werden. Ohne Kompensationstransaktionen wird z.B. ein Dokumentenstorno (via ITI-57) so durchgeführt, dass der Status des zu stornierenden Dokumentes zwar auf „*deprecated*" gesetzt, der ELGA Hash-Wert aber nicht entsprechend aktualisiert wird. Der unveränderte Hash-Wert reflektiert in diesem Fall den vorherigen Status „*approved*" anstelle des neuen Status „*deprecated*". Somit wäre der Hash gebrochen und die Metadaten ungültig.

Der genaue Ablauf von Dokument-Änderungen und Kompensationstransaktionen ist in der Tabelle 19 zusammengefasst.

3980

	entryUUID	setId (referenceIdList)
Storno via [ITI-57]	1. ZGF macht ein ITI-18 GetDocuments auf das zu stornierende Dokument 2. SubmissionSet (insbesondere AuthorInstitution) wird auf Übereinstimmung verglichen 3. ZGF errechnet den zukünftigen ELGA-Hash (auf den neuen Status = deprecated) 4. ZGF integriert zusätzlich zum ITI-57 Metadata Update availabilityStatus den berechneten ELGA-Hash	1. ZGF macht ein ITI-18 FindDocuments auf das zu stornierende Dokument 2. SubmissionSet (insbesondere AuthorInstitution) wird auf Übereinstimmung verglichen 3. ZGF errechnet den zukünftigen ELGA-Hash (auf den neuen Status = deprecated) 4. ZGF integriert zusätzlich zum ITI-57 Metadata Update availabilityStatus den berechneten ELGA-Hash
Replacement (RPLC via [ITI-41/42])	1. ZGF macht ein ITI-18 GetDocuments auf das alte Dokument 2. Metadaten des gefundenen Dokumentes werden mit den Metadaten vom Submission Set verglichen 3. Zukünftigen ELGA-Hash errechnen (auf den neuen Status = deprecated) 4. ITI-57 MetadataUpdate (ELGA-Hash) auf das alte Dokument ausführen. 5. ZGF schickt RPLC (ITI-41) an das Bereichsrepository weiter. Dadurch sollte aus dem alten approved Dokument ein deprecated werden und der Hash sollte OK sein.	1. ZGF macht ein ITI-18 FindDocuments auf das alte Dokument 2. Metadaten des gefundenen Dokumentes mit den Metadaten vom Submission Set verglichen 3. Zukünftigen ELGA-Hash errechnen (auf den neuen Status = deprecated) 4. ITI-57 MetadataUpdate (ELGA-Hash) auf das alte Dokument ausführen. 5. ZGF schickt RPLC (ITI-41) an den Bereichsrepository weiter. Dadurch sollte aus dem alten approved Dokument ein deprecated werden und der Hash sollte OK sein.

3981 *Tabelle 19: Schritte der ZGF beim Ändern von CDA*

3982 9.1.3.9. Proxy-Richtlinien für den Zugriff auf ELGA-Komponenten

3983 Spezifische Eigenschaften und interne Sicherheitsrichtlinien einzelner ELGA-
3984 Komponentenbetreiber erfordern maßgeschnittene Zugriffsrichtlinien, die in den vorherigen
3985 Überlegungen bereits angedeutet sind. In diesem Kapitel werden diese Erkenntnisse
3986 übersichtshalber noch einmal fokussiert zusammengefasst.

Grundsätzlich gilt, dass alle GDA/IHE Document Consumer und Document Source Akteure über die dafür freigegebenen IHE-Schnittstellen (URL-Endpunkte) der zuständigen AGW/ZGF Instanzen angebunden sind. Präzise aufgelistet geht es um die folgenden Transaktionen:

- Registry Stored Query ([ITI-18])
- Provide and Register Document Set ([ITI-41], [ITI-42]])
- XDS Metadata Update / Storno ([ITI-57])
- Retrieve Document Set ([ITI-43])
- Patient Demographic Query ([ITI-47]) bei direkten Z-PI Anfragen

GDA Document Consumer und Document Source Akteure greifen auf die Dienste der zentralen ELGA-Komponenten immer über die vorgeschalteten AGW (Proxy-) Instanzen zu. Gemeint sind folgende Transaktionen und Aufrufe:

- WS-Trust Zugriffe auf ETS und KBS
- Web Service Zugriffe auf GDA-I

L-PI Akteure in den einzelne ELGA-Bereichen greifen auf die Dienste von Z-PI direkt zu, und zwar:

- Patient Identity Feed ([ITI-44])
- PDQ-Query ([ITI-47])

Die speziellen Akteure ELGA-Portal und e-Medikation greifen auf ELGA-Services wie die angeführten IHE Document Consumer Akteure zu mit der Ausnahme von PDQ. Für diese beiden Akteure ist es erlaubt *Patient Demographic Query* Transaktionen direkt (ohne AGW Proxy) an den Z-PI zu stellen. Darüber hinaus greift das Portal auf die Dienste der A-ARR Komponente ausschließlich über die vorgeschaltete AGW Proxy Instanz.

Ein WIST-Akteur agiert ohne vorgeschalteten AGW Proxy und greift auf die zentralen Dienste von ETS und PAP direkt zu. Darüber hinaus nutzt WIST für Z-PI/PDQ-Abfragen einen internen Zugang, welcher auch für das Clearing Verwendung findet.

9.1.4. Konfiguration des ELGA-Anbindungsgateways/der Zugriffsteuerungsfassade

Die Zugriffssteuerungsfassade (in ein AGW eingebettet) ist eine dem ELGA-Bereich vorgeschaltete Sicherheitskomponente, welche auf Basis des Interceptor Design-Patterns realisiert ist. Typischerweise schützt die Zugriffssteuerungsfassade die Zugriffe auf die XDS Registry und Repositories im ELGA-Bereich.

Die ZGF ist in eine Virtuelle Maschine (VM) eingebettet. Die VM wird auch als ELGA-Anbindungsgateway bezeichnet. Die Inputs-Outputs werden von der VM kontrolliert. Alle eingehenden Anfragen werden zuerst an den, im AGW vorhandenen, internen Apache Server weitergeleitet (Abbildung 44). Diese Komponente muss wie ein Proxy vorkonfiguriert werden. Bestimmte Anfragen werden exklusiv an die ZGF geleitet; andere Anfragen werden terminiert und anschließend an externe Komponenten weitergeleitet. Die IHE-Anfragen ITI-18, 41, 42, 43, 57 werden immer an die ZGF weitergegeben.

Anfragen, die an zentrale Komponenten (ETS, KBS, GDA-I, etc.) gerichtet sind, werden vom VM-internen Apache Server terminiert und über einen Web Application Firewall (WAF) geführt. Anschließend wird eine neue TLS-Verbindung zu den zentralen Komponenten aufgebaut. Das AGW authentifiziert sich mit dem eigenen ATNA Secure Node Zertifikat, der von der ELGA Core-PKI ausgestellt ist. Diese Vorgehensweise gewährleistet, dass mit den externen (zentralen) Komponenten ausschließlich ein vertrauenswürdiger (trusted) ATNA Secure Node kommuniziert. Die entsprechenden Server (ZGF-) Zertifikate sind auch von der ELGA Core-PKI auszustellen.

An die VM angeschlossene GDA-Systeme (und sonstige IHE Akteure) müssen nur gegenüber der eigenen AGW/VM getrustet werden. Die VM bürgt für die weitergeleiteten Anfragen der angeschlossenen Clients (GDA-Systeme). Die Vertrauenswürdigkeit nach oben (zentrale und externe Komponenten) und nach unten (angeschlossene Akteure) ist mit Client/Server Zertifikaten konfiguriert (siehe auch Kapitel 3.13).

Die Ausgänge (Outputs) werden über die virtuelle Netzwerkkarte der VM geschleust. Die VM wird mit mehreren Netzwerkkarten ausgestattet bzw. vorkonfiguriert werden. Diesbezügliche Details sind im AGW Servicehandbuch nachzulesen. Wenn Registry und Repository angeschlossen werden, dann ist es sinnvoll diese Ressourcen über eine dedizierte Netzwerkkarte der VM direkt anzubinden. Dadurch wird die eigentliche Schutzfunktion, die Zugriffssteuerung gegenüber der eigentlichen schützenswerten Ressourcen (Registry & Repository), unmittelbar umgesetzt.

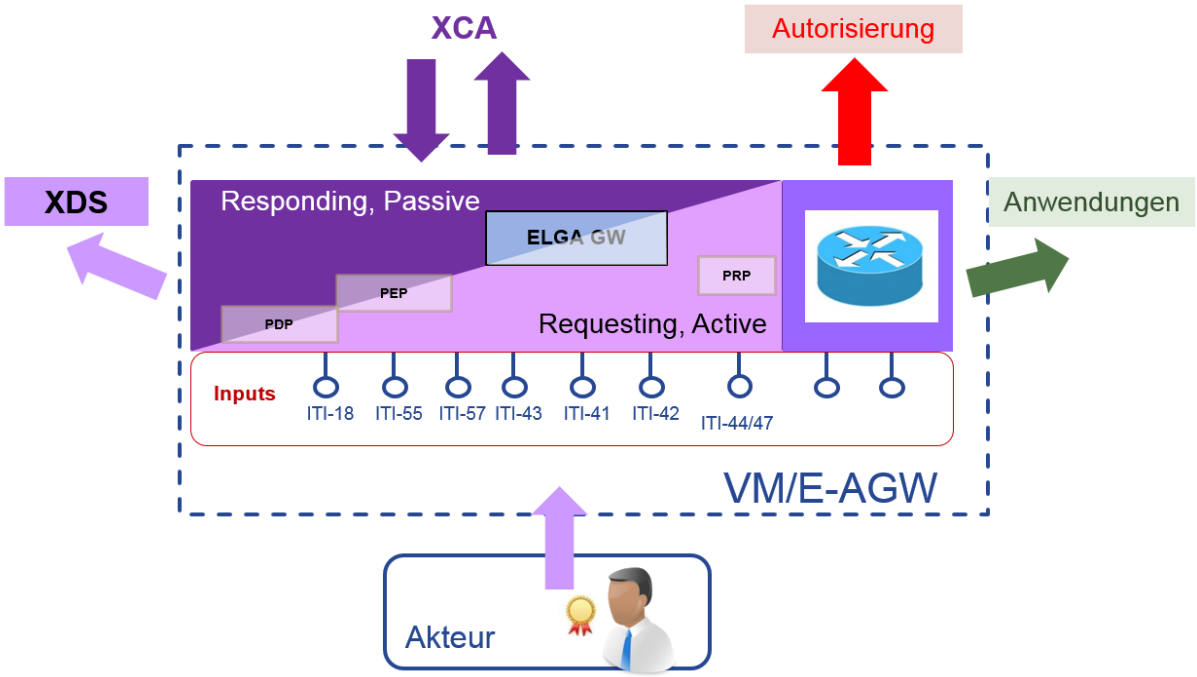


Abbildung 44: Zugriffssteuerungsfassade eingebettet in eine Virtuelle Maschine (ELGA-Anbindungsgateway) mit Proxy-Funktionalität.

Außerdem muss ein ELGA Bereichsbetreiber entscheiden, ob die am Output hängenden Ressourcen (Registry & Repository) ausschließlich für ELGA bestimmt sind oder auch andere (interne) e-Health Anwendungen zugreifen dürfen. Aus dieser Sicht sind die in der Tabelle *20* aufgezählten und in der Abbildung 45 dargestellten XDS-Konfigurationen erlaubt. Konfigurationen 4 und 5 sind speziell zur Anbindung von ELGA-Portal und e-Medikation erforderlich. *EBP* und *Read-Only* unterscheiden sich, da das *EBP* auch PAP lesen/schreiben und A-ARR lesen darf, Read-Only aber nicht.

In jeder hier angeführten XDS-Konfiguration muss ein für ELGA bestimmtes Dokument über die ZGF in ELGA veröffentlicht werden. Das Veröffentlichen wird von der ZGF mitprotokolliert und die Protokolle über das ELGA-Portal für ELGA-Teilnehmer zugänglich gemacht.

No.	Konfiguration	XDS Registry	Repository	Variante
1	XDS-Standard (Full Control)	*Read & Write*	*Read & Write*	*A*
2	XDS-Custom	***C**ustom*	*Read-Only*	*C*
3	Read-Only GDA Zugang (ROZ)	*Kein*	*Kein*	*ROZ*
4	e-Medikation	*Read & Write*	*Read & Write*	*eMed*
5	ELGA-Portal	*Kein*	*Kein*	*EBP*

Tabelle 20: Grundlegende XDS-Konfigurationsmöglichkeiten der Zugriffssteuerungsfassade (siehe auch grafisch in der Abbildung 45)

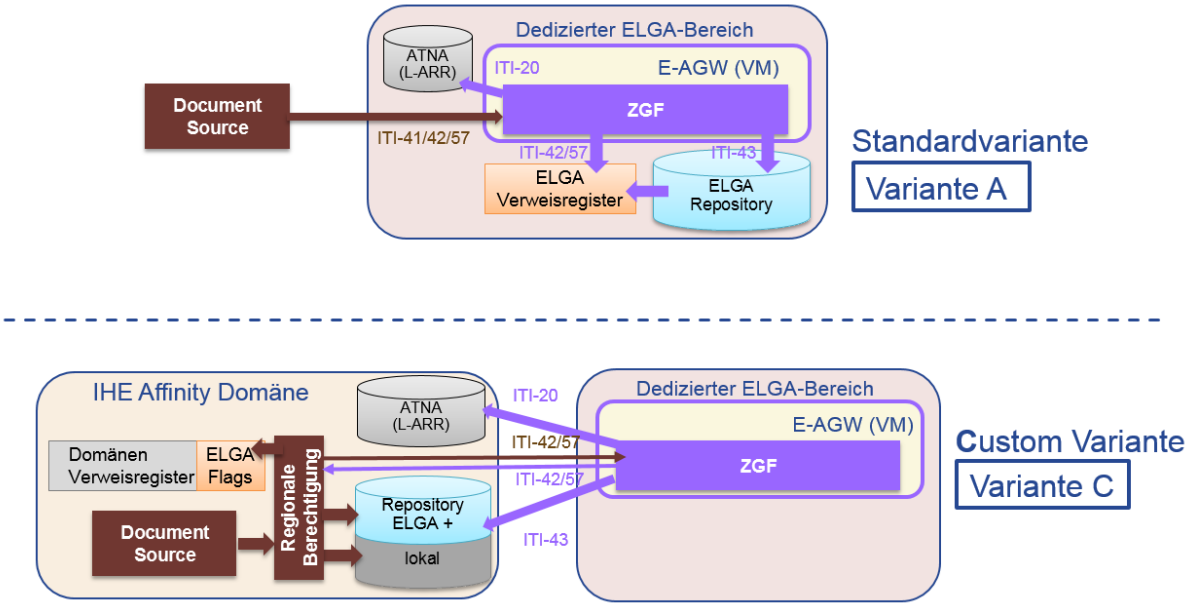


Abbildung 45: Zugelassene XDS Konfigurationsmöglichkeiten der Zugriffssteuerung grafisch dargestellt (siehe auch Tabelle 20)

9.1.4.1. Standardvariante A mit dediziertem ELGA Registry und Repository

Standardvariante „*ELGA full control*“ Konfiguration (**Variante A**, Abbildung 45) bestehend aus einem für ELGA dedizierten ELGA-Verweisregister und einem ELGA-Repository. Enthält ausschließlich Kopien der ELGA-relevanten Gesundheitsdaten und ist in der exklusiven Transaktionsverwaltung der ZGF. Administrative Zugriffe (seitens L-PI) auf die Registry müssen jedoch erlaubt werden. Das Einbringen der ELGA-relevanten Dokumente kann direkt oder indirekt über die ZGF erfolgen.

- **Direkt via ZGF**: Document Source sendet Provide and Register Document Set [ITI-41] unmittelbar über die ZGF. Die ZGF übernimmt die Anfrage, überprüft die entsprechenden individuellen Berechtigungen des betroffenen Patienten und entscheidet, ob das Dokument in ELGA veröffentlicht werden darf. Über einige ausgewählte Attribute der zu registrierenden Metadaten wird zusätzlich eine Prüfsumme in Form eines Hashwertes erzeugt und die Anfrage mitprotokolliert.
- **Indirekt via ZGF**: Document Source sendet Provide and Register Document Set [ITI-41] an ELGA-Repository, ELGA-Repository sendet [ITI-42] an ELGA-Registry (ZGF wird überbrückt). Danach wird der Satz via [ITI-57] Association Type „*NonVersioningUpdate*“ in ELGA veröffentlicht. Sollte wegen individuell gesetzten Zugangseinschränkungen das Einbringen des Dokumentes vom Berechtigungssystem untersagt werden, muss das Dokument vom Repository unbedingt gelöscht werden. Diese Aufgabe lastet auf dem Einbringer des abgelehnten Dokumentes.

ELGA-relevante lesende IHE-Transaktionen (insbesondere ITI-43, 18) werden in beiden Fällen ausschließlich über die ZGF geleitet bzw. von der ZGF durchgeführt. Nicht ELGA-relevante lesende administrative Zugriffe bedingt durch **Clearing** müssen nicht über die ZGF geführt werden (siehe detailliert im Kapitel 9.7 Clearing in ELGA).

Die so um den Hashwert erweiterten Metadaten werden anschließend via regulärer Transaktionen ([ITI-42]) an das für ELGA dedizierte ELGA-Verweisregister weitergeleitet. Bei lesenden Transaktionen überprüft die ZGF die Metadaten auf Integrität mithilfe des ELGA-Hashwertes.

9.1.4.2. Custom Konfigurationsvariante XDS-Registry mit ELGA-Flag

Die „*Custom*“ Konfiguration (**Variante C**, Abbildung 45) ist nur eine View einer internen Affinity Domäne, welcher durch das Flaggen (ELGA-Flag) der Metadaten der betroffenen XDS-Registry erzielt wird. Es gibt weder ein dediziertes ELGA-Repository noch dedizierte ELGA-Verweisregister. Das Einbringen der ELGA-relevanten Dokumente kann auch hier direkt oder indirekt via ZGF erfolgen.

- **Direkt via ZGF**: Document Source sendet Provide and Register Document Set [ITI-41] an ein bereichsinternes Repository. Repository registriert das Dokument via [ITI-42] unmittelbar über die ZGF. Wenn individuelle Berechtigungen das Veröffentlichen in ELGA erlauben, erzeugt die ZGF ein ELGA-Flag das auf True gesetzt und in die Metadaten integriert wird. Wenn das Dokument nicht veröffentlicht werden darf, weil individuelle Berechtigungen dies verhindern, wirft entweder die ZGF einen SOAP-Fault oder es wird der ELGA-Flag explizit auf FALSE gesetzt. Die gewählte Strategie ist vom Bereichsbetreiber zu bestimmen und via ZGF-Konfiguration zu bewirken.
- **Indirekt via ZGF**: Document Source sendet Provide and Register Document Set [ITI-41] an ein Repository. Repository sendet [ITI-42] an den Registry (ZGF wird überbrückt). Danach wird der Satz via [ITI-57] Association Type „*NonVersioningUpdate*“ in ELGA veröffentlicht. Die ZGF übernimmt die Anfrage, überprüft die entsprechenden individuellen Berechtigungen des betroffenen Patienten und entscheidet, ob das Dokument in ELGA veröffentlicht werden darf. Wenn individuelle Berechtigungen das Veröffentlichen in ELGA erlauben, erzeugt die ZGF ein ELGA-Flag das auf True gesetzt und in die Metadaten integriert wird. Wenn das Dokument nicht veröffentlicht werden darf, weil individuelle Berechtigungen dies verhindern, wirft die ZGF einen SOAP-Fault.

Eine schreibende ELGA IHE-Transaktion Provide and Register Document Set ([ITI-41]) wird weder unterstützt noch durchgelassen. Wird dennoch eine solche Anfrage an die Zugriffssteuerungsfassade gestellt, wird diese mit einem Fehler (etwa *Acces Denied*) beantwortet.

Der Unterschied zwischen beiden Szenarien (direkt oder indirekt) liegt in der gewählten Strategie bei der Registrierung der Dokumente in ELGA via ZGF.

Die Anfragen werden immer mitprotokolliert.

Beim Lesen via *Registry Stored Query* seitens ELGA werden nur die mit dem ELGA-Flag auf True gesetzten Einträge (Sätze) an die Zugriffssteuerungsfassade übermittelt. Die ZGF überprüft die Metadaten mithilfe der Prüfsumme um eventuelle Manipulationen zu entdecken.

Es ist wichtig anzumerken, dass ein Datensatz in einem beliebigen Verweisregister, der mit dem ELGA-Flag TRUE gekennzeichnet ist, in ausschließlicher Hoheit des ELGA-Berechtigungssystems liegt. Als Konsequenz, darf nur das ELGA-Berechtigungssystem über die ZGF den entsprechenden Datensatz manipulieren oder verändern.

9.1.4.3. Umsetzung der Anwendungsfälle, die mit dem Löschen von ELGA-Daten verbunden sind

Anwendungsfälle, deren Umsetzung mit explizitem Löschen von ELGA-Daten verbunden ist, fasst der Anwendungsfall ET.1.3 zusammen. Hierbei geht es um zwei Sub-Anwendungsfälle:

1. **Löschen eines einzelnen CDA-Dokumentes** im Auftrag des berechtigten ELGA-Teilnehmers. Hierfür wird eine XACML-Policy mit der Liste der zum unwiderruflichen Löschen freigegebenen Dokumente gespeichert. Die Policy wird sofort aktiviert, indem die vom ELGA-Teilnehmer vermerkten Dokumente vom Berechtigungssystem ausgefiltert und weder beim GDA- noch beim ELGA-Teilnehmerzugriff ersichtlich werden. Es wird ein zentraler Verzeichnisdienst des Policy Administration Point eingerichtet, welcher die zum Löschen freigegebenen Dokumenten-IDs verwaltet.

   Die zum Löschen freigegebenen Dokumente sind noch für eine gewisse Zeit (einige Tage - Quarantäne) unangetastet im System vorhanden. In diesem Zeitraum wird sicherheitstechnisch überprüft, ob das Löschen nicht durch verdächtige Angriffsvektoren verursacht wurde. Hält der Auftrag zum Löschen dieser Überprüfung stand, können die Dokumente einzeln physisch aus ELGA gelöscht werden. Hierfür greift die ZGF auf die zentrale Liste der zum Löschen freigegeben Dokumente zu. Die ZGF löscht die ELGA-Daten und zwar in Abhängigkeit der umgesetzten und zugelassenen XDS-Konfigurationsvarianten (A oder C).

2. **Löschen aller CDA-Dokumente** im Auftrag des berechtigten ELGA-Teilnehmers, der Opt-Out erklärt hat (bzw. partielles Opt-Out für e-Befunde). Hierfür wird ein XACML Opt-Out Policy im PAP gespeichert. Anschließend wird die bPK-GH des ELGA-Teilnehmers im zentralen Verzeichnisdienst des PAP (siehe oben) veröffentlicht. Die Vorgehensweise ist wie oben dargestellt. Die zum Löschen freigegebenen Dokumente sind noch eine gewisse Zeit (einige Tage) unangetastet im System vorhanden. In

diesem Zeitraum wird sicherheitstechnisch überprüft, ob das Opt-Out nicht durch verdächtige Angriffsvektoren verursacht wurde. Die ZGF fragt regelmäßig die bPK-GH jener ELGA-Teilnehmer ab, deren ELGA-Daten durch Opt-Out Policy implizit zum Löschen freigegeben worden sind. Die ZGF setzt das Löschen in Abhängigkeit der umgesetzten und zugelassenen XDS-Varianten um.

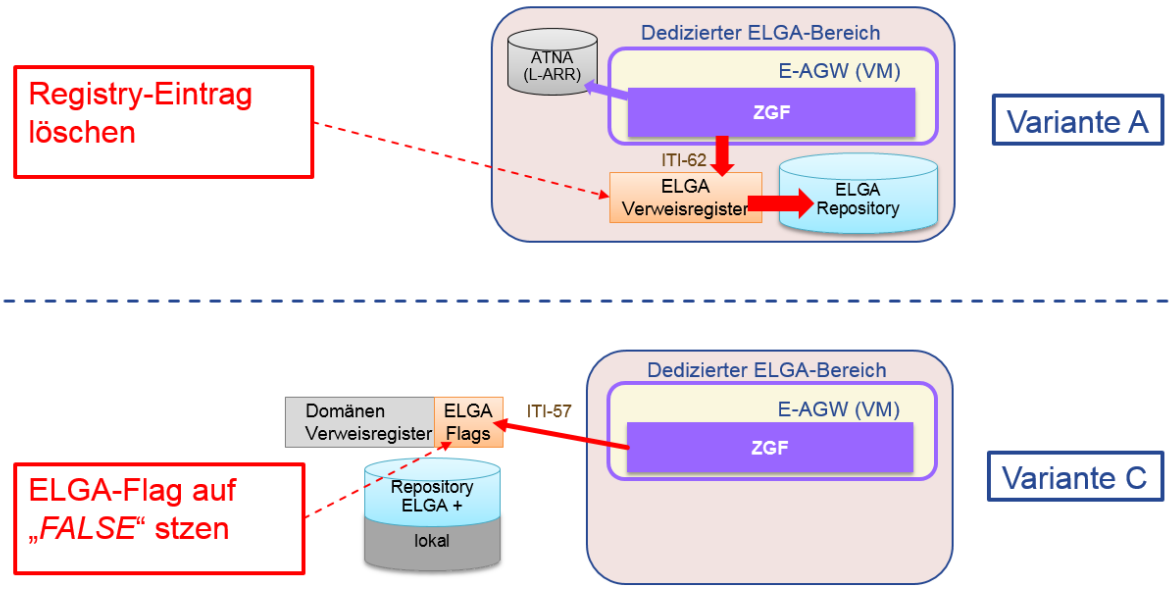


Abbildung 46: Löschen in den ELGA-Bereichen in Abhängigkeit von der verwendeten XDS-Variante

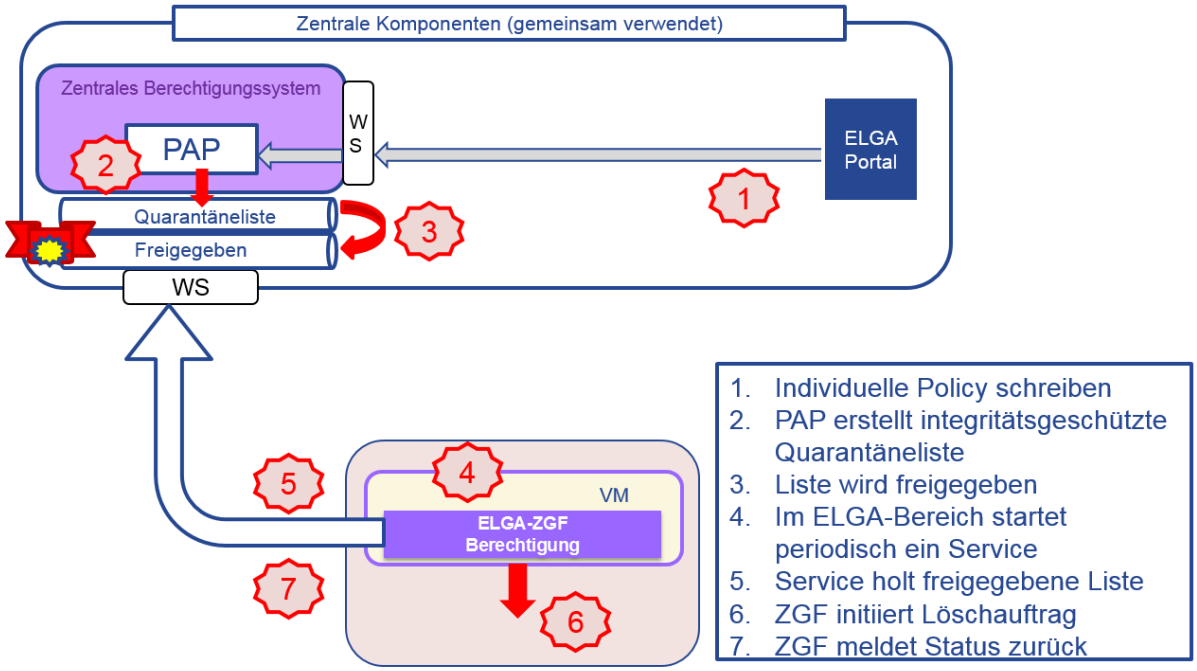
Löschen in der Standardvariante A (Abbildung 46): Das CDA-Dokument wird vom entsprechend autorisierten Service der ZGF von der Registry gelöscht (via ITI-62). Das Löschen der zugehörigen Dokumente in den Repositories ist seitens des Bereichsherstellers anknüpfend an den Registry-Löschvorgang durchzuführen.

Löschen in der Custom-Variante C: Das CDA-Dokument wird vom entsprechend autorisierten Service der ZGF aus ELGA gelöscht, indem via ITI-57 das ELGA-Flag auf ***False*** gesetzt wird.

9.1.4.4. Sicherheitstechnische Absicherung vom Löschen

Das physische Löschen von Gesundheitsdaten von ELGA ist in Abbildung 47 dargestellt. Ein zentrales Service stellt die Liste der zu löschenden Daten zur Verfügung (sog. Quarantäneliste) und ein lokaler autorisierter Service exekutiert das zentral angeordnete Löschen.

4173



4174

4175 *Abbildung 47: Schematische Darstellung des Lösch-Workflows in ELGA*

4176 Die Liste der zu löschenden Daten wird automatisch freigegeben soweit der autorisierte
4177 Sicherheitsadministrator dies nicht bewusst verhindert. Ein ELGA-Teilnehmer gibt nur das
4178 CDA-Dokument zum Löschen frei. Dadurch wird eine „zum Löschen freigegeben“ XACML-
4179 Policy im Berechtigungssystem (PAP) gespeichert, die den genannten Datensatz sofort und
4180 unwiderruflich (für GDA und ELGA-Teilnehmer) verbirgt. Dies funktioniert ähnlich wie eine
4181 „ausgeblendet“ Policy, mit dem Unterschied, dass bei „zum Löschen freigegeben“ selbst der
4182 Auftraggeber (ELGA-Teilnehmer) den so markierten Datensatz (CDA) nicht mehr sieht.

4183 Im Hintergrund kommt der Identifier des Datensatzes auf eine integritätsgeschützte
4184 Quarantäneliste, welche für berechtigte Sicherheitsadministratoren einsehbar ist. Der Status
4185 der Einträge in der Quarantäneliste ändert sich nach einem konfigurierbaren Zeitfenster
4186 (empfohlen 24 bis 72 Stunden) auf „freigegeben“ wodurch diese zum Abholen von den
4187 entsprechend berechtigten Services der Zugriffssteuerungsfassaden zur Verfügung stehen.

4188 Die dafür bestimmten Abhol-Services (Lösch-Dämon) der ZGFs holen sich die Liste der zum
4189 Löschen freigegeben Dokumente, um die Lösch-Operationen lokal durchführen zu lassen.
4190 Diese Services können bei Verdacht auf Missbrauch oder aus betrieblichen Gründen gestoppt
4191 werden, um das Löschen der Dokumente bis zur Klärung oder Durchführungsbereitschaft zu
4192 verhindern.

Nach erfolgreichem Löschen wird eine entsprechende Rückmeldung an den PAP erfolgen. Ab Empfang einer solchen Bestätigung gilt der Auftrag des ELGA-Teilnehmers als tatsächlich erfüllt. Wenn ein GDA eine neue Version eines bereits gelöschten CDA-Dokuments in ELGA veröffentlichen will, wird die noch vorhandene Policy ausgeführt und verhindert das Veröffentlichen in ELGA.

Obige Maßnahmen bieten eine mehrstufige Sicherheitsschleuse um ungewollten Missbrauch effektiv Riegel vorzuschieben:

1. Ein Datensatz kommt nur dann auf die Quarantäneliste, wenn in der signierten Willenserklärung des ELGA-Teilnehmers der vom Client berechnete Hashwert der technischen XACML-Policy mit dem Hashwert vom Service (PAP) berechneten „zum Löschen freigegeben“ XACML-Policy übereinstimmt (sog. *Client-Server Policy Handshake*).
2. Die Quarantäneliste ist nicht manipulierbar, weil kryptografisch geschützt ist.
3. Die Quarantänezeit bietet zusätzliche Möglichkeiten, bei aufgedeckten Angriffen rechtzeitig Maßnahmen zu ergreifen.
4. Die Durchführung der Löschoperationen in den ELGA-Bereichen ist von Administratoren steuerbar, indem die Aktion jederzeit gestoppt werden kann.

9.1.4.5. Wiederherstellung der Quarantäneliste bei identifiziertem Angriff

Wenn ein Sicherheitsadministrator eine Kompromittierung des Systems feststellt und annimmt, die Quarantäneliste könnte betroffen sein, muss diese Liste umgehend gelöscht werden, da inhaltlich nicht mehr für die Konsistenz der Liste garantiert werden kann. Soweit der PAP nicht in Mitleidenschaft gezogen wurde, entsteht dadurch in ELGA keine Inkonsistenz. Dies lässt sich damit begründen, dass die entsprechenden Lösch-Policies im PAP noch immer wirksam sind und jeglichen Versuch die damit markierten CDA zu lesen verhindern.

Ein Lösch-Dämon meldet dem PAP ein erfolgreiches Löschen. Im PAP muss somit klar vermerkt werden, welche individuellen Lösch-Policies bereits physisch ausgeführt worden sind. Dadurch ist es möglich den Lösch-Auftrag (ausstehende Lösch-Aufträge) und die Quarantäneliste restlos wiederherzustellen. Hierfür müssen die individuellen Lösch-Policies im PAP gescannt werden und jene Policies vermerkt werden, die physisch noch nicht ausgeführt worden sind. Am Ende des Scan-Vorganges muss eine valide Quarantäneliste mit aktuellen Lösch-Aufträgen wiederhergestellt werden.

Sollte allerdings die Analyse der Angriffsvektoren ergeben, dass auch der PAP kompromittiert wurde, dann muss vorerst ein saubereres Backup der PAP-Datenbank eingespielt werden, welches einen Zustand vor dem Angriff abbildet. Erst danach ließe sich das oben

beschriebene Scan-Vorgehen zur Wiederherstellung der Quarantäneliste durchführen. Für die Zeit der Widerherstellung des PAP muss ELGA außer Betrieb genommen werden.

9.1.5. Anwendungsfälle aus der Sicht der Zugriffssteuerungsfassade

Die im Kapitel 2.7 aufgelisteten logisch-funktionalen Anwendungsfälle werden größtenteils durch gezielte Aufrufe gegenüber den entsprechenden Endpunkten der zuständigen AGW realisiert. Wie die Abbildung 44 deutlich zeigt, werden manche dieser Aufrufe direkt von der Zugriffssteuerungsfassade (ZGF) des AGW bearbeitet (meistens IHE), andere nur terminiert und über eine neu aufgesetzte TLS-Verbindung an die zentralen Komponenten weitergeleitet. Im Weiteren wird die technische Umsetzung der logisch-funktionalen aller Anwendungsfälle ET und GDA (siehe Kapitel 2.7) festgehalten (Tabelle 21 und Tabelle 22). Es werden konkrete Transaktionen und Schnittstellen, sowie Bedingungen und Schlüssel der einzelnen Transaktionen genannt, die bei der Realisierung der einzelnen Use-Cases weitergegeben werden und bekannt sein müssen.

9.1.5.1. Umsetzung logisch-funktionaler Anwendungsfälle der ELGA-Teilnehmer

Nr.	Anwendungsfall	Technische Umsetzung a. Aufrufe / Funktionen / Methode b. Vorbedingungen c. Schlüssel (ID) d. Inhalt der Authentication-Header e. Resultat	Akteur-Kette Request-Target
ET.1.1	ELGA Login (Anmelden)	a. WS-Trust RST / Issue Request b. Identity Assertion (PVP Citizen Token) c. bPK-GH d. Identity Assertion (PVP Citizen Token) e. RSTR: ELGA User I Assertion	GHP/EBP AGW ETS
ET.1.2	Token erneuern	a. WS-Trust RST / Renew Request b. ELGA User I Assertion (noch gültig und noch nicht erneuert oder höchstens einmal erneuert: Renew-Count<=1) c. bPK-GH d. ELGA User I Assertion (noch gültig) e. ELGA User I Assertion (erneuert, Renew-Count++)	EBP AGW ETS
ET.1.3	Zugriffsrechte verwalten, Consent Dokument signiert speichern	a. WS zum PAP (Read / Write) b. ELGA User I Assertion gültig c. bPK-GH, Hash über das PolicySet d. ELGA User I Assertion e. XACML-PolicySet, Consent Document (PDF Format)	EBP AGW PAP
ET.1.4	Liste bisheriger gültiger GDA-Kontakte abrufen	a. WS zum KBS (Read-Only) b. ELGA User I Assertion gültig c. bPK-GH, GDA OID d. ELGA User I Assertion e. Kontaktliste je nach Filterkriterien	EBP AGW KBS
ET.1.6	Ausgewählte Protokolle über stattgefundene Zugriffe ansehen	a. WS zur A-ARR (Read-Only) b. ELGA User I Assertion gültig c. bPK-GH, GDA-OID d. ELGA User I Assertion e. Liste ausgewählter Protokolle je nach Filterkriterien	EBP AGW A-ARR
ET.1.7	Ausgewählte Teile des Protokolls als PDF herunterladen/ausdrucken	Das Berechtigungssystem (AGW/ZGF) ist bei der Operation nicht beteiligt. Betrifft Anwendungslogik des Portals	EBP

ET.1.8	Liste ausgewählter Gesundheitsdaten ansehen	a. IHE ITI-18 (dann ITI-38 soweit XCA) entsprechend Profilierung (Kapitel 3.18) b. ELGA User I Assertion gültig c. bPK-GH oder L-PID d. ELGA User I Assertion e. Liste der Gesundheitsdaten (Metadaten) je nach Filterkriterien der Abfrage. Enthält setId und/oder entryUUID der Dokumente	EBP AGW ZGF Initi. XDS/XCA ZGF Resp. Registry
ET.1.9	Ein bestimmtes CDA-Dokument auswählen, öffnen	a. IHE ITI-43 (dann ITI-39 soweit XCA) b. ELGA User I Assertion gültig und ein zeitnah (nicht älter als 30 Minuten) ausgeführter Geschäftsfall ET.1.8 c. Document setId oder entryUUID d. ELGA User I Assertion e. Ausgewähltes CDA-Dokument	EBP AGW ZGF Init. XDS/XCA ZGF Resp. Repository
ET.1.10	Eigene Medikationsliste einsehen	a. IHE PHARM-1 (FindMedicationList) b. ELGA User I Assertion gültig c. bPK-GH oder L-PID d. ELGA User I Assertion e. Medikationsliste - OnDemandDocument	EBP AGW ZGF Init. ZGF Resp. e-Medikation
ET.1.11	Ein referenziertes Bildmaterial auswählen, öffnen	a. IHE RAD-69 (bzw.RAD-75 wenn XCA-I) b. ELGA User Assertion I gültig und entsprechende Referenz auf das Bildmaterial (KOS-Object) c. Community-ID, Repository-ID, Study, Series & Image Information ID d. ELGA User Assertion I e. Bidlmaterial als JPEG	EBP AGW ZGF Init. XCA-I ZGF Resp. Adapter PACS
ET.1.12	Vorversion eines bestimmten CDA-Dokumentes öffnen	a. IHE ITI-43 (bzw. ITI-39 wenn XCA) b. ELGA User I Assertion gültig und ein zeitnahe (nicht älter als 30 Minuten) ausgeführter Geschäftsfall ET.1.8 c. Document setId oder entryUUID der Vorversion d. ELGA User I Assertion e. Vorversion des CDA-Dokumentes	EBP AGW ZGF Init XDS/XCA ZGF Resp. Repository
ET.1.13	Ein bestimmtes Dokument/Bild als PDF herunterladen (drucken)	Das Berechtigungssystem (AGW/ZGF) ist bei der Operation nicht beteiligt. Betrifft Anwendungslogik des Portals	EBP
ET.1.14	Logout (Abmelden) Session -Zeit ist limitiert (einige Stunden).	a. WS-Trust RST / Cancel Request b. ELGA User I Assertion gültig c. <CancelTarget> ELGA User I Assertion d. ELGA User I Assertion	EBP AGW ETS

		e. RSTR: <RequestedTokenCancelled>	
ET.1.15	Optional: Personalisierte GUI	Das Berechtigungssystem (AGW/ZGF) ist nicht beteiligt	EBP

Tabelle 21: Anwendungsfälle eines ELGA-Teilnehmers am ELGA-Portal. Im Falle eines Vertreters (siehe Tabellen 1 und 2) ist die ELGA User Assertion I mit der ELGA Mandate Assertion I zu ersetzen.

9.1.5.2. Umsetzung logisch-funktionaler Anwendungsfälle der ELGA-GDA

	Anwendungsfall	**Technische Umsetzung** **a. Aufruf/ Funktion /Methode** **b. Vorbedingung** **c. Schlüssel** **d. Inhalt Authentication-Header** **e. Resultat**	**Akteur-Kette** **Request Target**
GDA.3.1	ELGA-Login GDA	a. WS-Trust RST / Issue Rewuest b. Identity Assertion vom IdP (z.B. e-Card) c. GDA-OID (im GDA-I geführt) d. Identity Assertion e. RSTR: ELGA HCP-Assertion	GDA AGW ETS
GDA.3.2	Login-Token erneuern	a. WS-Trust RST / Renew Request b. ELGA HCP Assertion (noch gültig und noch nicht erneuert, Renew-Count=0) c. GDA-OID d. ELGA HCP Assertion (noch gültig) e. ELGA HCP Assertion (erneuert, Renew-Count=1)	GDA AGW ETS
GDA.3.3	Demografische Patientensuche	Das Berechtigungssystem (AGW/ZGF) ist nicht beteiligt. Anfrage wird sinngemäß direkt an L-PI gestellt. L-PI kann Z-PI kontaktieren.	GDA L-PI / Z-PI
GDA.3.4	Situatives Opt-Out umsetzen	Das Berechtigungssystem (AGW/ZGF) ist nicht beteiligt und wird nicht im ELGA-Berechtigungssystem umgesetzt (siehe Organisationshandbuch)	GDA
GDA.3.5	Patient identifizieren und einmelden	Das Berechtigungssystem (AGW/ZGF) ist nicht beteiligt. Anfrage wird sinngemäß direkt an L-PI gestellt. L-PI verbindet sich bei Bedarf mit dem Z-PI	GDA L-PI / Z-PI
GDA.3.6	Behandlungs-zusammenhang schaffen	a. WS-Trust RST an KBS, claims:trtype= urn:elga:trtypes:AmbulanterKontakt oder urn:elga:trtypes:Aufnahme b. ELGA HCP-Assertion, GDA.3.5 c. GDA-OID (im GDA-I geführt) und L-PID (oder bPK-GH) des Patienten d. ELGA HCP-Assertion	GDA AGW KBS

		e. RSTR: TRID der Kontaktbestätigung	
GDA.3.7	Behandlungszusammenhang (Kontakt) delegieren	a. WS-Trust RST an KBS, claims:trtype= urn:elga:trtypes:Delegation b. ELGA HCP-Assertion gültig, Patient identifiziert c. GDA-OID von beiden GDA (Source und Ziel), L-PID (oder bPK-GH) des Patienten d. ELGA HCP-Assertion e. RSTR: TRID des delegierten Kontaktes	GDA AGW KBS
GDA.3.8	Behandlungszusammenhang (Kontakt) stornieren	a. WS-Trust RST / Cancel an KBS b. ELGA HCP-Assertion gültig c. TRID des Kontaktes zum Stornieren d. ELGA HCP-Assertion e. Kontakt mit angeführtem TRID ungültig	GDA AGW KBS
GDA.3.9	Dokumentenliste zu einem Patient abrufen	a. IHE ITI-18 (bzw. ITI-38 wenn XCA) entsprechend Profilierung (Kapitel 3.18) b. ELGA HCP-Assertion gültig, Patient identifiziert c. bPK-GH oder L-PID d. ELGA HCP-Assertion e. Liste der Gesundheitsdaten (Metadaten) je nach Filterkriterien der Abfrage. Enthält setId und/oder entryUUID der Dokumente	GDA AGW ZGF Init. XDS / XCA ZGF Resp. Registry
GDA.3.10	Dokument(e) zu einem Patienten abrufen	a. IHE ITI-43 (bzw. ITI-39 wenn XCA) b. ELGA HCP-Assertion gültig und ein zeitnah (nicht älter als 30 Minuten) ausgeführter Geschäftsfall GDA.3.9 c. Document setId oder entryUUID d. ELGA HCP-Assertion e. Ausgewählte CDA-Dokumente	GDA AGW ZGF Init. XDS / XCA ZGF Resp. Repository
GDA.3.11a	Medikationsliste des Patienten abrufen (GDA-Arzt, Krankenhaus, Pflegeheim-Szenario)	a. IHE PHARM-1 (*FindMedicationList*) b. ELGA HCP-Assertion gültig, Patient identifiziert, Kontaktbestätigung gültig c. bPK-GH oder L-PID d. ELGA HCP-Assertion e. Medikationsliste	GDA AGW ZGF Init. ZGF Resp. e-Med.
GDA.3.11b	Medikationsliste des Patienten abrufen (GDA-Apotheker via e-Med-ID)	a. IHE PHARM-1 (*FindMedicationList*) b. ELGA HCP-Assertion gültig, e-Med-ID ist bekannt (eingescannt), e-Med-ID-Token vom eSTS abgerufen c. e-Med-ID d. ELGA HCP-Assertion, e-Med-ID-Token e. Liste beschränkt auf e-Med-ID	GDA AGW ZGF Init. ZGF Resp. e-Med.

GDA.3.12a	Ein oder mehrere e-Med-ID holen	a. EMEDAT-1 *GenerateDocumentId* b. ELGA HCP-Assertion gültig c. kein Schlüssel d. ELGA HCP-Assertion e. Ein oder mehrere e-Med-ID (Liste)	GDA AGW ZGF Resp. e-Med.
GDA.3.12b	Verordnung eines oder mehrerer Medikamente speichern	a. IHE ITI-41/42 b. ELGA HCP-Assertion gültig, Patient identifiziert, Verordnung ist erfasst und via EMEDAT-1 (*GenerateDocumentId*) ein e-Med-ID geholt (siehe GDA.3.12a), Kontaktbestätigung gültig c. bPK-GH oder L-PID, e-Med-ID, setId d. ELGA HCP-Assertion e. Verordnung gespeichert	GDA AGW ZGF Init. ZGF Resp. e-Med.
GDA.3.12c	e-Med-ID Token holen	a. WS-Trust RST b. ELGA HCP-Assertion gültig c. E-Med_ID d. ELGA HCP-Assertion e. E-Med-ID Token	GDA AGW ZGF Resp. e-Med.
GDA.3.13a	Abgabe eines oder mehrerer Medikamente speichern (ohne e-Med-ID, mit Kontaktbestätigung)	f. IHE ITI-41/42 g. ELGA HCP Assertion gültig, Patient ist identifiziert, Kontaktbestätigung gültig h. bPK-GH oder L-PID i. ELGA HCP Assertion j. Abgabe gespeichert	GDA AGW ZGF Init. ZGF Resp. e-Med.
GDA.3.13b	Abgabe eines oder mehrerer Medikamente speichern (Hausapotheke oder Apotheke)	a. IHE ITI-41/42 b. ELGA HCP Assertion gültig, e-Med-ID vorhanden (eingescannt), e-Med-ID Token vorhanden (abgefragt via WS-Trust vom eSTS, siehe GDA.3.12c) c. e-Med-ID d. ELGA HCP Assertion, e-Med-ID-Token e. Abgabe gespeichert	GDA AGW ZGF Init. ZGF Resp. e-Med.
GDA.3.14	Ein bestimmtes Dokument (oder mehrere) der bildgebenden Diagnostik abrufen	a. IHE RAD-69 (oder RAD-55/WADO) bzw. RAD-75 bei XCA-I b. ELGA HCP-Assertion gültig und entsprechende Referenz auf das Bildmaterial (KOS-Object) c. WADO-URL bzw. Community-ID, Study, Series & Image Information ID d. ELGA HCP-Assertion e. Bildmaterial (JPEG)	GDA AGW ZGF Init XDS/XCA-I ZGF Resp. Adapter PACS

GDA.3.15	Vorherige Version eines bestimmten Dokumentes abrufen	a. IHE ITI-43 (bzw. ITI-39 wenn XCA) b. ELGA HCP-Assertion gültig und ein zeitnah (nicht älter als 30 Minuten) ausgeführter Geschäftsfall GDA.3.9 c. Document setId und entryUUID der Vorversion d. ELGA HCP-Assertion e. Ausgewählte Vorversion des CDA	GDA AGW ZGF Init. XDS XCA ZGF Resp. Repository
GDA.3.16	Ausgewählte Dokumente des Patienten herunterladen und lokal speichern	AGW/ZGF ist nicht involviert. Vorbedingung ist Anwendungsfall GDA.3.10	GDA Lokales KIS System
GDA.3.17	Registrieren (freigeben) eigener Dokumente in ELGA Details sind bei den Bereichsvarianten A und C erklärt	a. IHE ITI-41 bzw. ITI-42/ITI-57 (je nach ELGA-Bereichsvariante A oder C) entsprechend Profilierung (Kapitel 3.18) b. ELGA HCP Assertion gültig, Patient identifiziert c. bPK-GH oder L-PID, setId, referenceIdList d. ELGA HCP-Assertion e. Dokumente in ELGA-freigegeben	GDA AGW ZGF Init. XDS Repository Registry
GDA.3.18.a	Updaten von ELGA-Dokumenten	a. RPLC via IHE ITI-41 und/oder ITI-42 (je nach Bereichsvariante A oder C) entsprechend den Einschränkungen in Kapitel 3.18 b. ELGA HCP Assertion gültig, Patient identifiziert, GDA-OID muss jener des Autors des Originaldokuments entsprechen, dies betrifft die GDA-OID in den XDSSubmissionSet und XDSDocumentEntry -Metadaten c. bPK-GH oder L-PID, setId, referenceIdList (alternativ entryUUID) d. ELGA HCP-Assertion e. Neue Version des Dokumentes ist „approved“ alte Version ist „deprecated“	GDA AGW ZGF Init XDS Repository Registry
GDA.3.18.b	Storno von ELGA-Dokumenten	a. IHE ITI-57 entsprechend der Profilierung (Kapitel 3.18) b. ELGA HCP Assertion gültig, Patient identifiziert c. setId oder entryUUID d. ELGA HCP-Assertion e. Dokumentes storniert („deprectated“)	GDA AGW ZGF Init XDS Registry
GDA.3.19	ELGA-Logout GDA	a. WS-Trust RST / Cancel Request b. ELGA HCP-Assertion gültig c. <CancelTarget> ELGA HCP-Assertion	GDA AGW ETS

GDA.3.20		d. ELGA HCP-Assertion e. RSTR: <RequestedTokenCancelled>	
	Update von ELGA-Dokumenten bei abgelaufener Kontaktbestätigung	Wie Anwendungsfälle GDA.3.18.a und 3.18.b mit dem Unterschied, dass eine abgelaufene (bis zu einem Jahr) Kontaktbestätigung ausreichend ist	GDA AGW ZGF Init XDS

Tabelle 22: Siehe Tabelle 3, Anwendungsfälle eines ELGA-GDA

9.1.6. Nutzung von existierenden elektronischen Vollmachten in ELGA

Das ELGA-Berechtigungssystem unterstützt das Handeln im Auftrag eines Vertretenen. Hierbei basiert das Konzept auf zwei Säulen. Die eine wird durch die entsprechenden Bestimmungen von WS-Trust definiert (Kapitel 9 des OASIS Dokumentes Version 1.4 *Key and Token Parameter Extensions*) und die andere durch das Online Vollmachten-Service, das im Rahmen des e-Governments bereitgestellt wird. Das Online Vollmachten-Service bildet existierende Vollmachten elektronisch ab und ermöglicht gleichzeitig die Überprüfung eines Stellvertretungsverhältnisses mittels der Module für Online Applikationen (MOA) basierend auf der Nutzung der Bürgerkarte bzw. Handy-Signatur. Die zwei Säulen werden wie folgt näher erläutert:

- **WS-Trust** definiert Methoden der Ausstellung von SAML-Assertions für Bevollmächtigte. Die erforderliche *Request Security Token* Anfrage an das ETS muss die ELGA-*User-Assertion I* des zu vertretenden ELGA-Teilnehmers referenzieren.
- Die zweite Säule stellt das **Online Vollmachten-Service des E-Government** dar. Hierbei reduziert sich die Aufgabe des ELGA-Berechtigungssystems auf den Empfang von elektronischen Vollmachten, die durch das sogenannte *Mandate Issue Service* (MIS) ausgestellt und signiert wurden. Der Bevollmächtigte übermittelt als Erstes seine eigene elektronische Identität anhand der Bürgerkarte sowie damit verbundene elektronische Vollmachten an den ETS. Basierend auf diesen elektronischen Vollmachten generiert das ETS eine ELGA-*Mandate-Assertion I*. Die *ELGA-Mandate-Assertion* ermöglicht es dem Bevollmächtigten im Namen des Vollmachtgebers zu agieren, d.h. dessen medizinische Dokumente zu suchen und abzurufen, Zugriffsprotokolle einzusehen und individuelle Zugriffsberechtigungen zu warten.

9.1.7. ELGA-Proxy

Wie im Kapitel 3.9 vermerkt, können niedergelassene GDA über die GINA und über eine zentrale Vermittlungskomponente des Hauptverbandes, den ELGA-Proxy (siehe Abbildung 48), an einen ausgewählten ELGA-Bereich angebunden werden. Wie der Name schon sagt, ist die Komponente als tatsächlicher Proxy zwischen GDA-Software und dem ausgewählten ELGA-Bereich zu verstehen. Das Protokoll für die Kommunikation zwischen der GDA-

Software und der GINA entspricht dabei jenem, das vom angesprochenen Zielsystem erwartet wird (IHE-Transaktionen, WS-Trust Request bzw. ELGA spezifische SOAP-Requests).

GDA, die eine solche Vermittlungsfunktion verwenden wollen, müssen einen entsprechenden Antrag beim e-Card System stellen. Danach kann anhand der jedem ELGA-Request beigefügten HCP-Assertion die Zugehörigkeit des GDAs zum ELGA-Zielbereich bestimmt werden. Dementsprechend muss die ELGA-Proxy Komponente die HCP-Assertion prüfen. Der ELGA-Proxy muss in der HCP-Assertion in der Liste der autorisierten Service Provider (<AudienceRestriction>) explizit angeführt sein. Ist in der HCP-Assertion die ELGA-Proxy nicht angeführt, darf die Anfrage nicht weitergeleitet werden und die Transaktion muss abgewiesen werden. Die GDA-Software muss bei der Beantragung der HCP-Assertion (RST) die Information, dass auch der ELGA-Proxy angesprochen wird, mitsenden. Dementsprechend stellt ETS die HCP-Assertion mit erweiterter <AudienceRestriction> auch für ELGA-Proxy aus.

Der ELGA-Proxy ist eine reine Vermittlungskomponente, wodurch keine ELGA-seitigen Anforderungen an Protokollierung (A-ARR / L-ARR) und Zeitmessung bestehen. Innerhalb des Proxies wird jedenfalls für interne Zwecke protokolliert und gemessen.

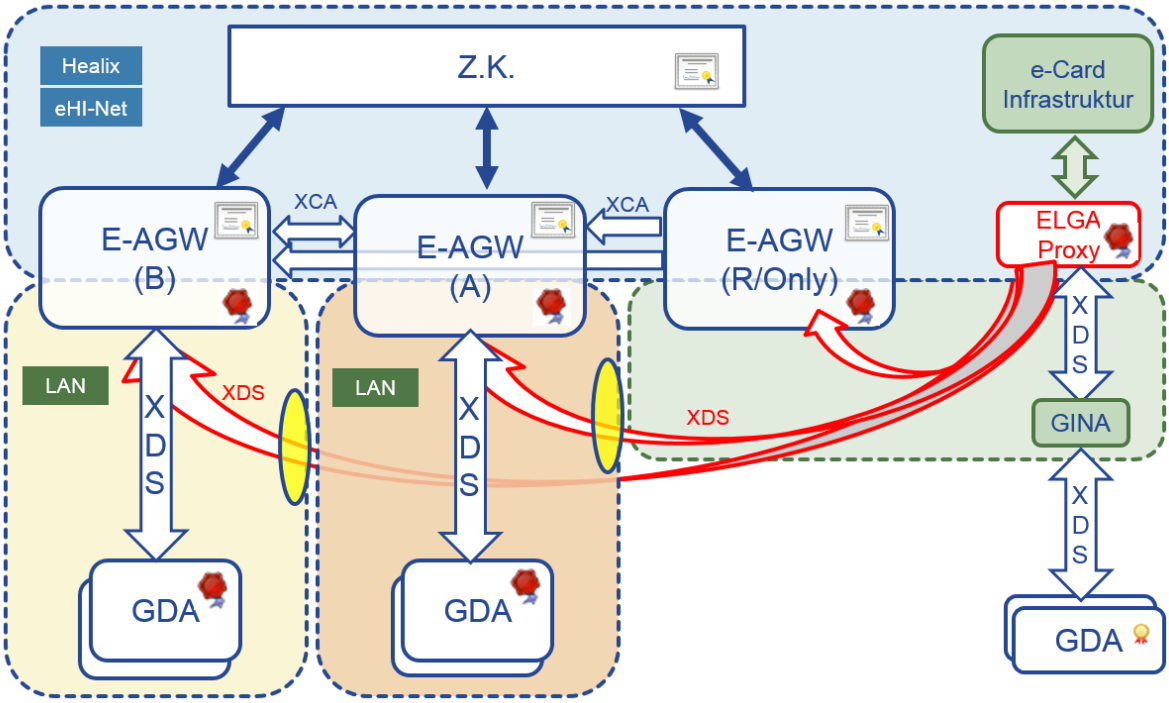


Abbildung 48: ELGA-Proxy in Überblick. Z.K. == zentrale Komponenten

ELGA-Proxy kann nur mit jenen ELGA-Bereichen zusammenarbeiten, welche die Anbindung von externen GDA anbieten bzw. akzeptieren. Hierfür müssen die ELGA-Bereiche, wie in der Abbildung 48 mit gelben Ellipsen dargestellt, ihr Netzwerk für die eingehende XDS-Kommunikation mit dem ELGA-Proxy öffnen.

Details über die exakte Funktionsweise von ELGA-Proxy sind im [25] nachzulesen.

9.2. Protokollierungssystem

9.2.1. Allgemeines

Sinn der Protokollierung ist es, die Nachvollziehbarkeit und Transparenz aller Aktionen innerhalb ELGA umzusetzen. Dies umfasst insbesondere alle Operationen auf Patientenindices, den GDA-Index, Zugriffsberechtigungen, Willenserklärungen der ELGA-Teilnehmer, Protokollspeicher sowie die ELGA-Gesundheitsdaten gemeinsam mit den entsprechenden Verweisen (Dokument-Metadaten). Protokollinhalte werden in Übereinstimmung mit den legistischen Anforderungen spezifiziert.

Alle im Kontext von ELGA zum Einsatz kommenden IHE Konzepte müssen entsprechend den zugeordneten IHE Transaktionen in Übereinstimmung mit den Vorgaben in [1] und [11] protokollieren. ELGA-berechtigungs- und protokollierungssystemspezifische Constraints im Hinblick auf Protokollstruktur und -inhalt sind zu berücksichtigen.

Das ATNA Profil setzt das IHE Integrationsprofil *Consistent Time* (CT) voraus. Dieses spezifiziert die Verwendung des *Network Time Protocols* (NTP), RFC 1305, und setzt voraus, dass die Zeitgeber aller ELGA Komponenten sowie in ELGA integrierte Document Repositories mit einer maximalen mittleren Abweichung (median error) von einer Sekunde synchronisiert sind.

Jede von Akteuren ausgelöste Aktion in ELGA wird protokolliert und im lokalen Audit Record Repository (L-ARR) gespeichert. Jeder ELGA-Bereich hat ein L-ARR einzurichten, wobei dies als Mindestanforderung für alle ELGA-Bereiche zu sehen ist. Die Zugriffssteuerungsfassade des ELGA-Berechtigungssystems protokolliert (siehe Abbildung 49) in das L-ARR* des zuständigen ELGA-Bereichs. Die Bezeichnung L-ARR* bezieht sich auf jenen Teil eines L-ARR, welcher ausschließlich Audits einer ZGF gewidmet ist. So gesehen sind L-ARR und L-ARR* nur logisch getrennt (können auch physisch getrennt aufgestellt werden) und beide in der Verwaltung des ELGA-Bereichs. Der ELGA-Bereich hat vollen Zugriff sowohl auf L-ARR wie auch auf L-ARR*.

Zentrale ELGA-Services die in der Zuständigkeit eines bestimmten Betreibers liegen (ETS, KBS, PAP und GDA-I) protokollieren in ein zentral aufgestelltes L-ARR (Z-L-ARR). Andere ELGA-bereichsübergreifend genutzte Komponenten wie der Z-PI protokollieren in die selbst aufgestellte L-ARR Instanz. Alle Protokoll-Nachrichten sind entsprechend der Fristen des ELGA-Gesetzes aufzubewahren.

Die ELGA-Transaktionsklammer (siehe Kapitel 3.10.1) ist ein verpflichtender Teil der Protokoll-Aufzeichnungen. Egal ob L-ARR, Z-L-ARR oder A-ARR, die Transaktionsklammer ist vom

jeden protokollierenden Akteur immer und ohne Ausnahmen anzuführen. Dies gewährleistet die Nachverfolgung einzelner verteilt ausgeführter Transaktionen ELGA-weit.

Personen- bzw. hardwarebezogene Identitätsinformationen sind essentiell, um das Ziel einer lückenlos nachvollziehbaren Protokollierung aller Aktionen sowie beteiligter Personen und technischer Systeme in ELGA zu erreichen. Im Kontext von ELGA liegen diese gemeinsam mit der Information über die Art des Zugriffs (u.a. regulär, „on behalf of“) in verifizierter, digital signierter Form als Teil jeder Aktion vor und werden daher entsprechend in die Protokollgenerierung übernommen.

Die über die L-ARR übergeordnete ELGA-Protokollierungsauswertung ermöglicht einen direkten bereichsübergreifenden Nutzen aus den lokal (bereichsintern) aufgezeichneten ATNA-Protokolldaten. Die ELGA-Protokollierungsauswertung besteht aus zwei definierten Datenpools mit unterschiedlichen Aufgaben (siehe Abbildung 49):

1. Datenpool bestehend aus Aufzeichnungen der lokalen IHE Akteuren (L-ARR)
2. Datenpool geschrieben von der ZGF-Komponente (siehe L-ARR*)

Das aggregierte Audit Record Repository (A-ARR) ermöglicht es, auf die von den einzelnen GDA angestoßenen und von den Zugriffssteuerungsfassaden generierten Protokolldaten zuzugreifen und – dem ELGA-Gesetz entsprechend – den Bürgern am ELGA-Portal Auskunft geben zu können, wer, wann, auf welche ihrer Gesundheitsdaten zugegriffen hat. Das A-ARR befindet sich im ELGA-Kernbereich. Zugriff ist ausschließlich auf die eigene Protokolle gestattet (inbegriffen Zugriff aufgrund von Vertreterverhältnissen).

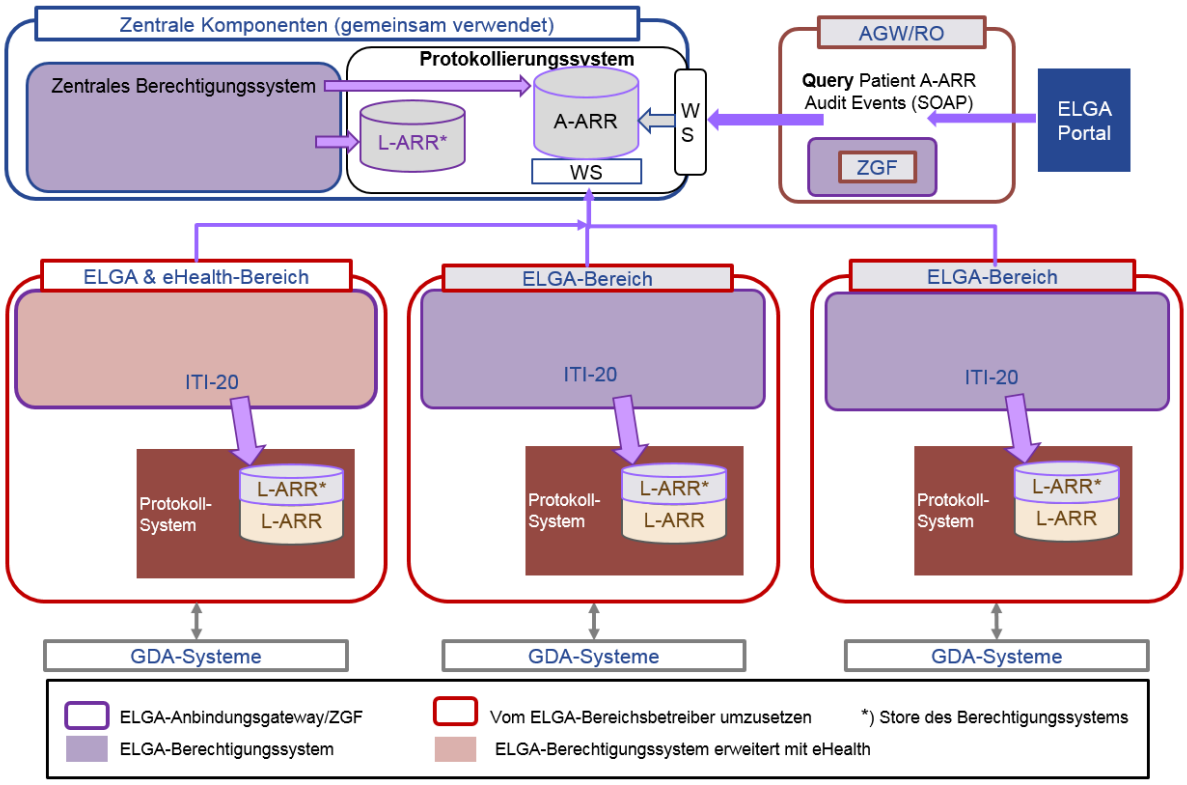


Abbildung 49: Komponentenübersicht des ELGA-Protokollierungssystems. Ein eHealth-Bereich ist ein mit eHealth-Applikationen (nicht ELGA) erweiterter ELGA-Bereich.

9.2.2. Lokale Audit Record Repositories

In jedem ELGA-Bereich existiert zumindest ein lokales Audit Record Repository (L-ARR). Dieses ist dafür verantwortlich, auf IHE ATNA aufbauende, ELGA-konforme *Audit Trail* Nachrichten der Komponenten eines ELGA-Bereichs entgegen zu nehmen und diese in persistenter Form abzulegen. Aus funktionaler Sicht entsprechen L-ARRs mindestens einem Audit Repository, wie es durch das Integrationsprofil ATNA definiert ist (jedoch mit zusätzlichen Möglichkeiten zum Transport und schemakonformen Ergänzungen der Inhalte).

Die in der Abbildung 49 dargestellten L-ARR* Instanzen sind Repositories die unmittelbar und ausschließlich vom ELGA-Berechtigungssystem gespeist werden. L-ARR* wie auch L-ARR Instanzen sind in der Verwaltung der Betreiber der ELGA-Bereiche und persistieren Protokollnachrichten von allen relevanten lokalen IHE-Akteuren, einschließlich Nachrichten gesendet vom ELGA-Berechtigungssystem.

Eine kontinuierliche und lückenlose Protokollierung der ZGF-Tätigkeit muss gewährleistet sein. Hierfür müssen alle betroffenen L-ARR* Instanzen TCP/TLS-Protokollbasierendes (statt UDP) synchrones Logging seitens ZGF unterstützen (laut Syslog RFC5424). Wenn die

zuständige L-ARR* Instanz nicht zur Verfügung steht bzw. seitens ZGF nicht erreicht werden kann, muss die komplette Funktion der ZGF des betroffenen ELGA-Bereiches sofort gestoppt werden. Die ZGF darf das Ergebnis einer angestoßenen Transaktion dem initiierenden Akteur (GDA) nur dann liefern, wenn die betroffene Transaktion bereits im Protokollsystem (L-ARR*) aufgezeichnet wurde. Im gegenteiligen Fall erhält der initiierende Akteur eine entsprechende Fehlermeldung mit dem Hinweis auf die Nichterreichbarkeit des Protokollierungssystems.

Insbesondere bei schreibenden Transaktionen muss die lückenlose L-ARR* Protokollierung gewährleistet werden. Hierfür ist es nicht ausreichend, bereits gespeicherte und sog. „*commited*" Transaktionen im Nachhinein zu protokollieren (weitere Details siehe im Kapitel 9.2.6).

Anmerkung: Die von der ZGF gesendeten ITI-20 Nachrichten sind ausschließlich für die lokalen ARR (L-ARR) bestimmt und dürfen im Normalfall nicht in sonstigen AGW/Server-Logs zwischengespeichert werden (außer Error-Level).

9.2.3. Das Aggregierte Audit Record Repository (A-ARR)

Dem ELGA-Gesetz entsprechend ist ein zentrales Service zu errichten, das es ELGA-Teilnehmern (Bürgern) ermöglicht, Einsicht in die aufgezeichneten Protokolldaten, die ihre eigenen Gesundheitsdaten und Berechtigungsregeln betreffen, zu ermöglichen. Informationen über die Zugriffe auf die eigenen Gesundheitsdaten sind am ELGA-Portal zugänglich zu machen. Hierfür ist eine entsprechende bedienerfreundliche graphische Oberfläche (GUI) zur Verfügung zu stellen.

Das A-ARR-Service muss grundsätzlich auf Request/Response basierenden Messaging-Pattern realisiert werden. Das Protokollierungssystem muss für das ELGA-Portal eine entsprechende Web-Service Schnittstelle zur Verfügung stellen.

***Anmerkung**: In den im A-ARR gespeicherten Protokolldaten ist nur das bPK-GH (als Schlüssel) des ELGA-Teilnehmers enthalten, auf dessen Gesundheitsdaten zugegriffen wurde. Name oder sonstige Klartext-Hinweise auf den betroffenen Patienten sind im Protokoll nicht enthalten. Aufgrund der Historisierungsfunktion des GDA-I müssen Display-Namen von GDA und deren Rolle in den Protokollnachrichten nicht zwingend aufgelöst gespeichert werden. Es genügt das Mitprotokollieren der eindeutigen Identifier. Dies betrifft die GDA-Organisation. **Die konkret zugreifenden Identitäten (Personen) müssen im Klartext mitprotokolliert werden**.*

9.2.4. Identifizierte Quellen des A-ARR

Protokollnachricht-Schreiber sind alle ELGA-Akteure inklusive der Komponenten des ELGA-Berechtigungssystems. Aufgrund der Tatsache, dass in ELGA jegliche Kommunikation und alle relevanten Transaktionen über die Komponenten des ELGA-Berechtigungssystems

laufen, ist es prinzipiell ausreichend, ATNA-Protokollnachrichten nur von den unmittelbaren Akteuren des ELGA-Berechtigungssystems, insbesondere der ELGA-Zugriffsteuerungsfassade, zu betrachten.

Die Relevanz der Protokollnachrichten aus Sicht des ELGA-Portals kann noch weiter eingeschränkt werden. Grundsätzlich genügt es, für die Bedürfnisse des A-ARR nur jene ATNA-Protokollnachrichten zur Verfügung zu stellen, welche aufgrund direkter Anfrage eines IHE Document Consumer Akteurs im eigenen ELGA-Bereich am Eingang (Input) der ELGA-Zugriffsteuerungsfassade aufgezeichnet wurde. IHE ATNA-Protokolle von weiteren betroffenen Akteuren könnten zwar aus Sicht der Betriebsführung oder der Sicherheit maßgeblich werden, sind jedoch für das ELGA-Portal irrelevant. ELGA-GDA greifen ausschließlich über IHE konforme Document Consumer Akteure zu.

Für die ELGA-Teilnehmer ist es maßgeblich, neben erfolgten GDA-Anfragen auf die eigenen Gesundheitsdaten auch über modifizierende PAP-Zugriffe auf die eigenen Policies informiert zu werden.

Mit Inbetriebnahme der ELGA-Ombudsstellen (OBST), für die bekanntlich keine explizite OBST-Assertion vorgesehen ist, erfolgen die Anmeldungen bei ELGA mit einer PVP Mandate-Assertion. Aus Sicht eines ELGA-Teilnehmers ist es wichtig zu erfahren, wann ein OBST-Mitarbeiter seine Rechte ausübt und im Namen des ELGA-Teilnehmers in ELGA einsteigt. OBST-Anmeldungen müssen daher auch in A-ARR mitprotokolliert werden.

IHE-Protokollnachrichten werden aufgrund eines Zwei-Phasen-Konzeptes in die A-ARR gespeichert. Das Zwei-Phasen-Konzept hat den sicherheitstechnischen Vorteil, dass sowohl Anfang wie auch das Ende einer Transaktion protokolliert werden. Dadurch sind zwangsläufig alle Transaktionen lückenlos aufgezeichnet. Bei einem Ein-Phasen-Konzept nur am Ende einer abgeschlossenen Transaktion, könnte hingegen einen durch (einen Angreifer) erzwungenen Abbruch, der Protokolleintrag fehlen.

Das Zwei-Phasen-Konzept wird praktiziert, indem das ETS in die zu protokollierenden Transaktion aktiv eingebunden wird. Dies ist immer der Fall bei regulären IHE-Transaktionen und zwar konkret dann, wenn das ETS eine ELGA-Treatment-Assertion, User II - Assertion oder Mandate II – Assertion ausgibt. Das Zwei-Phasen-Konzept schaut im Detail wie folgt aus:

- **Erste Phase**: IHE Akteur initiiert eine IHE Transaktion im Besitz einer ELGA HCP-Assertion, ELGA User I – Assertion oder Mandate I - Assertion. Die zuständige ZGF fragt vom ETS um eine entsprechende Autorisierung. ETS protokolliert die ankommenden Autorisierungsanfragen im zur Verfügung stehenden Umfang (wer, wann, was, welche Query, welcher Request) im A-ARR (und sinngemäß immer auch im L-ARR). Dadurch entsteht ein Datensatz im A-ARR, welche über die bloße Tatsache informiert, dass eine Transaktion angefangen hat. Wenn der ETS kein Tickt ausstellen kann (weil die

Berechtigungen dies verhindern), dann wird kein Protokolleintrag im A-ARR geschrieben, sehr wohl aber im L-ARR.

- **Zweite Phase**: Wenn die Transaktion durchgeführt wird und das Resultat bei der initiierenden ZGF ankommt, wird vom ZGF ein entsprechender zweiter Event-Satz im A-ARR protokolliert (und auch im L-ARR). Dieser Datensatz ist durch die entsprechende Transaktionsnummer (Transaktionsklammer) mit dem ersten Datensatz im A-ARR verbunden. Dieser zweite Datensatz ist um zusätzliche Parameter der ausgeführten Transaktion angereichert, und beinhaltet auch das Resultat der Transaktion (Success oder Error/Exception), siehe Abbildung *50*.

Neben dem Zwei-Phasen-Konzept muss in bestimmten Fällen auch einfach (ohne Phasen) protokolliert werden, da das ETS nicht in alle Transaktionen eingebunden ist. Alle modifizierenden PAP-Zugriffe initiiert vom ELGA-Teilnehmer selbst bzw. von der ELGA-Ombudsstelle (OBST) und/oder ELGA-Widerspruchstelle (WIST) werden direkt im A-ARR gespeichert (ETS ist ja nicht beteiligt). Darüber hinaus wird beim Löschen auch kein extra Ticket vom ETS ausgegeben (siehe Kapitel Konfiguration des ELGA-Anbindungsgateways) daher muss die ZGF das Löschen direkt in A-ARR protokollieren.

Die zweite Phase der Protokollierung ist kritisch, weil sie als Teil einer verteilten Transaktion resultiert. Aus diesem Grund muss die Übertragung Reliable-Messaging verwenden. Für die Realisierung des Zwei-Phasen-Konzeptes in der ZGF ist daher eine **persistente** Queue-Komponente vorzusehen, die FIFO-Pattern implementiert (First In – First Out). Diese Komponente sollte die Nachrichten der zweiten Phase für geringe Zeit (wenige Sekunden, bis maximal 1 bis 3 Minuten) aufheben können, um eventuelle kurzzeitige Fluktuationen in der Verbindung mit dem zentralen A-ARR zu kompensieren. Bei ausreichender Bandbreite und entsprechender A-ARR-Verfügbarkeit reduziert sich die Länge der Queue automatisch auf Zero. Die Einführung einer Queue ermöglicht die Auflösung der sonst engen Kopplung zum zentralen A-ARR.

Sollte die maximal vordefinierte Länge der Queue erreicht werden (Queue Full), muss die ZGF die eigene Tätigkeit stoppen, da ein Verlust der Transaktionsresultate droht. Ein Komplettausfall der A-ARR Protokollierung ist auch bei eventuellem Queue-Verlust ausgeschlossen (z.B. Absturz des AGW/ZGF), da die Nachrichten der ersten Phase zentral vom ETS garantiert in das A-ARR eingebracht werden. In diesem Sonderfall ist jedoch keine Aussage möglich ob die Transaktion prinzipiell Daten geliefert hat.

Für Transaktionen, bei denen das ETS nicht beteiligt ist (modifizierende PAP-Zugriffe und Löschen von Dokumenten), muss vom initiierenden Akteur ein Audit Event synchron ohne dazwischengeschaltete Message Queue im A-ARR transaktionssicher gespeichert werden.

Wichtige Anmerkung: Die Architektur der Zugriffssteuerungsfassade muss sicherstellen, dass bei einem kontrollierten Abschalten (Shutdown) des Systems die hier beschriebene Queue der

Nachrichten ordentlich entleeren kann und das Abschalten entsprechend verzögert wird, bis alle sich in der Queue befindenden Nachrichten vom A-ARR entgegengenommen wurden.

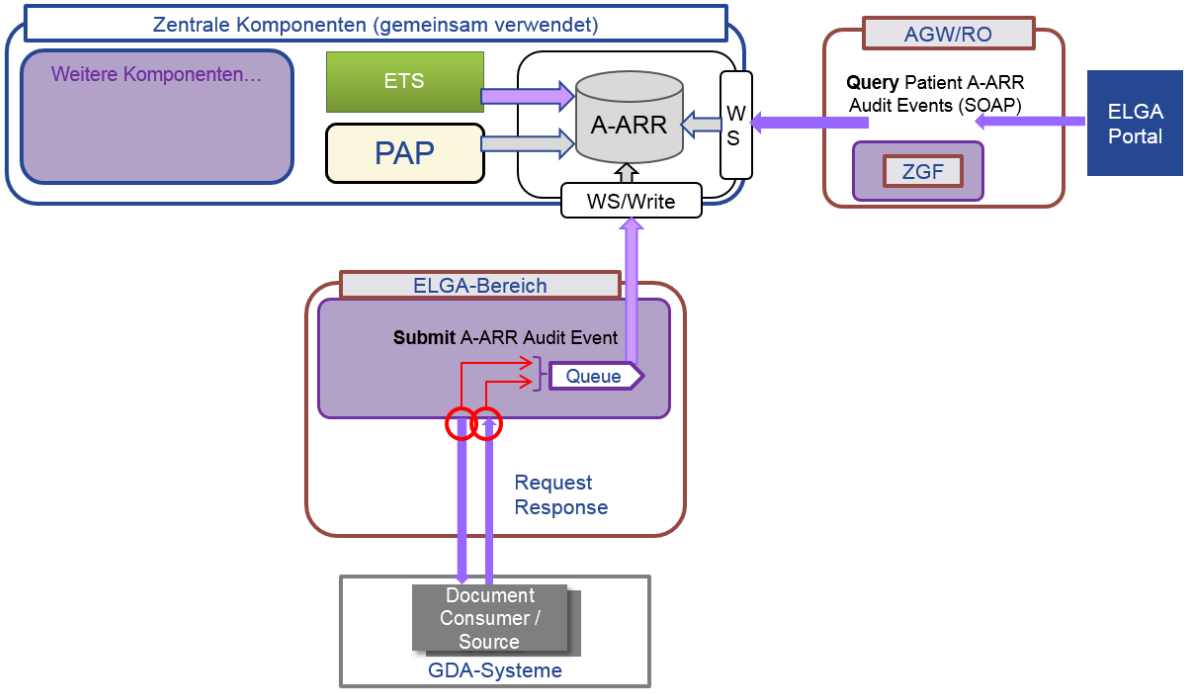


Abbildung 50: Die an den jeweiligen Zugriffsteuerungsfassaden generierten Protokollnachrichten der Document Consumer/Source Akteure sind an das A-ARR via Reliable-Messaging weiterzuleiten

9.2.5. Inhalt einer Protokollnachricht

Die in diesem Kapitel angeführten Informationen beziehen sich im Allgemeinen auf jene Akteure die gemäß IHE standardisierte Protokollnachrichten erzeugen müssen. Die Inhalte einer Protokollnachricht umfassen zumindest die hier angeführten Attribute, die bei jeder ELGA-Transaktion zu protokollieren sind:

- Transaktions-ID (Transaktionsklammer), welche vom zwischengeschalteten Berechtigungssystem zu vergeben ist
- Art des Zugriffs (lesend, schreibend, modifizierend oder löschend)
- MessageID (laut WS-Addressing Standard) bzw. Verweise auf diese ID
- Datum/Zeit der Transaktion (UTC Format)

- Zentraler Identifier des ELGA-GDAs (OID laut GDA-I) und des ELGA-Teilnehmers (bevorzugt bPK-GH)
  - Wenn Vertreterverhältnisse, dann bPK-GH von Vollmachgeber und -nehmer
- Name und Rolle der Person, die die Transaktion ausgelöst hat (SAML-Subject, siehe das Objekt Human-Requestor weiter unten)
- Ursprung/Ziel der Transaktion
- Metadaten je nach Typ der Transaktion
- Erfolgs- oder Fehlermeldung

Es sind alle Aktionen in ELGA zu protokollieren, wie:

- Einbringen/Abfragen/Ändern von ELGA-Gesundheitsdaten
- Suchen nach ELGA-Gesundheitsdaten
- Anlegen/Ändern/Suchen von ELGA-Teilnehmern
- Definieren oder Ändern von Zugriffsberechtigungen und Consent Documents
- Authentifizierung (von den zuständigen IdP)
- Autorisierung (Föderieren und das Ausstellen von Tokens über ETS)
- Abrufen von Protokoll-Nachrichten von A-ARR

Um die lückenlose Nachvollziehbarkeit aller Aktionen innerhalb ELGA zu gewährleisten, erfolgt ebenfalls eine Protokollierung protokollspezifischer Aktionen (Protokollübertragung, Protokolleinsicht). Darüber hinaus wird die Protokollierungsfunktion aller ELGA-Komponenten anhand regelmäßiger Testanfragen geprüft und die daraus resultierenden Protokolle hinsichtlich Konsistenz und Vollständigkeit validiert.

IHE Transaktionen sind gemäß IHE IT-Infrastructure Technical Framework zu protokollieren. Darüber hinaus gelten die unten angeführten globalen Audit Objektdefinitionen für alle Transaktionen, IHE und nicht-IHE.

- Globales *Human Requestor* Audit Objekt
- Globales *ELGA Transaction* Audit Objekt

Die Beschreibung der Protokollnachrichten ist dem Pflichtenheft des Berechtigungssystems [18] zu entnehmen und bezieht sich ausschließlich auf Nachrichten der Client-Systeme (GDA Systeme, ELGA-Portal, PAP Admin Tool).

Protokollnachrichten der zentralen Systeme (PAP, KBS, ETS) werden in einem optimierten, proprietären Format im Pflichtenheft des A-ARR beschrieben [19].

Die Beschreibung entspricht der Definition gemäß IHE Transaktion "Record Audit Event [ITI-20]".

9.2.6. Zusammenspiel von L-ARR und A-ARR

Die ZGF des AGW spielt eine zentrale Rolle bei der Protokollierung, da sie für das Erzeugen der ATNA-konformen L-ARR Nachrichten und der zweiten Phase der optimierten A-ARR Nachrichten zuständig ist. Die Vorgehensweise der ZGF lässt sich anhand eines zu protokollierenden Registry Stored Query ([ITI-18]) Beispiels wie folgt beschreiben:

1. Initiierende ZGF empfängt vom GDA-Akteur eine ITI-18 Anfrage. ZGF fordert beim ETS um ELGA Treatment Assertions (TA) an.
2. ETS stellt nach entsprechenden Überprüfungen eine Liste von TA aus
    a. Bevor die TA-Liste via RSTRC an die initiierende ZGF gesendet wird, findet die erste Phase der A-ARR Protokollierung statt.
        i. Wenn kein Audit geschrieben werden kann, wird der initiierenden ZGF ein Audit-spezifischer Fehler zurückgesendet.
        ii. Obiger Fault wird im zentralen L-ARR (Z-L-ARR) protokolliert
    b. Es wird zusätzlich im Z-L-ARR ein optimiertes Audit geschrieben.
        i. Wenn hier kein Audit geschrieben werden kann, wird der initiierenden ZGF ein Audit-spezifischer Fehler zurückgesendet.
3. Die initiierende ZGF hat nun eine TA-Liste erhalten und kontaktiert parallel die Responding Gateways (XCA) der entsprechenden ELGA-Bereiche. Auch wenn lokal zugegriffen wird (XDS), wird die Anfrage über das Gateway der initiierenden ZGF geführt.
4. Die betroffene ZGF (Gateway) bearbeitet die Anfrage und bevor noch eine Antwort an die initiierende ZGF gesendet wird, wird ein Audit in das L-ARR* geschrieben.
    a. Wenn wegen L-ARR* Unerreichbarkeit (oder sonstige Behinderungen) kein Audit geschrieben werden kann, wird dem initiierenden Akteur ein Audit-spezifischer Fehler gesendet.

5. Die initiierende ZGF empfängt die Resultate der Transaktion und schreibt einen Audit-Event in das L-ARR*

    a. Wenn wegen L-ARR* Unerreichbarkeit (oder sonstige Behinderungen) kein Audit geschrieben werden kann, dann muss die Transaktion abgebrochen werden. Dem initiierenden GDA wird ein Audit-spezifischer Fehler zurückgesendet.

        i. Es wird in die dafür bereitgestellte Message-Queue die zweite Phase der A-ARR Audits geschrieben, welche den Audit-spezifischen Fehler beinhaltet.

6. Die initiierende ZGF schreibt einen Audit-Event (wie oben) für die zweite Phase des A-ARR Audits in die dafür eingerichtete Message-Queue.

    a. Sollte die Message-Queue bereits übergelaufen oder das A-ARR-Service unerreichbar sein, es wird ein entsprechender Fehleraudit-Eintrag in die lokale L-ARR* geschrieben. Dem initiierenden GDA wird ein Audit-spezifischer Fehler zurückgesendet.

9.2.7. Protokollierung von schreibenden Transaktionen im L-ARR

Obiges Szenario gilt nur für lesende Transaktionen. Generell gilt, dass wenn kein Audit geschrieben werden kann, dann ist dem aufrufenden Akteur kein Dokument auszuliefern.

Da schreibende Transaktionen wegen Fehler im Auditsystem nicht rückgängig gemacht werden können, muss die Audit-Strategie dementsprechend angepasst werden. Hierfür müssen Anfang und Ende der Transaktion zweiphasig in L-ARR* dokumentiert werden.

1. Die ZGF muss bereits beim Anstoßen eines Provide an Register Document Set ([ITI-41]) die erste Phase in das L-ARR* Audit schreiben. Alternativ ist es ausreichend, einen Handshake in dieser ersten Phase mit dem L-ARR* durchzuführen und die Verbindung bis zur zweiten (End-)Phase offen zu halten.

    a. Wenn kein L-ARR* geschrieben werden kann, muss die Transaktion abgebrochen werden und dem aufrufenden Akteur eine Audit-spezifische Fehlermeldung zurückgemeldet werden.

2. Ist die schreibende Transaktion erfolgreich, dann ist die zweite Phase in die L-ARR* zu schreiben. Hierbei handelt es sich aber um eine unwiderrufliche Änderung in Registry und Repository.

    a. Wenn die zweite Phase des Protokolls nicht geschrieben werden kann (z.B. wegen L-ARR Unerreichbarkeit – was wegen des Handshakes in der ersten Phase sehr unwahrscheinlich ist), muss dem aufrufenden Akteur ein *Partial*

Success gemeldet werden, d.h. die Transaktion war zwar erfolgreich, jedoch konnte kein Audit geschrieben werden (z.B. „*Partial Success: Transaction succeeded, Audit failed*“).

Details zur Protokollierung sind im Pflichtenheft des Berechtigungssystems auszuarbeiten. Dies inkludiert die konkreten Ausprägungen der Fehlermeldungen und Fehlercodes bei Nichterreichbarkeit von Auditsystemen.

9.3. Kryptographische Algorithmen und Protokolle

Die technischen Details kryptographischer Algorithmen orientieren sich generell an gesetzlichen Anforderungen. Folglich sollten die verwendeten Algorithmen zumindest der aktuell gültigen Fassung des österreichischen Signaturgesetzes sowie der Signaturverordnung 2008 genügen. Adaptierungen spezifischer Parameter an den aktuellen Stand der Technik sind zu unterstützen.

9.3.1. Zufallszahlen und Schlüsselgenerierung

Zufallszahlen im Bereich der Kryptographie sind ausschließlich von kryptographisch sicheren Zufallszahlengeneratoren (sog. PRNG) zu erstellen. Im zentralen Bereich sind diese Aufgabe sowie das nachfolgende Generieren von symmetrischen und asymmetrischen Schlüsseln bevorzugt an HSM-Module zu delegieren.

9.3.2. Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren müssen gemäß Advanced Encryption Standard (AES) durchgeführt werden wobei die Schlüssellänge für temporäre Verschlüsselungen zumindest 128 oder 192 Bit beträgt. Für Verschlüsselung von sensitiven Daten, die längerfristig (Monate oder Jahre) aufzubewahren sind, ist eine Schlüssellänge von mindestens 256 Bit zu wählen. Wenn begründet, kann für temporäre Verschlüsselung auch Triple DES mit einer Schlüssellänge von 168 Bit verwendet werden.

9.3.3. Hashwerte

Für die Berechnung von Hash-Werten (z.B. in Signaturen) in ELGA dürfen MD5 und SHA1 nicht verwendet werden. Stattdessen müssen alle Hash-Verfahren SHA-2, zumindest aber SHA256 verwenden. Längere SHA-2 Hash-Algorithmen (SHA384 oder SHA512) sowie die Verwendung von SHA-3 sind explizit erlaubt und empfohlen.

Die Bedingungen für die Verwendung von Message Authentication Code (MAC) ergeben sich aus den bereits angeführten Einschränkungen. Dementsprechend ist ein Cipher-Based Message Authentication Code in Verbindung mit AES oder Triple DES zu verwenden.

9.3.4. Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselungen müssen RSA-Verfahren mit einer Mindestlänge der privaten Schlüssel von 2048 Bit entsprechen (siehe kryptografische Suite im Kapitel 9.3.8). Die Verwendung von ECDSA (Elliptic Curve DSA) ist auch erlaubt, wobei die NIST-standard prime Kurven P-256, 384 oder 512 zu verwenden sind. Die Verwendung und Unterstützung von sonstigen elliptischen Kurven (binäre Kurven, Koblitz Kurven, Menezes-Qu-Vanstone Kurven, etc.) ist nicht vorgesehen.

9.3.5. Digitale Signaturen

Für digitale Signaturen gilt der oben definierte Rahmen, wonach RSA oder ECDSA zu verwenden sind (DSA ist nicht vorgesehen). Diese Rahmenbedingungen sind auch für das Ausstellen von X.509 Zertifikaten (ELGA Core-PKI) zu beachten.

9.3.6. Private Schlüssel

Private Schlüssel sind grundsätzlich via entsprechende HSM zu schützen. Dies gilt sowohl für die zentralen Dienste (ETS) wie auch für das AGW/ZGF.

9.3.7. Absicherung der Transportschicht

Für die Absicherung der Transportprotokolle dürfen SSL V3.0 sowie TLS 1.0 nicht mehr verwendet werden. Es muss zumindest TLS V1.2 eingesetzt werden. Mit Ausnahme des ELGA-Portals ist es nicht erforderlich, flächendeckend Extended-Validation-TLS-Zertifikate zu verwenden. Am Portal muss die Kommunikation mit ELGA-Teilnehmern über Extended-Validation-TLS-Zertifikate abgesichert werden.

Als Konsequenz bedingt diese Anforderung für Softwareentwickler die Verwendung von zumindest Java in der Version 1.8 oder höher. Ältere Versionen dürfen NICHT eingesetzt werden.

9.3.8. Kryptographie-Anforderungen in ELGA

Obigen Anforderungen genügt die Verwendung der kryptographischen Suite TLS_RSA_WITH_AES_128_CBC_SHA256 oder die Verwendung von TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 oder TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384. Darüber hinaus sind die Alternativen mit GCM (Galois Counter Mode) als geleichwertig und zulässig einzustufen. Gemeint sind konkret die Suites TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

Kryptographie muss in ELGA in den hier aufgelisteten Anwendungsbereichen verpflichtend eingesetzt werden

- Für Server- und Client-Zertifikate mit dem Ziel, Node-Authentication gemäß IHE ATNA Profil zu unterstützen. Darüber hinaus für verschlüsselte TLS-Kommunikation zwischen beteiligten Akteuren.
- Für Token-Signaturen ausgestellt von den einzelnen vertrauenswürdigen Identity Providern und ETS.
- Für Transparent Data Encryption (TDE) in den zentralen Datenbanken zur Aufbewahrung von sensitiven Daten (PAP, KBS)
- Optional für Verschlüsselung von persistenten Daten mit sensitiven Informationen. Gemeint sind Verschlüsselungen von Tabellen und/oder Spalten in Datenbanken sowie Daten im Filesystem
- Das Signieren von CDA-Dokumenten ist in ELGA vorerst nicht vorgesehen, aber auch nicht verboten. Das Validieren von eingebrachten digitalen Signaturen kann nur bereichsintern durchgeführt werden. Hierfür muss jeder ELGA-Bereich eigene Lösungen erarbeiten. Wenn CDA signiert in ein Repository gespeichert wird, kann bereichsübergreifend derzeit die Verifikation der Signatur nicht gewährleistet werden.
- Für kryptografische Berechnungen und für die sichere Aufbewahrung von privaten Schlüsseln auf der zentralen Ebene (insbesondere ETS) sind entsprechende Hardware Security Module (HSM) vorzusehen.

9.4. Token Validierung und Identitätsföderation

Autorisierung und Zugangskontrolle zu sensitiven Daten und Services in ELGA erfolgt über gültige ELGA Authorisation Assertions. Ein Service-Provider (Relying Party) validiert die empfangenen Token zumindest im hier angeführten Umfang:

1. Die XML-Struktur der SAML Assertion ist wohlgeformt und valid im Sinne des entsprechenden XML Schemas (XSD)
2. Das zur Signatur des Tokens verwendete Zertifikat ist vertrauenswürdig konfiguriert, zeitlich gültig und wurde in den letzten Stunden nicht zurückgezogen (Zeitspanne konfigurierbar). Überprüfung aufgrund CRL oder OCSP, nicht seltener jedoch als einmal in 12 Stunden bei CRL und nicht seltener als einmal in 2 Stunden bei OCSP.
   - Darüber hinaus ist zu prüfen, ob das Zertifikat, mit dem die Signatur erstellt wurde, nicht zweckentfremdet verwendet wird. Damit ist der missbräuchlichen Verwendungen von sonst als vertrauenswürdig eingestuften Zertifikaten vorzubeugen.

- Die Prüfung (CRL oder OCSP) ergibt sich automatisch aus dem eigentlichen Zertifikat. Ist das Attribut „*CRL Distribution points*“ angeführt, muss die Gültigkeit des Zertifikates anhand der vom so angeführten URL-Endpunkt zurückgelieferten Liste festgestellt werden. Ist aber unter den „*Certificate Extensions*“ das Attribut „*Authority Information Access*“ vorhanden, muss via OCSP die Gültigkeitsprüfung stattfinden.
- In ELGA-Core ist die Prüfung ausschließlich via OCSP durchzuführen. Bei externen Zertifikaten (z.B. e-Government) ist der jeweilige CA in Verantwortung für die Offenlegung der CRL oder OCSP-Endpunkte. Wenn der CA solche Informationen nicht anführt, kann das ELGA-Berechtigungssystem hierfür nicht haftbar gemacht werden.
- Bei der Prüfung von TLS-Zertifikaten ist statt OCSP-Responder OCSP-Stapling zu verwenden

3. Die Signatur des Tokens ist kryptografisch gültig (nicht gebrochen), daher ist die Integrität des Tokens nachweislich nicht kompromittiert.
4. Der Issuer (Ausgabestelle) des Tokens entspricht dem Signaturzertifikat
5. Angegebene <Conditions> sind restlos erfüllt, und zwar
   - Aktuelles Datum/Zeit der Verarbeitung liegt innerhalb der zeitlichen Gültigkeit des Tokens
   - URL/URN-Angaben in <AudienceRestrictions> entsprechen exakt dem aktuellen Empfänger
6. Angaben in <Subject> sind restlos valide, und zwar
   - <NameID> ist ein Identifier dessen Zulässigkeit und Gültigkeit bestätigt werden kann (hierfür sind die externen Kataloge GDA-I und Z-PI, bzw. für WIST die interne Konfiguration des Berechtigungssystems zu konsultieren)
   - Methode angeführt in <SubjectConfirmation> entspricht
     - *Sender-vouches* bei Treatment-Assertion, User II und Mandate II – Assertions, Community – Assertions
     - *Bearer* bei HCP-Assertion, User I und Mandate I sowie WIST-Assertions
7. Angaben in <AuthnStatement> sind valide und entsprechen dem Context
8. Es muss ein Attribut in <AttributeStatement> mit der Angabe von „*Purpose-of-Use*“ vorhanden sein. Der angeführte Wert muss dem erwarteten zulässigen Wert entsprechen und dem angeführten Subjekt nicht widersprechen.

9. Weitere Attribute in <AttributeStatement> sind gültig und widersprechen dem Subjekt nicht. Eine Überprüfung der Attribute erfolgt in Abhängigkeit des angeführten „*Purpose-of-Use*“ und ist anhand davon abgeleiteter Konformitätskriterien zu validieren.

10. Sender-vouches Assertions zwischen den einzelnen ZGF (ELGA Treatment-Assertion, ELGA User II - Assertion und ELGA Mandate II - Assertion) sind nur einmalig zu verwenden. Eine wiederholte Verwendung bereits präsentierter Assertions - auch wenn sie zeitlich noch gültig wären - muss mit einem entsprechenden Fault (Schutzverletzung, Access Violation) beantwortet werden.

Wenn nur eine einzige Überprüfung in der Kette fehlschlägt, muss die Transaktion mit SOAP-Fault abgebrochen werden.

Darüber hinaus muss sichergestellt werden, dass Token-Inhalte und zugehörige Inhalte der SOAP-Nachricht (Body) kohärent sind, d.h. sich nicht widersprechen. Wenn z.B. ein in einer Treatment-Assertion angeführter ELGA-Teilnehmer nicht mit jenem in *Registry Stored Query* angeführten übereinstimmen, dann muss die Transaktion mit einem SOAP-Fault abgebrochen werden.

Aufgrund vertrauenswürdiger Identity Assertions (IDA) können die einzelnen Akteure föderierte ELGA-Identitäten, oder sogenannte ELGA Login-Tokens vom ETS anfordern. Ein Akteur muss hierfür einen Request Security Token (RST) über die AGW (als Proxy für dezentrale Akteure) an das ETS initiieren, wobei im Security Header der SOAP-Nachricht die IDA eingebettet sein muss. Darüber hinaus müssen im RST Request die Klasse des angeforderten ELGA Login-Tokens und die behauptete ELGA-Rolle des Akteures als „Claim“ angeführt werden. Das ETS verifiziert die zur Anfrage (RST) beigefügte IDA wie oben detailliert aufgelistet. Resultierend wird entsprechend den gültigen RST-Claims eine HCP-Assertion, User I, Mandate I Assertion oder WIST-Assertion ausgestellt.

9.5. Das Verhalten des Berechtigungssystems im Fehlerfall

Im Allgemeinen muss dafür Sorge getragen werden, dass die laufende Software des Berechtigungssystems unter keinen Umständen in einen unkontrollierten Zustand gerät. Damit sind Maßnahmen zur Gewährleistung von Transaktionssicherheit einerseits und zum Abfangen von Fehlern, Ausnahmezuständen, Abstürzen und Einfrieren des Systems andererseits gemeint. Das diesbezügliche Vorgehen muss im Pflichtenheft des BeS klar beschrieben werden. Darüber hinaus wird definiert, wie diese Fehler nach außen transportiert und an die einzelnen Akteure in der Aufrufkette weitergegeben werden bzw. wie und was zu protokollieren ist.

In ELGA geht man von hier angeführten unterschiedlichen Zuständen und Logging-Levels eines Programmes aus:

- Kritische Fehler (Critical) - sind Ausnahmesituationen, die ursächlich auf zwei Gründe zurückzuführen sind.
  - Permanenter oder längerfristiger **Ausfall von zentralen Systemkomponenten** oder des AGW/ZGF. ELGA ist dadurch generell nicht funktionsfähig. Der Zustand von essentiellen zentralen Systemkomponenten ist etwa durch permanentes Monitoren der Heartbeats von diesen Komponenten zu gewährleisten. Akteure sind gefordert bis auf Widerruf keine weiteren Anfragen an ELGA zu stellen. Ein Ausfall der hier angeführten Komponenten bedingt eine komplette Einstellung jeglicher Funktionalität von ELGA (diesbezügliche Details müssen im Pfilchtenheft des Berechtigungssystems, sowie im Pfilchtenheft der AGW erfasst werden).
    - Z-PI (Identität der ELGA-Teilnehmer kann nicht bestätigt werden)
    - KBS (Kontaktbestätigungen können weder gemeldet noch vom ETS gelesen werden wodurch keine ELGA Treatment Assertion, User II Assertion sowie Mandate II Assertion ausgestellt werden können)
    - ETS (Keine Identität kann in ELGA föderiert werden, Assertions können nicht ausgestellt werden)
    - A-ARR (Protokolle können bereits in der ersten Phase der A-ARR Protokollierung vom ETS nicht geschrieben werden, wodurch keine Treatment Assertion, User II Assertion sowie Mandate II Assertion ausgestellt werden können)
    - Zentrale L-ARR (zentrale Komponenten können nicht protokollieren wodurch alle Anfragen mit einem kritischen Fehler beantwortet werden müssen)
  - **Unvorhersehbare Ausnahmesituationen** (sog. unbekannte Fehler), die vorher nicht getestet werden konnten, weil die Konstellation der Komponentenzustände und der Betriebs-Parameter, welche zu solchen Ausnahmen führen, noch unbekannt waren. Vor weiteren ELGA-Aufrufen müssen sich Akteure über den Gesamtzustand von ELGA informieren.
- **Schutzverletzungen** (Access Violation) im Bereich der Berechtigungen der Akteure wie unzureichende Berechtigungen, keine Autorisierung, unerlaubte Zugriffe. Initiierende Akteure erfahren nur die Tatsache der unzureichenden Berechtigungen für den jeweiligen Aufruf, nicht aber die konkreten Einzelheiten. Nach einer Schutzverletzung darf der Client-Akteur die Transaktion im gleichen Kontext nicht mehr wiederholen.
- Fehler (Error) - betrifft alle erwarteten und im Vorfeld auch getesteten Fehler, die überwiegend auf die folgend angeführten Ursachen zurückzuführen sind:

- Falsche Aufrufe der angebotenen Services. Syntax des Aufrufes ist nicht korrekt. Falsche Parameter, unerwartete Werte, unbekannte Codesysteme usw. Akteure müssen genug Hinweise erhalten, um zu erfahren, dass der Fehler im eigenen Aufruf (Syntax) liegt.
- Ausfall oder Nichterreichen von Systemkomponenten, die von temporärer Natur sind. Akteure können nach wenigen Sekunden/Minuten versuchen, den Aufruf zu wiederholen.

- Warnungen (Warnings) – sind Warnungen, welche jedoch den allgemeinen Betrieb von ELGA nicht gefährden. Warnungen sind an Akteure nicht weiterzugeben. Im Betrieb muss den Ursachen der Warnungen unverzüglich auf den Grund gegangen werden, da die Häufung von Warnungen oftmals ein Vorbote für gröbere Systemausfällen sein kann.
- Informationen (Verbose Informations) – sind verbale Mitteilungen der Komponenten über den Ablauf der abgearbeiteten Schritte, welche nur bei Bedarf zu aktivieren sind (etwa Fehlersuche).

Fehlerzustände sind ausnahmslos an Ort und Stelle des betroffenen Akteures zu protokollieren (dies ist ein Default-Verhalten), und zwar:

1. Den Aufruf mit allen Parametern, der die Ausnahme verursacht hat
2. Die detaillierte Fehlermeldung des Systems (inklusive UTC-Zeit und Angaben über die beteiligten Komponenten)
3. Bei Ausnahmen (Exception) die zugehörigen (alle) Call-Stacks (Stapel).

Dem aufrufenden Akteur ist eine reduzierte Fehlermeldung zurückzusenden. Der Detailgrad der Fehlermeldung ist davon abhängig, ob es sich um einen Initialakteur handelt, oder ob der Akteur ein Vermittler in der Mitte der Aufrufkette ist. Grundsätzlich gilt, dass Call-Stacks unter keinen Umständen weiterzureichen sind. Einem Vermittler (z.B. eine ZGF ist immer ein Vermittler) können Informationen in einem hohen Detailgrad weitergegeben werden. Demgegenüber darf einem Initialakteur aus Sicherheitsgründen (um potentiellen Angreifern so wenig Angriffsfläche wie möglich zu liefern) nur eine Fehlermeldung übergeben werden, die keine Aufschlüsse auf interne Informationen zulässt.

Einem Initialakteur muss zumindest folgender Informationsinhalt vermittelt werden (Response teilweise von IHE Profilen festgelegt):

- **Fehler aufgrund falschen Aufrufs (Kategorie 1)**. Dem Initialakteur wird mitgeteilt, dass die Ursache des Fehlers im eigenen System/Aufruf liegt. Der Aufruf muss entsprechend geändert/angepasst werden.

- **Fehler (Access Violation) aufgrund unzureichender Berechtigungen (Kategorie 2)**. Der Initialakteur darf diesen Aufruf nicht mehr wiederholen. Es sind keine Details angeführt, warum und welche Berechtigung nicht vorhanden sind.
- **Sonstige auch temporäre (System-)Fehler (Kategorie 3)**. Der Aufruf war korrekt, ist jedoch aufgrund temporärer Komponentenausfälle oder sonstigen Zustände in der Verkettung der Akteure schiefgegangen. Der Initialakteur kann (darf) den Aufruf nach wenigen Sekunden/Minuten erneut probieren. Im Pflichtenheft (Schnittstellendokumentation) ist anzuführen wie oft und mit welchem zeitlichen Abstand erneut werden darf (meistens 2 bis 3-mal nach 5 – 10 Sekunden).
- **Fehler aufgrund dauerhafter Nichterreichbarkeit von ELGA-Services (Kategorie 4)**. Der Initialakteur muss entweder den Bereichsbetreiber/Hotline kontaktieren oder sich über den aktuellen und erwarteten Betriebszustand von ELGA informieren.

Darüber hinaus ist es wichtig zu vermerken, dass transaktionales Verhalten imperativ ist. Im Fehlerfall müssen durchgeführte Änderungen zurückgenommen werden und das System ist in einen sicheren, konsistenten Zustand zu versetzen.

9.6. Risikoanalyse des Berechtigungssystems

Die Aufgabe dieses Kapitels ist es, ELGA-spezifische Schwachstellen in der Struktur des Berechtigungssystems ausfindig zu machen, die auf prinzipielle und/oder architektonische Mängel zurückzuführen sind. Ziel ist es, eventuelle Risiken zu finden und Maßnahmen zur Risikominderung zu definieren. Auf nicht ELGA-spezifische, sog. allgemeine und gängige hochvirulente Angriffsmuster (z.B. *Brute-Force Attacks, Dos/DDos, Zero-Day Exploits*) wird hier explizit nicht eingegangen. Diese Risiken und die dadurch entstandenen Schäden können mehrheitlich durch entsprechende betriebliche Maßnahmen vermindert, jedoch nicht restlos ausgeschlossen werden.

Das verteilte Berechtigungssystem von ELGA muss so verwirklicht, aufgebaut und betrieben werden, dass die hier aufgelisteten Risiken entsprechend betrachtet, und dort wo es möglich ist, die genannten Maßnahmen zur Risikominderung umgesetzt werden. Die Analyse beansprucht keine Vollständigkeit, da das Risikomanagement und weitere Sicherheitsaspekte von ELGA in den entsprechenden Dokumenten der Sicherheitskommission dargestellt sind. Es werden ausschließlich softwaretechnische Risiken betrachtet, organisatorische, physische oder bauliche Schwachstellen sind nicht Gegenstand von dieser Untersuchung.

Grundsätzlich ist das Berechtigungssystem **internen** und **externen** Risiken ausgesetzt. Die Quelle der externen Risiken ist das Internet und die dort frei agierenden potentielle Angreifer. Bei internen Risiken in den abgesicherten Gesundheitsnetzwerken kann Gefahr von vertrauenswürdigen Insidern ausgehen, die sonst als „normale“ Akteure eingestuft sind.

9.6.1. Externe Risiken

Zu den externen Risiken zählen die Zugangscomputer (Laptop, Desktop, Tablet etc.) der ELGA-Benutzer, die eine aktive Verbindung zum Internet pflegen und über explizite Internetverbindung auf ELGA zugreifen. Es kann seitens des Berechtigungssystems technisch weder garantiert noch überprüft werden, ob all diese Zugangsgeräte in einem geschützten Zustand sind. Der geschützte Zustand definiert sich wie folgt:

- Das Betriebssystem hat einen aktuellen Virenschutz mit aktuellen Signaturdaten im Betrieb.
- Das Zugangsgerät ist nicht kompromittiert (ist frei von Schädlingen).
- Das Betriebssystem der Zugangsgeräte ist auf dem aktuellen Letztstand laut Vorgaben des jeweiligen Herstellers/Lieferanten etc. Aktualisierungen (Patches/Updates werden regelmäßig bezogen).
- Der verwendete Browser ist aktuell laut Vorgaben und Lebenszyklus-Management der jeweiligen Browserhersteller.

Das größte Sicherheitsrisiko geht von kompromittierten Geräten aus. Laut einschlägiger Studien sind weltweit 20 bis 40% der privaten Geräte durch Schadsoftware (Malware) befallen. Hierbei wird die Lage in Österreich zwar nicht ausufern, aber es muss damit gerechnet werden, dass zumindest jedes fünftes Gerät, das für ELGA-Zugang verwendet wird, bereits kompromittiert gewesen sein könnte. Ein kompromittiertes Gerät birgt folgende konkrete Risiken:

- Das Stehlen von Passwörtern (oder Chipkarten PIN-Code) und dadurch das Beschaffen von direktem oder indirektem Zugang zu ELGA-Daten. Dies inkludiert die Übernahme von Browser-Sessions und dadurch einen autorisierten Zugang zu ELGA.
- Das Stehlen und Weiterleiten von Gesundheitsdaten an Unbefugte (an Angreifer)
- Unbefugter Zugriff auf individuellen Berechtigungen inklusive das direkte oder indirekte Löschen (durch generelles Opt-Out) von Gesundheitsdaten sowie das Löschen von XACML-Policies.

Risikominimierung: Das ELGA-Berechtigungssystem ist nicht im Stande, zu überprüfen ob das Zugangsgerät in einem geschützten Zustand ist. Nachdem aber vom Internet kommend ELGA nur über das Portal erreicht werden kann, muss das Portal zumindest Version und Typ des verwendeten Webbrowsers überprüfen und den Zugang von veralteten Browsern (welche auf eventuell veraltetes Betriebssystem hinweist) verweigern.

Die oben aufgelisteten Risiken sind direkt proportional zur Mächtigkeit des am jeweiligen kompromittierten Gerät verwendeten Account, und zwar:

1. Das geringste Risiko geht von einem ELGA-Teilnehmer Account aus. Der Angreifer kann nur innerhalb des ELGA-Teilnehmerkontextes auf die Daten und Einstellungen des ELGA-Teilnehmers zurückgreifen.

   Risikominimierung: Wenn Gesundheitsdaten auf ein kompromittiertes Gerät heruntergeladen werden, dann könnten diese Daten vom Angreifer weitergeleitet werden, ohne später auf die Quelle der Lücke schließen zu können. Aus diesem Grund ist es notwendig, Gesundheitsdaten, die auf nicht verwaltete (frei im Internet stehende) Geräte heruntergeladen werden, zu kennzeichnen. Dadurch könnte die Lücke eindeutig identifiziert werden, bzw. nachgewiesen werden, dass die entwendeten Daten nicht von einem geschützten XDS-Repository entwendet worden sind. Grundsätzlich dürften daher CDA nicht unverschlüsselt auf die Geräte der ELGA-Teilnehmer heruntergeladen werden. Integritätsschutz von eventuell gekennzeichneten CDA-Dokumenten (XML Daten) ist nicht ausreichend, da sowohl die digitale Signatur wie auch eingebettete Merkmale leicht (etwa mit Notepad) entfernbar sind. Es dürfen CDA-Dokumente nur in konvertierter Fom (PDF Format) und mit Wasserzeichen (z.B. ID des ELGA-Teilnehmers) versehen angeboten und heruntergeladen werden.

2. Ein größeres Risiko geht von kompromittierten ELGA-GDA Accounts aus, da alle Gesundheitsdaten von ELGA-Teilnehmern mit gültigen Kontaktbestätigungen missbraucht werden können. Da ein GDA grundsätzlich keinen Zugriff auf die individuellen Berechtigungen des ELGA-Teilnehmers hat, können individuelle Berechtigungen nicht manipuliert werden.

   Risikominimierung: Es muss organisatorisch gewährleistet werden (ISMS), dass die Zugangsgeräte von (niedergelassenen) GDA im geschützten Zustand sind. Die IT der ELGA-Bereiche, mit denen sich der GDA zwecks ELGA-Zugangs vertraglich bindet, ist gefordert hier entsprechende Maßnahmen zu setzen. Die Kommunikation mit GDA-Akteuren muss über ein gesichertes Netzwerk erfolgen.

3. Das weit größte Risiko geht von kompromittierten Ombudsstellen-Accounts (OBST) aus. Da OBST-Mitarbeiter keine Kontaktbestätigung benötigen, um als berufsmäßiger bevollmächtigter Vertreter auf die Gesundheitsdaten von ELGA-Teilnehmern zuzugreifen, kann ein Angreifer praktisch die Gesundheitsdaten von beliebigen ELGA-Teilnehmern missbräuchlich entwenden. Darüber hinaus können auch individuelle Berechtigungen des ELGA-Teilnehmers durch die OBST beliebig manipuliert werden.

   Risikominimierung: ELGA-Ombudsstellen dürfen nur über gesicherte Netzwerke zugreifen können. Wenn OBST nur über das Internet zugreifen kann, dann müssen zusätzliche Schutzmaßnahmen getroffen werden. Zugangsgerät der OBST-Mitarbeiter müssen via Zertifikate eindeutig identifiziert und authentifiziert werden. Das Portal

muss beim TLS-Handshake die Zugangsgeräte authentifizieren (etwa via *Client Certificate Authentication*).

Weitere externe Risiken können auch von nicht unmittelbar kompromittierten Zugangsgeräten ausgehen. Hierfür sind zwei Fälle auseinander zu halten:

- Das Ausnutzen von unbeabsichtigtem Fehlverhalten der ELGA-Benutzer
  - Eine Browsersession wird auf einem öffentlich zugänglichen Computer nicht explizit beendet, wodurch ein Fremder unbemerkt im Namen des noch angemeldeten ELGA-Benutzers agieren kann.
  - Durch *Social-Engineering*. Die Gewohnheiten eines ELGA-Benutzers könnten ausspioniert werden um in der Folge PIN und Chipkarte zu entwenden. Besonders gefährdet Bürgerkarten mit OBST-Bestandsgeber Zertifikate
- Voll beabsichtigte und gezielte Angriffe durch professionelle Kriminelle
  - Die Schwachstellen in der Bürgerkartenumgebung werden erforscht und ausgenutzt. Sonstige Angriffe auf andere Identity Provider mit dem konkreten Ziel eines Identitätsdiebstahls.
  - Die Schwachstellen durch nicht rechtzeitig erfolgte und angewandte Patches & Updates von Host-Betriebssystemen werden erforscht und ausgenutzt.
  - Zero-Day Attacken und sonstige Methoden (Brut-Force), breit angewendet in Cybercrime.

Risikominimierung: Effektive Prävention ist durch entsprechende Intrusion Detection und Filtertechniken möglich. Aufgrund der Verwendung von XML-basierenden SOAP-Protokollen ist das Einsetzen von XML Filtertechnik in Form von Web Application Firewalls unumgänglich. Die Aufgaben zwischen einem WAF und dem schützenswerten Service (ZGF oder zentrale Services) sind in der Abhängigkeit der einzelnen bekannten Angriffs-Vektoren wie folgt (Tabelle 23: Zusammenfassung bekannten Angriffsvektoren und Maßnahmen) aufzuteilen:

Technik	Beschreibung	Aufgabe / Maßnahmen
Schema Poisoning	Manipulierung der Nachrichtenstruktur	WAF muss alle SOAP-Nachrichten gegenüber WSDL validieren
XML Parameter Tampering	Einfügen von bösartigen Scripts in die XML-Parameter	WAF muss die SOAP-Nachrichten gegenüber XSD-Schemas validieren
XDoS	Absichtlich irregulär kodierte XML/SOAP Nachricht um das Web-Service zu Fall zu bringen	WAF muss XML Kodeschema (UTF-8) entsprechend durchsetzen und sonstige Kodierungen ablehnen

WSDL Scanning	Analysieren von WSDL um gezielte Attacken durchführen zu können	Services dürfen WSDL nicht ausgeben
Coercive Parsing	Einfügen von bösartigen Inhalten in die SOAP-Nachricht	WAF muss die Nachrichten gemäß standardisiertem WS-I Profile prüfen
Oversized Payload	Das Überfluten des Systems mit großen Nachrichten	WAF muss Nachrichten, die eine bestimmte Größe überschreiten, ablehnen.
Recursive Payload	Das Senden von Nachrichten mit massenhaft verschachtelte XML-Strukturen um den XML-Parser zu Fall zu bringen	WAF muss die Nachrichten gegenüber WSDL, XSD und WS-I überprüfen
SQL Injection	Das Einfügen von SQL-spezifischen Befehlen in die Nachricht	WAF muss die Nachrichten gegenüber WS-I Profile überprüfen
Replay Attacks	Service mit mehrfach gesendeten Nachrichten überfluten	WAF muss sog. Request-Level Throttling Technologie implementieren und umsetzen
External Entity Attack	Die Nachricht enthält Verweise (URL) auf nicht vertrauenswürdige Quellen	Nachrichten mit unbekannten externen URI-Referenzen müssen von WAF abgelehnt werden
Information Disclosure	Nachrichteninhalte werden zugänglich gemacht	TLS muss flächendeckend implementiert und eingesetzt werden
Malicious Code Injection	Die Nachricht enthält bösartige Skripten	…wie oben
Identity Centric Attack	Versucht die Identität eines berechtigten Anwenders vorzutäuschen	Services müssen die Vertrauenswürdigkeit der ELGA-Assertions in erster Linie prüfen
Processing Instructions	Fügt XML PI (Processing Instructions) in die Nachricht ein, die vom XML-Parser als Text ignoriert werden.	WAF darf Nachrichten mit entdeckten PI nicht durchlassen

Tabelle 23: Zusammenfassung bekannten Angriffsvektoren und Maßnahmen

9.6.2. Interne Risiken

Es ist zwischen voll beabsichtigten Angriffsvektoren und Gelegenheitsangriffen durch unachtsames Fehlverhalten von ELGA-Benutzern (GDA, OBST) zu unterscheiden. Letzteres wurde im vorherigen Kapitel ausführlich erörtert. Es wird hier darauf verwiesen, da prinzipiell damit gerechnet werden muss (*Social-Engineering*, unbeaufsichtigte Sessions mit

angemeldetem User am KIS-System, Verlust von Chipkarten, etc.). Beabsichtigte Angriffsvektoren von Insidern mit kriminellen Energien lassen sich wie folgt betrachten:

- Kompromittierte Zugangsgeräte (vor allem Server) als primärer Risikofaktor sind auch als interne Risiken einzustufen. Insbesondere gilt dies durch die im letzten Jahrzehnt wesentlich veränderten Angriffsmuster der Schädlinge. Wenn diese früher eher auf eine größtmögliche Auffälligkeit durch den errichteten Schaden programmiert waren, sind sie mittlerweile getarnt und still, mit dem Ziel, so lange wie möglich unentdeckt zu bleiben um im richtigen Moment zuzuschlagen und entsprechende Informationen (Passwörter, Dokumente) an Angreifer unbemerkt weiterzuleiten.
  - Ein Spezialfall ist das Kompromittieren von **Identity Providern**, welches als größtes internes Gefahrenpotential einzustufen ist. Durch einen übernommenen Identity Provider kann sich ein beliebiger Angreifer als GDA für ELGA eine ordentliche SAML Identity Assertion ausstellen lassen, der dem ETS voll vertraut.

  Risikominimierung: Entsprechende IT-Maßnahmen zum Schutz der IT-Infrastruktur und der Computerlandschaft durch wohlbekannte Maßnahmen. Ausgesprochen rigorose Maßnahmen müssen zum Schutz der eingesetzten Identity Provider umgesetzt werden. Der Identity Provider muss etwa überprüfen, ob die angeforderte Identity Assertion mit dem TLS-Zertifikat des Zugriffpunktes korreliert. Identity Provider müssten grundsätzlich von entsprechenden Stellen via Zertifizierung zugelassen werden.

- Kompromittierte CDA-Dokumente sind XML Dokumente mit eingebetteten Schädlingen, meistens in Form von Scripts. Diese können etwa bei einer XML/XSLT/HTML Transformation aktiviert werden.

  Risikominimierung: Rigorose Validierung und inhaltliche Überprüfung der zu speichernden Dokumente. Gezielter Virenscan von zu speichernden CDA am AGW (nur in der Bereichsvariante „A“ möglich). Darüber hinaus Virenschutz und periodische Scans der Repositories auf bekannte Malware-Signaturen.

- Ordentlich autorisierte Zugänge

  a) GDA, die heruntergeladene Gesundheitsdaten an Unautorisierte weiterreichen

  b) GDA, die Gesundheitsdaten ändern wollen um Fehlverhalten zu verschleiern (Einstellen von neuen CDA-Versionen, Stornieren von Befunden)

  c) Regelwerk-, Datenbank- oder Sicherheitsadministratoren auf der zentralen Ebene, die Zugang zu ELGA-Daten (A-ARR) und/oder PAP (XACML-Policies) haben

  Risikominimierung: Hierfür sind keine direkten Maßnahmen möglich. Wiederholungstäter könnten jedoch durch gezielte Analyse von Auffälligkeitsmustern in den aufgezeichneten Protokollen überführt werden.

- Teilweise autorisierte Zugänge mit manipulativer Absicht sind Anfragen jener handelnden Personen in ELGA, die zwar softwaretechnisch gesehen autorisiert sind (weil im Besitz von entsprechenden HCP-Assertion), jedoch organisatorisch, seitens der Organisation (GDA), nicht befugt wurden, die ausgeführte Tätigkeit durchzuführen.

- GDA, die Kontakte beim KBS anmelden, um auf die Gesundheitsdaten von nicht in Behandlung stehenden Patienten zuzugreifen (nicht autorisierte Zugriffe). In der Regel dürfen GDA, die nicht am e-card System angeschlossen sind, Kontakte selbst einmelden. Der GDA (Organisation) bestimmt intern, wer genau autorisiert ist (z.B. Aufnahmekanzlei) Kontaktbestätigungen zu managen. Das ELGA Berechtigungssystem kann nicht zwischen intern autorisierten oder nicht autorisierten Kontaktmeldungen unterscheiden. In beiden Fällen ist der Anfrage eine vertrauenswürdige HCP-Assertion beigefügt.

  Risikominimierung: Meldung eines Kontaktes via expliziter Middleware die (etwa mit einer digitalen Signatur) für die Kontaktmeldung bürgt. Alternativ könnte eine neue ELGA GDA-Rolle (etwa Aufnahmekanzlei) eingeführt werden, welche durch den jeweiligen externen vertrauenswürdigen Identity Provider bestätigt werden könnte.

- Administratoren in den lokalen Bereichen, die via Bypass (z.B. um reguläre Clearingsaufgaben wahrnehmen zu können) autorisierten Zugang zu ELGA Gesundheitsdaten haben. Registry und Repository sind Datenbanken, die durch Administratoren verwaltet und gewartet werden. Ein Zugang auf der Datenbankebene verlangt keine explizite ELGA-Autorisierung. Gleiches gilt für den Zugang zur ATNA-Protokollierung (L-ARR).

  Risikominimierung: Hierfür sind leider keine direkten Maßnahmen möglich.

9.7. Clearing von Metadaten

Unter Clearing werden jene Geschäftsprozesse bezeichnet, die falsch zugeordnete CDA-Dokumente richtigstellen. Es gibt unterschiedliche Gründe, die dazu führen, dass einer elektronischen Identität Gesundheitsdaten falsch zugeordnet werden. Grundsätzlich muss zwischen folgenden Identitätsqualitäten unterschieden werden:

- Unbekannte Identität mit temporärem lokalen Identifier. Es geht hier in überwiegender Mehrheit um Notfälle und Aufnahmen, wo der Patient entweder nicht ansprechbar ist oder die Dringlichkeit der lebensrettenden Maßnahmen wichtiger ist, als die korrekte administrative Identifikation der Person. Hierfür werden temporäre Identifier angelegt, die später der eindeutig identifizierten Identität zugeordnet werden. Nachdem hier an den Z-PI keine PIF-Meldung erfolgen kann, können diese Gesundheitsdaten in ELGA technisch **nicht** veröffentlicht werden. Das ETS wird kein entsprechendes bPK-GH finden können und die versuchte Veröffentlichung in ELGA wird abgelehnt.

- Dem lokalen Identifier bekannte Identitäten, die entweder versehentlich falsch identifiziert sind oder doppelt angelegt sind. Die Gesundheitsdaten von falsch identifizierten Identitäten können technisch gesehen in ELGA erfolgreich veröffentlicht werden, was später Clearing erfordert. Bei doppelt angelegten Identitäten wird eine entsprechende PIF-Meldung an Z-PI fehlschlagen und die Veröffentlichung der Gesundheitsdaten in ELGA abgelehnt werden. Nach internem Clearing müssen Gesundheitsdaten in ELGA nachträglich veröffentlicht werden. Hierfür ist es wichtig, dass interne Clearingprozesse den gesetzlichen Rahmen einer Kontaktbestätigung nicht überschreiten, da ansonsten die Veröffentlichung in ELGA problematisch bis unmöglich ist.
- Dem lokalen Identifier bekannte und mit dem Z-PI via bPK-GH des Patienten abgeglichene Identitäten. Theoretisch gesehen gibt es in ELGA keinen Clearingbedarf, weil ja die lokal geführte Identität auch österreichweit (global) bestätigt ist. Ausnahmefälle sind jedoch nicht ganz auszuschließen.

Grundsätzlich wird davon ausgegangen, dass Clearing zwar in ELGA nicht ausgeschlossen, jedoch eher als Irregularität bzw. Ausnahmefall angesehen wird. Organisatorisch muss nämlich dafür Sorge getragen werden, dass nur Gesundheitsdaten von eindeutig identifizierten ELGA-Teilnehmern in ELGA veröffentlicht werden und ein Clearing der zu veröffentlichenden Gesundheitsdaten lokal bereits stattgefunden hat.

Aus Sicht des Berechtigungssystems ist Clearing in ELGA über AGW/ZGF zu führen mit dem Ziel, diese Fälle in L-ARR und A-ARR entsprechend protokollieren zu können, bzw. den vordefinierten ELGA-Hash nicht zu brechen.

9.7.1. Allgemeine Clearing Richtlinien in ELGA

Clearingfälle sind im administrativen Alltag des Gesundheitswesens Routine. Sie resultieren aus Fehlern, die wie aufgelistet zusammengefasst werden können:

- Begrenzte Qualität der Patientenidentifizierung, die zu Mehrfachidentitäten (Doubles) und falschen Identitäten führen
- Menschliche Fehler (etwa Tippfehler) beim Aufnahmeprozess, falsche Annahmen, falsche Zuordnung von Befunden
- Technische- oder Software-Fehler, werden in der Regel rasch behoben und spielen dadurch eher eine untergeordnete Rolle
- Grundsätzlich gilt: Clearingfälle müssen im GDA-System/KIS richtiggestellt werden (gilt natürlich heute auch schon) und müssen auch in ELGA „nachgezogen“ werden

Bei GDAs, in den einzelnen KIS-Systemen sowie in den lokalen Patientenindices (L-PIs) der Bereiche sind Werkzeuge im Einsatz, um inkorrekte Daten sauber, nachvollziehbar und gesetzeskonform richtigstellen zu können. Bei routinemäßiger und nicht koordinierter

Verwendung dieser Werkzeuge werden jedoch integritätsgeschützte XDS Registry-Einträge (ELGA-Hash) gebrochen. Um diese Diskrepanz aufzulösen, wird die direkte Anwendung von HL7 *XAD-PID Change Notification* Nachrichten für ein ELGA-Verweisregister (in beiden Varianten A und C) **zugelassen**. Darüber hinaus muss seitens des Auslösers des gebrochenen ELGA-Hashes dafür Sorge getragen werden, dass die **Reparaturtransaktion** [ELGA-1] genutzt wird.

- Hierbei ist zu beachten, dass Dokumente mit gebrochenem ELGA-Hashes verschwinden, ohne dabei protokolliert zu werden, aus ELGA. Diese Dokumente sind erst nach Durchführung der Reparatur in ELGA wieder sichtbar.

Die Verwendung der Reparaturfunktion [ELGA-1] ist ein bewusster Akt der Bestätigung der intern durchgeführten Clearingfälle in ELGA. Hierfür ist organisatorisch vom Bereich/GDA sicherzustellen, dass nur befugte Stellen (L-PI, GDA, Document Source Akteure) diese Transaktion ausführen. Bei der Beschreibung und Definition der Vorgänge des Clearings für ELGA wird von hier aufgelisteten grundlegenden Bedingungen ausgegangen:

- Die Qualität der Patientenidentifizierung ist durch die unmittelbare Verwendung der qualitätsgesicherten Dienste des Z-PI wesentlich erhöht. Dies wird auch im ELGA-Gesetz §4 (2) (3), sowie §18 festgehalten:
  - ELGA-G § 4: Bei ungerichteter Kommunikation haben darüber hinaus Nachweis und Prüfung der eindeutigen Identität (§ 2 Z 2 E-GovG) von Personen, deren Gesundheitsdaten weitergegeben werden sollen, zu erfolgen
  - E-GovG § 2: „eindeutige Identität“: die Bezeichnung der Nämlichkeit eines Betroffenen (Z 7) durch ein oder mehrere Merkmale, wodurch die unverwechselbare Unterscheidung von allen anderen bewirkt wird
  - ELGA-G § 18: Der Hauptverband hat im übertragenen Wirkungsbereich einen Patientenindex einzurichten und zu betreiben. Dieser dient:
    - der Überprüfung der eindeutigen Identität (§ 2 Z 2 E-GovG) natürlicher Personen im Rahmen von ELGA oder anderen eHealth-Anwendungen sowie
    - der Lokalisierung von Verweisregistern, in denen sich Verweise auf ELGA-Gesundheitsdaten dieser natürlichen Personen befinden können.
- Menschliche Fehler bei Aufnahme und Identifizierung können durch Einsatz von unterstützenden Maßnahmen (etwa: Kartenlesegeräte schließen Tippfehler aus) wesentlich reduziert werden
- Technische Fehler müssen grundsätzlich soweit irgend möglich ausgeschlossen werden
- Durch obige Maßnahmen (nur qualitativ hochwertige, via Z-PI eindeutig verifizierte Daten mit übereinstimmender Sozialversicherungsnummer und/oder bPK-GH, Geburtsdatum

und Geschlecht können in ELGA eingemeldet werden) reduziert sich der Anzahl der ELGA-Clearingfälle dramatisch, dennoch können solche Fälle nicht ausgeschlossen werden

Auf oben aufgelisteten Grundlagen gibt es in ELGA zwei diametral unterschiedliche Möglichkeiten (Strategien) Clearing durchzuführen. Die Bereiche bestimmen selbst die eigene Strategie:

- Direkte Verwendung von HL7 XAD-PID Link Change Nachricht mit bewusster Brechung eventuell existierenden ELGA-Hashes und anschließende Anwendung der [ELGA-1] Hash-Reparaturtransaktion.
- Ohne Brechen von ELGA-Hashes immer über AGW/ZGF geführten Storno [ITI-57] von falsch zugeordneten Dokumenten und anschließender Neuveröffentlichung der betroffenen (stornierten) Dokumenten via AGW/ZGF geführten [ITI-57] Assoziation Type NonVersioningUpdate

9.7.2. Clearing-Geschäftsfälle in ELGA

- Dokumente sind inhaltlich korrekt, bezeichnen den Zustand einer Identität L-PIDy, sind aber bei der Registrierung mit einer anderen Identität (L-PIDx) verlinkt worden (falschen Patienten zugeordnet). Beim Clearing müssen solche Dokumente inhaltlich nicht geändert werden. Das Clearing betrifft ausschließlich Änderungen in der XDS-Registry. Das Dokument Repository bleibt unangetastet.
- Dokumente sind inhaltlich korrekt, bezeichnen den Zustand einer Identität L-PIDx, müssen aber mit einer anderen L-PIDy verlinkt werden, wobei sowohl L-PIDx wie auch L-PIDy die elektronische Identitäten der gleichen physischen Personen bezeichnen (Patient wurde zweimal aufgenommen und wird durch Merge-Operation bereinigt. In ELGA kaum vorstellbare Konstellation).
- Dokumente sind auch inhaltlich falsch, weil identifikationsrelevante (aus der Sicht des Z-PI: VSNR, Geschlecht, Geburtsdatum) personenbezogene Attribute falsch sind. Dokument muss aufgrund falscher CDA-Inhalte neu erstellt und in ELGA neu veröffentlicht werden.

9.7.3. Richtlinien zur Verwendung von Metadata Update mit Association Type „*NonVersioningUpdate*“

Die nicht IHE-konforme Ausprägung von Metadata Update [ITI-57] mit Accociation Type *NonVersioningUpdate* wurde in ELGA eingeführt, um bereits in einem XDS-Verweisregister registrierten Metadaten in ELGA veröffentlichen zu können. Durch solche Veröffentlichung wird der betroffene Satz von Metadaten mit einem ELGA-Flag (True/False) und einem ELGA-Hash erweitert.

- Die Verwendung dieser Transaktion ist korrekt bei jenen XDS-Registry Metadaten, die in ELGA noch nicht veröffentlicht worden sind. Solche Einträge haben weder einen ELGA-Flag noch einen ELGA-Hash. Bei der ELGA-Bereichsvariante „C“ dürfte dies (bei Veröffentlichung von ELGA Dokumenten) der Regelfall sein, aber unter bestimmten Bedingung ist es auch in der ELGA-Bereichsvariante „A indirekt“ vorstellbar und nicht verboten.
- Darüber hinaus ist die Verwendung dieser Transaktion bei bereits oben genannten Clearingfällen erlaubt und korrekt. Solche Fälle zeichnen sich dadurch aus, dass documentEntry.patienID (LPID) geändert wird.
- Die Verwendung ist in allen anderen Fällen untersagt, insbesondere die Manipulation von nicht personenbezogenen Metadaten, wie Author, Status, CreationDate usw. Im Allgemeinen wäre ein solches Vorgehen grober Verstoß bezüglich Datenintegrität und muss als Missbrauch eingestuft werden.

10. ELGA-Portal

10.1. Allgemeines

Dieses Kapitel beschreibt das ELGA-Portal nur allgemein. Eine detaillierte Darstellung und das komplette Anforderungsprofil befinden sich im Anforderungsdokument ELGA-Portal V2.0 [14].

Grundsätzlich übernimmt das ELGA-Portal einerseits das Bündeln (*Mashup*) der Hintergrundservices und andererseits die Visualisierung (Präsentationsschicht) der Anwendungen in der Abhängigkeit der Autorisierung des ELGA-Benutzers. Der Datenzugriff (Data Access Layer) und die Geschäftslogik (Business Logic) wird von den abgekapselten (zentralen) Web Services implementiert. Die am ELGA-Portal implementierte Geschäftslogik integriert die Services in das Profil und in die Umgebung des jeweiligen ELGA-Benutzers.

Der Funktionsumfang des ELGA-Portals ist im ELGA-Gesetz definiert. ELGA-Teilnehmer können am ELGA-Portal zumindest folgende Funktionen abrufen:

- Einsicht in die eigenen ELGA-Gesundheitsdaten
- Wartung der individuellen Zugriffsberechtigungen
- Einsicht in die Zugriffsprotokolle betreffend die eigenen ELGA-Gesundheitsdaten
- Qualitätsgesicherte und sichere Informationsquelle für den Bürger zu Gesundheitsthemen
- Applikations-Container für weitere (künftige) ELGA-Anwendungen (wie derzeit z.B. für die e-Medikation). Künftige ELGA-Applikationen dürfen nicht zur kompletten Neuentwicklung

des Portals führen. Ein Container ist ein leerer konfigurierbarer Platzhalter für künftige ELGA-Applikationen (siehe Kapitel 11).

Protokollierungsvorgänge erfolgen gemäß den Vorgaben des ELGA-Protokollierungssystems. Sie sind aus Gründen der Übersichtlichkeit in der Abbildung *51* nicht eingezeichnet. Auch wird an dieser Stelle nicht auf Komponenten bzw. Rollen eingegangen, die aus Sicht der Administration bzw. des Supports erforderlich sind.

In der aktuellen Version des Portals sind alle Funktionen der Berechtigungsverwaltung umgesetzt worden. Eine detaillierte Darstellung der vom ELGA-Teilnehmer festgelegten individuellen Zugriffsberechtigungen wird durch das ELGA-Portal zur Verfügung gestellt. Die festgelegten individuellen Zugriffsberechtigungen (Willenserklärungen) müssen mit einer digitalen Signatur versehen und abschließend in ELGA (PAP) sicher gespeichert werden. Die diesem signierten Dokument entsprechenden individuellen Zugriffsberechtigungen sind formal als XACML Strukturen bereitgestellt.

Die Protokoll-Einsicht kann die folgenden Informationen/Tatsachen enthalten:

- Ein ELGA-GDA hat ein Dokument eingestellt, gelesen, aktualisiert bzw. storniert.
- Ein ELGA-Benutzer hat auf ein Dokument zugegriffen.
- Ein ELGA-Benutzer hat eine Dokument-Suchabfrage gemacht.
- Autorisierungen (auch fehlgeschlagene) für sich oder in Vertretung.

Der grundlegende Aufbau des ELGA-Portals entspricht den allgemein gültigen Web-Design Prinzipien und besteht aus einer Präsentationsschicht, die auf die Prozess- und Businesslogikschicht aufbaut und zuletzt über die Datenschicht auf Nutzinhalte zugreift. Für das ELGA-Portal in der aktuellen Ausbaustufe werden die folgenden Abgrenzungen definiert:

- keine integrierte Workflow Unterstützung für (institutionsübergreifende) Prozesse
- keine direkte oder indirekte Kommunikationsunterstützung über das ELGA-Portal (z.B. Messaging, Chat, Foren, etc…)
- keine Front-Office Integration
- kein Cloud-Storage/Computing

10.2. Funktionalität und Aufbau

Die primäre Funktion des ELGA-Portals ist die Vermittlung und benutzerfreundliche Darstellung von ELGA-relevanten Daten, wie der eigenen Gesundheitsakte, der individuellen Berechtigungen, der aktuellen Behandlungszusammenhänge sowie der Zugriffe auf die eigenen Gesundheitsdaten. Die zu vermittelnden Portal-relevanten Daten werden außerhalb des Portals, in den jeweiligen ELGA-Bereichen bzw. zentral gesammelt und sicher persistiert.

Die Vermittlung erfolgt durch Anbindung von spezifischen Web Services. Somit ist das Portal wie ein typischer Mashup aufgebaut, welches in seiner Basisfunktion Dienste von externen Web Services bündelt und diese orchestriert.

Die Nutzung des ELGA-Portals ist ausschließlich für authentifizierte und autorisierte ELGA-Teilnehmer möglich. Die Abbildung 51 zeigt die Komponenten des ELGA-Portals mit den am Back-End angebundenen Web Services.

10.2.1. Anonymer Zugang - Informationsportal

Das allgemein zugängliche Gesundheitsinformationsportal (*gesundheit.gv.at*) ermöglicht einen anonymen Zugang zu allgemeinen Gesundheitsinformationen, wie Hinweise und Anleitungen zur Benutzung bzw. rechtliche Belehrung. Diese Sicht bietet den eigentlichen Zugang zum ELGA-Portal, ein Sicherheitsbereich der ausschließlich über Login und Authentifizierung zugänglich wird. Der externe Identity Provider für die Authentifizierung des ELGA-Benutzers ist die Bürgerkartenumgebung (BKU) und anschließend das entsprechende Identity Provider initiated SSO STS (Single Sing On Security Token Service) des Gesundheitsportals. Die Bürgerkarten/Handysignatur-Anmeldung und der Login ist mehrsprachig in kompatibler Form anzubieten (National Language Support wird in einem künftigen Release implementiert, siehe Kapitel 10.2.5).

10.2.2. Authentifizierung und Autorisierung - Identity Management

Als grundlegendes Authentifizierungsprinzip in ELGA wird davon ausgegangen, dass die organisatorische Frage des Identity Managements externalisiert wird. Die Identifikation und Authentifizierung wird nicht durch ELGA sondern durch vertrauenswürdige (Trust) Identity Provider umgesetzt. Diese Identity Provider erstellen elektronische Authentifizierungsbestätigungen (SAML-Assertions) wie in Abbildung 3 dargestellt.

Die von einem zugelassenen (vertrauenswürdigen) externen Identity Provider ausgestellte Assertion ist explizit für ELGA bestimmt und wird folglich als ELGA-Identity-Assertion bezeichnet. Dieser Umstand muss im SAML-Element <AudienceRestriction> angeführt werden. Der konkrete Wert (Name, URN oder Domain-Name) muss im Rahmen der Pflichtenhefterstellung betreffend das ELGA-Berechtigungs- und Protokollierungssystem spezifiziert werden.

Darüber hinaus unterliegt die Struktur einer ELGA-Identity-Assertion der in der Tabelle 15 angeführten Regeln sowie verpflichtenden (und optionalen) SAML 2.0 Attributen.

Für Bürger (ELGA-Teilnehmer) ist die Authentifizierung mit der Bürgerkarte vorgesehen. Ein hierfür bestimmter Identity Provider wird unter Verwendung von MOA-ID (Module für Online Applikationen des e-Governments) und BKU online Komponenten (online Bürgerkartenumgebung) am Gesundheitsportal (*gesundheit.gv.at*) realisiert. Das

Gesundheitsportal bietet ein Identity Provider initiated Single Sign **On/Off** Service (PVP) an und dient als Drehscheibe für sichere Web-Anwendungen, etwa für das ELGA-Portal.

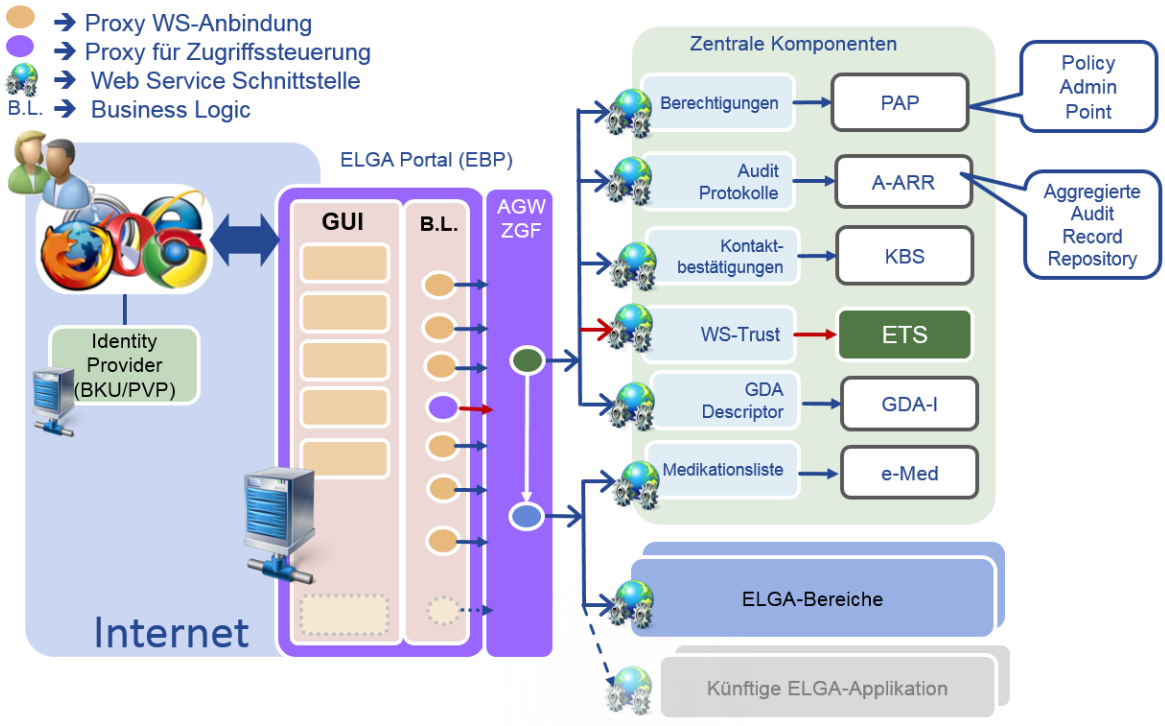
Die elektronische Abbildung von Identitäten Bevollmächtigter (gesetzlich, gewillkürt) ist gegenständliche Entwicklung im e-Government Bereich (vgl. Personenstandsregister). In jeglichen Szenarien sind als Bevollmächtigte ausschließlich die vom e-Government ausgestellten elektronischen Stellvertretungsverhältnisse anzunehmen.

Wenn die Zugriffssteuerung des EBP die präsentierte ELGA-Identity-Assertion erhält, ist die Authentifizierungsphase beendet. Ab diesem Zeitpunkt beginnt die Autorisierung (Föderation) des ELGA-Teilnehmers. Hierfür wird vom Portal (Geschäftslogik) ein WS-Trust Request Security Token (RST) an das zentrale ETS abgesetzt. Die Zugriffssteuerung des EBP präsentiert im Authentication-Header der abgesetzten SOAP-Anfrage die ELGA-Identity-Assertion und agiert im Namen des ELGA-Teilnehmers (Delegation). Das ETS verifiziert die präsentierte ELGA-Identity-Assertion gemeinsam mit den im RST mitgesendeten Informationen (ELGA-Teilnehmer, sonstige Optionen) und verifiziert diese Angaben je nach Benutzerkontext mit Hilfe des Z-PI. Anschließend wird eine gültige ELGA-*User-Assertion I* (bzw. ELGA-Man*date Assertion I* – siehe Abbildung 35) ausgestellt und an das Portal zurückgesendet (RSTR). Ab diesem Zeitpunkt ist der Anwender am ELGA-Portal erfolgreich angemeldet und entsprechend seiner Rolle (Bürger / ELGA-Teilnehmer) autorisiert Funktionen zu benutzen und Transaktionen zu initiieren.

Aufgrund modular aufgebauten autonomen ELGA-Services ist es vorstellbar, dass neben dem EBP (Abbildung *51*) auch andere Alternativportale (etwa für GDA) beauftragt und aufgebaut werden. Abbildung 52 zeigt ein solches Alternativbeispiel für ein bereichsinternes GDA-Portal, welches die auch für GDA zugänglichen ELGA-Services integriert. Die Umsetzung eines ähnlichen zentralen GDA-Portals wäre ebenso möglich.

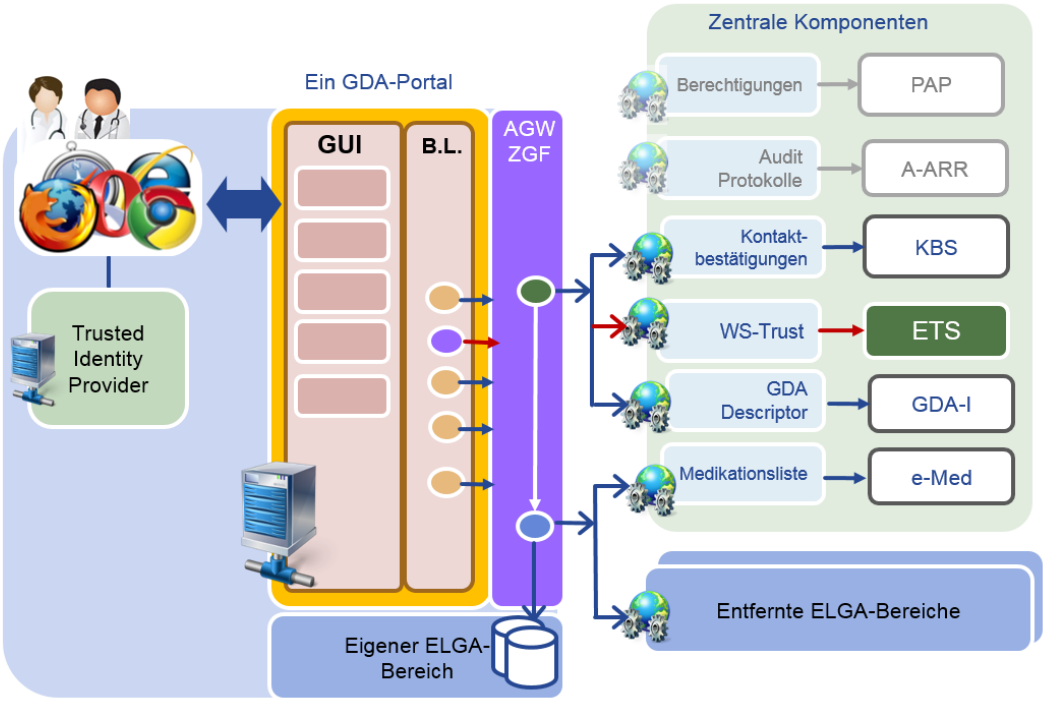
Das ELGA-Portal protokolliert (in L-ARR) erfolgreiche und fehlgeschlagene Autorisierungen gemäß den Anforderungen des ELGA-Protokollierungssystems. *Anmerkung: Fehlgeschlagene Authentifizierungen können ausschließlich auf der Seite der Identity Provider erkannt werden. Protokolle des ELGA-Portals zeichnen die anschließende Phase der Föderierung bzw. Autorisierung auf.*

5260



5261

5262 *Abbildung 51: Komponenten und Services des zentralen ELGA-Portals (EBP) mit*
5263 *Kommunikationsbeziehungen*



5264

5265 *Abbildung 52: Ein Beispiel für ein GDA-Portal. ELGA Web-Services werden über die eigene*
5266 *AGW/ZGF konsumiert*

10.2.3. Zugang basierend auf elektronischen Vollmachten

Generell werden am ELGA-Portal Bevollmächtigte nur über elektronische Vollmachten, welche durch das e-Government abgebildet sind, akzeptiert. Hierfür wählt der Bürger bei der Anmeldung vor der Auswahl der Art der Authentisierung (Karte oder Handy – siehe auch Abbildung 53) die Rolle als Bevollmächtigter aus (Checkbox für Vertretung wird gesetzt). Nach erfolgreicher Authentifizierung wird der Browser des Bürgers auf die Web-Page der Stammzahlregisterbehörde weitergeleitet (*Mandate Issuing Service*, e-Government).

Der ELGA-Teilnehmer wählt nun aus der angezeigten Liste eine zu vertretende Person aus und drückt anschließend den Button „Fortfahren“. Der Browser wird erst jetzt zum EBP umgeleitet. Dem EBP wird die ausgestellte Assertion via http-POST zugestellt. EBP überprüft die Signatur der Assertion und leitet diese an das ETS weiter, wie dies im vorherigen Kapitel detailliert erläutert wurde. Das ETS identifiziert den Bevollmächtigten sowie den Vollmachtgeber via Z-PI und stellt anschließend eine ELGA-*Mandate-Assertion I* aus. Die ELGA-*Mandate-Assertion I* repräsentiert die föderierte ELGA-Identität als Basis für die Zugriffsautorisierung.

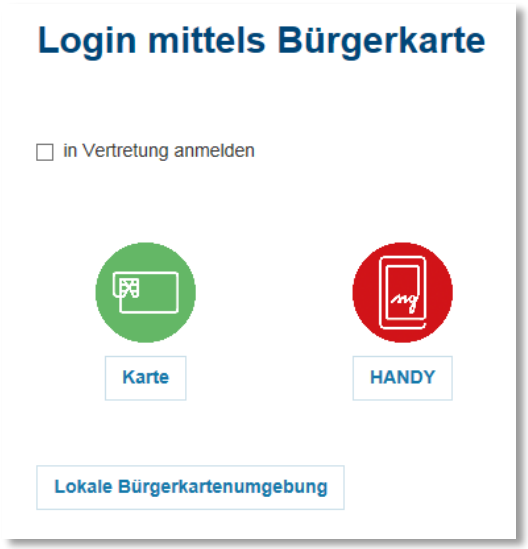


Abbildung 53: Stellvertretungsverhältnisse mittels e-Government Infrastruktur beziehen

10.2.3.1. Zugang für Ombudsstelle

Der Zugang der Ombudsstelle (OBST) wird wie ein Zugang durch einen Vertreter des Bürgers behandelt. Das physische Front-End des OBST-Portals ist netzwerktechnisch vom EBP getrennt. Es handelt sich hier um zwei getrennte Instanzen. Reguläre Vertretungen (nicht OBST) haben keinen Zugang zum OBST-Portal. Die Rolle und Identität der Ombudsstelle wird vom ETS via GDA-I bestätigt, erst danach wird eine entsprechende ELGA-Man*date-Assertion I* ausgestellt.

10.2.3.2. Zugang für Eltern in Vertretung ihrer Kinder

Das ELGA-Vertretungsmodul (VEMO siehe [26]) ermöglicht den Zugriff auf ELGA in Vertretung für:

- Eltern für Ihre Kinder, welche das 14. Lebensjahr noch nicht vollendet haben (Anwendungsfall BET.2.1a, siehe Kapitel 2.7.2) und
- Sachwalter für ihre besachwalteten Personen

Die Anmeldung in Vertretung kann in Anspruch genommen werden, sobald der ELGA-Teilnehmer authentifiziert ist und einen autorisierten Zugang zum EBP aufgebaut hat. Über die Sozialversicherungsnummer des Kindes oder der besachwalteten Person, wird die zu vertretende Person ausgewählt. Hierfür wird von e-Government die entsprechende Oberfläche (GUI) bereitgestellt. EBP sorgt bei Aktivierung der Funktion für die Umleitung des Browsers auf diese Auswahlseite. Wenn die Auswahl der Person abgeschlossen ist, wird der Browser zum EBP zurückgeleitet und das Vertretungsmodul (als Businesslogik-Komponente) aktiviert.

- Prüfung der Bedingungen für eine positive Vertretungsbefugnis aus dem Titel „*Eltern für Kinder*“
  - Das zu vertretende Kind hat das 14. Lebensjahr noch nicht vollendet.
  - Es liegt vom Vertreter ein abgeleiteter Krankenversicherungsanspruch vor.
  - Die Wohnadresse des Vertreters und des zu vertretenden Kindes laut Zentralen Melderegister (ZMR) sind ident.
- Prüfung der Bedingungen für eine positive Vertretungsbefugnis aus dem Titel einer „*Sachwalterschaft*“
  - Es liegt eine eingetragene Sachwalterschaft im Standardprodukt „Zentrale Partnerverwaltung (ZPV)“ vor.

Die Feststellung der Vertretungsbefugnis aus einem der beiden Titel erfolgt parallel. Sind alle Vorbedingungen eines Titels („Eltern für Kinder“ oder „Sachwalterschaft“) erfüllt, wird für den Vertreter eine normale ELGA Mandate-Assertion I ausgestellt.

10.2.4. Funktionsumfang

Autorisierten ELGA-Benutzern stehen abhängig von deren authentifizierten Rollen entsprechende Funktionen zur Verfügung. Das ELGA-Portal stellt diese Funktionen via spezifischer Visualisierungskomponenten (GUI) zur Verfügung. Die Liste der möglichen und angedachten Funktionen für autorisierte ELGA-Teilnehmer lautet wie folgt:

- **Opt-Out Erklären:** Wenn ein ELGA-Teilnehmer Opt-Out erklärt, werden sämtliche vorher für ELGA registrierte Gesundheitsdaten und Berechtigungsregeln gelöscht oder dauerhaft

unzugänglich gemacht (siehe Kapitel 7.1.4, Variante C). Ab diesem Zeitpunkt kann ein authentifizierter Bürger am ELGA-Portal nur mehr Opt-Out-Widerruf erklären.

- **Opt-Out Widerruf**: Es sind weder Gesundheitsdaten noch individuelle Berechtigungsregeln im System vorhanden. Der ELGA-Teilnehmer startet mit einer inhaltlich leeren ELGA (mit Ausnahme bereits vorhandener Protokolle). Ab diesem Zeitpunkt eingestellte (registrierte) Gesundheitsdaten sowie alle Zugriffsprotokolle (auch jene vor dem Opt-Out, soweit nicht älter als 3 Jahre) werden ganz normal sichtbar. Individuelle Berechtigungen werden aufgezeichnet.

- **Behandlungszusammenhang (Kontaktbestätigungen)**: Nach erfolgreicher Anmeldung kann der ELGA-Teilnehmer die aktuelle Behandlungszusammenhangs-Liste (Synonym: Kontaktbestätigung) angezeigt bekommen. Aufgrund des aktuellen Behandlungszusammenhangs können Zugriffe der in Relation stehenden GDA, erweitert oder eingeschränkt werden. Aktuelle Behandlungszusammenhänge (Arztkontakte) werden über eine Schnittstelle (Web Service) in das zentrale KBS gespeichert.

- **Dokumenten Browser**: Diese Komponente erlaubt dem ELGA-Teilnehmer, nach seinen medizinischen Dokumenten (und in künftigen Versionen des Portals auch nach Bildern) zu suchen und diese abzurufen. Die Abfrage unterstützt diverse Filterkriterien wie Datum, Dokumentenklasse, Aufenthalt etc. Der **Dokumenten Browser** nutzt die serviceorientierte Schnittstelle (Web Service) eines *Document Consumers* im eigenen Bereich (Abbildung *51*). Der *Document Consumer* setzt die Abfrage auf standardisierte IHE-Transaktionen um.

- **Berechtigungsverwaltung**: Diese erlaubt es dem ELGA-Teilnehmer seine individuellen Zugriffsberechtigungen zu warten. Das Berechtigungsverwaltungs-GUI ist an eine zentrale serviceorientierte Schnittstelle (Web Service) angebunden, welche mit dem zentralen *Policy Administration Point* (PAP) verbunden ist. Die gesetzten Zugriffsberechtigungen werden gemäß dem Integrationsprofil *Basic Patient Privacy Consent* dokumentiert, digital signiert und gespeichert. Im Hintergrund werden XACML Regeln (Policies) erstellt und im PAP persistiert. Einschränkende Regeln können gemäß gesetzlichen Möglichkeiten definiert werden.

Protokollbrowser: Diese Komponente bietet dem ELGA-Teilnehmer die Möglichkeit, die Protokolldaten einzusehen. Die Realisierung erfolgt über eine serviceorientierte Schnittstelle (Web Service), welche mit dem A-ARR verbunden ist. Der Protokollbrowser liefert dem ELGA-Teilnehmer eine kumulative Standardsicht der aufgezeichneten Ereignisse bezüglich der Datenzugriffe zur eigenen Gesundheitsakte. Ist der zugreifende ELGA-GDA eine Organisation (Krankenanstalt), dann bietet die Standardansicht zumindest diese Information an (Name der Anstalt). Ist der ELGA-GDA keine Organisation sondern eine natürliche Person (Arzt), dann werden vom ETS Zugriffsberechtigungen an diese Person vergeben, folglich enthält auch die Standardsicht zumindest die Angaben (Name) der zugreifenden Person. Als Design-Prinzip

wird angenommen, dass die Darstellung für den ELGA-Teilnehmer in transparenter und übersichtlicher Form zu erfolgen hat:

- Die lesenden Zugriffe innerhalb eines definierten Zeitraums durch einen ELGA-GDA werden aggregiert (z.B. Angabe des Tages aber ohne Uhrzeit).
- Bei schreibenden Zugriffen werden alle Zugriffe mit genauem Zeitpunkt angeben.
- Weitere Detaildaten können gespeichert, aber nur für Nachforschungen einem Administrator sichtbar gemacht werden bzw. auf Anfrage dem Bürger schriftlich zugestellt werden.
- Darüber hinaus hat der ELGA-Teilnehmer die Möglichkeit, Protokolle im Detail zu betrachten. Dadurch wird im Falle *Zugriff durch eine Organisation* auch der Name der natürlichen Person, die auf ELGA zugegriffen hat, ersichtlich. Hierfür muss der ELGA-Teilnehmer aus der Liste der in der Standardansicht angezeigten Protokollzeilen eine bestimmte auswählen und dann die Detail-Ansicht anfordern. Dadurch werden alle Einzelheiten des ausgewählten Zugriffs vom A-ARR geholt und dargestellt.

10.2.5. UML Komponentendiagramm der Portal-Infrastruktur

Die in der Abbildung *51* schematisch dargestellte Portal Web-Applikation wird über ein ELGA-Anbindungsgateway (AGW) an die ELGA-Infrastruktur angebunden. Aus der Abbildung 54 ist es klar ersichtlich, dass alle Anfragen, die an das Portal über ein Web-Browser (User-Agent) gestellt sind, über den zuständigen AGW einerseits an die zentralen Komponenten weitergeleitet werden (Proxy-Funktion des AGW) und andererseits von der ZGF-Komponente bearbeitet und an die entfernten ELGA-Bereich weitergeleitet werden. Das Innenleben von AGW (ZGF, Proxy und WAF) ist in der Abbildung 42 detailliert angeführt.

Schnittstellen, die vom Portal über die Proxy-Funktionalität des AGW erreicht werden:

- ETS via WS-Trust
- KBS via WS-Trust
- A-ARR lesende Schnittstelle
- GDA-Index lesende Schnittstelle
- PAP via WS-Trust Protokoll
- PDQ an Z-PI

Schnittstellen, die über die zwischengeschaltete ZGF erreicht werden

- PHARM-1 an die ELGA-Anwendung e-Medikation
- ITI 38 und 39 an die entsprechende XCA responding Gateways der ELGA-Bereiche

Schnittstelle zum Terminologieserver

- Die Anbindung an den Terminologieserver erfolgt über eine proprietäre SOAP-basierte Webserviceschnittstelle. Mehr diesbezüglich ist im Kapitel 12 Terminologieserver angeführt.

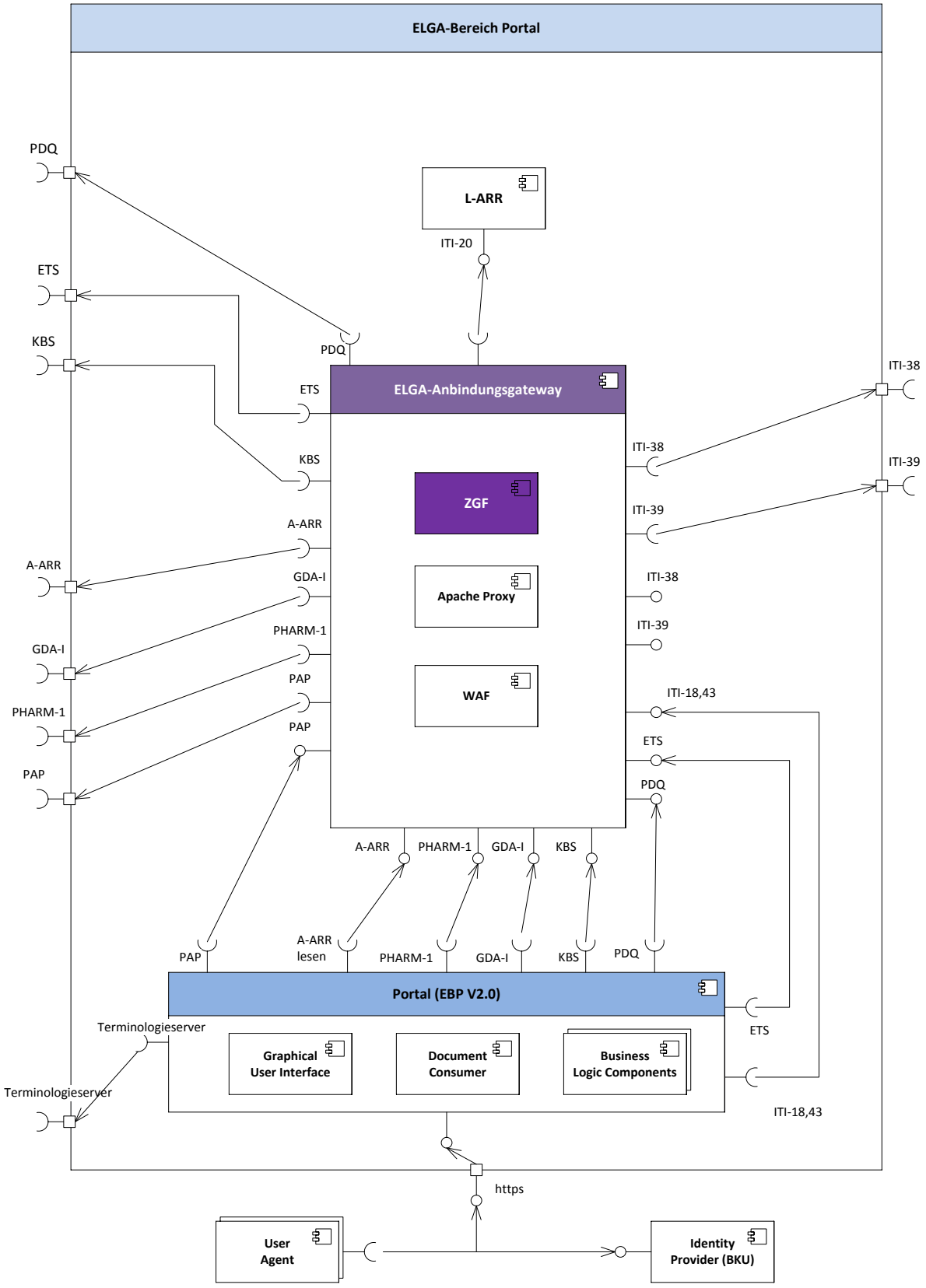
Abfrage Codesystems/Valuesets

Periodische Übernahme von Anzeigetexten für GDA-Rollen, Fachgebiete und Dokumententypen. Im Regelfall fragt der Batch den Terminologieserver danach ab, ob eine aktuellere Version des Codesystems/Valuesets vorhanden ist. Falls ja, so wird dieses geladen und an den Aufrufer zurückgeliefert. Die Abfrage und das Update der lokal am Portalserver gespeicherten Codesystems/Valuesets muss mindestens monatlich erfolgen.

National Language Support

Dient dazu, den Austausch von Gesundheitsdaten mit europäischen Patienten zu erleichtern. Die Ablage der einzelnen Textelemente in verschiedenen Sprachen hat am Terminologieserver zu erfolgen. Hilfetexte, Feldinhalte (XDS-Metadaten) und Protokolleinträge sind in die ausgewählte Sprache zu übersetzen. Alle vom Portal generierten Dokumente (z.B. Willenserklärungen) sind zweisprachig auszugeben: Im selben Dokument ist der Text in Deutsch und darunter in der ausgewählten Sprache auszugeben. Die Abfrage und das Update der lokal am Portalserver gespeicherten Texte müssen mindestens wöchentlich erfolgen (wird in einer künftigen Release implementiert.)

Anmerkung: Die Auflistung der eigenen Komponenten des Portals (GUI, Document, Consumer, Business Logic) in der Abbildung 54 ist nicht vollständig.



5415

5416 *Abbildung 54: UML-Komponentendiagramm des ELGA-Bereiches zur Anbindung des Portals*

5417

11. ELGA-Applikationen

11.1. Allgemeine Definitionen

e-Befund und e-Medikation sind zwei freigegebenen ELGA-Anwendungen (Services), welche den einheitlichen Rahmenbedingungen des ELGA-Berechtigungssystems bzw. dessen Autorisierungs- und Schutzfunktionalität folgen. Beide ELGA-Anwendungen sind im Codesystem OID 1.2.40.0.34.5.159 mit den Werten 101 (e-Befunde) und 102 (e-Medikation) abgebildet.

Die ELGA-Architektur ermöglicht die Erweiterung der ELGA-Funktionalität durch die Integration weiterer spezialisierter ELGA-Applikationen (Anwendungen oder Services). Eine ELGA-Applikation muss sich nahtlos in die bestehende Architektur der ELGA sowie deren Sicherheitskonzept integrieren lassen. Jede ELGA-Applikation ist als Relying Party (RP) im Sinne von OASIS WS-Trust zu betrachten. Daraus ergibt sich die Voraussetzung, dass der Zugang ausschließlich auf Basis von präsentierten SAML2 Assertions, die vom ELGA-Token-Service (ETS) ausgestellt worden sind, möglich ist.

Konsumenten (Akteure) von ELGA-Applikationen sind GDA-Systeme oder das ELGA-Portal. Konsumenten müssen von externen vertrauenswürdigen Identity Providern authentifiziert werden und anschließend eine SAML Assertion vom ETS anfordern (ELGA-HCP-Assertion, oder ELGA-User-Assertion, usw.).

Eine ELGA-Anwendung (synonym: ELGA-Applikation) muss zusätzlich alle folgenden, taxativ zu verstehenden Anforderungen erfüllen:

Funktionale Anforderungen

- Eine ELGA-Anwendung ist eine Software oder ein Verbund von Softwarekomponenten, mit dem Zweck, nützliche oder gewünschte Funktionalitäten für Patienten oder GDA in vernetzter Form bereitzustellen. Diese besteht aus mindestens zwei Funktionsblöcken: Der Eingabe (input), der mehrwertschaffenden Verarbeitung oder Speicherung und der Ausgabe (output). Ein- und Ausgabedaten sind dabei in jedem Fall Patientengesundheitsdaten.

Organisatorische Anforderungen

- Eine Anwendung wird durch Gesetz, ministerielle Verordnung oder durch die ELGA-Generalversammlung als ELGA-Anwendung definiert, approbiert oder beauftragt. Bei der Implementierung und im Betrieb ist jede ELGA-Anwendung den ELGA-Informationssicherheitsmaßnahmen und weiteren, durch die der ELGA-Systempartner beschlossenen Regelwerke, unterworfen.

Technische Anforderungen. Eine ELGA-Applikation muss folgende Kriterien erfüllen:

- Verwendung des ELGA-Berechtigungssystems
- Verwendung des ELGA-Protokollierungssystems
- Eine eindeutigen ELGA-Anwendungsnummer im Codesystem mit der OID 1.2.40.0.34.5.159
- Unterstützung der durch die ELGA-Entscheidungsträger beschlossenen Architektur und Standards und zwar:
  - Unterstützung der im OASIS Standard WS-Trust V1.4 definierten Protokolle.
  - Angebotene Dienste werden via serviceorientierter Schnittstellen, bevorzugt über Web Services, realisiert.
  - Es wird zumindest eine serviceorientierte Data Service Schnittstelle angeboten, welche zum Anbinden von konsumierenden und speichernden GDA-Systemen zur Verfügung gestellt werden.
  - IHE Transaktionen können laut entsprechenden IHE XDS und/oder XCA Integrationsprofile initiiert werden.

Beispiele für weitere ELGA-Anwendungen sind e-Patientenverfügung, e-Impfpass. Erstere ist im nächsten Kapitel als mögliches Beispiel demonstriert.

11.2. e-Befunde

11.2.1. Ausgangssituation

Die Bereitstellung von Gesundheitsdaten (CDA-Dokumente) der ELGA-Teilnehmer an autorisierte Akteure ist die Basisfunktion von ELGA, welche auch als erste (primäre) ELGA-Anwendung oder erstes ELGA-Service angesehen werden kann. Im Weiteren wird auf diese Basisfunktion mit der Bezeichnung e-Befunde referenziert. Das Fachkonzept e-Befunde ist im Codesystem OID 1.2.40.0.34.5.159 mit dem Wert 101 festgeschrieben.

11.2.2. Aufzählung der relevanten Anwendungsfälle

In den folgenden Tabellen sind nur spezielle Anwendungsfälle ausgewählt und entsprechend kommentiert, die von der ELGA Anwendung e-Befunde implementiert werden und auch bereits in den Tabellen: Tabelle 2, Tabelle 3, Tabelle 4, Tabelle 6 aufgelistet sind.

Akteur / User-Agent	No	Anwendungsfall	Anmerkung / Beispiel
ELGA-Teilnehmer via Web-Browser oder Touch-Screen	ET.1.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken

Applikation (Zugriff vom Internet)	ET.1.9	Ein bestimmtes CDA-Dokument auswählen, öffnen	CDA ist als XML zur Verfügung zu stellen (Darstellung ist ausgelagert am Portal)
	ET.1.11	Ein bestimmtes Bildmaterial auswählen bzw. öffnen	Bildmaterial wird via KOS-Objekte referenziert (Darstellung über das Portal)
	ET.1.12	Vorversionen eines bestimmten CDA-Dokumentes öffnen	Ausgehend von einer geöffneten aktuellen Version

5479 *Tabelle 24: e-Befund Anwendungsfälle von ELGA-Teilnehmern*

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
Bevollmächtigter ELGA-Teilnehmer via Web-Browser oder Touch-Screen Applikation (Zugriff vom Internet)	BET.2.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen (im Namen des Vertretenen)	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken
	BET.2.9	Ein bestimmtes CDA-Dokument im Namen des Vertretenen auswählen bzw. öffnen	Darstellung ist Aufgabe des Portals
	BET.2.11	Ein bestimmtes Bildmaterial im Namen des Vertretenen auswählen bzw. öffnen	Bildmaterial ist via KOS-Objekte zugänglich
	BET.2.12	Vorversionen eines bestimmten CDA-Dokumentes im Namen des Vertretenen öffnen	Ausgehend von einer geöffneten aktuellen Version

5480 *Tabelle 25: e-Befund Anwendungsfälle von bevollmächtigten Vertretern*

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-GDA via KIS-System oder Arztsoftware (Kein Internet-Zugriff erlaubt)	GDA.3.9	Dokumentenliste zu einem Patienten abrufen	Registry Stored Query wird ausgelöst
	GDA.3.10	Dokument(e) zu einem Patienten abrufen	Retrieve Document Set wird ausgelöst.
	GDA.3.14	Ein oder mehrere Instanzen (Studien) der bildgebenden Diagnostik auswählen und abrufen	Bildmaterial ist ausschließlich via KOS-Objekte zugänglich
	GDA.3.15	Vorherige Version eines bestimmten Dokumentes abrufen	Verlinkte ältere Version des Dokumentes kann abgerufen werden

	GDA.3.16	Ausgewählte Dokumente des Patienten speichern	Wie GDA.3.10 mit anschließendem Speichern
	GDA.3.17	Registrieren (freigeben) eigener Dokumente in ELGA	Provide and Register Document Set wird ausgelöst
	GDA.3.18.a	Updaten von ELGA-Dokumenten	Einstellen neuer Versionen von CDA-Dokumenten
	GDA.3.18.b	Storno von ELGA-Dokumenten	Dokumente stornieren und dadurch unzugänglich machen
	GDA.3.20	Update von ELGA-Dokumenten bei abgelaufener Kontaktbetätigung	Wie Anwendungsfälle GDA.3.18.a und 3.18.b mit dem Unterschied, dass eine abgelaufene (bis zu einem Jahr) Kontaktbestätigung ausreichend ist

Tabelle 26: e-Befund Anwendungsfälle von GDA

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Ombudsstelle via Web-Browser (Zugriff über das ELGA-Portal vom gesicherten Netzwerk)	OBST.5.8	Liste ausgewählter Gesundheitsdaten (CDA) ansehen (im Namen des Vertretenen)	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken
	OBST.5.9	Ein bestimmtes CDA-Dokument im Namen des Vertretenen auswählen, öffnen	Darstellung ist Aufgabe des Portals
	OBST.5.11	Ein bestimmtes Bildmaterial im Namen des Vertretenen auswählen bzw. öffnen	Darstellung ist Aufgabe des Portals
	OBST.5.12	Vorversionen eines bestimmten CDA-Dokumentes im Namen des Vertretenen öffnen	Ausgehend von einer geöffneten aktuellen Version

Tabelle 27: e-Befund Anwendungsfälle von OBST

11.2.3. Profilierung

Es ist anzumerken, dass sich die Anwendungsfälle ET.1.8, BET.2.8, GDA.3.9 sowie OBST.5.8 grundsätzlich und sehr allgemein auf die Suche nach relevanten Gesundheitsdaten beziehen, welche technisch via Registry Stored Query ([ITI-18]) realisiert wird. Diese Transaktion erlaubt aber gemäß IHE eine breite Palette an spezifischen Query Methoden die mit Namen und ID definiert sind (siehe Liste in IHE_ITI_TF_Vol2a.pdf). Das ELGA-Berechtigungssystem und die

ELGA-Anwendung e-Befunde schränken jedoch ELGA Document Consumer Akteure entsprechend der vorgesehenen Anwendungsfälle ein, indem nur die vorgesehenen Query IDs verwendet werden dürfen.

- *GetAll* (urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3) für die Suche nach all jenen Dokumenten (bzw. DocumentSets) eines bestimmten Patienten (*PatientID*), die in einem bestimmten Status (*Approved*, *Deprecated – sog. avilabilityStatus*) vorhanden sind.
- *FindDocuments* (urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d) für die Suche nach bestimmten, den erlaubten Kriterien entsprechenden Dokumenten eines Patienten (*PatientID*). Zu den Kriterien zählen Metadaten wie *classCode* (Dokumentenklasse) *typeCode*, *authorPerson* (freie Zeichenkette, hier ist keine GDA-OID angeführt), *formatCode*, *availabilityStatus*, *serviceStartTime*, *serviceStopTime* (Beginn und Ende der Gesundheitsleistung), *creationTime* und *objectType*. Die Liste ist abschließend.

11.2.4. Interaktionsmuster

Das e-Befunde Interaktionsmuster eines GDAs bzw. ELGA-Teilnehmers ist in der Abbildung 55 dargestellt. Ein GDA interagiert mit der ELGA-Anwendung e-Befunde immer über ein entsprechendes KIS-System (oder Arzt-Software), welches als Web-Service Client e-Befunde anspricht. Darüber hinaus erfolgen Request/Response immer und ausschließlich über dafür zuständige AGW/ZGF-Pärchen. Ist der Zugriff innheralb XDS (bereichsintern), dann sind initiating- und respondig- AGW/ZGF ein und dasselbe. Im Unterschied zum GDA nutzt der ELGA-Teilnehmer das Portal (EBP), welches als Client für Service-Aufrufe etabliert ist. Hierfür sind initiating- und responding- AGW/ZGF immer getrennte Instanzen.

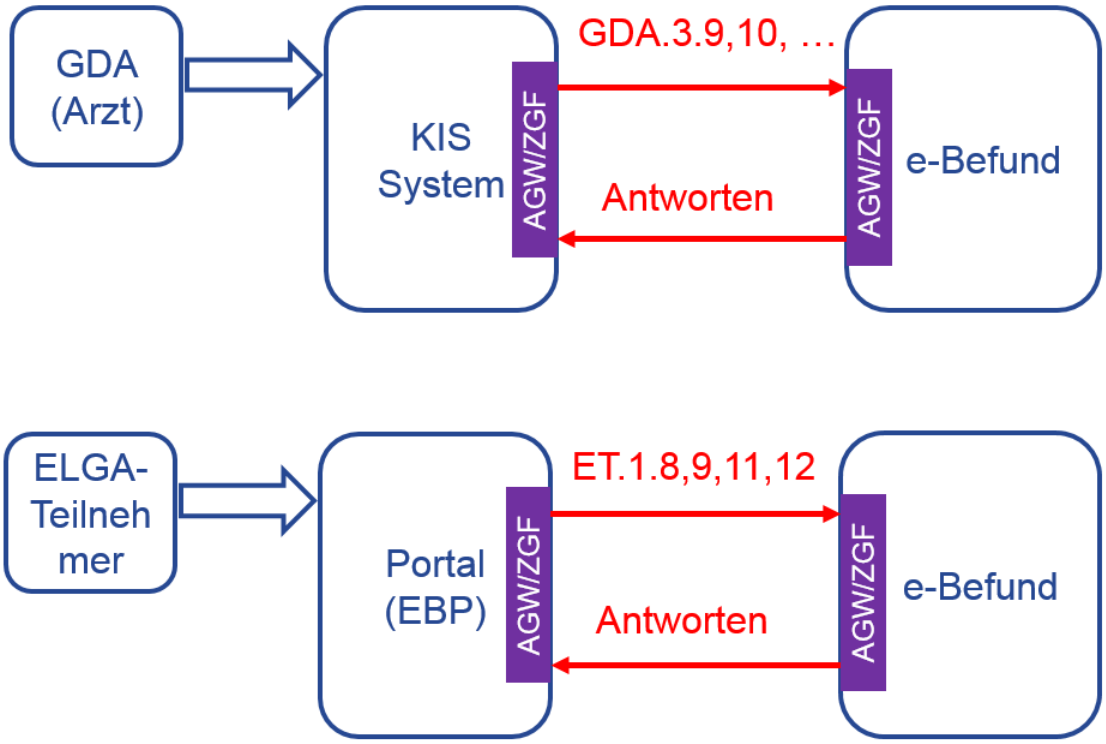


Abbildung 55: e-Befunde Interaktionsmuster

11.3. e-Medikation

11.3.1. Ausgangssituation

Von 04/2011 bis 12/2011 wurde das Pilotprojekt e-Medikation in drei Pilotregionen in Österreich durchgeführt. Die Evaluierung, die seit Mitte 2012 vorliegt, beinhaltet auch technische Aspekte und Anforderungen, die in die Planung der Österreichversion der e-Medikation einfließen. Die gegenständlichen Anforderungen stellen das Rahmenwerk dar, das in weiterer Folge im entsprechenden Projekt zur Errichtung der e-Medikation noch verfeinert werden muss.

11.3.2. Anforderungen

e-Medikation ist im Codesystem OID 1.2.40.0.34.5.159 mit dem Wert 102 festgeschrieben. Die konkreten Anforderungen bezüglich e-Medikation sind unter [15] detailliert nachzulesen. Darüber hinaus hat e-Medikation nachfolgenden Anforderungen zu genügen:

- e-Medikation ist eine ELGA-Anwendung, die über interne Datenspeicherung und Geschäftslogik verfügt und CDA-Dokumentenaustausch gemäß XDS zu unterstützen hat.

- e-Medikation kann (lesend dokumentenorientiert) über das ELGA-Portal angesprochen werden. Die primäre Anbindung erfolgt jedoch über ärztliche und pharmazeutische IHE Akteure (Prescription placer, Pharmaceutical adviser, Medication dispenser, siehe e-Med Consumer/Source in der Abbildung 57).
- Entsprechend der von allen Systempartnern gemeinsam beschlossenen Nutzung existierender Informations- und Kommunikationsstandards hat auch die e-Medikation auf Basis der relevanten IHE Profile zu beruhen.
- Darüber hinaus sind die allgemein gültigen IHE Profile und OASIS Standards (insbesondere XDS und XSPA) zu berücksichtigen, um einem ELGA-konformen Datenaustausch zu entsprechen.
- Auch die e-Medikation unterliegt der Hoheit des ELGA-Berechtigungssystems.

11.3.3. Aufzählung der relevanten Anwendungsfälle

Akteur / User-Agent	No	Anwendungsfall	Anmerkung / Beispiel
ELGA-Teilnehmer	ET.1.10	Eigene Medikationsliste einsehen	On-Demand Dokument stellt e-Medikation zur Verfügung, Darstellung am Portal
Bevollmächtigter ELGA-Teilnehmer	BET.2.10	Medikationsliste im Namen des Vertretenen einsehen	On-Demand Dokument stellt e-Medikation zur Verfügung
ELGA-GDA	GDA.3.11	Medikationsliste des Patienten abrufen	On-Demand Dokument von e-Medikation anfordern
	GDA.3.12a	Ein oder mehrere e-Med-ID holen	[EMEDAT-1] Anfrage an e-Medikation stellen
	GDA.3.12b	Verordnung bzw. Advice eines oder mehrerer Medikamente speichern	Dokumente via e-Medikation speichern
	GDA.3.12c	e-Med-ID Token abholen	e-Med STS wird angesprochen
	GDA.3.13	Abgabe eines oder mehrerer Medikamente speichern	Abgabe via e-Medikation dokumentieren
ELGA-Ombudsstelle	OBST.5.10	Medikationsliste im Namen des Vertretenen einsehen	Stellt e-Medikation zur Verfügung

Tabelle 28: e-Medikation Anwendungsfälle

11.3.4. e-Medikation Interaktionsmuster

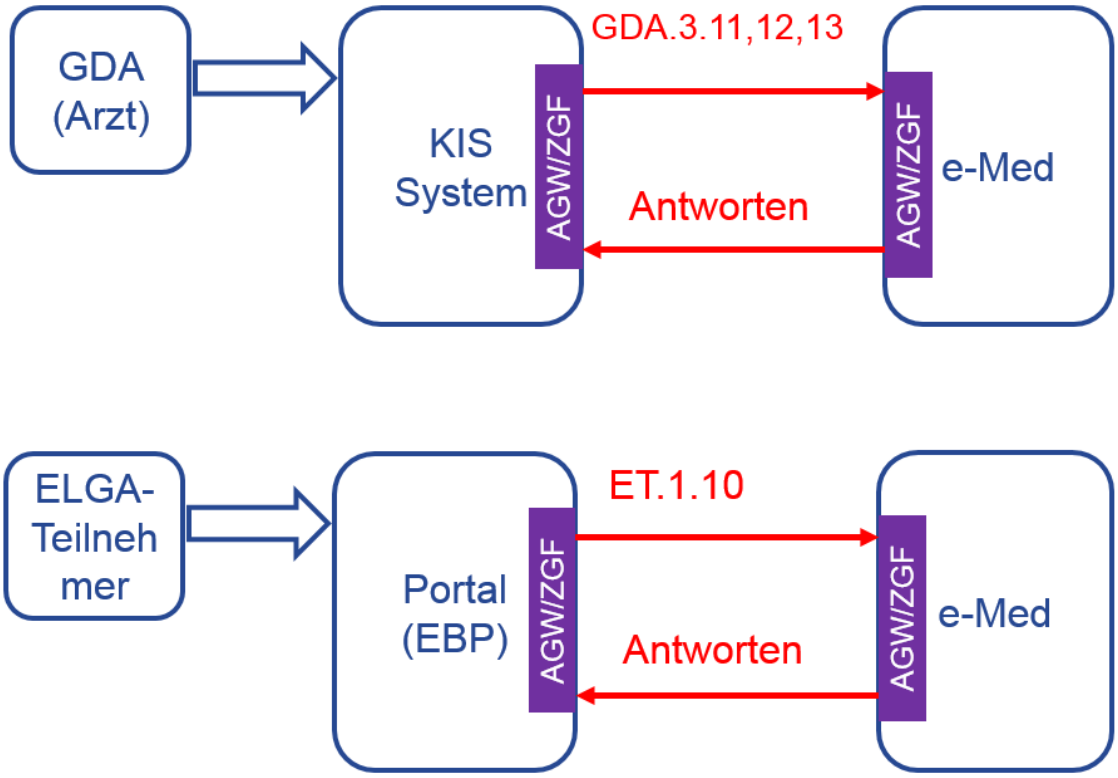


Abbildung 56: e-Medikation Interaktionsmuster

11.3.5. Architektur

Die ELGA-Anwendung e-Medikation ist ein Informationssystem laut ELGA-Gesetz §16a. Alle e-Medikation Zugriffe in ELGA unterliegen der Autorisierungspflicht des ELGA-Berechtigungssystems. Somit ist e-Medikation vollständig im ELGA-Kernbereich (siehe Kapitel 3.1) integriert.

Die innere Architektur der Anwendung wird durch die entsprechenden IHE Pharmacy Technical Framework Profile bestimmt (derzeit alle Supplements for Trial Implementation). Demnach kapselt e-Medikation eine selbstständige XDS Affinity Domain, die über die vorgeschaltete ELGA-Zugriffssteuerungsfassade (in der Abbildung 57 ZGF-2) zugänglich gemacht wird.

Die GDA Akteure (e-Medikation Source und e-Medikation Consumer) erreichen die zentrale ELGA-Anwendung e-Medikation über die Zugriffssteuerungsfassade des eigenen ELGA-Bereiches (in der Abbildung 57 ZGF-1). Hierfür muss die Schnittstelle der Zugriffsteuerungsfassade entsprechend erweitert werden (siehe Abbildung 58).

Anmerkung: Die Bezeichnung ZGF-1 und ZGF-2 beziehen sich auf unterschiedlich konfigurierte, jedoch funktional und inhaltlich ident ausgelieferte Instanzen eines ELGA-Anbindungsgateways mit eingebetteter Zugriffsteuerungsfassade.

Darüber hinaus muss die innere Fachlogik der ELGA-Zugriffssteuerungsfassade an den bereits vorhandenen schreibenden und lesenden Schnittstellen (ITI-41, 42 und 43) die Dokumentenklassen (*Document.Class* und *Document.Type*) richtig erkennen um das rollenabhängiges Speichern zu unterstützen. Apotheker dürfen z.B. keine Prescription-Dokumente speichern, nur Abgaben. Dies ist aber nicht ausschließlich für e-Medikation erforderlich.

Die Zugriffssteuerung bietet eigene Endpoints für e-Medikation an. Somit müssen e-Medikation Document Source-Akteure andere URLs ansprechen als einfache Document Consumer Akteure. Die Zugriffssteuerung routet dann diese Anfragen nahtlos an die ELGA-Anwendung e-Medikation weiter.

Die dadurch entstandenen entfernten (remote) Zugriffe sind zwar XDS-Transaktionen, müssen jedoch wie XCA-Transaktionen mit einer gültigen ELGA-Treatment Assertion autorisiert werden. Dies ist darin begründet, dass diese Transaktionen bereichsübergreifend stattfinden (zwischen anfragendem ELGA-Bereich und der antwortenden ELGA-Anwendung).

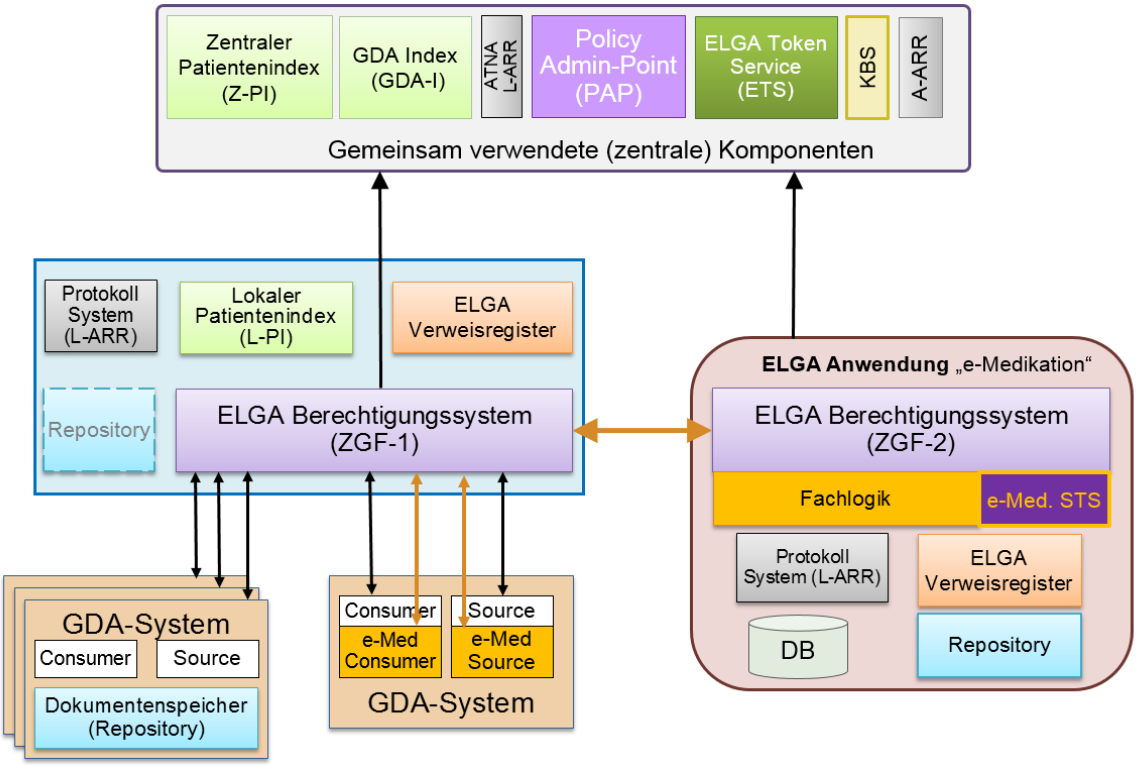


Abbildung 57: Übersicht der Architektur der ELGA-Anwendung e-Medikation

Die Zugriffsautorisierung auf die ELGA-Anwendung e-Medikation wird zusätzlich erweitert. Die e-Med-ID berechtigt einen ELGA-GDA für Zugriffe auch dann, wenn keine explizite Kontaktbestätigung vorliegt. Dieser Zugriff ist aber streng limitiert und beschränkt sich auf die

Dokumente, die unmittelbar mit der e-Med-ID verlinkt sind. Die Autorisierung solcher Transaktionen liegt in geteilten Verantwortungen des ETS und des STS der e-Medikation. Somit wird ermöglicht, Verschreibungen auch ohne explizite Patientenkontakte (Stecken der e-card) einzulösen. Die damit verbundene Vorgehensweise ist weiter unten detailliert beschrieben.

An der ELGA-Zugriffssteuerungsfassade sind folgende Schnittstellenerweiterungen vorzusehen (Abbildung 58), wobei die hier ankommenden Anfragen nach entsprechender Prüfung der Autorisierung immer an die ELGA-Anwendung e-Medikation weitergeroutet werden müssen:

1. Laut IHE Vorgaben *Query Pharmacy Documents* [PHARM-1] inklusive der spezialisierten Queries:
    a. *FindPrescriptionsForDispense*()
    b. *FindDispenses*()
    c. *FindPrescriptions*()
    d. *FindMedicationList*()
2. Österreicherweiterung Schnittstelle [EMEDAT-1] inklusive der Methoden
    a. *GenerateDocumentId*()
    b. *RequestSecurityToken() eine* WS-Trust Schnittstelle des e-Med-Security Token Service (STS)

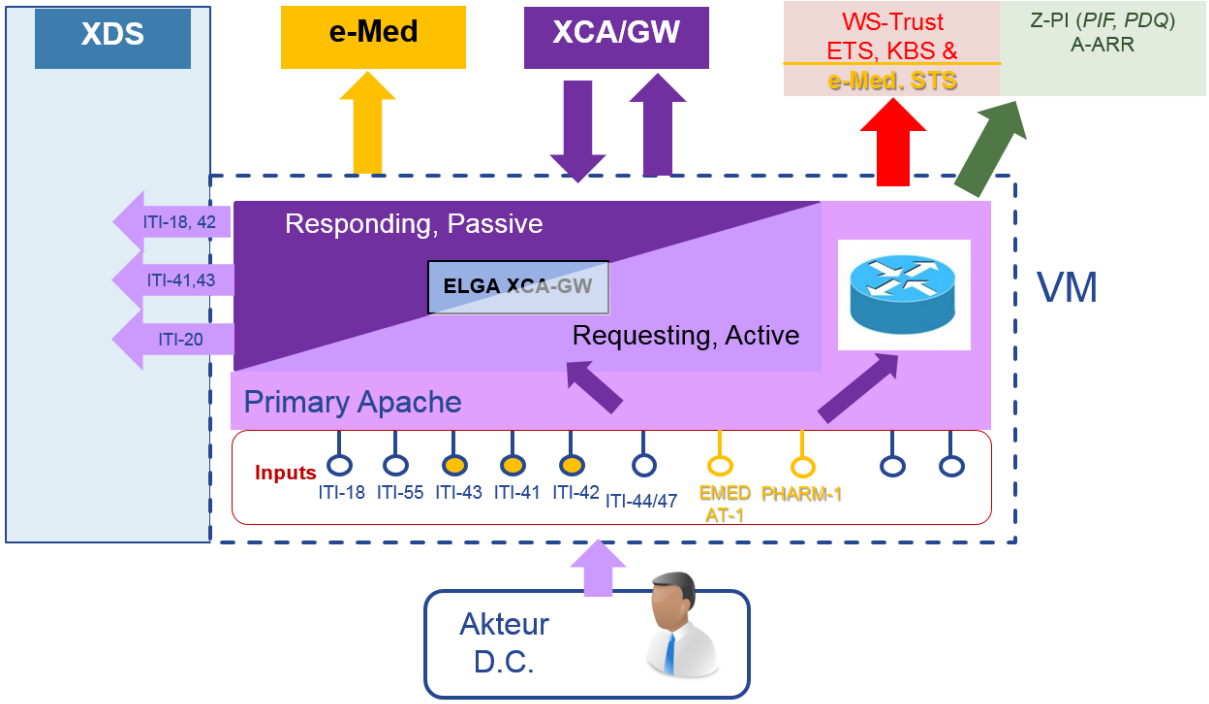


Abbildung 58: Erweiterung des ELGA-Anbindungsgateway (mit ZGF). Schnittstellen der e-Medikation sind gelb gekennzeichnet und markieren die notwendigen Erweiterungen.

In ELGA gilt grundsätzlich und ausnahmslos, dass für GDA-Zugriffe immer gültige Kontaktbestätigungen im KBS vorhanden sein müssen. Dieses Prinzip gilt zwar noch immer auch für e-Medikation, es wird aber eine zusätzliche Möglichkeit angeboten, für Berechtigte GDA auch ohne e-card Kontakt des Patienten einen eingeschränkten Zugriff auf die entsprechenden e-Medikationsdaten zu gewähren.

Wie im Kapitel 3.12 erläutert, entstehen Kontakte entweder automatisch beim Stecken der e-card oder über dafür vorgesehene Prozesse (Aufnahme/Entlassung) in Krankenanstalten bzw. Pflegeheimen. Für das Speichern von solchen Kontakten muss der Patient eindeutig identifiziert werden. Diese Vorgehensweise, insbesondere jene mit e-card, funktioniert grundsätzlich auch für e-Medikation. Es ist jedoch nicht davon auszugehen, dass dies der Regelfall wird, da beim Einlösen eines Rezeptes keine e-card gesteckt werden muss.

In der Regel ist der Prozess der Abgabe (*Dispense*) einer Verschreibung (*Prescription*) ein unpersönlicher Akt. Hierfür muss der Patient weder persönlich erscheinen noch die Identität der rezepteinlösenden Person geprüft werden. Dennoch muss es für den GDA (Apotheker) eine Möglichkeit geben, die Identität des Patienten zu erfahren, um auf die mit dem einzulösenden Rezept verlinkten Dokumente zugreifen zu können bzw. die Abgabe zu speichern.

Das diesbezügliche pharmazeutische Datenmodell, welche das obige Problem löst, ist rund um eine sog. Verordnungs-ID (oder e-Med-ID) aufgebaut. Die e-Med-ID ist eine weltweit

eindeutige Zahl, welche nach strengen kryptografischen Zufallsprinzipien generiert wird. Sie wird auf die Anfrage eines berechtigten Akteurs von der ELGA-Anwendung e-Medikation generiert (siehe EMEDAT-1/*GenerateDocumentId*) und auf das auszustellende Rezept (Verordnung) aufgedruckt (Abbildung 59).

Diese Zahl (e-Med-ID) wird auch beim Speichern der Verordnung herangezogen. Nämlich spätestens beim Speichern ([ITI-41]) der Verordnung verknüpft e-Medikation die e-Med-ID mit dem bPK-GH des betroffenen Patienten.

Anmerkung: Eine e-Med-Id kann zwar auch bereits bei der Anforderung (via GenerateDocumentId) mit einer Sozialversicherungsnummer verknüpft werden, es ist aber nicht erforderlich, da dies beim Speichern automatisch gewährleistet wird. Somit können e-Med-ID Zahlen auch auf Vorrat geholt werden, um notfalls offline Rezepte erstellen zu können.

Bei der Abgabe wird lediglich die so präsentierte e-Med-ID benötigt, um zuerst ein e-Med-ID Token vom Security Token Service (STS) der ELGA-Anwendung e-Medikation anzufordern (*RequestSecurityToken*). Das STS der e-Medikation überprüft die, in der gesendeten Anfrage als Claim enthaltene, e-Med-ID und versucht diese Zahl aufzulösen. Es wird die Patientenidentität bestimmt sowie die gesendete Zahl verifiziert. Die Patientenidentität (bPK-GH) wird folglich in ein signiertes Token verpackt. Der Token wird an den e-Med Document Consumer zurückgesendet. Im Besitz dieses Tokens und der im Token enthaltenen Informationen können nun die entsprechenden IHE-Transaktionen ordnungsgemäß angestoßen werden. Wichtig ist zu vermerken, dass der e-Med Document Consumer nun neben der ELGA HCP-Assertion auch das e-Med-ID Token im Authorisation Header der SOAP-Nachricht mitsendet. Eine gültige Kontaktbestätigung ist damit nicht mehr erforderlich.

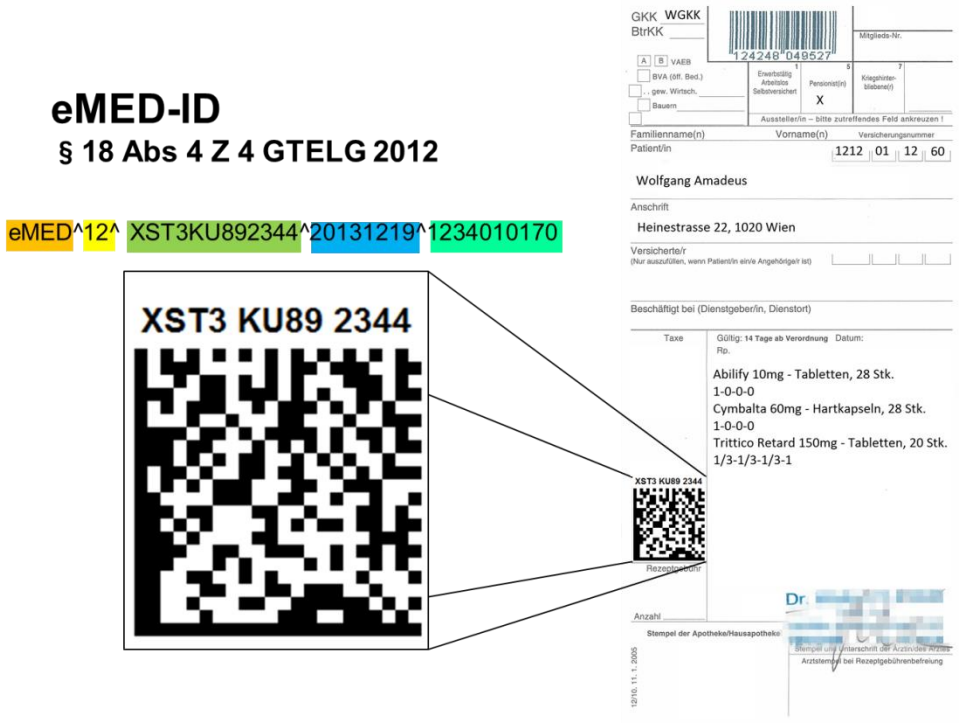


Abbildung 59: Aufdruck der e-Med-ID als 2D-Matrixcode auf einem Rezept

11.3.6. Workflow e-Med-ID

Nachfolgende Schritte beschreiben den kompletten Prozess von der Verordnung (Schritte 1 bis 4) bis zur Abgabe (ab Schritt 5) der Medikation:

1. GDA-Software erstellt Prescription-Document entsprechend den ELGA-CDA Implementierungsleitfäden für e-MEDAT. Als Patienten ID wird die L-PID des lokalen Bereichs bzw. SVNr beim niedergelassenen Arzt verwendet.
2. GDA-Software fordert über die ELGA-Zugriffssteuerung des eigenen ELGA-Bereichs eine e-Med-ID an (*GenerateDocumentId*) oder nimmt eine solche Zahl vom Vorratsspeicher (siehe vorherige Anmerkung im Kapitel 6.2.3).
3. GDA-Software speichert über die ELGA-Zugriffssteuerung des eigenen ELGA-Bereichs (ZGF-1) das erstellte Dokument mit der ermittelten e-Med-ID als Dokumenten-ID ([ITI-41] Provide and Register Document Set). Die Anfrage muss an den für e-Medikation freigeschalteten Endpunkt (URL) adressiert werden.
4. Die ELGA-Anwendung e-Medikation prüft Struktur (z.B. CDA valid, etc.) und Inhalt (z.B. Dokumentenklasse, Mime-Type, etc.) des übermittelten Dokuments und legt dieses im Falle eines positiven Prüfergebnisses im e-Medikations-Repository/Registry unter Verwendung des bPK-GHs des Patienten ab. Dabei werden alle Informationen die zur Erzeugung der Medikationsliste erforderlich sind, für einen schnellen Zugriff zusätzlich in der e-Medikationsinternen Datenbank strukturiert abgelegt.
5. Rezept wird nun (anonym) in einer Apotheke (ELGA-GDA) eingelöst. ELGA-GDA (Apotheker) scannt die e-Med-ID vom Rezept ein.
6. GDA-Software fordert über die Proxy-Funktion der ELGA-Zugriffssteuerung (ZGF-1) mit *RequestSecurityToken()* und einer gültigen ELGA-HCP-Assertion sowie der vorher eingescannten e-MED-ID des einzulösenden Rezeptes einen sog. ***e-Med-ID Token*** an.
7. GDA-Software leitet die Anfrage an das *Security Token Service* (STS) der e-Medikation. e-Med-STS prüft die gelieferte e-Med-ID und stellt bei positivem Prüfergebnis einen ***e-Med-ID Token,*** eingeschränkt auf die gelieferte e-Med-ID, aus. Dieser Token enthält die bPK-GH des Patienten und die e-Med-ID. Als zusätzliches Response-Attribut des *RequestSecurityTokenResponse* wird das bPK-GH des Patienten geliefert.
8. GDA-Software (e-Med. *Document Consumer*) empfängt den für eine maximale Dauer von 2 Stunden ausgestellten und signierten ***e-Med-ID Token***, der den GDA zum Absetzen

der damit verbundenen IHE-Abfragen berechtigt - und zwar ohne Vorhandensein einer expliziten Kontaktbestätigung.

9. GDA-Software fordert nun über die ELGA-Zugriffssteuerung (ZGF-1) mit der IHE-Transaktion [PHARM-1] *Query Pharmacy Documents* (*FindPrescriptionsForDispense*) die relevanten Dokumente an. Für diese Abfrage sind die gescannte e-Med-ID und das bPK-GH des Patienten mitzugeben.

10. Die ELGA-Zugriffssteuerungsfassade (ZGF-1) überprüft nun die Autorisierung der Anfrage (*ELGA-HCP-Assertion* und ***e-Med-ID-Token***) und holt vom ETS eine entsprechende *e-MED-Treatment-Assertion* ab. Die *e-MED-Treatment-Assertion* unterscheidet sich von einer regulären *Treatment Assertion* dadurch, dass sie auch ohne eine gültige Kontaktbestätigung ausgestellt werden darf. Sollte aber der Patient entweder:

    - ein generelles Opt-Out oder
    - ein partiell auf e-Medikation beschränktes Opt-Out erklärt haben oder
    - den GDA gesperrt haben (0 Tage Zugriff)

    antwortet das ETS mit einem SOAP-Fault und die Transaktion wird beendet. Ist dies nicht der Fall, wird die ursprüngliche PHARM-1 Anfrage mit der gültigen *eMED-Treatment-Assertion* und ***e-Med-ID Token*** an die ELGA-Anwendung e-Medikation weitergeleitet.

11. Die vor e-Medikation vorgeschaltete ELGA-Zugriffssteuerungsfassade (ZGF-2) prüft die Autorisierung der Anfrage (*eMED-Treatment Assertion*) und leitet diese mit dem ***e-Med-ID-Token*** an die unmittelbar angeschlossene e-Medikation weiter.

12. Die e-Medikation ermittelt die Metadaten der entsprechenden Dokumente sowie etwaiger vorhandener zugehöriger Dokumente (z.B. Pharmaceutical Advices für Änderungen, Dispense-Dokumente falls bereits Abgaben auf der Basis dieses Rezepts existieren) und retourniert das Ergebnis.

13. Die vor der e-Medikation vorgeschaltete ELGA-Zugriffssteuerungsfassade (ZGF-2) exekutiert nun die individuell erstellten Filterkriterien (*Enforcement*). Wenn die Anfrage mit ***e-Med-ID Token*** (bzw. *eMED-Treatment-Assertion*) autorisiert war, verlässt sich die ZGF auf die von der e-Medikation gelieferte Liste.

14. Die GDA-Software bekommt nun das Resultat der PHARM-1 Query

15. GDA-Software holt nun über die ELGA-Zugriffssteuerung (ZGF-1) das zu der e-Med-ID gehörige *Prescription-Dokument* und alle weiteren zugehörigen Dokumente über die Transaktion [ITI-43] *Retrieve Document Set*. Hierfür müssen im *SOAP-Authorisation Header* immer *ELGA-HCP-Assertion* und ***e-Med-ID-Token*** eingebettet werden.

16. GDA-Software ermittelt den Status jeder einzelnen Verordnung (*Prescription Item*) auf dem Rezept (*Prescription*) mittels der Verlinkung mit den eventuell vorhandenen zugehörigen Dokumenten. Die Verlinkung erfolgt über die *Prescription Item ID*, welche die Verbindung der Verordnung über alle zugehörigen Dokumente darstellt. Nach diesem Schritt liegt die endgültige Form jeder einzelnen Verordnung vor (Status offen/bereits abgegeben, nachträgliche Änderungen eingearbeitet, etc.)

17. GDA-Software erstellt pro Abgabe einer Verordnung auf einem Rezept ein Dispense-Document entsprechend den ELGA-Leitfäden für e-MEDAT mit Referenzen auf die jeweilige Verordnung (*Prescription Item ID)*.

18. GDA-Software speichert jedes erstellte Dispense-Document (via [ITI-41] *Provide and Register Document Set*) in der e-Medikation. Die ELGA-Anwendung (Fachlogik) prüft die Daten vom ***e-Med-ID Token*** gegen die im Dispense-Document referenzierte Verordnung (*Prescription Item* im CDA-Element substanceAdministration). Es dürfen nur jene Abgaben (Dispense-Items) gespeichert werden, die auf Prescription-Items referenzieren, und mit dem ***e-Med-ID Token*** verlinkt sind.

19. Die ELGA-Anwendung e-Medikation prüft Struktur und Inhalt jedes übermittelten Dokuments und legt es im Falle eines positiven Prüfergebnisses im e-Medikations-Repository/Registry unter Verwendung des bPK-GHs als Patient-ID ab. Dabei werden alle Informationen die zur Erzeugung der Medikationsliste erforderlich sind für einen schnellen Zugriff zusätzlich strukturiert abgelegt.

11.4. Patientenverfügung (Zukunftsausblick beispielhaft)

11.4.1. Ausgangssituation

Derzeit werden die Patientenverfügungen durch Notare, Rechtsanwälte und die Patientenanwaltschaft verwahrt. Die Notare betreiben eine zentrale Applikation zum Ablegen der Patientenverfügungen, welche mit dem Dokumentenarchiv der Notare verbunden ist. Das Rote Kreuz hat, sofern die Patientenverfügung vom Notar entsprechend gekennzeichnet wurde, Einsicht in das Archiv. Es stellt ein rund um die Uhr besetztes Call-Center bereit, das GDA zur Recherche nutzen.

Rechtsanwälte verwalten Patientenverfügungen ebenfalls elektronisch, jedoch (noch) nicht gemeinsam mit den Notaren. Über die IT-Unterstützung der Patientenanwaltschaft ist nichts bekannt.

Die Identifikation des Bürgers erfolgt über die von e-Government zur Verfügung gestellte Infrastruktur betreffend elektronische Vollmachten. Dies ist möglich, wenn die Notare mit einer Bürgerkartenumgebung ausgestattet sind. Die Identifizierung (Authentifizierung) erfolgt über

eine personenbezogene, vom Bestandsgeber ausgestellte, elektronische Karte, welche ein vom e-Government unterstütztes Zertifikat präsentieren kann.

11.4.2. Annahmen

- Ziel ist die Bereitstellung der Patientenverfügung in ELGA mit möglichst geringfügiger Anpassung der Erfassungsprozesse.
- Die Funktionserweiterung sollte in Form einer ELGA-Applikation bereitgestellt werden.
- Das Registrieren in ELGA erfolgt durch Notare, Rechtsanwälte oder Patientenanwälte, die durch Bürger bevollmächtigt wurden und in ELGA somit den ELGA-Benutzer *Bevollmächtigter* in der Rolle *Verwalter PV* einnehmen. Die Autorisierung basiert auf Prinzipien und Funktionen des e-Governments. Transaktionen in ELGA werden anhand des ELGA-Berechtigungssystems autorisiert.
- Der Lesezugriff ist für definierte GDA-Rollen (z.B. Krankenanstalt, Arzt) und den Bürger selbst möglich. Zum Lesen der Patientenverfügung dürfen keine weiteren Anforderungen für den Zugriff gestellt werden. Eine individuelle Veränderung dieser Policies durch den Bürger ist daher nicht erforderlich.

11.4.3. Architektur

Es wird vorgeschlagen, die Patientenverfügung als Dokumentenklasse zu registrieren. Für diese Dokumentenklasse werden spezifische generelle Zugriffsberechtigungen definiert, die den Zugriff für festgelegte Rollen steuern.

Die Registrierung erfolgt einheitlich in einem ELGA-Verweisregister. Die Datenquellen (Document Source) werden durch das Archiv der Notare und weitere Archive (Rechtsanwälte) implementiert. Das Speichern der PV erfolgt entweder im Repository eines dafür bestimmten ELGA-Bereiches (organisatorische Maßnahme notwendig) oder die Funktion der Akteure *Document Source* und *Document Repository* wird lokal in der Applikation selbst gruppiert. Für den letzteren Fall muss die PV ELGA-Applikation die entsprechenden lesenden IHE-Transaktionen unterstützen.

Die *Abbildung 60* zeigt eine Übersicht über die Einbindung der Patientenverfügung in ELGA. Es werden die wesentlichen Akteure, Komponenten und Datenflüsse dargestellt. Im Folgenden werden die Registrierung und der Abruf sequenziell erläutert.

1. Der Notar, Rechtsanwalt oder Patientenanwalt, der zur Aufbewahrung der Patientenverfügung autorisiert ist, nutzt wie bisher sein existierendes (oder künftiges) IT-System zur Verwaltung der Patientenverfügung. Die Patientenverfügung wird in das lokale Dokumentenarchiv gespeichert.

2. Der Notar, Rechtsanwalt oder Patientenanwalt steigt am ELGA-Portal ein und wird zum Identity Provider des e-Government umgeleitet (BKU/MOA-ID). Die präsentierte elektronische Karte berechtigt diese Berufsgruppen generell die Rolle des Bevollmächtigten auszuüben, sofern auch Stellvertretungsverhältnisse existieren. Nach Authentifizierung erfolgt eine weitere Umleitung zur Stammzahlenregisterbehörde, wo der Vollmachtgeber auszuwählen ist. Eine eingeschränkte (berufsgruppenspezifische) Bestätigung existierender Stellvertretungsverhältnisse wird ausgestellt.

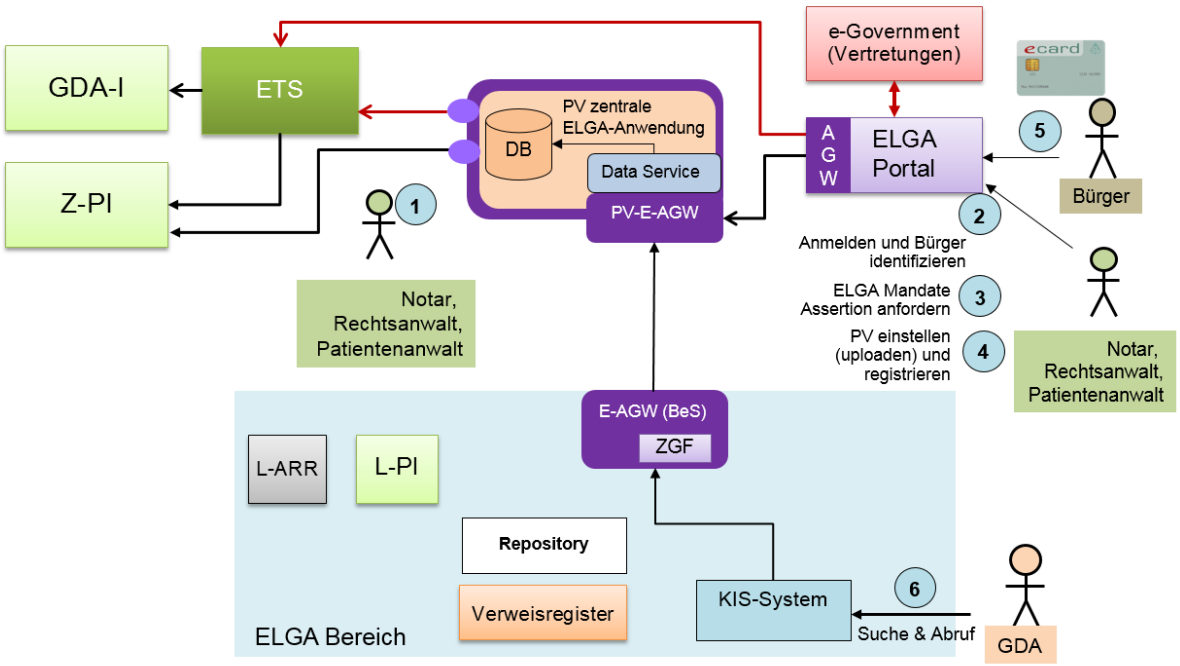


Abbildung 60: Übersicht Patientenverfügung (übersichtshalber sind nicht alle relevanten Verbindungen eingezeichnet)

3. Der Browser wird zum ELGA-Portal zurückgeleitet. Die vom e-Government bestätigte Vollmacht wird dem ELGA-Token-Service weitergereicht. Das ETS sendet dem Portal eine ELGA-Man*date-Assertion I.*

   Der Bevollmächtigte kann nun die Dienste der PV ELGA-Anwendung im Master-Modus benutzen, d.h. existierende Patientenverfügung suchen oder neue Patientenverfügung registrieren.

   Bemerkung: Aus Sicht des Berechtigungssystems ist zu beachten, dass die Dokumentenklasse „Patientenverfügung“ nur von ELGA-Benutzern in der Rolle „Verwalter PV“ eingebracht werden dürfen. Master-Modus setzt diese Rolle voraus (Verwaltung und Upload von mehreren PV-Dokumenten).

4. Das Registrieren von Patientenverfügungen (vorhanden etwa als PDF oder sonstige Formate) erfolgt in Form von CDA-Dokumenten. Die notwendigen Schritte für die Registrierung und Protokollierung übernimmt die Geschäftslogik der PV ELGA-Anwendung.

5. Wenn der Bürger am ELGA-Portal einsteigt, informiert die PV ELGA-Applikation über erfolgte Transaktionen (erfolgreiches Registrieren in ELGA). Anschließend kann der Bürger das CDA-Dokument (Patientenverfügung) wie auch sonstige CDA-Dokumente suchen und einsehen.

6. Der ELGA-GDA kann die Patientenverfügung wie gewöhnlich über sein KIS-System einsehen. Die Suche und der Zugriff auf das Dokument erfolgen über eine normale IHE Such- und anschließende Ladefunktion [ITI-18]/[ITI-43] aus dem GDA-System. Alternativ ist auch die Verwendung des XCF-Profils (Cross Community Fetch) möglich.

Ein wichtiger Punkt für die Akzeptanz ist auch die Ersterfassung existierender Patientenverfügungen. Im Gegensatz zur Registrierung von Befunden scheint diese für die Patientenverfügung unverzichtbar zu sein, um den ELGA-GDA eine einheitliche Möglichkeit für die Recherche bieten zu können.

12. Terminologieserver

Über den zentralen Terminologieserver werden alle für CDA und allgemein für e-Health-relevanten Terminologien (Codelisten, Klassifikationen, Value Sets) elektronisch verfügbar gemacht.

Die Terminologien können in standardisierten Formaten (ClaML, IHE SVS, CSV) heruntergeladen werden. Auch alte Versionen bleiben verfügbar.

Der Terminologieserver bietet die Möglichkeit, über eine Webservice-Schnittstelle auf die Terminologien zuzugreifen, beispielsweise kann so automatisiert immer die aktuelle Version von Terminologien abgefragt werden.

In den Metadaten der Terminologien wird für jede Version ein „Gültig Ab“ Zeitstempel mitgeführt. Ob eine Terminologie verpflichtend anzuwenden ist, erschließt sich aus dem Anwendungskontext (z.B. Implementierungsleitfaden, LKF-Vorgaben etc.).

Die Anbindung an den Terminologieserver erfolgt über eine proprietäre SOAP-basierte Webserviceschnittstelle, die aber nicht für hochfrequente Online-Abfragen dimensioniert ist. Aktualisierungen sind mit einer Frequenz von höchstens einmal am Tag zu holen und von Client-Akteuren persistent aufzuheben. Die Kommunikation zum Terminologieserver erfolgt jeweils über SSL/TLS mittels Serverzertifikatsprüfung. Der Integritätsschutz am Terminologieserver ist herzustellen. Hierfür müssen digital signierte Hashwerte der abgefragten Terminologien separat zur Verfügung gestellt werden. Client Akteure müssen in

der Lage sein die Hashwerte zu verifizieren. Diese Maßnahme muss die inhaltliche Korrektheit und einen nicht modifizierten Zustand der abgefragten Terminologien garantieren.Der Terminologieserver ist über www.gesundheit.gv.at bzw. direkt über https://termpub.gesundheit.gv.at/TermBrowser/ erreichbar.

13. Mengengerüst

In diesem Kapitel sind die in ELGA zu verarbeitenden Datenmengen aus statischer und dynamischer Sicht definiert. Daten stammen primär aus der Erhebungen des Herstellers (Siemens) aus der Pilotierungsphase der e-Medikation.

Anzahl der GDA	Wert
Ärzte intramural	20.000
Ärzte extramural	20.000
Ärzte	35.000 – 40.000
Zahnärzte	5.000
Krankenanstalten	450
Anzahl Apotheken	1.200
Apotheker	5.100
Hausapotheken	1.000
KA Apotheken (interner Bedarf)	50
Pflege intramural	48.000
GuK: Dipl. Gesundheits- und Krankenschwester/-pfleger	40.000
Hebammen	1.700
Ges.Psych.	5.129
Klin.Psych	5.149
ELGA-Benutzer in der Summe (GDA)	**100.000**

Tabelle 29: GDA, Mengengerüst

GDA Besuche	Jährlich
Stationäre Aufnahmen/ Entlassungen	2.600.000
Ambulante Frequenzen	16.000.000
Arztkonsultation mit e-card	120.000.000
Konsultation Wahl-Arzt und privat	40.000.000
nicht mit e-card versorgt	1.200.000
Ausländer, Touristen	12.000.000
Arztbesuche gesamt	173.200.000

Tabelle 30: GDA Besuche

Befunde (inklusive CDA-Dokumente)	Jährlich
Fallzahl Labor niedergelassen	2.330.000
Befunde Labor	12.190.000
Fallzahl Radiologie Ambulant	2.900.000
Fallzahl Radiologie Stationär	3.230.000
Fallzahl Radiologie niedergelassen	2.350.000
Befunde Radiologie gesamt	10.120.000
Arztbriefe gesamt	2.600.000
Befunde gesamt	**25.000.000**
Befunde: Lesende Zugriffe gesamt	**142.000.000**

Tabelle 31: Befunde, Mengengerüst

14. Antwortzeiten

14.1. Antwortzeitmessung

Um die Einhaltung der Antwortzeitvorgaben überprüfen zu können, ist es im verteilten, serviceorientierten System von ELGA essenziell, ein einheitliches Verfahren zur Messung und Auswertung von Antwortzeiten zu definieren.

Da die Kommunikation auf Basis des ATNA-Profils verschlüsselt erfolgt, und auch zu erwarten ist, dass unterschiedliche Monitoring Werkzeuge zum Einsatz kommen, wird eine einheitliche Antwortzeitmessung auf Applikationsebene durchgeführt.

Bei der Aufzeichnung der Antwortzeiten handelt es sich um eine implementierungsspezifische konfigurierbare Erweiterung, die alle ELGA Komponenten unterstützen müssen, da dies eine unverzichtbare Basis für das Monitoring der Service-Qualität und die Optimierung bildet.

Abbildung 61 zeigt das Modell, das für die Antwortzeitmessung zur Anwendung kommt.

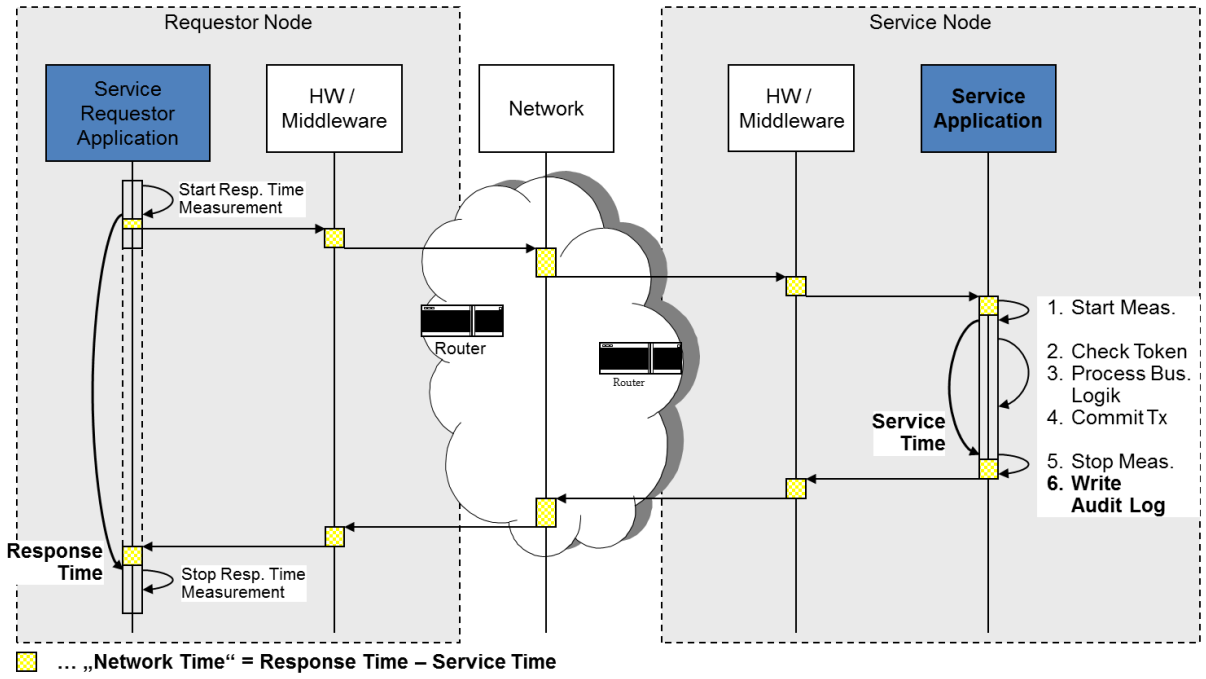


Abbildung 61: Modell für Antwortzeitmessung

Einerseits messen die Services (rechte Seite der Abbildung) ihre Antwortzeit auf Applikationsebene, indem sie sich als erste Aktion einen Startzeitstempel merken und unmittelbar vor der Protokollierung die Messung beenden und die gemessene Zeit (Service Time) in einen separaten Tracing-Protokollsatz mit aufnehmen. Der Tracing-Protokollsatz enthält somit einerseits den Zeitstempel, der aufgrund des CT-Profils auch gute Qualität haben sollte und näherungsweise die Service Zeit (soweit diese aus Sicht der Applikation messbar ist).

Andererseits erfolgt auch eine applikatorische Messung der Service Aufrufe durch den „Service Requestor“. Dieser misst die Antwortzeit (Response Time) aus seiner Sicht. Gemessen wird die Antwortzeit der Aufrufe von externen Services, d.h. die Aufrufe von anderen Akteuren. Ein Requestor kann mehrere Services aufrufen.

Die Zeit, die im Netzwerk verbraucht wurde, wird näherungsweise durch Subtraktion der Service Time von der Response Time ermittelt. Die Zeiten werden in Millisekunden (ms) gemessen und protokolliert.

Detaillierte Festlegungen für die zu benutzenden Datenformate erfolgen im Rahmen der Pflichtenhefterstellung des Berechtigungssystems. Gleiches gilt für die Regeln zur Aggregation der Tracing-Protokolle bzw. für die Anforderungen an die Auswertungen.

14.2. Protokollierung und Auswertung

Es sollen Protokolleinträge für die eigene Verarbeitung (Service-Time aus Server-Sicht) und Protokolleinträge für alle im Rahmen dieser Verarbeitung aufgerufenen Services (Response-Time aus Client-Sicht) erstellt werden. Die Protokollierung aus Server-Sicht soll so erfolgen, dass die Zeitmessung möglichst den gesamten Verarbeitungsablauf enthält, z.B. bei JEE in Form des äußersten Servlet Filters.

Die Protokolleinträge sollen zumindest:

- einen Zeitstempel in Millisekunden-Genauigkeit,
- die Transaktionsnummer (ELGA-Transaktionsklammer) (vgl. Kapitel 3.10),
- den URI des aufgerufenen Services,
- den Transaktionstyp (z.B. ITI-18),
- die Message-Id,
- den Typ der Messung (Client oder Server),
- die Id Komponente, die die Messung durchgeführt hat (z.B. Application ID) und
- die Antwortzeit des Services in Millisekunden

enthalten.

Um ein übergreifendes Reporting zu ermöglichen, sollen die Protokolldaten in einer Datenbanktabelle gesammelt werden. Die Sammlung kann asynchron erfolgen, z.B. indem die Daten durch regelmäßige Batch Jobs transferiert und importiert werden. Alternativ sind auch der Transport über eigens dafür definierte ITI-20 Nachrichten (bzw. Erweiterungen von existierenden ITI-20 Nachrichten) und die Auswertung über ein ARR möglich.

Im Rahmen der Auswertung sollen so die Servicequalität bereichsübergreifend dargestellt und Probleme, die bei der Kommunikation zwischen Bereichen auftreten, lokalisiert werden.

14.3. Antwortzeitvorgaben

Grundsätzlich wird für Transaktionen (Service Aufrufe) eine durchschnittliche Antwortzeit von maximal 3 Sekunden vorgeschrieben. Hierbei lässt sich dieses Zeitintervall auf eine Antwortzeit des Berechtigungssystems (bis zu maximal 1000 ms inklusive ETS, GDA-I, Z-PI und PAP Aufrufe) und auf die Antwortzeit eines ELGA Zielbereiches aufteilen (bis zu 2 Sekunden inklusive Initiating Gateway, Responding Gateway, PEP, PDP, PIP, Verweisregister bzw. Repository). Hinzu kommt noch die Zeit (exklusiv) für die Ergebnis-Aufbereitung und -Darstellung im Client, die in der Verantwortung der GDA-Software liegen.

Dies gilt für die von ELGA bereitgestellten Transaktionen ohne Berücksichtigung von Anteilen, die ggf. für die Visualisierung erforderlich sind. Bei der Antwortzeitfestlegung wird auch auf die Problematik eingegangen, dass bei großen Abweichungen vom mittleren Mengengerüst unverhältnismäßig hoher Aufwand für die Erreichung der Antwortzeiten erforderlich wird. Es werden daher Rahmenbedingungen bezüglich des Mengengerüstes angeben, bis zu denen die Antwortzeitforderungen erfüllt sein müssen.

Da in komplexen IT-Systemen Ausreißer auftreten (wie z.B. beim Neustart von Systemkomponenten) wird zusätzlich festgelegt, dass in maximal 3% der Fälle (gerechnet über eine Stunde) die maximale Antwortzeit bis zum Faktor 4 oder höchstens 5 überschritten werden darf. Größere Abweichungen gelten jedenfalls als SLA-Verletzung.

In der serviceorientierten Architektur von ELGA, wo die erforderlichen Services durch unterschiedliche Betreiber zu verantworten sind, ist es erforderlich die Antwortzeitvorgaben auf die einzelnen Services bzw. die beteiligten Systemkomponenten herunterzubrechen.

Zu diesem Zweck werden im Folgenden die wesentlichen Abläufe analysiert. Zum Verständnis ist hier auch die Kenntnis der Lastenhefte der betroffenen Projekte erforderlich.

14.3.1. Parameter bzw. Zielvorgaben für Hochrechnung

Um eine Hochrechnung von Antwortzeiten durchführen zu können, wurden die konkreten Zahlen zu Datenvolumina und daraus abgeleitete Werte für die Antwortzeiten von Systemkomponenten in der Tabelle 32 zusammengefasst. Die hier angeführten Angaben sind teilweise (z.B. bei Z-PI) tatsächlich vermessene reale Werte. Ergänzt werden diese mit Zielvorgaben für Komponenten, die bisher nicht vermessen werden konnten (z.B. ETS weil noch nicht implementiert).

Name	Mittelwert	Einheit	P97	Beschreibung
Netzwerk und zentrale Services				
NW0	40	ms	150	Netzwerkzeit (Latency, bis 20 KB) intern
NW1	150	ms	400	Netzwerkzeit (Latency, bis 20 KB) schnelle DSL Verbindung
NW2	500	ms	2.000	Netzwerkzeit (Latency, bis 20 KB) langsame ISDN Verbindung
ST_PIX	200	ms	800	Service Time für PIX Query
ST_PDQ_1	400	ms	2000	Service Time für PDQ Query mit Identifier/Schlüssel
ST_PDQ_2	1500	ms	3000	Service Time für PDQ Query ohne Schlüssel
ST_PAP	200	ms	1.000	Service Time für PAP (Request policies by ID)
ST_PDP	150	ms	750	Service Time für Policy Decision Point (PDP)
ST_PDPx	400	ms	2.000	Service Time PDP für multiple Resource Profile (bis 10)
ST_ETS	50	ms	250	Service Time für ETS (ohne Aufrufe untergeordneter Services)
ST_GDAI	100	ms	300	Service Time für GDA Index
Registry, Repository, ZGF (Gateway und Policy Enforcement Point)				
ST_Reg	600	ms	3.000	Query bis zu 50 Dokumente zur PID registriert und <= 10 Treffer
ST_RegX	1.500	ms	7.000	Extended Query bis zu 200 Dokumente zur PID
ST_PEP	50	ms		PEP bei Dokumentenabfrage
ST_PEPq	100	ms		PEP bei Standard Registry Stored Query
ST_PEPqX	150	ms		PEP bei Extended Query
ST_GWi	200	ms	1.000	Service Time Initiating Gateway (ohne Z-PI und ETS Aufrufe)
ST_GWr	100	ms	500	Service Time Responding Gateway
ST_Rep	300	ms	1.500	Service Time Repository, Basiswert für Dokument bis 800kB

Tabelle 32: Parameter für die Hochrechnung von Antwortzeiten

14.3.2. Anwendungsfall: ELGA-Kontaktbestätigung ausstellen (GDA.3.6)

Abbildung 62 zeigt in einem Sequenzdiagramm den Standard-Ablauf beim Anfordern einer ELGA Kontaktbestätigung. Es wird von einem Krankenhausszenario z.B. mit Aufnahmekanzlei ausgegangen. Zusätzlich wird vorausgesetzt, dass die Aufnahme des Patienten entsprechend erfolgreich durchgeführt wurde.

Auf der Zeitleiste sind rechts Nummern angegeben anhand derer der Ablauf im Folgenden beschrieben wird. Die Beschreibung erfolgt logisch unter Verwendung von Variablen. Konkrete Werte der Variablen sind aus der obigen Tabelle zu entnehmen.

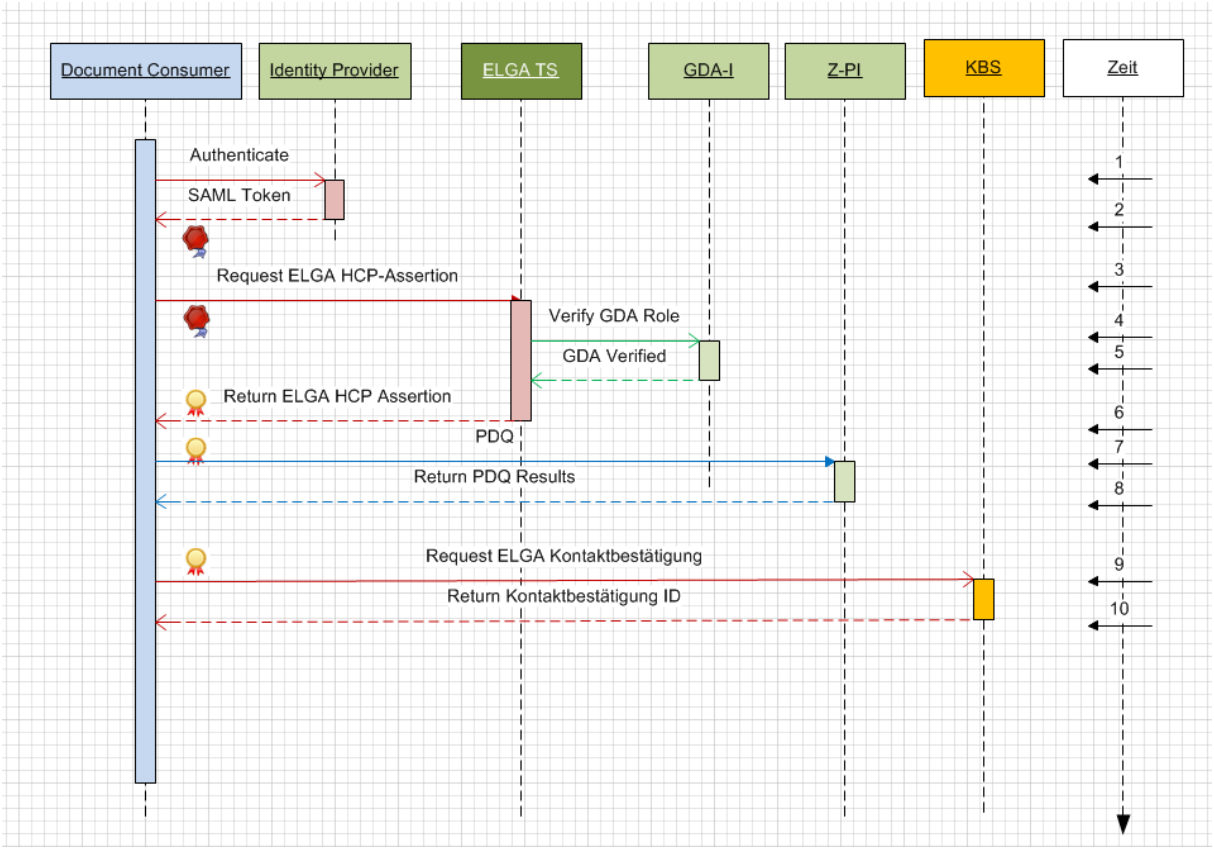


Abbildung 62: Sequenzdiagramm: Kontaktbestätigung senden / anfordern

1. Der GDA meldet sich beim lokalen System (KIS-System bzw. Arztsoftware) an. Es wird eine Authentisierung (via lokalen Identity Provider, z.B. Active Directory) durchgeführt. Es wird angenommen, dass eine schnelle interne Verbindung benutzt wird, mit der von ATNA geforderten Verschlüsselung.
    a. Für die Laufzeit am Netzwerk (Network Time) wird daher NW0 (kurze Laufzeit) angenommen. Hinzu kommt die Service-Zeit für den Identity Provider (ST_IP).
2. Die Antwort des Identity Providers trifft ein und es wird eine Protokollmeldung geschrieben.
3. In diesem Schritt wird ELGA Single Sign On (SSO) transparent für den angemeldeten ELGA-GDA durchgeführt. Die Arztsoftware schickt automatisch einen ELGA-HCP-Assertion Request (RST) an das zentrale ETS und präsentiert die im vorigen Schritt ausgestellte ELGA-Identity-Assertion.
    a. Als Netzwerkzeit wird NW1 kalkuliert (optimiertes Netz).
    b. Im niedergelassenen Bereich muss mit NW2 gerechnet werden

4. Das ETS extrahiert aus der präsentierten ELGA-Identity-Assertion die ID des Anwenders bzw. die ID der *IssuingAuthority* und startet damit eine GDA-I Abfrage, um die Rolle des ELGA-Benutzers bestätigen zu lassen.
    a. Als Netzwerkzeit wird NW1 kalkuliert (optimiertes Netz).
5. Die Identifikation des GDAs erfolgt. Hinzu kommt die Service-Zeit für den GDA-Index (ST_GDAI).
6. Die Antwort (RSTR) trifft ein. Vom SOAP Message Body ist die ausgestellte ELGA-HCP-Assertion zu entnehmen und für die Dauer der Gültigkeit lokal durch die GDA-Software aufzuheben.
7. Optional: der Patient trifft bei GDA ein und es wird angenommen, dass seine L-PID noch nicht vorhanden ist. Hierfür kann eine PDQ [ITI-47] Transaktion gestartet werden.
    a. Als Netzwerkzeit wird NW1 kalkuliert (optimiertes Netz).
    b. Im niedergelassenen Bereich ist mit NW2 zu kalkulieren
8. Die Antwort trifft ein. Die Service-Zeit für die Abfrage wird zur Netzwerkzeit addiert (ST_PDQ).
9. Im nächsten Schritt meldet die GDA-Software eine gültige Kontaktbestätigung bei KBS. Hierfür präsentiert die GDA-Software die vorher ausgestellte ELGA-HCP-Assertion und schickt im RST die Identifikation (z.B. L-PID oder bPK-GH) des Patienten mit.
    a. Als Netzwerkzeit wird NW1 kalkuliert (optimiertes Netz).
    b. Im niedergelassenen Bereich wird NW2 angenommen
10. Das KBS empfängt die Anfrage mit der erhaltenen ID des Patienten und sendet eine Bestätigungs-ID zurück.

14.3.3. Anwendungsfall: ELGA-Verweisregister abfragen (GDA.3.9)

Die Abfrage des ELGA-Verweisregisters ist in Abbildung 63 in analoger Form zum vorangegangenen Kapitel beschrieben. Hierbei wurde auf die Darstellung der Zeitachse verzichtet.

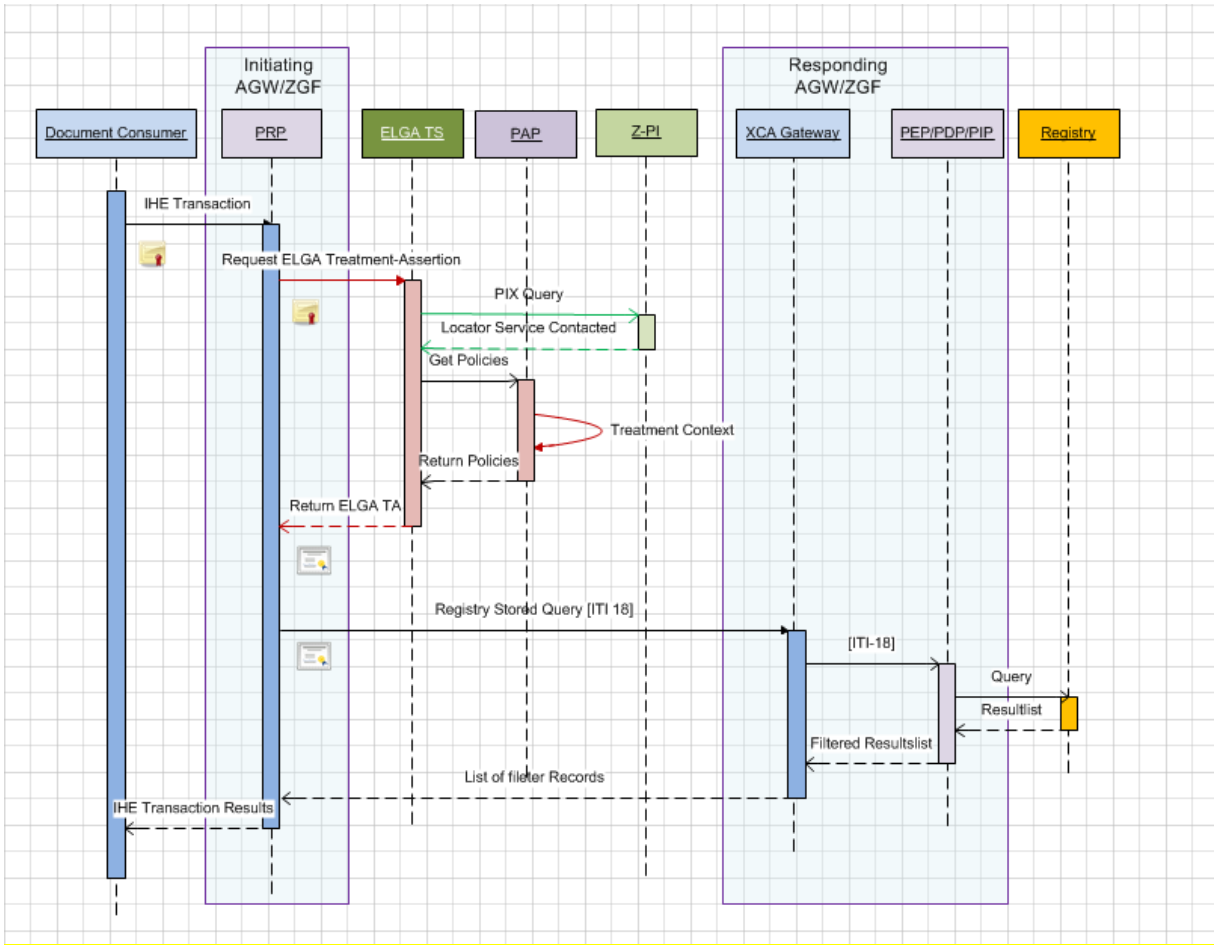


Abbildung 63: Sequenzdiagramm: ELGA-Verweisregister abfragen

1. Die GDA Software (Document Consumer) richtet eine Dokumentenabfrage an das Initiating Gateway. Es wird die vorher ausgestellte ELGA-HCP-Assertion im SOAP Authorisation-Header präsentiert. Am zugeordneten Port innerhalb des Initiating Gateways horcht der Policy Retrieval Point (PRP). Für die Laufzeit am Netzwerk (Network Time) wird internes Netzwerk NW0 (kurze Laufzeit) angenommen.
2. Der PRP am Initiating Gateway überprüft die mitgesendete HCP-Assertion und wendet sich damit an die zentrale ETS Komponente. Hierbei führt PRP eine Identity-Delegation durch und agiert im Namen des Document Consumers (GDA-Software). Die Service-Time des PRP muss addiert werden. Für die Laufzeit am Netzwerk (Network Time) wird ein optimiertes Netzwerk NW1 angenommen.
3. Das ETS verifiziert die präsentierte HCP-Assertion und ermittelt die entsprechende Kontaktbestätigung beim KBS. Danach werden durch eine Abfrage beim Z-PI die ELGA-Bereiche, in denen der Patient registriert ist ermittelt.
4. Der Z-PI antwortet dem ETS mit einer Liste der ELGA-Bereiche (Community IDs und L-PIDs) in denen der Patient registriert ist.

5. Das ETS wendet sich nun an ein internes Service (PAP/PDP), um die generellen und individuellen Berechtigungen (Policies) des Patienten zu ermitteln. Die Service-Time des PAP/PDP muss hier addiert werden.

6. Das ETS kann nun eine Liste (Collection) von gültigen ELGA-Treat*ment-Assertions* ausstellen. Die Anzahl der ELGA-Treat*ment-Assertions* entspricht der Anzahl der ermittelten ELGA-Bereiche. Jede ELGA-Treatment-Assertion enthält nur die für den Zielbereich bestimmten XACML Policies. Wenn der Bürger keine oder nur wenige individuelle Berechtigungen gesetzt hat, unterscheiden sich die einzelnen ELGA-Treat*ment-Assertions* kaum (zumindest aber durch die Adresse des Zielbereiches im Element *AudienceRestriction*). Dies ist bei Optimierung in Betracht zu ziehen. Die Service-Time des ETS muss hier addiert werden, welche auch die Service-Time von PAP/PDP mitenthält.

7. Das ETS antwortet dem PRP mit einer *Request Security Token Response Collection* (RSTRC).

8. Der PRP (aktiver Teil des Initiating Gateways) schickt die notwendigen Anfragen (IHE Transaktionen) parallel (gemeint ist asynchron) an die jeweiligen Responding Gateways der ELGA-Bereiche, in denen der Patient registriert ist. Auf dem Sequenzdiagramm ist einfachheitshalber nur ein Bereich dargestellt. Die Netzwerkzeit wird als „lang“ angenommen, weil hier die langsamste Verbindung den Ausschlag gibt.

9. Das Responding Gateway empfängt die Anfrage und überprüft zuerst die präsentierte ELGA-Treat*ment-Assertion*. Die Berechtigungen werden nun vom Token extrahiert und zweckmäßig dem *Policy Enforcement Point* (PEP) weitergereicht. Für die Laufzeit am Netzwerk (Network Time) wird internes Netzwerk NW0 (kurze Laufzeit) angenommen. Der PEP konsultiert seine Business Logic, welche der Policy Decision Point (PDP) ist.

10. Der PEP reicht nun die Anfrage an das Verweisregister weiter, soweit dies vom PDP erlaubend bestätigt wird. Eine Möglichkeit der Optimierung besteht darin, die Query an das Verweisregister so abzusetzen, dass dieses nur jene Records liefert, welche den mitgeschickten Berechtigungen entsprechen. Für die Laufzeit am Netzwerk (Network Time) wird internes Netzwerk NW0 (kurze Laufzeit) angenommen. Die Service-Time von PEP/PDP muss zusätzlich addiert werden.

11. Das ELGA-Verweisregister führt die Abfrage durch. Die Service-Time des Verweisregisters muss addiert werden.

12. Das ELGA-Verweisregister antwortet an den PEP mit einer standardisierten IHE-Response.

13. Wenn in der ELGA-Treatment-Assertion gefordert, muss der PEP die Antwort des ELGA-Verweisregisters filtern, um nur jene Records durchzulassen, welche den

Berechtigungen entsprechen. Hierfür ruft der PEP den PDP auf, um die Zugriffsentscheidungen zu treffen. In der Antwort erhält er die Liste der Zugriffsentscheidungen je Dokument.

14. Der PEP filtert nun die Einträge entsprechend und sendet die Antwort an das Responding Gateway. Die Service-Time von PEP/PDP für das Filtern wird addiert.
15. Der Responding-Gateway sendet die Antwort an das Initiating Gateway.
16. Dieser sammelt die Antworten von allen ELGA-Bereichen, bildet die Vereinigungsmenge und sendet diese gesammelt an das GDA-System zurück (siehe hierfür auch die Gateway Pipelines in der Abbildung 31).

15. Betriebsanforderungen

Grundsätzlich wird vermerkt, dass detaillierte Betriebsanforderungen im Dokument *ELGA Service Levels* [16] definiert sind. Darüber hinaus werden einige sonstige Bemerkungen und Bedingungen aus der Sicht der Softwarearchitektur gestellt.

15.1. Verfügbarkeit

Es ist äußerst wichtig zu vermerken, dass die grundlegende Systemarchitektur von ELGA auf dem Konzept eines generellen virtuellen Gesamtregisters (siehe Abbildung 2) setzt und davon abhängig ist. Das Gesamtregister ist nur dann funktionstüchtig, wenn die einzelnen physischen Akteure (lokale XDS Verweisregister), deren Gesamtsumme dieses virtuelle Verweisregister ergibt, Teile von Systemen mit hoher Verfügbarkeit sind. Hohe Verfügbarkeit benötigt zusätzliche Investments und ist letztendlich ein Trade-Off zwischen Kosten, Vorgaben und tatsächlicher Notwendigkeit.

Die Notwendigkeit eines Rahmenwerkes mit Hochverfügbarkeitsvorgaben ist mit dem Konzept des ELGA-weiten virtuellen Verweisregisters gegeben. Demnach müssen lokale ELGA-Komponenten in der Verfügbarkeitsklasse 3 (~ 99,9%) betrieben werden, und zwar unabhängig davon, ob ein sofortiger Support zur Verfügung steht und operativ in die Geschehnisse eingegriffen werden kann oder nicht. Die in dieser Verfügbarkeitsklasse erlaubten 10 Minuten Ausfallzeit (pro Woche) können nur durch entsprechende Automatismen und Redundanzen mit Lastverteilung (Load Sharing, Fail-Over Clustering, Spiegelung, Wechsel der geografischen Standorte etc.) erreicht und garantiert werden. Es ist beinahe unmöglich ein ausgefallenes komplexes und verteiltes System ausschließlich durch manuelle Eingriffe im gegebenen Zeitfenster wiederherzustellen.

Zentrale Komponenten müssen in einer höheren Verfügbarkeitsklasse betrieben werden. Dies ergibt sich aus der Tatsache, dass die Erreichbarkeit der ELGA-Bereiche von den zentralen Komponenten abhängig ist.

Weiters sollte in Betracht gezogen werden, dass die ELGA Verfügbarkeit beim Endverbraucher an der Schnittstelle zum gesicherten Netz zu messen ist. Ein typischer Endverbraucher ist das ELGA-Portal, weil es an der Grenze zwischen Internet und gesichertem Netzwerk platziert ist.

Die Verfügbarkeit versteht sich exklusive geplanter und vorvereinbarter Wartungsarbeiten mit Unerreichbarkeit. Anbei jene Punkte, welche bei Hochverfügbarkeit mit besonders großer Sorgfalt zu planen sind:

- Redundante Standorte (geografische Trennung):
  - Jeder Standort kann für sich die gesamte geforderte Last abwickeln.
  - Für die betriebenen Services wird eine für die Nutzer weitgehend transparente Fail-Over Funktion eingerichtet.
  - Beide Standorte sind aktiv, sodass bei einem Ausfall keine, für einen angemeldeten Anwender, bemerkbaren Umschaltzeiten entstehen.
  - Der Datenbestand (Datenbanken) ist standortübergreifend gespiegelt (etwa synchrones SQL-Mirroring), sodass es beim Ausfall eines Standorts zu keiner Betriebseinschränkung kommt.
  - Auch innerhalb eines Standorts sind die Daten gespiegelt (ohne „Single Point of Failure“) gespeichert.
  - Jeder Standort verfügt über ein vollständiges Backup bzw. Backup-System, sodass auch bei Zerstörung eines Standorts der Betrieb ohne Risiko eines Datenverlustes fortgesetzt werden kann.
  - Die Standorte sind aus Netzwerksicht über zwei vollständig getrennte Wege erreichbar.
- Redundante Stromversorgung (unterschiedliche Stromquellen mit automatischem Fail-Over).
- Ersatzleitungen für Datenübertragung (auch bei Beschädigung oder Ausfall der Hauptleitung müssen Reserveleitungen vorhanden sein).
- Online Wartung, Austausch und Reparatur von HW ohne Systemshutdown.

- Upgrade der SW-Versionen entweder ohne Restart oder, wenn dies doch erforderlich ist, als Teil einer Load-Balancing Lösung (Farm), welche das beliebige Zu- oder Abschalten von Knoten ermöglicht.

In obige Verfügbarkeitsklasse fallen die zentralen Komponenten Z-PI, GDA-I, ETS, PAP, KBS sowie Komponenten des Protokollierungssystems (A-ARR).

Bemerkung: Die Verfügbarkeitsanforderungen an die ELGA-Bereiche werden hier nicht ausgeführt. Es sei hier nur auf die Aussagen in Kapitel 3.11.2 verwiesen.

Darüber hinaus muss weitestgehend Schutz gegen Datenverlust garantiert werden. Es müssen Notfallkonzepte für die eventuelle Zerstörung eines geografischen (ELGA-) Standortes in Betracht gezogen und entsprechende Wiederherstellungs- und Fail-Over Maßnahmen vorgesehen werden. Siehe hierfür die weiteren Kapitel (Datensicherheit).

15.2. Skalierbarkeit

Die Zentralsysteme sind auf die österreichweit geschätzte Ziel-Last + 50% Sicherheitsreserve zu dimensionieren. Spitzenzeiten mit überdurchschnittlich vielen Arztbesuchen sind zu berücksichtigen, wobei die Last insbesondere auf die zentralen Komponenten vervielfacht werden kann. Es ist nachzuweisen, dass der geforderte Durchsatz mit den geforderten Antwortzeiten beim geforderten Mengengerüst erbracht werden kann. Beim Nachweis ist insbesondere zu berücksichtigen, dass mit realistischer Verteilung von Daten und Zugriffsprofilen gearbeitet wird.

Unter Skalierbarkeit versteht sich die Skalierbarkeit eines Systems laut *Universal Scalability Law* (USL) von Neil Gunther (1993). Dies ist die Fähigkeit des Systems bei Erhöhung der zugesprochenen Ressourcen (CPU, Bandbreite, I/O-Rate) mit einer annähernd linearen Erhöhung des maximalen Durchsatzes (C) zu reagieren. Dies wird durch die Funktion C(N) = N ausgedrückt, wo N die zugesprochenen Ressourcen repräsentiert. Auf die Darstellung der kompletten USL-Formel wird hier verzichtet. Die Linearität ist aber von anderen Faktoren wie Verluste durch konkurrierende Ressourcen (*Contention* = α) und Verluste durch das Warten auf Zusammenhänge im Pipeline (*Coherency* = β) insbesondere bei dramatisch erhöhter Last, deutlich verzerrt. Gut skalierende Systeme zeichnen sich trotz allem mit guter Linearität des Durchsatzes aus.

Bemerkung: Systeme mit hohen Ressourcen (z.B. viele CPU) zeichnen sich bei Steigerung der Last durch eine nahezu waagerechte Antwortzeit-Kurve bis kurz vor dem maximalen Durchsatz aus. Damit können drohende Engpässe nur durch genaues Monitoring der Last vorhergesagt werden und nicht durch Beobachtung der Antwortzeiten.

Skalierbarkeit muss primär durch die sogenannte *Scale-Out* Fähigkeit des Systems gewährleistet sein. Hierbei wird unter *Scale-Out* (im Gegensatz zu *Scale-Up*) die Fähigkeit des

Systems verstanden, erweitert zu werden, indem ein höherer Durchsatz einfach durch Inbetriebnahme oder Installation von parallelen Instanzen (Komponenten) abgefedert werden kann. Wenn zum Beispiel bei ständig erhöhter Last die anfänglich installierten Front-End Web-Server keine annähernd konstanten Antwortzeiten mehr aufrechterhalten können, dann ist das Durchsatzlimit erreicht und es muss mit Inbetriebnahme von weiteren baugleichen Front-End Web-Servern die Last so umverteilt werden, dass sich der maximale Durchsatz des Gesamtsystems erhöht.

Scale-Out ist möglich, wenn die Software-Komponenten dies ermöglichen. Die Bedingung hierfür ist das Design und die Entwicklung von sogenannten *State-Less* Komponenten, welche den Zustand einer User-Session und/oder Transaktion nicht auf einen bestimmten physischen Server binden. Eine *State-Less* Architektur der Komponenten garantiert im Weiteren den nahtlosen Einsatz von Lastenverteilern (Load-Balance) mit zu- und abschaltbaren aktiven Server-Knoten. Dieses Prinzip ist wesentlich für die Hochverfügbarkeit, da schadenerleidende Server bei automatischer Lastübernahme durch andere Knoten einfach abgeschaltet werden können.

Hierbei ist es zu vermerken, dass *Session-State* (unterstützt durch sinnvoll eingesetzte Technologieerweiterungen) Scale-Out nicht komplett ausschließen, auch wenn dies dadurch erschwert wird.

Das *Scale-Out* Prinzip muss in allen Schichten des Systems zur Anwendung kommen. Dies gilt nicht nur für *Präsentation-Layer* und *Business-Logic-Layer* sondern auch für die Schicht der Datenzugriffe und Datenspeicherung. Scale-Out ist im Data-Access Layer viel schwieriger zu erreichen und basiert vorwiegend auf Cluster-Techniken in Verbindung mit Partitionierung, die vom zugrundeliegenden Datenbanksystem angeboten werden, wobei das Design der Applikationen die optimale Nutzung von Cluster-Techniken unterstützen muss. Außerdem, im Sinne des eingeschlagenen Trends im IT-Bereich, Systeme sind bevorzugt virtualisiert zu betreiben.

Anmerkung: Unter Scale-Up versteht man die Erhöhung des Durchsatzes Ausbau der Maschinen (mehr CPU, IO Kapazität, etc.).

Die Leistungsfähigkeit der Komponenten ist frühzeitig durch Load- und Performancetests sowie durch ein „Proof of Concept“ nachzuweisen. Dies kann mit reduzierten Mengen erfolgen, muss jedoch mindestens mit einem Drittel der geforderten Mengen durchgeführt werden. Im Fall der Verwendung reduzierter Mengen, muss die Skalierbarkeit auf die Ziel-Last dargestellt und begründet werden.

15.3. Datensicherheit

Datensicherheit steht für ordnungsgemäße Verwendung von sensiblen Daten, die über entsprechende Datensicherheitsmaßnahmen gewährleistet werden kann. Das

Datenschutzgesetz (DSG 2000) definiert organisatorische, personelle und technische Maßnahmen zur Datensicherheit. Die Kernpunkte der Maßnahmen zielen darauf ab, Unbefugten den Zugriff auf Daten zu verweigern und gleichzeitig die Daten vor Zerstörung und Verlust effektiv zu schützen. Datensicherheit beruht aus technischer Sicht auf fünf grundlegende Prinzipien, und zwar:

1. Authentifizierung (Authentication)
2. Autorisierung bzw. Zugangsberechtigungen (Authorisation)
3. Datenintegrität (Integrity)
4. Vertraulichkeit (Confidentiality & Privacy)
5. Backup & Desaster Recovery

Authentifizierung und **Autorisierung** sind im Kapitel 9 Berechtigungs- und Protokollierungssystem, erläutert und detailliert ausgeführt.

15.3.1. Datenintegrität

Datenintegrität betrifft sowohl die Datenhaltung und Datenspeicherung als auch die Datenübermittlung.

Lokale Datenhaltung

Für die lokale Datenhaltung in den Komponenten (Repository, Registry, PAP, KBS) wird davon ausgegangen, dass Datenbanksysteme zur Speicherung von Daten eingesetzt werden, die die bekannten ACID Kriterien (**A**tomicity, **C**onsistency, **I**solation, **D**urability) erfüllen. Darüber hinaus müssen jedoch Alternativen wie das NoSQL-Model (BASE) auch betrachtet werden, insbesondere für das Speichern von Audits oder KBS, wo gemeldete Kontakte einem NoSQL-Key/Value-Store Model tatsächlich näher stehen.

Gültige, schematreue Daten

Die zum Speichern gesendeten Daten müssen den vordefinierten Schemas und die in den technischen ELGA-Leitfäden festgelegten Normen entsprechen. Andernfalls droht die Gefahr, dass die eingebrachten Daten später (beim Lesen) nicht korrekt dargestellt werden können. Hierfür muss gewährleistet werden, dass die in ELGA freigegebenen Daten einer strengen Validierung (z.B. via Schematron Validator) unterzogen werden. Die Validierung muss vom Document Source Akteur offline (vor der Veröffentlichung in ELGA) durchgeführt werden.

Übergreifende Konsistenz

Die fachlichen Anwendungsfälle von ELGA, die Business Objekte schreiben bzw. aktualisieren, sind als Ketten von Verarbeitungsschritten aufgebaut, die komponentenübergreifend ausgeführt werden. Als Beispiele sind hier allen voran das

Registrieren von Dokumenten (→ Repository, Registry) aber auch das Einbringen von Kontaktbestätigungen (→ KBS), Berechtigungsregeln (→PAP) oder Patienten-Identitäten (→ Z-PI) zu nennen.

Bei allen Verarbeitungsketten ist es wesentlich, dass der Aufrufer bei schreibenden Aufrufen davon ausgehen kann, dass die Daten in der Service Komponente sicher gespeichert sind, wenn der Aufruf mit Erfolgsmeldung beendet wird. Weiters muss sichergestellt sein, dass ein Aufruf, der einen technischen Fehler liefert (z.B. wegen Timeout) vom Aufrufer wiederholt werden kann, ohne dass das fachliche Resultat und Konsistenz der Daten beeinflusst wird (sog. Idempotenz).

Die Prozesse in ELGA sind so aufgebaut, dass bei Einhaltung der obigen Kriterien keine übergreifende Transaktionssicherung erforderlich ist, da der Auslöser des Vorgangs immer eine Information über den aktuellen Zustand des Prozesses hat. Bei kurzfristigen Störungen kann der Prozess durch Wiederholung der fehlgeschlagenen Transaktion weitergeführt werden. Bei einer längeren Störung können zusätzlich technische Schritte wie die Erneuerung von Zugriffs-Tokens erforderlich werden. Bei langen Störungen muss ggf. der fachliche Prozess neu initiiert werden. Ein Beispiel dafür wäre, dass das Melden einer e-card Kontaktbestätigung so lange fehlschlägt, bis diese abgelaufen ist. Im Extremfall muss also der Patient vom GDA neu einberufen werden, um seine e-card erneut zu stecken.

Bezüglich der Konsistenz der Protokollierung gilt ebenfalls, dass die erforderlichen Protokolleinträge sicher gespeichert sein müssen, wenn der Aufruf erfolgreich zurückkehrt. Das Caching der A-ARR Einträge stellt hier die einzige Ausnahme dar die oben detailliert beschrieben und begründet wird. Im Fall des Erfolgs eines fachlichen Vorgangs (z.B. Dokumentensuche ITI-18) kann der Auslöser daher wieder davon ausgehen, dass auch alle erforderlichen Protokolleinträge sicher gespeichert sind. Im Fall des Fehlschlagens der Transaktion, sind, je nach Prozessschritt in dem der Fehler auftritt, nur Teile der Protokolleinträge gespeichert. Dies ist in der Architektur bewusst so vorgesehen und dient der eindeutigen Nachvollziehbarkeit des Ablaufs.

Elektronische Signatur

ELGA-relevante Daten (CDA-Dokumente) werden in den Repositories der Subsysteme (beispielsweise in KIS-Systemen) dezentral gespeichert und die Verweise auf diese Dokumente (Metadaten) in den dafür vorgesehenen ELGA-Registries abgelegt. Datenintegrität wird im Regelfall dadurch gewährleistet, dass die schützenswerten Daten entsprechend digital signiert werden. Die IHE definiert in einem Trial *Implemention Supplement* das *„Document Digital Signature Content Profile“ (DSG)*. Dieses definiert insbesondere, wie im Zusammenhang mit dem XDS Profil Dokumente signiert werden. Dabei wird technisch ein eigenes XML-Dokument (unter Verwendung des XAdES Profils) registriert,

welches einen signierten Hashwert und eine Referenz auf das bzw. die eigentlichen Dokumente enthält.

Neben der Technik muss auch der Zweck einer Signatur klar definiert sein. Es werden daher folgende Fälle betrachtet:

1) Der Autor signiert das Dokument zum Nachweis der Authentizität des Inhalts. Dies scheint bei oberflächlicher Betrachtung wünschenswert, ist aber in der Praxis mit folgenden Nachteilen verbunden:

   a) Gemäß ELGA CDA-Leitfaden dient das CDA-Dokument primär dem Transport von Information und stellt in der Regel eine Kopie von Daten aus einem GDA-System (z.B. KIS) dar. Der Verantwortliche für das Original ist im Attribut „*Custodian*“ angegeben. Eine Signatur durch den Autor würde somit einen weiteren Prüfschritt im Rahmen der Publikation des ELGA-Dokuments nach sich ziehen.

   b) Die technische Ausstattung der GDA-Systeme ermöglicht höchstens eine schrittweise Einführung dieser Forderung.

2) Die Software (Document Source oder nachgelagerte Komponente) signiert automatisch, um die technische Integrität zu bestätigen. Dies garantiert, dass im Document Repository (z.B. durch einen Administrator) keine Veränderungen vorgenommen wurden. Letzteres würde aber voraussetzen, dass der Angreifer keine Möglichkeit hat, selbst die automatische SW-Signatur aufzubringen.

Derzeit gibt es seitens Systempartner keine konkreten Anforderungen eine Signatur wie oben dargestellt umzusetzen, daher gibt es auch keine Vorgaben zur Signatur von CDA-Dokumenten.

Eine Betrachtung der Datenintegrität ausschließlich aus Sicht der vermittelten (gesendeten) Dokumente wäre unvollständig. Datenintegrität muss auch auf der Ebene der gesendeten Nachrichten (SOAP-Messages) gewährleistet werden. Somit wird die Integrität der gesamten gesendeten Nachricht (Message) gefordert, die auch die Kohärenz zwischen SOAP-Header und SOAP-Body garantiert. Die konsequente Umsetzung der im WS-Security SAML Token Profile und WS-Trust Standards geforderten Richtlinien bezüglich „Proof-of-Possession“ Schlüssel ist unausweichlich. Jeder aktive Client (Requestor), der an einer WS-Trust-unterliegenden Kommunikation teilnimmt, ist entweder:

- ein direkter *Holder-of-Key* (laut WS-Trust 1.4) oder
- ein Client dessen Identität ein vertrauenswürdiger zwischengeschalteter Akteur (Zugriffssteuerungsfassade) via *Sender-Vouches* (laut WS-Trust 1.4) garantiert.

In beiden Fällen ist vorgesehen, dass der Client mit kryptographischen Mitteln die Integrität der Nachricht schützt und nachweist, dass er der autorisierte Sender ist. Im Standardfall wird

dies durch Signatur der Nachricht implementiert, die an eine Relying Party versendet wird. Da in ELGA grundsätzlich eine wechselseitige Authentisierung der Kommunikationspartner mit TLS und verschlüsselt erfolgt wird dieses Verfahren ebenso für den geforderten Nachweis zugelassen.

15.3.2. Vertraulichkeit (Confidentiality & Privacy)

Vertraulichkeit der Daten wird durch entsprechende kryptographische Verschlüsselungsverfahren gewährleistet. In ELGA spricht man zumindest über drei unterschiedliche Arten von hochsensiblen Daten, deren Vertraulichkeit garantiert werden muss:

1. Gesundheitsdaten (mehrheitlich CDA-Dokumente)
2. Individuelle Berechtigungen (in Form von XACML-Policies) von ELGA-Teilnehmern
3. Inhalte der ausgestellten SAML Tokens (insbesondere wenn XACML-Policies eingebettet sind, Beispiel *ELGA-Treatment-Assertion*)

Im Idealfall sind die CDA-Dokumente und die Policies auf der Ebene der verwendeten Datenbankinstanzen verschlüsselt gespeichert (via *Transparent Data Encyption*), wobei hier auch sonstige Maßnahmen in Erwägung gezogen werden können. Die Umsetzung von ausreichenden physischen und organisatorischen Zugangseinschränkungen (gemäß §14 DSG 2000) zu den jeweiligen Datenträgern, Verschlüsselung etc. ist von den Betreibern der Datenspeicherungsinstanzen (z.B. Repositories) im Einklang mit den geltenden ELGA ISMS-Richtlinien zu entscheiden.

Datenvertraulichkeit auf der Transportebene wird auf jeden Fall durch Umsetzung von TLS Verbindungen (Version 1.2 oder höher) gewährleistet. Die Übertragung von nativ verschlüsselten Daten (*Message Level Encryption*) in ELGA ist nicht vorgesehen, da ein entsprechend aufwendiges Key-Management aufgebaut werden müsste. Dies wurde von Experten (Technologiebeirat) erörtert und schlussendlich nicht beauftragt. SAML-Token (*Sender-Vouches*) werden integritätsgeschützt (via Signatur), aber nur mit TLS-Verschlüsselung (also ohne Anwendung von XML-Encryption) transportiert.

15.3.3. Datensicherung

In dem verteilten, serviceorientierten System, wie es zur Implementierung von ELGA zur Anwendung kommt, ist es von besonderer Bedeutung, die Daten abgeschlossener Transaktionen sicher zu speichern. Auch bei Ausfällen muss der Verlust von Daten vermieden werden, d.h. es muss möglich sein, im Rahmen von Recovery-Vorgängen, alle abgeschlossenen Transaktionen wiederherzustellen. Das beinhaltet zumindest eine redundante Speicherung der erforderlichen Daten und der damit verbundenen Dateien in einer

Weise, dass der Ausfall eines Mediums (z.B. einer Platte) zu keinem Datenverlust führt. Ist ein Ausfallsstandort gefordert, so sind die erforderlichen Dateien zusätzlich standortübergreifend zu spiegeln.

Neben der redundaten Speicherung des online Datenbestands ist auch ein regelmäßiges, zumindest tägliches, Backup der Daten durchzuführen.

Das Backup dient als letztes Instrument um eine ELGA-Komponente bzw. das ELGA System vor einer kompletten Zerstörung zu bewahren, falls Daten trotz der primären Mechanismen zur Bewältigung absehbar (HW-)Ausfälle verloren gehen bzw. verfälscht wären. Ursachen hierfür könnten bislang unentdeckte Softwarefehler, Bedienfehler (z.B. unbeabsichtigtes Überschreiben) und Katastrophen unberücksichtigten Ausmaßes (gleichzeitige Zerstörung von HW an mehreren Standorten) sein. Zusätzlich soll das Backup auch den Schutz gegen beabsichtigte Zerstörung (böswilliges Löschen durch einen Administrator) verbessern.

Aus letzterer Überlegung heraus besteht eine Präferenz für die Nutzung von Backup Systemen, die ein Löschen vor der Aufbewahrungszeit nicht zulassen, auch nicht durch den Administrator. Der Zugang zu den Backup Systemen und Medien muss strikt beschränkt sein. Backup Medien dürfen, z.B. durch die Nutzung von Verschlüsselung, nur auf den dafür vorgesehenen Systemen lesbar sein. Im Rahmen der Entsorgung ist für eine sichere Vernichtung der Daten zu sorgen.

Die Umsetzung des Backup und Restore Prozesses muss auf folgende Prinzipien bauen:

- Zeit in die Planung investieren. Backup-Strategien inklusive Desaster-Recovery Strategien detailliert ausarbeiten. Pläne müssen alle realistischen Bedrohungsszenarien in Betracht ziehen.
- Personal ausbilden
- Hardware Investments vorsehen. Voraussetzungen für regelmäßige Backups beschaffen
- Softwaretechnische Voraussetzungen schaffen
- Backup ins Monitoring einbinden
- Obige Punkte, Pläne, Hardware und Software gezielt und regelmäßig testen und die Resultate protokollieren und mit früheren Erfolgsquoten vergleichen. Es muss zumindest ein Restore-Test im Rahmen der Inbetriebnahme und in der Folge zumindest ein Restore-Test jährlich erfolgen.

15.4. Restore

Dieses Kapitel betrachtet jenen Fall in dem es erforderlich wird die Daten durch Einspielung eines Backups auf einen früheren Stand zurückzusetzen. Im Fokus steht die übergreifende

Konsistenz der Business-Objekte innerhalb der ELGA-Architektur, die im Rahmen der beschriebenen Anwendungsfälle angelegt, modifiziert oder gelesen werden.

Nicht im Scope sind Dateien, die im Rahmen der IT Infrastruktur benötigt werden. Darunter fallen unter anderem Programm- und Konfigurationsdateien aber auch alle Protokolldateien und Daten für das Reporting und Monitoring, die nicht explizit im Rahmen der ELGA-Anwendungsfälle benötigt werden. Ebenfalls nicht betrachtet werden Auswirkungen, die nur intern in einem ELGA-Bereich relevant sind.

Für das Audit Log gemäß ATNA Profile bedeutet das, dass nur das A-ARR betrachtet wird. Alle anderen ARRs dienen lokalen Zwecken. Bei diesen wird davon ausgegangen, dass Daten vom Betreiber gemäß den vereinbarten SLA und den gesetzlichen Verpflichtungen geschützt werden. Eine Unterstützung zur Wiederherstellung solcher Daten aus den Datenbeständen anderer Betreiber wird von der ELGA Architektur nicht unterstützt.

15.4.1. Schadenspotential durch einen Datenverlust

Im Folgenden werden die Auswirkungen kategorisiert, die im Rahmen von ELGA durch einen Datenverlust auftreten können, der durch einen Restore-Vorgang verursacht wird.

1) **Gesundheitsakt fehlerhaft**: Der Gesundheitsakt eines ELGA-Teilnehmers hat nicht den Inhalt den man aufgrund der Benutzereingaben erwarten darf. Dieser Fall stellt das gravierendste Problem dar, da hier zumindest mittelbar Gefahr für Leib- und Leben besteht, weil der behandelnde Arzt auch nach Rückfrage beim Patienten im Allgemeinen nicht erkennen kann, dass er auf die Daten nicht vertrauen darf.
   Beispiel: Die Aktualisierung eines Befundes geht verloren, die lebenswichtige Ergänzungen enthält.
   Die Tatsache, dass ein ELGA-Teilnehmer Befunde ausblenden kann, relativiert diese Problematik nicht, da im Fall des Ausblendendens einerseits der ELGA-Teilnehmer die Verantwortung übernimmt und andererseits auch keine unaktuellen Befunde für aktuell gehalten werden können. Darüber hinaus müssen Arzt und ELGA-Teilnehmer darauf vertrauen können, dass ELGA im Rahmen der gesetzlich festgelegten Funktionen technisch korrekt funktioniert.

2) **Datenschutzrechtliches Problem**: Datenschutzrechtliche Anforderungen, wie die Durchsetzung von Berechtigungsregeln, die Anzeige von Protokolldaten oder das Löschen von Dokumenten werden nicht, teilweise oder fehlerhaft erfüllt. Hier kommt es potentiell zu einer Gesetzesverletzung und es kann ein finanzieller Schaden entstehen. Darüber hinaus sind die immateriellen Schäden viel bedeutender.

3) **Verfügbarkeitsproblem**: ELGA ist in Teilen nicht bzw. nur erschwert nutzbar. Diese Situation könnte z.B. durch den Verlust von Kontaktbestätigungen, durch den Verlust von Eintragungen im GDA-Index oder den Verlust einer Verordnung im Rahmen der

e-Medikation entstehen. Auch der Verlust eines Dokuments wird als Verfügbarkeitsproblem eingestuft, da in diesem Fall klar erkenntlich ist, dass Informationen fehlen und bei Bedarf erneut erhoben werden müssen.

Allen 3 Kategorien ist gemein, dass zusätzlich noch ein Image-Schaden für ELGA zu befürchten ist der wesentlich von der Störbreite abhängen wird.

Darüber hinaus muss auch bei allen Kategorien geklärt werden ob ein Sicherheitsproblem vorliegt (d.h. ein Zusammenhang mit einem Angriff existieren könnte der z.B. verschleiert werden soll).

15.4.2. Auswirkungen bei Datenverlust nach Komponenten

In diesem Kapitel werden je Komponente die Auswirkungen eines Datenverlustes analysiert, kategorisiert und Möglichkeiten zur Analyse bzw. zur Rekonstruktion betrachtet. Die angeführten Möglichkeiten sind als Entscheidungsoption zu sehen. Konkrete Festlegungen zur Vorgehensweise sind explizit gekennzeichnet oder erfolgen dann allgemein im darauf folgenden Kapitel 15.4.3.

Wichtig ist zu vermerken, dass ein Datenverlust in ELGA durch entsprechend eingesetzte professionelle Technologie theoretisch ausgeschlossen ist. Die derzeitig verwendeten Datenbanken im Backend garantieren eine verlustfreie Datenhaltung bis auf die zuletzt ausgeführte Transaktion. Somit gesehen ist ein eventueller Datenverlust ausschließlich durch grobe Fahrlässigkeit oder durch extreme Gewalt möglich. Dennoch sind die hier angeführten Überlegungen vollständigkeitshalber aufgelistet.

1) PAP

a) Individuelle Berechtigungsregeln

Problem:	Verlust von Änderungen an individuellen Berechtigungsregeln, die im Allgemeinen durch unterschiedliche Quellen (z.B. EBP und WIST) eingebracht werden.
Kategorie:	Datenschutzrechtliches Problem.
Analyse:	Auf Basis Logs lokal, A-ARR; zusätzlich ggf. durch Abgleich mit Datenbestand von EBP und WIST.
Rekonstruktion:	Praktisch derzeit keine. Theoretisch auf Basis eines Transaktionsprotokolls von EBP, WIST, PAP (und zentrale L-ARR) soweit diese Protokolle neben Metadaten (derzeit) auch den gesamten Request (Inhalt) mitprotokollieren.

b) Generelle Berechtigungsregeln

Problem:	Verlust von generellen Berechtigungsregeln.
Kategorie:	Datenschutzrechtliches Problem und vermutlich massives Betriebsproblem.
Analyse:	lokal.
Rekonstruktion:	Erneutes Einbringen. Dies sollte aufgrund des geringen Umfanges möglich sein.

6405 c) Liste zu löschender Dokumente

Problem:	Verlust von Einträgen in den Listen für zu löschende Dokumente. Unterfall 1: Geht ein Eintrag aus der öffentlichen Liste verloren, so wird angenommen, dass dieser automatisch erneut aus der Quarantäneliste übernommen wird. Unterfall 2: Geht ein Löschkennzeichen verloren so wird davon ausgegangen, dass ein erneuter Löschversuch erfolgt bei dem festgestellt wird, dass das Dokument nicht mehr vorhanden ist und in der Folge der Eintrag in der öffentlichen Liste auf gelöscht gesetzt wird. Unterfall 3: Einträge aus der Quarantäneliste gehen verloren. In diesem Fall können nur lokale Rekonstruktionsmaßnahmen greifen, sofern verfügbar.
Kategorie:	Datenschutzrechtliches Problem.
Analyse:	lokal.
Rekonstruktion:	Praktisch derzeit keine. Theoretisch auf Basis eines Transaktionsprotokolls von EBP, WIST, L-ARR und zentralem L-ARR (siehe oben).

6406 d) Liste zu löschender Dokumente bei Angriffsvektor

Problem:	Es wurde festgestellt, dass einige (vielleicht auch zahlreiche) Einträge in der Quarantäneliste auf eine erkannte Cyberattacke zurückzuführen sind. Hier geht es auch um Wiederherstellung eines gesunden Zustandes der Quarantäneliste.
Kategorie:	Datenschutzrechtliches Problem.
Analyse:	lokal.
Rekonstruktion:	Auf Basis der aktuellen Lösch-Policies im PAP bzw. bei bekanntem Zeitpunkt der letzten erfolgreichen Löschoperation könnte die Quarantäneliste wiederhergestellt werden. Organisatorische Maßnahmen für Sicherheits- und Regelwerksadministratoren sind erforderlich.

6407

6408 **2) KBS**

Problem:	Verlust von gespeicherten Kontaktbestätigungen. Das können Kontaktbestätigungen vom e-card STS, delegierte Kontakte und vom GDA (Spital) selbst ausgestellte Kontaktbestätigungen sein.
Kategorie:	Verfügbarkeitsproblem. Anmerkung: Das Problem ist eher unangenehm, da der GDA darauf vertraut, dass er Zugriff hat und im Anlassfall die erneute Einmeldung eines Kontaktes nicht trivial bis unmöglich ist.
Analyse:	Nur lokal sofern entsprechende Protokolle vorhanden sind. Ein Abgleich mit den einmeldenden Systemen ist hier nicht sinnvoll möglich.
Rekonstruktion:	Keine. Je länger eine Rekonstruktion dauert, desto weniger bringt sie. Grundsätzlich können GDA-Systeme neu einmelden sofern die Voraussetzungen noch gegeben sind. Eine generelle Empfehlung eine Prozess-Unterstützung für die erneute Einmeldung (z.B. in Form einer zeitgesteuerten Wiederholung bei Fehler) zu implementieren wird jedoch nicht gegeben.

3) A-ARR

Das A-ARR erhält die Events

- Synchron vom ETS und PAP.
- Mit In-Memory Queuing („near realtime“) von der ZGF (theoretisch können hier Events verloren gehen, was akzeptiert wird, weil ein zugehöriger Eintrag vom ETS schon existieren muss).
- Im Fall des Löschens: Synchron von der ZGF.

Problem:	Verlust von Protokolleinträgen für Anzeige am Portal.
Kategorie:	Datenschutzrechtliches Problem.
Analyse:	Lokal; eventuell durch Vergleich mit L-ARRs, für letzteres existiert jedoch kein Prozess.
Rekonstruktion:	Denkbar wäre eine Übertragung von den L-ARR in denen auch alle relevanten Informationen vorhanden sind. Es müssten Funktionen zur Bereitstellung der relevanten Protokolleinträge geschaffen werden. Relevant wären hier die Einträge eines wählbaren Zeitbereichs, die durch das AGW erfolgt sind Interessant wären diese Funktionen eventuell auch um eine Überprüfung der Protokollierung vorzunehmen.

4) GDA-I

Problem:	Verlust von Indexeinträgen führt dazu, dass bestimmte GDA nicht zugreifen können, oder bereits auf inaktiv gesetzte GDA wieder zugreifen können.
Kategorie:	Verfügbarkeitsproblem bzw. datenschutzrechtliches Problem.
Analyse:	Durch Vergleich mit den Lieferungen aus den bestehenden Verzeichnissen bzw. dem eHIM (lokal).
Rekonstruktion:	Durch Anwenden der Lieferungen aus den bestehenden Verzeichnissen auf einen rückgesetzten Datenbestand. Voraussetzung: Getrennte Speicherung und Backup der Zulieferungen.

6418 **5) Z-PI**

6419 a) Einmeldung von ELGA-Bereich fehlt

Problem:	Verlust von Einmeldungen durch die L-PI mittels PIF Transaktion führt zur Unvollständigkeit des Gesundheitsaktes, weil sich die LPID des ELGA-Bereichs nicht in der PIX-Query Antwort befindet und damit bei der Registerabfrage nicht alle ELGA-Bereiche angefragt werden.
Kategorie:	Gesundheitsakt fehlerhaft. Anmerkung: Der betrachtete Fehler führt dazu, dass potentiell Teile im Gesundheitsakt fehlen ohne dass ein Fehlerhinweis gegeben wird. Die Anzeige veralteter Dokumente kann dadurch nicht verursacht werden.
Analyse:	Lokal (sollte immer möglich sein wegen der Protokollierung auf getrenntem, standortübergreifend gespiegelten Filesystem)
Rekonstruktion:	Durch kontrolliertes Nachfahren eines Transaktionsprotokolls.

6420 b) bPK fehlt

Problem:	Verlust von Einmeldungen durch die L-PI mittels PIF Transaktion führt zum Fehlen des bPK. Anmerkung: Für die Übernahme aus der ZPV (Zentrale Partnerverwaltung) wird dieser Fall nicht betrachtet, da hier bei einem Restore, der (nur) den Z-PI betrifft die Übernahme der Verständigungen wiederholt werden kann.
Kategorie:	Verfügbarkeitsproblem, da für den Teilnehmer keine bPK vorliegt (bzw. nicht im Z-PI gefunden wird) und dieser damit nicht an ELGA teilnehmen kann.
Analyse:	Wie oben.
Rekonstruktion:	Wie oben.

6421 **6) e-Medikation**

Problem:	Verlust von Verordnung und / oder Abgaben .
Kategorie:	Gesundheitsakt fehlerhaft. Anmerkung: Ein Problem durch verlorene E-Verordnungen blockiert nicht die Abgabe. Auch kann ggf. später nachgetragen werden (setzt aber dann das Vorhandensein der e-card voraus).
Analyse:	Lokal mittels L-ARR bzw. ggf. weiterer Protokolle.
Rekonstruktion:	Lokal, sofern entsprechende Vorkehrungen (wie z.B. das Führen eines Transaktionsprotokolls) gegeben sind.

6422 **7) L-ARR**

Problem:	Verlust von Audit Messages.
Kategorie:	Keine unmittelbaren Auswirkungen (aus Sicht der Anwendungsfälle von ELGA).
Analyse:	Lokal, sofern geeignete weitere Protokolle verfügbar sind.
Rekonstruktion:	Es ist keine Rekonstruktion vorgesehen, da die nachtägliche Ergänzung bzw. Veränderung von Audit Records aus Sicherheitsgründen nicht zielführend ist.

6423 Da das L-ARR ein wesentliches Mittel bei der Analyse anderer Fehler ist, soll es auf getrennten
6424 Ressourcen liegen und auch eine redundante Datenhaltung verwenden.

6425 **8) Verweisregister**

Problem:	Verlust von Registereinträgen bzw. Änderungen oder Löschungen
Kategorie:	Gesundheitsakt fehlerhaft.
Analyse:	Vergleich mit L-ARR Einträgen (lokalen Protokollen); daher die Empfehlung, das L-ARR auf getrennten Ressourcen (Datenbank, Filesystem) umzusetzen.
Rekonstruktion:	Welche Optionen zur Rekonstruktion zur Verfügung stehen ist von den Gegebenheiten im ELGA-Bereich abhängig. Folgende Aspekte sind zu betrachten: • Interne Konsistenz im ELGA-Bereich (L-PI, Registry, Repositories) • Wiederherstellung aller verlorenen Registereinträge. Dabei muss die setId beibehalten werden damit mögliche Referenzen aus dem PAP weiter verwendbar sind. • Außerdem muss beachtet werden, dass durch die ZGF je nach XDS Konfigurationsvariante Metadaten ergänzt werden (ELGA-Hash). Es ist nicht vorgesehen, dass diese durch den Betreiber erstellt werden. Daher könnte ein erneutes Einbringen bei

	Konfigurationsvariante A nur im Zusammenwirken mit der ZGF erfolgen (Speichern und Registrieren über die entsprechende AGW/ZGF-Instanz). Für das erneute Einbringen müssten spezielle Berechtigungsregeln gelten: So darf z.B. die Kontaktbestätigung schon abgelaufen sein. Auch sollen Dokumente die schon in ELGA registriert waren unabhängig von anderen Regeln (z.B.: „GDA jetzt gesperrt“) rekonstruiert werden können. Zu beachten ist jedoch, dass (mittlerweile) gelöschte Dokumente nicht rekonstruiert werden, oder nach einer Rekonstruktion erneut gelöscht werden sollten. Diese Funktion müsste beim Hersteller der ZGF beauftragt werden und steht daher vorerst nicht zur Verfügung. • Löschungen von Dokumenten. Die Löschungen durch die ZGF müssten aus dem L-ARR und A-ARR rekonstruierbar sein und könnten, eine entsprechende SW-Unterstützung vorausgesetzt, wiederholt werden.

Die Vollständigkeit des Verweisregisters ist von zentraler Bedeutung für die Vollständigkeit des Gesundheitsakts. Fehlende Einträge können in der Regel durch den Benutzer nicht erkannt werden. Es ist daher von besonderer Wichtigkeit, dass ein Datenverlust im Datenbestand der Registry (und im damit verbundenen L-PI) nach Möglichkeit vermieden wird.

Es wird die Spiegelung auf 2 getrennte Storage Systeme und die Führung eines applikatorischen Transaktionsprotokolls empfohlen, auf Basis dessen auch Rekonstruktionsmaßnahmen durchgeführt werden können.

Anmerkung zu den XDS-Konfigurationsvarianten: Grundsätzlich bestehen bei Verwendung der XDS-Konfigurationsvariante A mehr Redundanzen. Ob diese im Krisenfall auch für Rekonstruktionszwecke genutzt werden können hängt einerseits vom Grad der physischen Trennung von ELGA- und internen Komponenten ab und andererseits von der Prozessunterstützung für die Übernahme nach ELGA.

9) Document Repository

Problem:	Verlust von Dokumenten zu registrierten Identifiern
Kategorie:	Betriebsproblem (da das Dokument für den Benutzer erkennbar fehlt)
Analyse:	Vergleich mit L-ARR Daten
Rekonstruktion:	Abhängig von den lokalen Gegebenheiten und der gewählten XDS-Variante.

	Bei XDS- Konfigurationsvariante A (hat ein dediziertes ELGA Repository) kann ggf. eine Übernahme aus dem internen (nicht ELGA) Repository erfolgen, wobei zu beachten ist, dass die setId nicht geändert wird und auch die Konsistenz mit den Einträgen im Dokumentenregister gegeben ist. Bei Variante C kann ggf. ein Befund aus dem Quellsystem neu registriert werden. Auch hier sollte beachtet werden, dass möglichst die setId beibehalten wird, weil möglicherweise Berechtigungsregeln existieren, die auf das Dokument referenzieren.

10) L-PI

Problem:	Verlust von Einträgen im L-PI führen zur Inkonsistenz mit Z-PI. Betrachtet wird hier nur die Inkonsistenz mit dem Z-PI Datenbestand; bereichsinterne Abhängigkeiten sind ausgenommen
Kategorie:	Betriebsproblem mit geringer Störbreite im ELGA Verbund (da folgende Einmeldungen fehlschlagen können)
Analyse:	L-ARR; Z-PI könnte Report mit den kürzlich erfolgten Einmeldungen bereitstellen.
Rekonstruktion:	Richtung Z-PI kann die Konsistenz zeitverzögert wieder hergestellt werden. Ein Problem stellt hier vermutlich jedoch die interne Konsistenz mit den Einträgen im Dokumentenregister dar.

15.4.3. Grundsätzlicher Prozess bei Datenverlust

In dem verteilten, serviceorientierten ELGA-System ist die sichere Datenspeicherung der einzelnen Komponenten von zentraler Bedeutung. Die Architektur sieht keine Mechanismen zum komponenten- bzw. betreiberübergreifenden Rücksetzen von Daten vor weil ein Rücksetzvorgang unabsehbare Auswirkungen hätte, die sich bis in die GDA-Systeme kaskadieren würden. Des Weiteren sieht die Architektur auch keine vorgefertigten Werkzeuge zur komponenten- bzw. betreiberübergreifenden Rekonstruktion von Daten vor, weil die Analyse oben zeigt, dass aufgrund der Vielfalt der Ausfallsszenarien keine Ansätze vorhanden sind, die mit hinreichender Wahrscheinlichkeit und Kosteneffizienz einen Nutzen bringen. Stattdessen werden bei kritischen Komponenten zusätzliche lokale Maßnahmen wie redundante Speicherung und die Führung eines Transaktionsprotokolls umgesetzt. Sollte es trotz aller Vorkehrungen zu einem Datenverlust kommen, werden die definierten Mechanismen des Krisenmanagements genutzt, um den Schaden zu minimieren.

Transaktionsprotokoll

Mit dem Begriff Transaktionsprotokoll wird hier ein Protokoll bezeichnet, das die gesamten Ein- und Ausgangsnachrichten der SOAP Serviceaufrufe beinhaltet. Zusätzlich muss dieses Protokoll ein Ordnungskriterium (z.B. Sequenznummer) enthalten, die zumindest für Serviceaufrufe die einer Synchronisation bedürfen, Aufschluss darüber gibt, in welcher Reihenfolge sie bearbeitet wurden. Im ELGA Kontext besteht der Synchronisationsbedarf hauptsächlich bei Serviceaufrufen die zu einer Person erfolgen. Das Zugriffprotokoll soll eine andere Technologie als die eigentliche Datenspeicherung einsetzen (als z.B. XML-Files versus relationaler Datenbank), und auf getrennten Ressourcen (Disks) liegen.

Auf Basis des Transaktionsprotokolls können im Anlassfall auch komplexe Problemstellungen bis hin zu unbeabsichtigten oder vorsätzlichen Datenverfälschungen analysiert werden. Auch kann das Transaktionsprotokoll zur Rekonstruktion von Daten herangezogen werden. Sollte die Nutzung des Transaktionsprotokolls notwendig werden handelt es sich im Allgemeinen nicht um eine Aufgabe des Regelbetriebs sondern um eine Aufgabe des Third Level Supports. Aufgabe des Regelbetriebs ist es hier nur die Prozesse für die Einbindung des Third Level Supports bereitzustellen.

Das Transaktionsprotokoll unterliegt den gleichen Datenschutzanforderungen wie die Originaldaten. Es gelten die weiter unten erläuterten Maßnahmen für den Zugriffsschutz.

Krisenmanagement

Wenn bei einer Komponente in ELGA im Rahmen eines Ausfalls ein Fall von Datenverlust vorliegt oder anzunehmen ist, so stellt das für ELGA eine Krise dar und der Prozess zum Krisenmanagement kommt zur Anwendung. Der Betreiber darf die Komponenten in diesem Fall nicht in Betrieb nehmen sondern muss den für das Krisenmanagement vorgesehenen Prozess auslösen. Die Entscheidung über die erneute Inbetriebnahme der Komponente, und die Koordination von Analyse- und Rekonstruktionsmaßnahmen erfolgen durch das Krisenteam.

In analoger Weise sind Fälle zu behandeln, wo im online Betrieb festgestellt wird, dass Daten in irgendeiner Weise verfälscht sind. In diesem Fall ist die Komponente abzuschalten und der Prozess für das Krisenmanagement zu starten.

Abgrenzung: Kann der Datenbestand nach einem Ausfall innerhalb der RPO vollständig wiederhergestellt werden, so liegt ein Service Level Problem, jedoch kein Krisenfall bezüglich Datenmanagement vor.

Das Krisenmanagement umfasst im Wesentlichen folgende Schritte:

- Information der Partner (wie für eine Krise festgelegt; zumindest ELGA und Serviceline)
- Feststellung der Störungsbreite und der Möglichkeiten zur Rekonstruktion verlorener bzw. zur Korrektur fehlerhafter Daten.

- Entscheidung über weiteres Vorgehen, insbesondere der Ablauf von Restore-, Rekonstruktions- bzw. Korrektur-Maßnahmen. Bei Fehlern die den Gesundheitsakt betreffen muss in jedem Fall eine Rekonstruktion ohne Datenverlust angestrebt werden. Alternativ ist die Information der betroffenen ELGA-Teilnehmer in Betracht zu ziehen.
- Durchführung der Maßnahmen
- Verifikation, Dokumentation und Schließen des Krisenfalls

Abhängig von der Kategorie des Schadenspotentials wird folgende Vorgehensweise für die Wiederaufnahme des Betriebs als Standard gewählt:

Verfügbarkeitsproblem

Bei einem Verfügbarkeitsproblem soll versucht werden die Auswirkungen der Störung, die sich aus dem Produkt von Störbreite und Ausfallszeit ergeben zu minimieren. Das bedeutet z.B. bei einem Verlust von einigen Kontaktbestätigungen, dass das KBS nach einem Ausfall möglichst rasch wieder in Betrieb genommen wird, um die Phase des daraus resultierenden Totalausfalls von ELGA zu beenden. Die Auswirkungen der verlorenen Kontaktbestätigungen werden in Kauf genommen. Wenn Rekonstruktionsmöglichkeiten zur Verfügung stehen, werden diese nachträglich am online System durchgeführt.

Die zentrale Bereitstellung von konkreten SW Bausteine für Rekonstruktionsmaßnahmen durch die ELGA GmbH ist hier nicht angedacht. Anzumerken ist jedoch, dass alle zentralen Systeme mit doppelt redundanter Datenhaltung ausgestattet sind. D.h. es erfolgt eine standortübergreifende Spiegelung auf zwei Storage Systeme mit jeweils redundanter Speicherung womit die Eintrittswahrscheinlichkeit eines Datenverlust-Ereignisses minimiert ist.

Datenschutzrechtliches Problem

Ergibt sich durch einen Datenverlust ein (mögliches) datenschutzrechtliches Problem so wird versucht, die Gesamt-Auswirkungen der Störung zu minimieren. Diese ergeben sich aus der Summe der Auswirkungen auf die Verfügbarkeit und den Auswirkungen auf die Patientenrechte. Wenn z.B. ein Verlust von einigen Änderungen an Berechtigungsregeln eintritt und eine rasche Rekonstruktion nicht möglich ist, so wird der PAP ebenfalls wieder online gesetzt um den Totalausfall von ELGA zu beenden. Wenn möglich wird in der Folge versucht, Rekonstruktionsmaßnahmen durchzuführen.

Analog zum vorhergehenden Punkt sind auch hier keine zentralen SW-Bausteine zur Unterstützung von Rekonstruktionsmaßnahmen vorgesehen.

Gesundheitsakt fehlerhaft

Bei dieser Kategorie von Störungen soll jedenfalls eine Rekonstruktion verlorener Daten erfolgen bevor die betroffene ELGA-Komponente wieder online geht. Das impliziert, dass die

Software des ELGA Bereichs geeignete Mechanismen zur Durchführung solcher Rekonstruktionsmaßnahmen bereitstellen soll.

Konkret können dies z.B. folgende Funktionen sein:

- Führen eines Transaktionsprotokolls auf getrennter Hardware.
- Analyse der Vollständigkeit der Registry Einträge auf Basis des L-ARR, des Transaktionsprotokolls oder auf Basis von Daten in den Quellsystemen (Document Source).
- Rekonstruktion von Registry Einträgen auf Basis der ermittelten Abweichungen unter Nutzung des Transaktionsprotokolls oder der Daten in den Quellsystemen. *Anmerkung: Aufgrund der Bildung des ELGA-Hash muss eine Rekonstruktion jedenfalls unter Nutzung des AGW erfolgen. In Kap. 15.4.2, Abschnitt „Verweisregister“ wird aufgezeigt, dass in Sonderfällen spezielle Berechtigungen erforderlich sind. Die Implementierung dieser stellt noch einen offenen Punkt dar.*

Zugriffsschutz

Die Maßnahmen zur Analyse der Störungsbreite und zur Rekonstruktion von Datensätzen werden in vielen Fällen die Außerkraftsetzung der normalen Regeln für den Zugriffschutz erfordern, da die Bearbeiter die diese Analysen durchführen jedenfalls lesenden Zugang zu den relevanten Produktivdaten benötigen. Solche Maßnahmen müssen daher strengen Sicherheitsrichtlinien unterliegen.

- Systemzugänge für Diagnose und Reparatur dürfen nur temporär für die Erledigung einer klar definierten Aufgabe freigeschalten werden.
- Die betrauten Mitarbeiter müssen explizit zur Geheimhaltung verpflichtet werden.
- Ggf. durchgeführte Abfragen und Datenänderungen sollen einem Audit durch Dritte unterzogen werden. Die mit der Diagnose und Reparatur beauftragen Mitarbeiter müssen explizit der Auswertung ihrer Tätigkeit zustimmen.
- Daten dürfen keinesfalls (auch nicht verschlüsselt) auf dem Mitarbeiter-PC oder auf portablen Medien gespeichert werden. Ist ein Austausch über Komponenten hinweg erforderlich, so darf dieser nur über speziell gesicherte Server Plattformen und nur in Form von verschlüsselten Files erfolgen.

15.5. Betriebseinstellung seitens ELGA-Bereich

Der Fall, dass ein ELGA-Bereich (z.B. durch einen Konkurs) den Betrieb einstellt, führt aus technischer Sicht dazu, dass etwaige Registeranfragen nicht mehr beantwortet werden und das Ergebnis eine ELGA Abfrage damit als „möglicherweise unvollständig“ gekennzeichnet werden muss.

Aus Sicht von ELGA besteht somit das Interesse, die Daten wieder verfügbar zu machen bzw. verfügbar zu halten. Das kann auf verschiedene Weise erfolgen.

a) Ein anderer Betreiber übernimmt den Betrieb zumindest für lesende Zugriffe (mit unveränderter Community Id). Das setzt voraus, dass zumindest ein Letztstand der Daten vom ursprünglichen Betreiber übernommen werden kann.
   Das Backup Konzept macht hier jedoch keine Vorgaben bezüglich regelmäßiger Hinterlegung eines Backups.

Ein anderer Betreiber übernimmt die Daten in seine Community. Dies sollte grundsätzlich aus Sicht des Berechtigungssystems ebenfalls möglich sein sofern die Dokumente übernommen und mit gleicher setId registriert werden können. Hierzu ist anzumerken, dass gemäß XDS-Metadaten Leitfaden auch die „CommunityId“ in die „setId“ mit aufgenommen wird. Die „CommunityId“ wird jedoch vom BeS nicht dazu verwendet die individuellen Response-Policies bei der Übermittlung an die ZGF zu filtern (es werden alle individuellen Response-Polices an alle ZGF gesendet). Damit können auch „setId“ korrekt bearbeitet werden, die aus anderen ELGA-Bereichen wegen Reorganisation übernommen wurden. Analog zur in Kap. 15.4.2 beschriebenen Rekonstruktion von Verweisregister-Einträgen benötigt man auch hier eine Funktion im BeS, die das Einbringen mit Sonder-Regeln für die Rekonstruktion ermöglicht. Hier ist insbesondere anzumerken, dass der „ELGA-Hash“ über die XDS-Metadaten auch die „Patient-Id“ enthält. Muss diese im Rahmen der Reorganisation geändert werden so wird der Hash ungültig.

15.6. Startup und Shutdown-Verhalten

ELGA-Services sind in der Reihenfolge mit der Berücksichtigung der vordefinierten Abhängigkeiten zu starten. Beim Hochfahren müssen zuerst immer jene Services ans Netz gehen, welche nicht im ELGA-Kernbereich liegen, und zwar Z-PI (L-PI in den ELGA-Bereichen) und GDA-I.

Danach müssen die Protokollierungssysteme hochgefahren werden, und zwar das Z-L-ARR und danach das A-ARR. Entsprechend muss in den ELGA-Bereichen der Betrieb mit dem Hochfahren des L-ARR beginnen.

Wenn die Protokollierungssysteme laufen, müssen KBS und PAP gestartet werden.

Wenn auch KBS und PAP einwandfrei laufen, muss der OCSP-Responder (bzw. Revocation List) die PKI in Betrieb gehen.

Auf zentraler Ebene ist abschließend das ETS zu starten. Mit Inbetriebnahmen des ETS sind die ELGA-Anwendungen zu starten und zwar beginnend mit e-Medikation. Wenn andere ELGA-Anwendungen in Betrieb gehen, muss die Reihenfolge des Hochfahrens bestimmt werden.

Wenn ETS und ELGA-Anwendungen laufen, dann sind in den einzelnen Bereichen die AGW hochzufahren, und zwar jener Reihenfolge folgend, mit der die Bereiche an ELGA angebunden worden sind.

Zuletzt ist der ELGA-Bereich des Portals bzw. das Portal selbst zu starten.

Beim geordneten Shutdown von ELGA ist eine umgekehrte Reihenfolge des Abschaltens notwendig, und zwar in dieser Folge:

1. Portal und AGW des Portals
2. AGW der ELGA-Bereiche in umgekehrten Reihenfolge des Hochfahrens
    a. L-ARR in den ELGA-Bereichen
3. ELGA-Anwendung bzw. AGW der ELGA-Anwendungen
4. ETS
5. KBS und PAP
6. A-ARR und zentrales L-ARR
7. OCSP-Responder/PKI
8. GDA-I und Z-PI

16. Offene Punkte

16.1. Cross-Enterprise Bilddaten Austausch

Die im Kapitel 8.5 angeführten Überlegungen bezüglich des bereichsübergreifenden Bilddatenaustausches sind nur sehr allgemeine Festlegungen, die unter [23] exakt auszuarbeiten und zu präzisieren sind.

Bei der Lösungsfindung sollte jedoch das *XCA-I Integration Profile* als Grundlage herangezogen werden, welche im *Radiology Technical Framework Supplement* präsentiert und beschrieben wurde [10]. ELGA geht davon aus, dass ein eigenes XCA-I Gateway zu errichten ist, wie dies die Abbildung 64 darstellt.

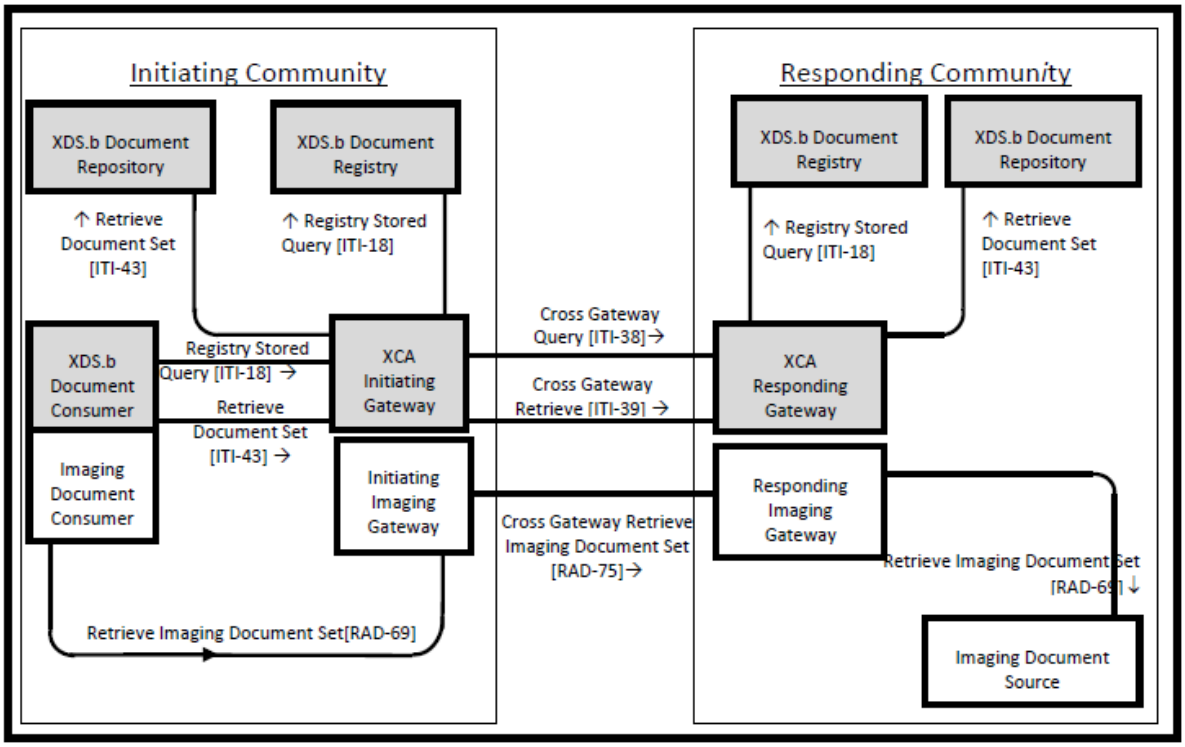


Abbildung 64: Bereichsübergreifender Zugriff für radiologische Bilddaten via XCA-I Profil

16.2. Recovery von Registry & Repository bei Datenverlust

Wie im Kapitel 15.4 angemerkt, bei Verlust von Registereinträgen müssen verlorene Einträge im direkten Zusammenwirken mit der ZGF wiederhergestellt werden. Hierfür müssen die entsprechenden IHE-Transaktionen zur Wiederherstellung des Systems ([ITI-41/42] bzw. [ITI-57/62]) über ZGF-Endpunkte mit speziellen Berechtigungsregeln (Policy) geführt werden.

Für die Rekonstruktion darf z.B. die Kontaktbestätigung schon abgelaufen sein. Auch sollen Dokumente die schon in ELGA registriert waren unabhängig von anderen Regeln (z.B.: „GDA jetzt gesperrt“) rekonstruiert werden können. Zu beachten ist jedoch, dass (mittlerweile) gelöschte Dokumente nicht rekonstruiert werden, oder nach einer Rekonstruktion erneut gelöscht werden müssen.

16.3. Recovery der Quarantäneliste bei identifiziertem Angriff

Punkt ist geschlossen. Siehe hierfür Kapitel 9.1.4.5. Thema ist im BeS Pflichtenheft detailliert auszuarbeiten.

17. Anhang A - Verwendete Farbschemas

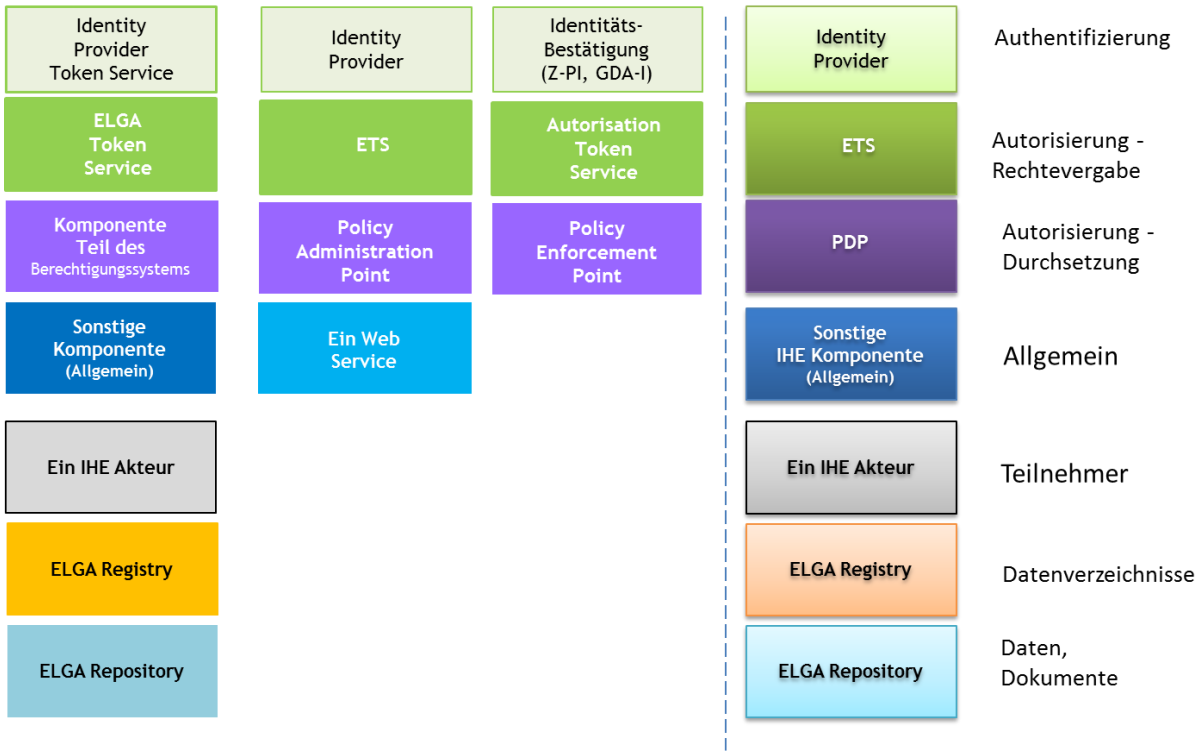
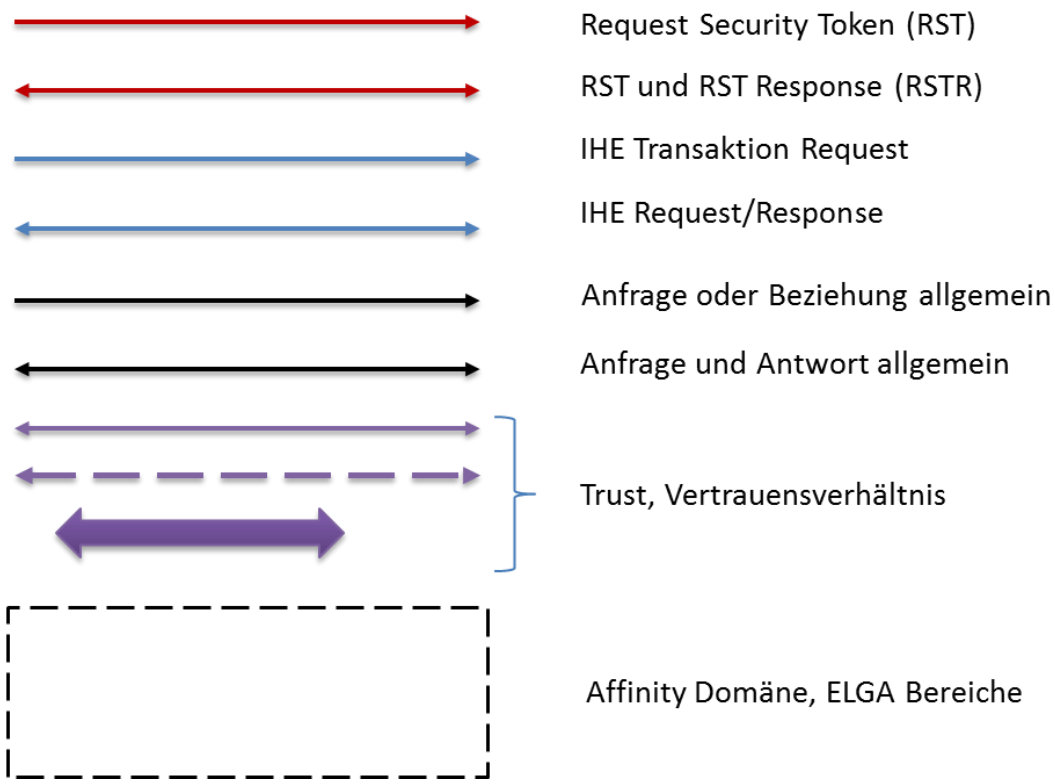


Abbildung 65: Farbschema der logischen und funktionalen Komponenten



6638

6639 *Abbildung 66: Farbschema der Verbindungslinien in den Abbildungen*

6640

18. Anhang B – Beschreibung der Anwendungsfälle

Im Kapitel 2.7 sind tabellarisch alle grundlegenden Anwendungsfälle erfasst. Darüber hinaus werden im Kapitel 9.1.59.1.4.3 bereits konkrete Schnittstellen und Aufrufe genannt, die zur Realisierung der einzelnen Anwendungsfälle von Bedeutung sind. In diesem Anhang werden bestimmte ausgewählte Anwendungsfälle, die aus der Sicht des ELGA-Berechtigungssystems (Zugriffssteuerung) besonders bedeutungsvoll sind, detailliert beschrieben (Darstellungen auf Architekturebene). Die nächste Tabelle verbindet die im Kapitel 2.7 verwendeten Reihennummern der Anwendungsfälle mit den Nummern der Prozessdiagramme.

Anwendungsfälle aus Sicht des Berechtigungssystems	Identifier der Anwendungsfälle	Prozessdiagram
ELGA-Login Teilnehmer	ET.1.1	BP01a
ELGA-Login GDA	GDA.3.1	BP01b
ELGA-Login Vertreter	BET.2.1	BP01c
ELGA-Teilnehmer für IHE Transaktionen autorisieren	ET.1.8 bis ET.1.12	BP01d
Bevollmächtigten ELGA-Teilnehmer für IHE Transaktionen autorisieren	BET.2.8 bis BET.2.12	BP01e
Behandlungszusammenhang schaffen	GDA.3.6	BP02
Demographische Patientensuche	GDA.3.3	BP03
ELGA-GDA für IHE Transaktionen autorisieren	GDA.3.9 bis GDA.3.13	BP05
Zugriffsrechte verwalten und anschließend Consent Dokument (PDF) signiert speichern	ET.1.3	BP06
Generelle Zugriffsrechte definieren/warten	RADM.6.2	BP07
Liste ausgewählter Gesundheitsdaten (CDA) ansehen	ET.1.8	BP08a
Dokumentenliste zu einem Patient abrufen	GDA.3.9	BP08b
Ein bestimmtes CDA-Dokument auswählen, öffnen (durch ELGA-Teilnehmer)	ET.1.9	BP08c
Dokument(e) zu einem Patienten abrufen	GDA.3.10	BP08d
GDA Zugriffe protokollieren	GDA.3.21	BP09
Ausgewählte Protokolle über stattgefundene Zugriffe auf die Gesundheitsdaten durch GDA ansehen	ET.1.6	BP10a
Ausgewählte Protokolle über stattgefundene Zugriffe auf die Gesundheitsdaten durch GDA ansehen (im Name des Vertretenen) durch OBST	OBST.5.6	BP10b

6650 *Tabelle 33: Verknüpfung der Anwendungsfälle mit den entsprechenden Prozessdiagrammen*

18.1. BP01: ELGA-Benutzer in ELGA anmelden und Assertion anfordern

18.1.1. Ausgangslage

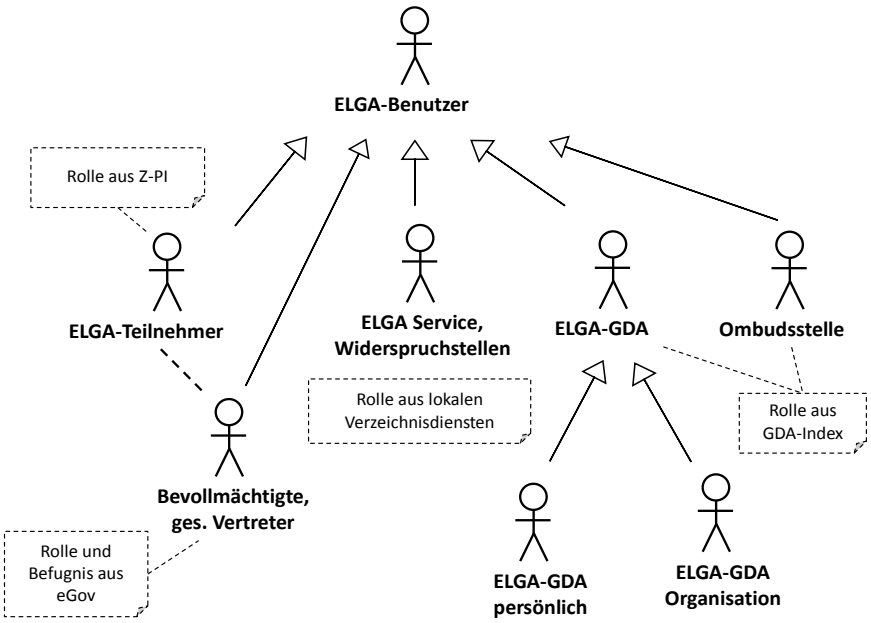


Abbildung 1 zeigt die Gliederung der ELGA-Benutzer auf hoher Ebene. Die verschiedenen Akteure wie ELGA-Teilnehmer bzw. dessen Bevollmächtigte und gesetzliche Vertreter, Mitarbeiter des ELGA-Service (wie z.B. Regelwerk- und Sicherheitsadministratoren) sowie ELGA-GDA als Person oder Organisation werden gesamthaft als ELGA-Benutzer bezeichnet. Identitäten der Ombudsstelle, welche vertretend für den ELGA-Teilnehmer operieren, werden durch den GDA-I verwaltet.

Der Nachweis der elektronischen Identität (Authentifizierung) basiert darauf, dass die Authentisierungsdaten der ELGA-Benutzer mit einem privaten Schlüssel des zuständigen IdP signiert sind. Die Signatur kann anhand des im verwendeten Zertifikat enthaltenen und von einer vertrauenswürdigen Zertifizierungsstelle bestätigten, öffentlichen Schlüssels geprüft werden. Die erfolgreiche Überprüfung resultiert in der Ausstellung einer föderierten ELGA-Identität in Form einer ELGA Authorisation-Assertion, die für eine festzulegende Zeitdauer gültig ist.

Zusätzlich zur Identitätsbestätigung, die der ELGA-Benutzer von einem gültigen IdP erhält, erfordert die Ausstellung einer ELGA Authorisation-Assertion durch das ELGA Token-Service (ETS) für einen GDA die Angabe der gewünschten Rolle (im Einklang mit den im GDA-I geführten Rollen). Die angegebene Rolle wird durch Einsicht im GDA-I verbindlich bestätigt.

In ELGA sind unterschiedliche IdP zugelassen. Der Anwendungsfall wurde so gestaltet, dass neue IdP und Authentifizierungsverfahren in einfacher Weise ergänzt werden können.

18.1.2. Ergebnisse bei Erfolg

Die elektronische Identität, Rolle und Zugriffsart des ELGA-Benutzers wurde explizit für ELGA von einem vertrauenswürdigen Identity Provider (IdP) bestätigt und zwar in Form eines digital signierten SAML 2.0 - Tokens (ELGA Identity-Assertion).

18.1.3. Vorbedingungen und Voraussetzungen

Authentifizierung von ELGA-Teilnehmern

- Besitz einer aktivierten Bürgerkarte und/oder Besitz einer auf Bürgerkartenfunktion aufbauenden alternativen Benutzerkennung wie die Handy-Signatur.
- Automatische Umleitung des User-Agents (z.B. Web-Browser) des Anwenders (ELGA-Benutzer) zur Bürgerkartenumgebung (BKU) beim Authentifizierungsverfahren am ELGA-Portal.
- Das bereichsspezifische Personenkennzeichen für den Tätigkeitsbereich Gesundheit (bPK-GH) muss im zentralen und kann optional auch im lokalen Patientenindex der jeweiligen Person zugeordnet sein.

Authentifizierung von GDA

- Besitz eines gültigen Vertragspartner-Logins im e/o-card System oder
- Benutzung eines für ELGA zugelassenen alternativen vertrauenswürdigen IdP.

18.1.4. Auslöser/Trigger

Die Initiierung dieses Anwendungsfalls (Benutzer Authentifizierung) erfolgt via Umleitungen im Rahmen des Logins am Gesundheitsportal (ELGA-Portal). Diese Aufrufe können u.a. im Rahmen des Logins am e-card System oder durch die GDA-SW bzw. ein vorgeschaltetes Identity Providing Gateway (idpGW - Teil von XDS Document Consumer- bzw. Document Source-Adaptoren) erfolgen.

18.1.5. Szenario

Das Hauptszenario der Authentifizierung von ELGA-Benutzern wird im Folgenden sowohl aus der Perspektive des Bürgers, des GDAs, des Bevollmächtigten als auch des ELGA-Regelwerk- und Sicherheitsadministrators erläutert. Dementsprechend beschreiben die nächsten Szenarien die Ausstellung einer ELGA User I & II Assertion, einer ELGA Healthcare Provider-Assertion, einer ELGA Mandate I & II Assertion bzw. einer ELGA Service-Assertion im Rahmen der Authentifizierung durch das ETS.

18.1.5.1. BP01a: ELGA User I Assertion anfordern (Anwendungsfall ET.1.1)

1. Der ELGA-Teilnehmer wählt via User-Agent (z.B. Web-Browser) die Adresse der vorgesehenen Zugangs-URL (Gesundheitsportal) (Abbildung 67) und auf der dort angebotenen Benutzeroberfläche die gewünschte Authentifizierungsart (reguläre Authentifizierung bzw. Authentifizierung als Bevollmächtigter). Danach erfolgt eine automatische Umleitung zur zuständigen BKU, um das Authentifizierungsverfahren durchzuführen. Anschließend wird der User-Agent (Web-Browser) des Anwenders samt ELGA Identity-Assertion zum ELGA-Portal (oder Gesundheitsportal) zurückgeleitet (über http-POST). Die vorgeschaltete Autorisierungslogik (Teil des Berechtigungssystems) des ELGA-Portals übernimmt die ausgestellte ELGA Identity Assertion und übermittelt zwecks Identitätsföderation die empfangene Assertion an das ETS (via WS-Trust RST delegiert).

   In der aktuellen Version des ELGA-Portals erfolgt die Authentifizierung eines ELGA-Teilnehmers über das Gesundheitsportal, wobei beim Anklicken des weiterführenden Links zum ELGA-Portal der BKU Token mit einem vom PVP ausgestellten Token ersetzt wird. Hierfür verhält sich PVP wie ein „Identity Provider initiated SSO“. Es wird vorausgesetzt, dass dieses Verhalten auch in den nachfolgenden Versionen des ELGA-Portals beibehalten wird. Dem ETS wird daher die vom PVP ausgestellte ELGA Identity Assertion präsentiert.

2. Das ETS validiert die präsentierte ELGA Identity-Assertion sowie die Zulässigkeit des IdP (BKU) und verifiziert als Nächstes die behauptete Identität des ELGA-Teilnehmers anhand des Z-PI.

3. Abschließend wird eine ELGA User I Assertion generiert und an das ELGA-Portal übermittelt. Dieses schafft eine föderierte Identitätsbeziehung, indem die empfangene ELGA User I Assertion der zugrunde liegenden ELGA Identity-Assertion zugeordnet wird. Der ELGA-Teilnehmer ist somit erfolgreich am ELGA-Portal angemeldet.

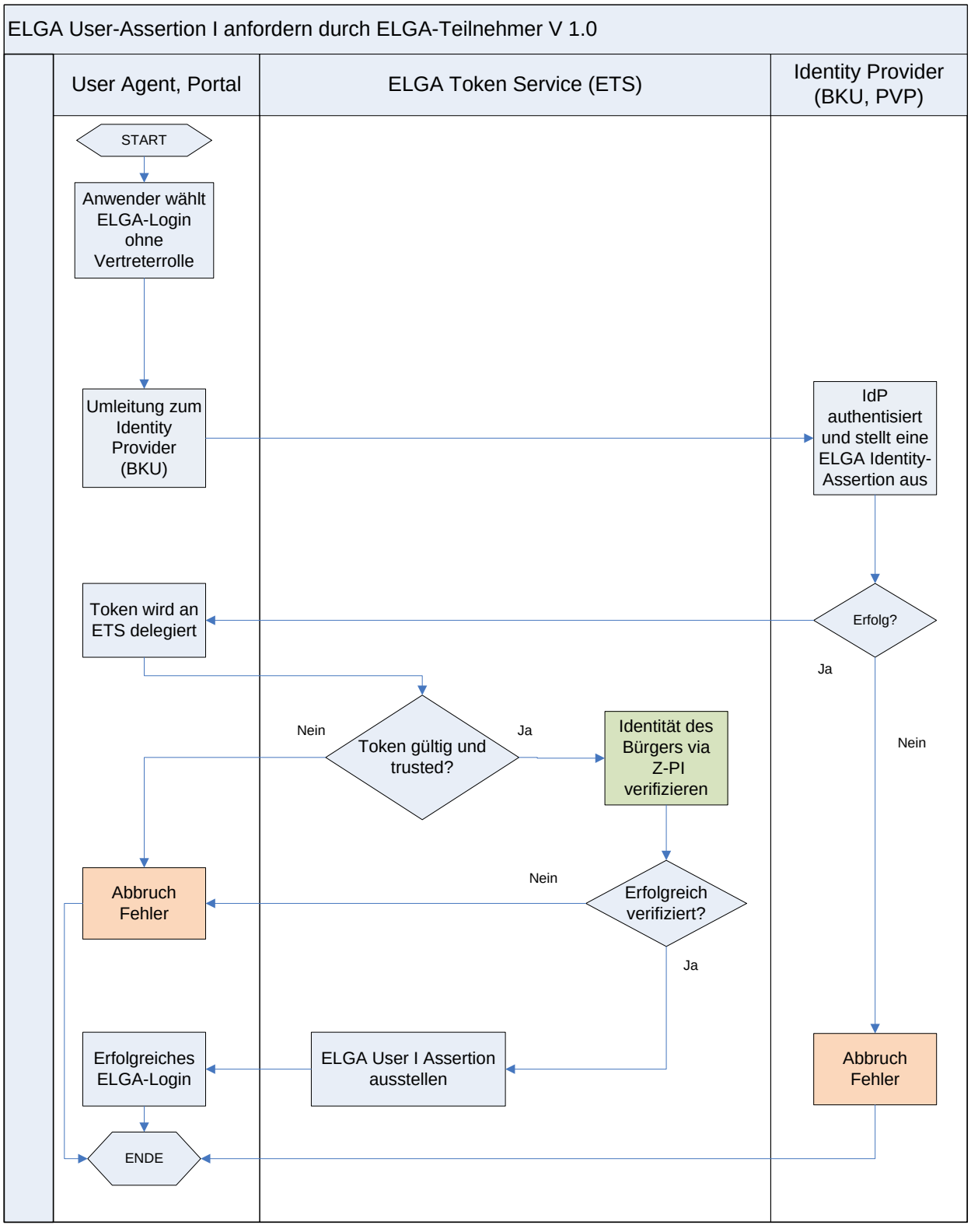


Abbildung 67: Darstellung des Anwendungsfalls BP01a auf Architekturebene (ET.1.1)

18.1.5.2. BP01b: ELGA Healthcare Provider-Assertion anfordern (GDA.3.1)

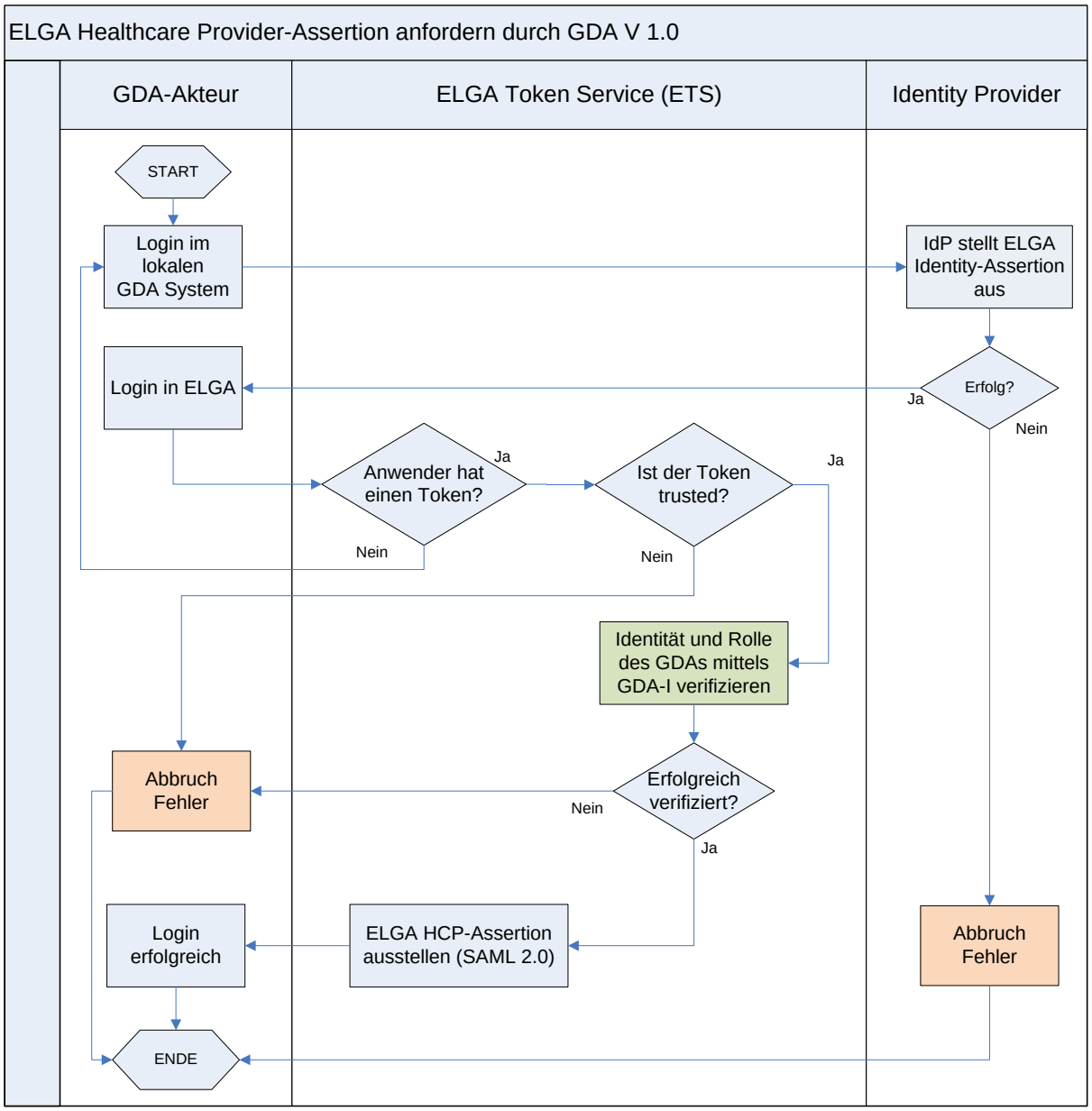
1. Der GDA meldet sich bei seiner lokalen Sicherheitsdomäne an (Login) und fordert mit Hilfe der benutzten Software eine ELGA Identity-Assertion an. Er erhält diese nach

Durchführung des entsprechenden lokalen (oder internen) Authentifizierungsverfahrens von seinem IdP (Username, Passwort, PIN, Biometrisches Verfahren, etc.).

2. Die benutzte GDA-Software (oder KIS-System) versucht nun im Hintergrund und ohne zusätzliche Anwenderaufforderung transparent einen ELGA-Login durchzuführen. Anders gesagt, es wird ein Single Sign On (SSO) in Gang gesetzt. Die GDA-Software bzw. die Identity Providing Gateway Komponente (idpGW) fordert eine ELGA Healthcare Provider-Assertion (HCP-Assertion) beim ETS an.

3. Das ETS prüft die ELGA Identity-Assertion und die Zulässigkeit (Vertrauensverhältnis) des IdP. Weiters wird überprüft, ob der GDA im GDA-I registriert und somit für ELGA zugelassen ist. Zusätzlich wird die vom IdP verwendete OID des GDAs (oder VPNR) auf die in ELGA zulässige OID des GDAs aufgelöst. Im RST wird auch die angeforderte Rolle des GDAs (als Claim) eindeutig vorgegeben und vom ETS via GDA-I geprüft.

4. Resultierend wird eine ELGA Healthcare Provider-Assertion (HCP-Assertion) durch das ETS erstellt und an die anfordernde Softwarekomponente (idpGW) via WS-Trust RSTR Protokoll retourniert. Der GDA ist erfolgreich in ELGA angemeldet.



6751

6752

6753 *Abbildung 68: Darstellung des Anwendungsfalls BP01b (GDA.3.1)*

6754

18.1.5.3. BP01c: ELGA Mandate I Assertion anfordern (Anwendungsfall BET.2.1)

1. Der ELGA-Teilnehmer wählt via User-Agent (z.B. Web-Browser) die Adresse der vorgesehenen Zugangs-URL (Gesundheitsportal), um sich gegenüber dem ELGA-Berechtigungssystem als ein bevollmächtigter Vertreter zu autorisieren (siehe Abbildung 69). Hierfür wählt der ELGA-Teilnehmer auf der angebotenen Benutzeroberfläche explizit die gewünschte Authentifizierungsart als Vertreter. Danach erfolgt eine automatische Umleitung zur zuständigen BKU, um einerseits das Authentifizierungsverfahren des Anwenders durchzuführen und andererseits den Vertretenen (Vollmachtgeber) auszuwählen. Anschließend wird der User-Agent (Web-Browser) des Anwenders samt ELGA Identity-Assertion zum ELGA-Portal zurückgeleitet (http-POST). Die vom IdP ausgestellte ELGA Identity-Assertion enthält neben der bestätigten Identität des Anwenders zusätzlich auch eine eingebettete elektronische Vollmacht des Vertretenen. Die vorgeschaltete Autorisierungslogik des ELGA-Portals übernimmt die ausgestellte ELGA Identity Assertion und übermittelt zwecks Identitätsföderation die empfangene Assertion an den ETS (via WS-Trust RST delegiert).
2. Das ETS validiert die ELGA Identity-Assertion und die eingebettete elektronische Vollmacht sowie die Zulässigkeit des IdP (BKU) und verifiziert als Nächstes die behauptete Identität des Bevollmächtigten und des Vollmachtgebers anhand des Z-PI.
3. Abschließend wird eine ELGA Mandate I Assertion generiert und an das ELGA-Portal übermittelt. Dieses schafft eine föderierte Identitätsbeziehung, indem die empfangene ELGA Mandate I Assertion der zugrunde liegenden ELGA Identity-Assertion zugeordnet wird. Der Bevollmächtigte ist somit erfolgreich am ELGA-Portal angemeldet bzw. föderiert. Die ELGA Mandate I Assertion bildet Identitäts- sowie Autorisierungsinformationen des Bevollmächtigten sowie des vollmachtgebenden ELGA-Teilnehmers in strukturierter Form ab und wird von nun an in der geöffneten Sitzung allen weiteren Aktionen des Bevollmächtigten in ELGA zum Zweck der Zugriffsautorisierung beigefügt.
4. Der Vertreter ist erfolgreich in ELGA angemeldet.

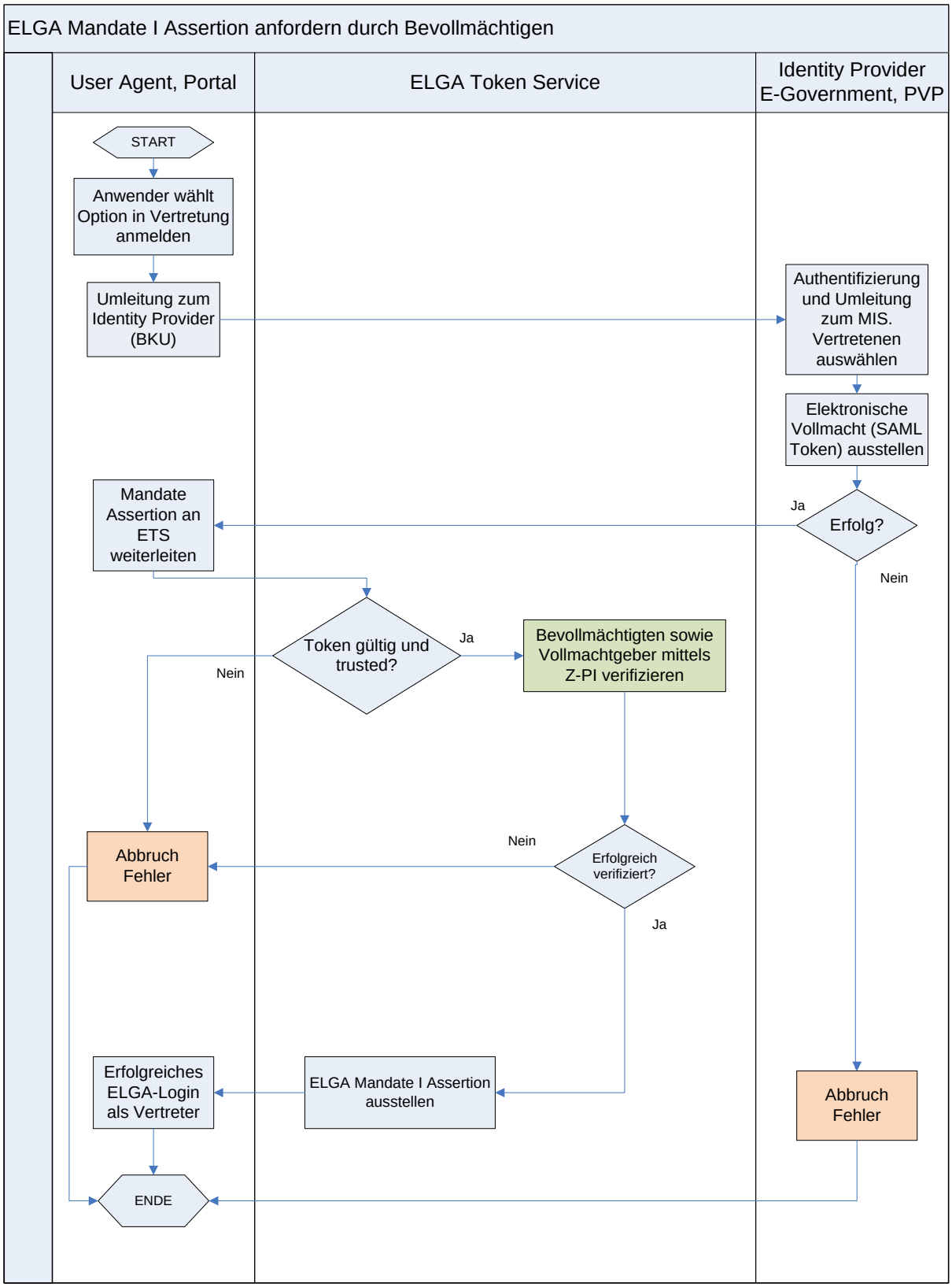


Abbildung 69: BP01c (MIS – Mandate Issuing Service) auf Architekturebene (BET.2.1)

18.1.5.4. BP01d: ELGA User II Assertion anfordern

1. Der ELGA-Teilnehmer initiiert über das ELGA-Portal (bzw. über seinen User-Agent) eine dokumentbezogene Aktion in ELGA (siehe Abbildung 70). Das ELGA-Portal initiiert hierfür im Hintergrund einen regulären Web-Service Zugriff und fügt hierfür im jeweiligen Authorisation Header der Nachricht die *ELGA User I Assertion* des ELGA-Teilnehmers bei.

2. Das ELGA-Portal leitet über einen *Document Consumer* Akteur die Dokumentanfrage an die Zugriffssteuerungsfassade (ZGF) des Berechtigungssystems des angeschlossenen ELGA-Bereichs weiter.

3. Die ZGF empfängt die gewünschte Aktion des ELGA-Teilnehmers, extrahiert daraus die *ELGA User I Assertion* und generiert anschließend eine Ausstellungs-Anfrage (RST) einer *ELGA User II Assertion* an das ETS.

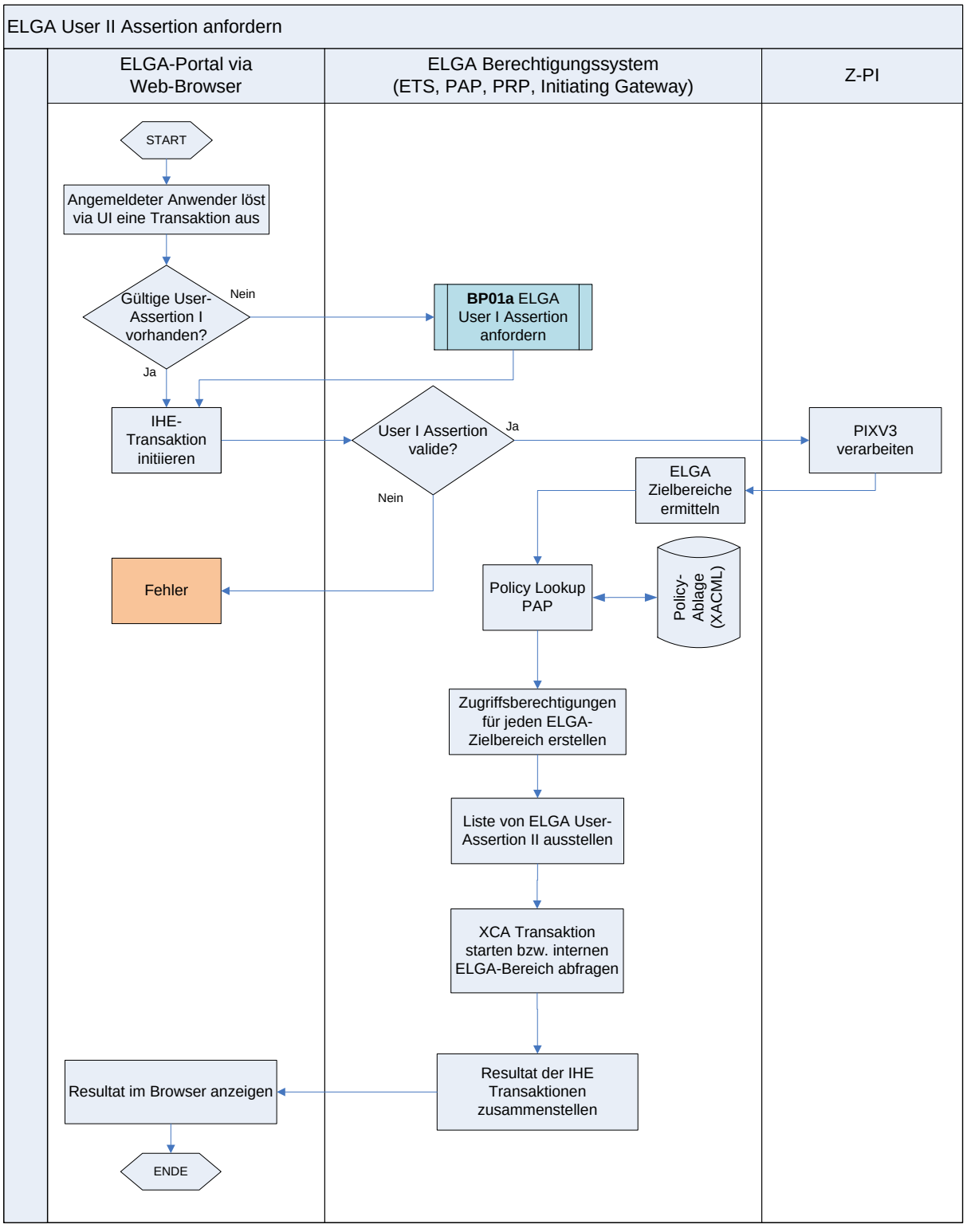
4. Das ETS validiert die erhaltene (präsentierte) *ELGA User I Assertion*. Als Nächstes wird der Z-PI kontaktiert, um ELGA-Zielbereiche (Community IDs), die potentiell medizinische Dokumente des Teilnehmers speichern, zu identifizieren. Hierfür generiert das ETS eine IHE konforme PIX-Anfrage.

5. Abschließend werden für jeden einzelnen identifizierten ELGA-Zielbereich die generellen und relevanten individuellen Zugriffsberechtigungen des ELGA-Teilnehmers vom Policy Administration Point (PAP) abgefragt und in Form von bereichsspezifischen *ELGA User II Assertions* strukturiert. Die dadurch entstandene Liste von *ELGA User II Assertions* wird via WS-Trust RSTRC an die aufrufende ZGF retourniert.

6. Die aufrufende ZGF ordnet die erhaltenen *ELGA User II Assertions* der zugrunde liegenden *ELGA User I Assertion* des ELGA-Teilnehmers zu. Für entfernte (remote) ELGA-Zielbereiche generiert die ZGF parallele Cross-Community (XCA) Requests und fügt die erhaltenen *ELGA User II Assertions* im Authorisation Header der Nachrichten bei. Für lokale Zugriffe ersetzt die ZGF die *ELGA User II Assertion* durch eine entsprechend ausgestellte *ELGA Community Assertion* und leitet so die Anfrage an das Backend (Registry oder Repository) weiter.

7. Die Ergebnisse der dokumentenbezogenen Aktion werden zusammengestellt und anschließend im Browser angezeigt.

6825



6826
6827

6828 *Abbildung 70: Darstellung des Anwendungsfalls BP01d*

18.1.5.5. BP01e: ELGA Mandate II Assertion anfordern

1. Der in ELGA angemeldete (föderierte) Bevollmächtigte initiiert über den verwendeten User-Agent (am ELGA-Portal) eine dokumentbezogene Aktion (z.B. Dokumentensuche). Das ELGA-Portal initiiert hierfür im Hintergrund einen regulären Web-Service Zugriff und fügt hierfür im jeweiligen Authorisation Header der Nachricht die vorhandene *ELGA Mandate I Assertion* des bevollmächtigten ELGA-Teilnehmers bei.

2. Das ELGA-Portal leitet über den Akteur *Document Consumer* die Dokumentanfrage an die ZGF des Berechtigungssystems des angeschlossenen ELGA-Bereichs weiter

3. Die ZGF empfängt die gewünschte Aktion des Bevollmächtigten, extrahiert daraus *die ELGA Mandate I Assertion* und generiert anschließend eine Anfrage (RST) einer *ELGA Mandate II Assertion*.

4. Das ETS validiert die erhaltene *ELGA Mandate I Assertion*. Als Nächstes wird via PIX-Anfrage der Z-PI kontaktiert, um ELGA-Zielbereiche, die wahrscheinlich medizinische Dokumente des vollmachtgebenden ELGA-Teilnehmers speichern, zu identifizieren.

5. Abschließend werden für jeden identifizierten ELGA-Zielbereich die generellen und relevanten individuellen Zugriffsberechtigungen des vollmachtgebenden ELGA-Teilnehmers sowie generellen Zugriffsberechtigungen des Bevollmächtigten vom PAP abgefragt und in Form von bereichsspezifischen *ELGA Mandate II Assertions* strukturiert. Die dadurch entstandenen Listen der *ELGA Mandate II Assertions* werden an die aufrufende Komponente (PRP) der ZGF via RSTRC retourniert.

6. Die ZGF ordnet die erhaltenen *ELGA Mandate II Assertions* der zugrunde liegenden *ELGA Mandate I Assertion* des Bevollmächtigten zu. Für entfernte (remote) ELGA-Zielbereiche generiert nun die ZGF einen Cross-Community (XCA) Request und fügt die erhaltene *ELGA Mandate II Assertions* bei. Für lokale Zugriffe ersetzt die Zugriffssteuerungsfassade die *ELGA Mandate II Assertion* durch die entsprechend zugeordneten *ELGA Community-Assertions* und leitet so die Anfrage an das zuständige lokale ELGA-Verweisregister oder Repository weiter.

7. Die Ergebnisse der Dokumentsuche werden zusammengestellt und anschließend im Browser angezeigt.

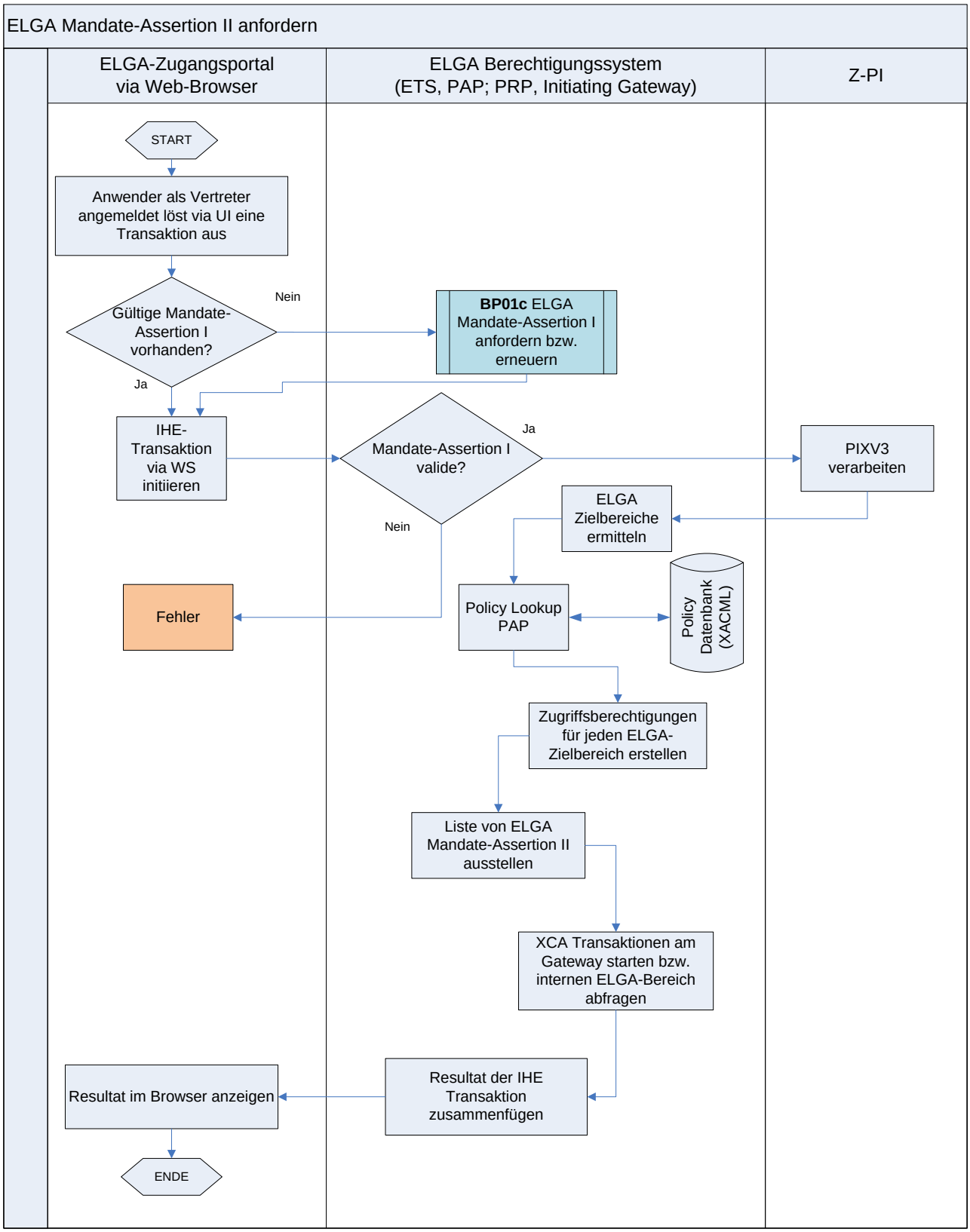


Abbildung 71: Darstellung des Anwendungsfalls BP01e

18.1.6. Ergebnisse bei Fehler

Jeder Fehler, egal ob erwartet oder unerwartet aufgetreten, muss in ELGA entsprechend nachvollziehbar dokumentiert, aufgezeichnet (Logging & Tracing) und in späterer Folge ausgewertet werden. Allgemein gilt, dass sicherheitstechnische Schutzverletzungen aufgrund ungenügender Berechtigungen zu Ausnahmen (sog. Exceptions) führen. Das aufrufende System bekommt als Rückmeldung einen SOAP-Fault. Sonstige Fehlerzustände lösen keine Ausnahmen aus, es wird lediglich ein entsprechender Fehlercode zurückgeliefert. Bei IHE-Transaktionen sind die tabellarisch aufgelisteten Fehlercodes vom ITI TF Volume 3 *Cross Transaction Specifications* zu entnehmen.

Um mögliche Angriffsflächen gering zu halten, wird dem unmittelbar aufrufenden System (GDA, KIS, Arztsoftware, EBP) der Grund der Schutzverletzung nicht mitgeteilt. Lediglich „Access Violation“ oder „Access Denied“ darf als Fehlermeldung mitgeteilt werden. In der Kommunikation von ZGF zu ZGF kann jedoch der exakte Fehlergrund zwecks Protokollierung gesendet werden.

Es ist darauf zu achten, dass Fehlermeldungen auf Benutzeroberflächen entsprechend User-Guidelines benutzerfreundlich zu präsentieren sind. Ein Durchschnittsanwender darf nicht mit systemtechnischen Begriffen, Nummern, Zahlen und/oder internen Bezeichnungen konfrontiert werden.

Zumindest folgende kritische Zustände müssen zur Schutzverletzung (Access Violation) führen:

- *ELGA Identity-Assertion* des IdP wird vom ETS als abgelaufen erkannt. Entsprechendes Umleiten zu IdP muss in die Wege geleitet werden. Ein erneutes Login muss durchgeführt werden.
  - Die mit dem ETS kommunizierende Komponente erkennt diesen Zustand anhand der RSTRC, welche als Antwort auf eine RST für ELGA HCP-Assertion, User I Assertion, Mandate I Assertion oder WIST-Assertion (bzw. Service-Assertion) gesendet wird.
  - Die Umleitung zum eigentlichen IdP führt das EBP bzw. das entsprechende KIS-System (Arztsoftware) durch.
- Eine *ELGA Authorisation-Assertion* wird vom ETS als abgelaufen erkannt. Wenn die zugrunde liegende *ELGA Identity-Assertion* noch gültig ist, muss ein Erneuern (Renew) des Tokens in die Wege geleitet werden (automatisch oder manuell). Wenn dem Token zugrundeliegende *Identity*-Assertion ungültig ist, kann der Token trotzdem auf Basis der noch gültigen Token erneuert werden:
  - *ELGA HCP-Assertion kann ohne IdP-Assertion nur einmal erneuert werden*

- *ELGA User I Assertion und Mandate I Assertion können ohne IdP-Assertion vom ETS zweimal erneuert werden*

- *ELGA Identity-Assertion* des IdP wird vom ETS als ungültig bzw. das zugrunde liegende Zertifikat als widerrufen erkannt. Dies führt zum Abbruch des Anmeldeprozesses in ELGA.
- ELGA-Teilnehmer/Vollmachtgeber kann mittels Z-PI nicht identifiziert werden. Der Anmeldeprozess wird abgebrochen.
- GDA existiert gemäß GDA-I nicht oder die identifizierte ELGA-Rolle ist für die Durchführung der Transaktion nicht berechtigt. Die Transaktion muss abgebrochen werden.

18.1.7. Ergänzungen bzw. Offene Punkte

Die Authentisierungsmechanismen für die **ELGA-Ombudsstelle** sind im Kapitel 5 erklärt. Wichtig ist zu vermerken, dass die ELGA-Ombudsstelle für einen lesenden Zugriff auf die Gesundheitsdaten des ELGA-Teilnehmers keine Kontaktbestätigung benötigt. Dementsprechend restriktiv muss die Rolle des Ombudsmannes ausgeübt und im Berechtigungssystem implementiert werden.

Anmerkung: Die Rolle ELGA-Ombudsstelle darf weder speichernd noch verändernd auf ELGA-Gesundheitsdaten zugreifen. Individuelle Anwenderberechtigungen des Patienten (XACML-Policies) dürfen jedoch geändert und gewartet werden.

Authentisierungsmechanismen für **ELGA-Widerspruchstellen** sind im Kapitel 4 beschrieben. Die ausgestellte föderierte Identität ist ausschließlich zur Durchführung von Opt-Out, partiellem Opt-Out (bzw. deren Widerruf) berechtigt.

Authentisierungsmechanismen für ELGA-Regelwerk- und ELGA-Sicherheitsadministratoren, System-, und Datenbankadministratoren müssen im BeS-Pflichtenheft detailliert ausgearbeitet werden. Diese Rollen sind voraussichtlich im ELGA Service-Index angeführt und die dafür berechtigten Personen namentlich eingetragen (etwa im entsprechenden Verzeichnisdienst).

18.2. BP02: Behandlungszusammenhang herstellen (Anwendungsfall GDA.3.6)

18.2.1. Allgemeines

Lesende und schreibende ELGA Transaktionen durch einen GDA zu einem ELGA-Teilnehmer sind im Allgemeinen nur dann zulässig, wenn sich der ELGA-Teilnehmer in einem aktuellen Behandlungszusammenhang mit dem GDA befindet (Ausnahme ELGA-Ombudsstelle). Ein gesetzlich definiertes, jedoch durch Bürger individuell einschränkbares und erweiterbares Zeitfenster, betreffend die Dauer des zulässigen Zugriffs ab dem Zeitpunkt der technischen Erstellung dieses Behandlungszusammenhangs, ist vorgesehen. Aus Sicht des Berechtigungssystems ist es deshalb notwendig, bei der Veröffentlichung, der Suche, sowie dem Abruf von ELGA CDA Dokumenten den Behandlungszusammenhang des Patienten mit dem GDA technisch zu verifizieren, um möglichen Missbrauch weitestgehend einzuschränken. Die Notwendigkeit eines technisch verifizierten Behandlungszusammenhangs als Voraussetzung einer Zugriffsautorisierung reduziert das Missbrauchspotential entscheidend.

Es existiert ein zentrales Kontaktbestätigungsservice (KBS), dem ein Kontakt gemeldet werden kann und das den gemeldeten Behandlungszusammenhang speichert. Hierfür sind zwei grundsätzlich unterschiedlichen Szenarien zu vorgesehen:

18.2.2. KBS in Zusammenarbeit mit dem e-card System

Im niedergelassenen GDA-Bereich wird das Bestätigungsservice des e-card Systems der Sozialversicherung verwendet. Es wird davon ausgegangen, dass dieses e-card Service in die Patientenadministration und Arztsoftware (Praxissoftware) integriert ist. Die Kontaktbestätigung des e-Card Systems, die beim Stecken der e-card erzeugt wird, wird vom Akteur in der Arztsoftware an das zentrale KBS weitergeleitet.

18.2.3. Zentrales Kontaktbestätigungsservice (KBS)

Eine Kontaktbestätigungsanfrage kann in einem Krankenhaus (oder Pflegeheim) auch ohne Stecken der e-card initiiert werden. Hierfür muss eine Kontaktbestätigung manuell oder in die Patientenadministration integriert durch einen berechtigten GDA gemeldet werden. Das KBS überprüft die ELGA-Rolle anhand der entsprechenden ELGA-HCP Assertion.

Bei erfolgreicher Verifizierung speichert das zentrale Kontaktbestätigungsservice (KBS) für den identifizierten ELGA-Teilnehmer eine Kontaktbestätigung ab. Die Kontaktbestätigung selbst wird dem anfragenden Benutzer nicht übermittelt, nur die ID des erstellten Kontaktes.

18.2.4. Ergebnisse bei Erfolg

Der Behandlungszusammenhang zwischen zugreifendem GDA und betroffenen ELGA-Teilnehmer ist immer in der ELGA Behandlungszusammenhang-Datenbank (KBS)

gespeichert. Der auslösende GDA erhält immer die Identifikation (ID) der Kontaktbestätigung, welche als Erfolgsmeldung verstanden werden kann.

18.2.5. Vorbedingungen und Voraussetzungen

Die Behandlungszusammenhang-Datenbanken müssen für ELGA-Teilnehmer am ELGA-Portal bekannt und lesend zugänglich sein. Dies ist notwendig, um individuelle Berechtigungen aufgrund bestätigter GDA-Kontakte zu erstellen oder warten.

Für die Verwendung der Kontaktbestätigungsservices des e-card Systems, sind die vom e-card System verlangten HW- und SW-technische Voraussetzungen zu erfüllen (etwa Anbindung via GINA-Box).

Für die Verwendung des zentralen Kontaktbestätigungsservices des ETS muss der Service zugänglich sein (URL-Endpoint Address) und der direkte Auslöser (die Komponente, GDA, Akteur) eines Kontaktbestätigungsereignisses muss die entsprechend bestätigte ELGA-Rolle ausüben.

18.2.6. Auslöser/Trigger

Im Falle der Verwendung des e-card Systems muss die e-card in das Lesegerät gesteckt werden, um ein entsprechendes Ereignis (Event) auszulösen (triggern).

Im Falle der Verwendung des zentralen Kontaktbestätigungsservices des ETS muss der Auslöser (Event) an einen entsprechenden Geschäftsprozess (Workflow) der jeweiligen Krankenanstalt (oder Pflegeheim etc.) gebunden werden. Als die am besten geeignete Möglichkeit wird hierfür die Aufnahme bzw. Entlassung eines Patienten angesehen.

18.2.7. Szenario (zentrales Kontaktbestätigungsservice, KBS)

1. Der Bürger wird durch einen GDA stationär aufgenommen.
2. Das lokale Gesundheitsinformationssystem übermittelt den einheitlich strukturierten Behandlungszusammenhang via WS-Trust RST an das ELGA-Kontaktbestätigungsservice, um dieses Ereignis (Event) in der Behandlungszusammenhang-Datenbank zu vermerken.
3. Die ELGA Behandlungszusammenhang-Datenbank persistiert die Tatsache eines stattgefundenen Kontaktes (Behandlungszusammenhang) mit den dazugehörigen Attributen (Datum, Zeit, Identität des GDA, Identität des Patienten etc.).
4. Antwort in Form einer Identifikation wird dem Auslöser zurückgesendet. Die Komponente kann die ID aufheben oder auch verwerfen.

Der zeitliche Ablauf wird durch Abbildung 72 deutlich.

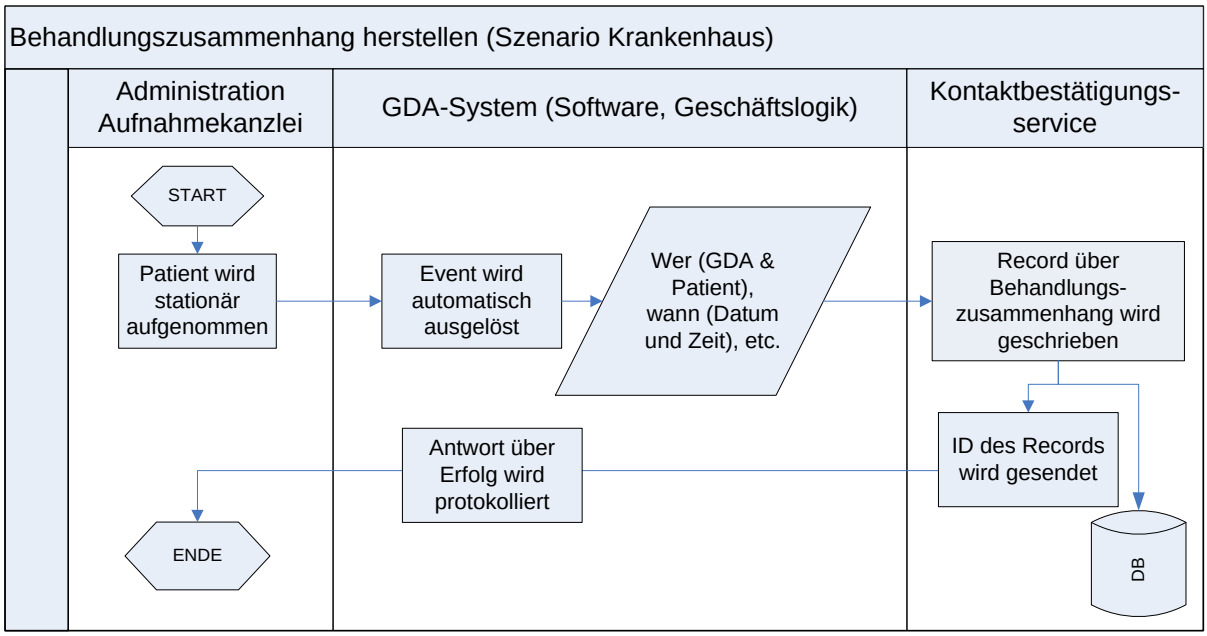


Abbildung 72: Darstellung des Anwendungsfalls BP02 (GDA.3.2)

18.2.8. Ergebnisse bei Fehler

Entsprechend Schnittstellendokumentation des Herstellers, SOAP-Fault bei allen Schutzverletzungen (*Access Violation*) oder Fehlercode bei sonstigen Aufrufen mit nicht akzeptablen Parametern.

18.3. BP03: Demographische Patientensuche (Anwendungsfall GDA.3.3)

18.3.1. Allgemeines

Ein GDA muss grundsätzlich in ELGA nicht angemeldet sein, um eine demografische Patientensuche (PDQ) starten zu können. Lediglich die Akteure Client (GDA-System) und Target (L-PI oder/und Z-PI) müssen sich gegenseitig als vertrauenswürdige ATNA Secure Nodes anerkennen. Zugriff auf den Z-PI erfolgt über eine vordefinierte IHE Transaktion *Patient Demographics Query* (PDQ).

Es ist wichtig zu vermerken, dass für die demografische Suche, ausgelöst durch ein GDA-System, primär der L-PI zuständig ist. Wenn der L-PI keine übereinstimmenden Sätze finden kann, muss er die Anfrage automatisch an den Z-PI weiterleiten. Somit ist der Zugriff seitens GDA völlig transparent. Eine explizite Anfrage an den Z-PI ist jedoch nicht ausgeschlossen auch wenn dies nicht den Hauptanwendungsfall repräsentiert.

18.3.2. Ergebnisse bei Erfolg

Der GDA hat den zu behandelnden ELGA-Teilnehmer anhand des L-PI oder Z-PI gefunden und eindeutig identifiziert.

18.3.3. Auslöser/Trigger

Der Auslöser einer PDQ-Anfrage ist eine manuell initiierte Suchfunktion des GDA-Systems, um den Patienten, auf dessen ELGA CDA Dokumente zugegriffen werden soll, eindeutig zu identifizieren.

18.3.4. Szenario

1. Der GDA erstellt eine demographische Suchanfrage. Die Übermittlung einer ELGA HCP-Assertion an den Zentralen Patientenindex ist dafür nicht erforderlich. Vertrauenswürdige (ATNA Secure Node) Akteure können PDQs beliebig starten.
2. Der Z-PI verarbeitet die demographische Suchanfrage.
3. Resultate der Suchanfrage werden an das aufrufende System des GDAs übermittelt.

Der zeitliche Ablauf wird durch Abbildung 73 deutlich.

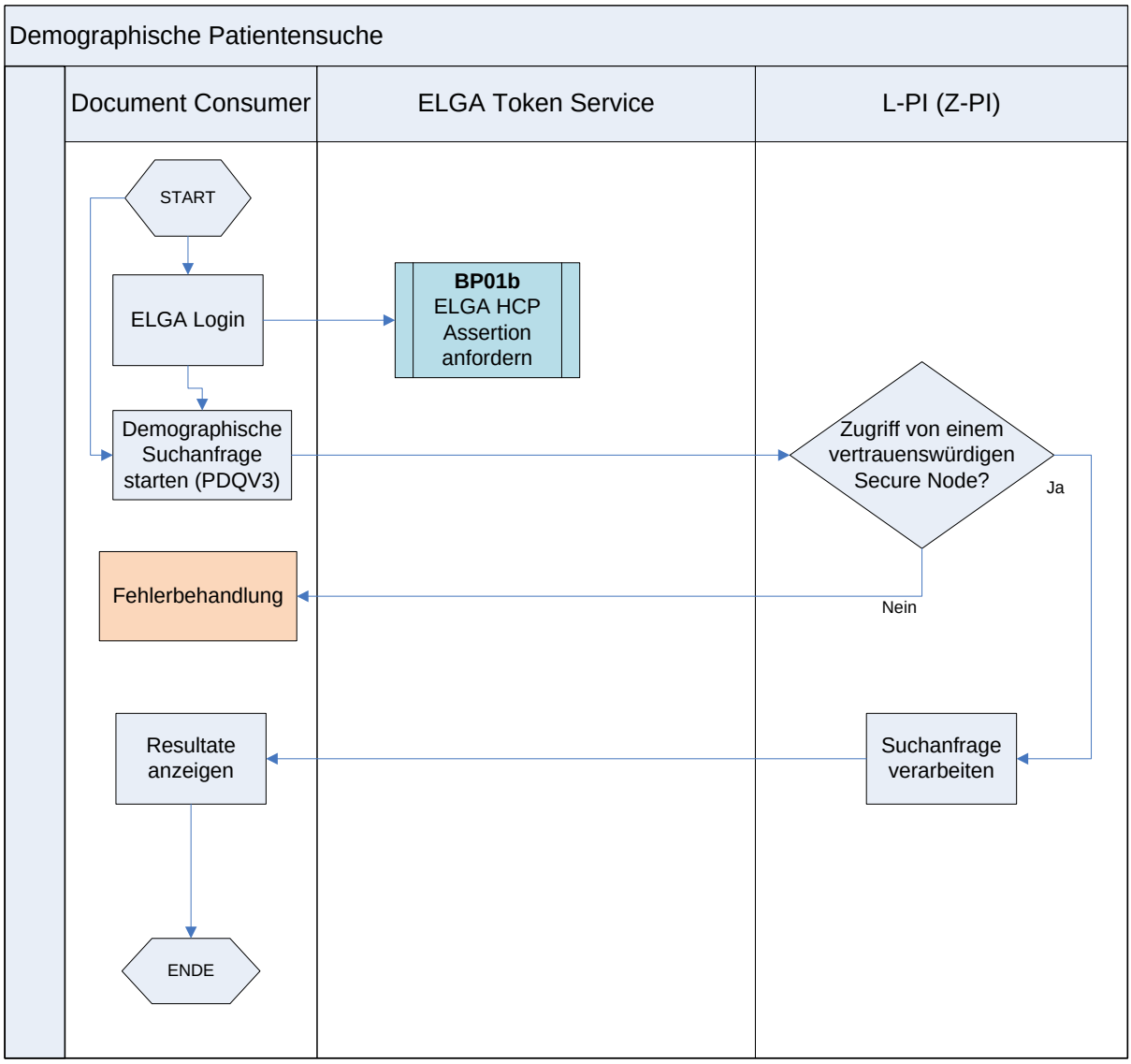


Abbildung 73: Darstellung des Anwendungsfalls BP03 (GDA.3.3)

18.3.5. Ergebnisse bei Fehler

Das auslösende GDA-System erhält einen SOAP-Fault (unauthorized access) bzw. eine Fehlermeldung.

18.4. BP05: ELGA Treatment-Assertion ausstellen

18.4.1. Allgemeines

Wie bereits erläutert, basiert die Autorisierung von Zugriffen auf personenbezogene medizinische Daten in ELGA durch GDA auf einer zweistufigen Autorisierung. Die erste Phase wurde bereits in BP01 beschrieben. Die zweite Autorisierungsstufe stellt die Voraussetzung für zulässige Zugriffe auf medizinische Daten in ELGA dar. Sie resultiert in der Ausstellung einer *ELGA Treatment-Assertion* für je einen ELGA-Zielbereich durch das ETS und umfasst die Verifikation der behaupteten Identifikationsdaten des Patienten, die technische Überprüfung des Behandlungszusammenhangs zwischen aufrufendem GDA und dem Patienten, sowie die Strukturierung relevanter genereller und individueller Zugriffsberechtigungen.

Die Initiierung der zweiten Autorisierungsstufe erfolgt durch den GDA implizit im Zuge einer personenbezogenen Aktion innerhalb von ELGA. Hierbei muss ein in ELGA zulässiger Patientenkontext bekannt sein. Dies ist in einigen Varianten möglich:

- Durch eine explizite Kombination von *ELGA HCP-Assertion* und Patientenkontext
  - Patienten-ID explizit im Nachrichtenheader anführen (nicht IHE konform)
- Durch eine implizite Kombination von *ELGA HCP-Assertion* und Patientenkontext
  - Patientenkontext von der Nachricht extrahieren und in ZGF zwischenspeichern

Die *ELGA Treatment-Assertion* wird an die ZGF ausgestellt. Die entsprechende Komponente der ZGF verkörpert den eigentlichen Akteur der im Namen des GDA agiert. In WS-Trust Kategorien kann dies entweder als Delegation (*ActAs*) oder auch als Impersonation (*OnBehalfOf*) implementiert werden. Im Allgemeinen gilt ersteres als die sicherere, zweites die einfachere Variante wobei diesbezügliche Details im Pflichtenheft zu erarbeiten sind.

Die eigentlichen Zugriffsberechtigungen (beigefügt in die *ELGA Treatment-Assertion*) sowie das Wissen, in welchen ELGA-Bereichen medizinische Dokumente des jeweiligen Patienten existieren, verbleiben in Form von *ELGA Treatment-Assertions* innerhalb des Berechtigungssystems und sind durch den GDA nicht einsehbar.

18.4.2. Ergebnisse bei Erfolg

Eine Liste von *ELGA Treatment-Assertions* wurde ausgestellt und an die entsprechende Komponente des Berechtigungssystems via RSTRC übermittelt. Dadurch agiert die besagte Komponente der ZGF im Auftrag des GDA-Akteurs. Bei Erfolg müssen die adressierten ELGA-Zielbereiche angesprochen werden (XCA oder XDS).

18.4.3. Vorbedingungen und Voraussetzungen

- BP01b: ELGA HCP-Assertion anfordern wurde erfolgreich durchgeführt.
- BP02: Behandlungszusammenhang herstellen wurde erfolgreich durchgeführt.
- Der Patient, dessen ELGA CDA Dokumente gesucht, abgerufen bzw. veröffentlicht werden sollen, wurde anhand des Z-PI eindeutig identifiziert. Dies ist u.a. nach erfolgreicher Durchführung des Anwendungsfalls BP03: demographische Patientensuche sichergestellt.
- Die Identität des Patienten (Patientenkontext) muss als Teil einer Aktion in ELGA abgebildet sein.

18.4.4. Auslöser/Trigger

Der GDA möchte im Rahmen eines existierenden Behandlungszusammenhangs mit einem identifizierten Patienten dessen medizinische Dokumente in ELGA veröffentlichen, suchen oder abrufen. Die Ausstellung einer *ELGA Treatment-Assertion* erfolgt, gegeben der erfüllten Voraussetzungen, implizit (im Hintergrund) im Rahmen einer personenbezogenen Aktion in ELGA.

18.4.5. Szenario

1. Nach erfolgreicher Authentifizierung erhält der GDA eine *ELGA HCP-Assertion*. Falls im lokalen System des GDAs kein in ELGA zulässiger Patientenidentifikator (z.B. bPK-GH) verfügbar ist, kann eine demographische Patientensuche (siehe BP03) durchgeführt werden.
2. Der GDA initiiert nun eine personenbezogene Aktion in ELGA (z.B. Anforderung einer Übersicht aller ärztlichen Entlassungsinformationen eines ELGA-Teilnehmers). Er initiiert hierfür eine *Registry Stored Query* autorisiert mit seiner *ELGA HCP-Assertion.* Die *ELGA HCP-Assertion* ist im *Authorisation Header* der SOAP-Nachricht und die L-PID des Patienten wird implizit in der Nachricht mitgeführt.
3. Die ZGF empfängt die gewünschte Aktion des GDAs, extrahiert daraus die *ELGA HCP-Assertion* sowie den L-PID und generiert anschließend die Anfrage einer *ELGA Treatment-Assertion*, um diese an das ETS zu übermitteln (RST).
4. Das ETS validiert die erhaltene *ELGA HCP-Assertion*.
5. Das ETS validiert auch die Identität des Patienten mit Hilfe des Z-PI (PIX-Anfrage).

6. Die Existenz und Gültigkeit eines Behandlungszusammenhangs zwischen dem aufrufenden GDA und dem betroffenen Patienten unter Verwendung des KBS wird überprüft.
7. Es werden aufgrund der empfangenen PIX-Antwort die ELGA-Zielbereiche, die wahrscheinlich medizinische Dokumente des Patienten speichern, bestimmt.
8. Basierend auf der Rolle des anfordernden GDAs werden dessen generelle Zugriffsberechtigungen, sowie die durch den betroffenen Patienten festgelegten individuellen Zugriffsberechtigungen vom (PAP) abgefragt. An dieser Stelle werden bestimmte Policies (sogenannte Request-Policies) bereits durch den Policy Decision Point verarbeitet und eine entsprechende Zugriffsentscheidung getroffen werden (z.B. bei Opt-Out des Patienten).
9. Bei genereller Zulässigkeit der initiierten Aktion werden abschließend die Identitätsinformation des Patienten, Identitäts- und Rolleninformationen des GDAs, generelle und individuelle Zugriffsberechtigungen sowie generelle Zugriffsentscheidungen in Form von ELGA bereichsspezifischen *ELGA Treatment-Assertions* einheitlich strukturiert an die aufrufende Komponente der ZGF retourniert (eine Treatment-Assertion pro ELGA-Bereich).
10. Die ZGF generiert entsprechende XCA-Anfragen und/oder leiten die Anfrage lokal (XDS) weiter.

Der zeitliche Ablauf wird durch Abbildung 74 deutlich.

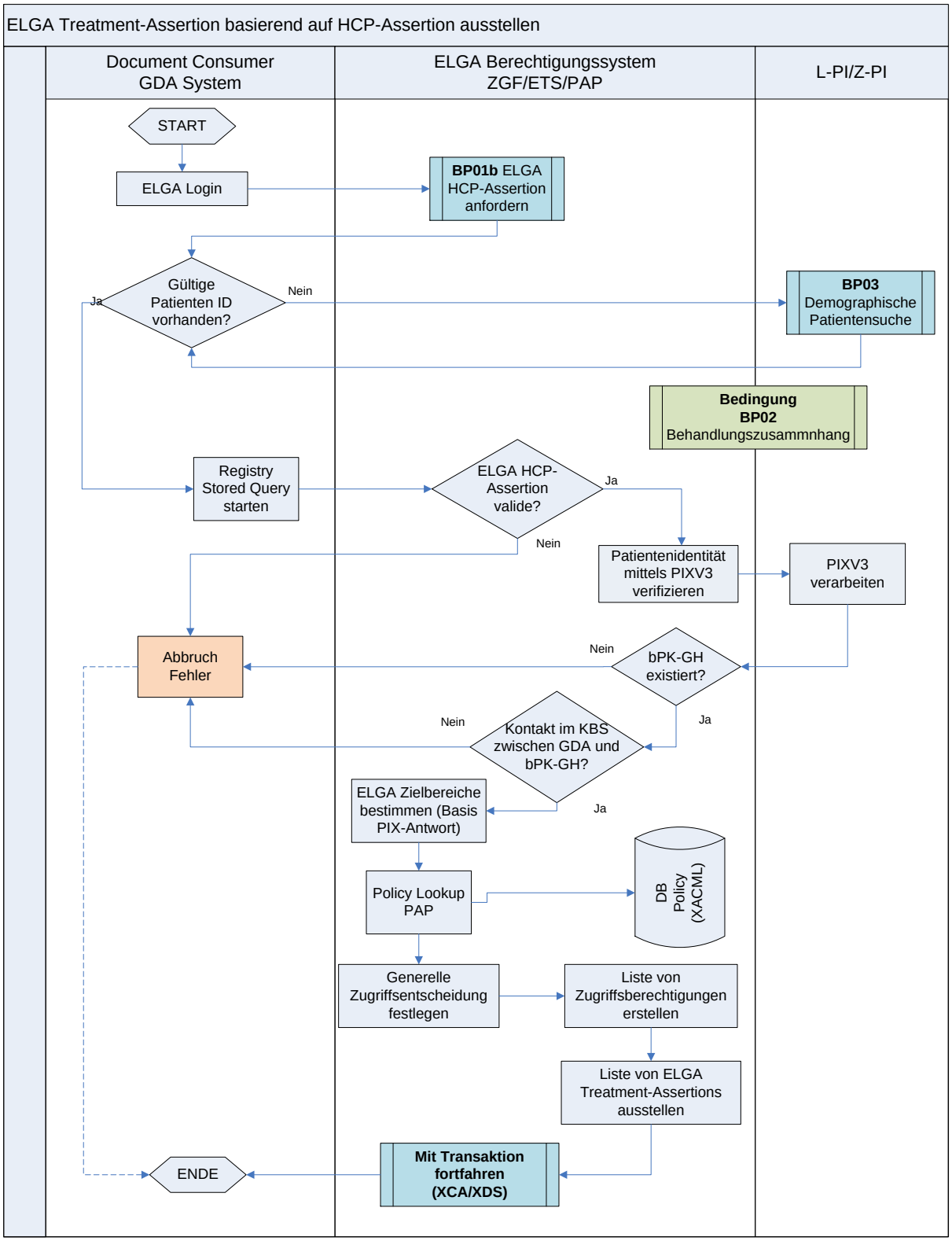


Abbildung 74: Darstellung des Anwendungsfalls BP05

18.4.6. Ergebnisse bei Fehler

- Bürger kann im Z-PI nicht identifiziert werden, es gibt kein bPK-GH zum angeführten Patienten (L-PID): Entsprechendes Fault an den Aufrufer.

- Kein gültiger Behandlungszusammenhang vorhanden: entsprechendes Fault an den Aufrufer.

18.5. BP06: Individuelle Berechtigungen bestimmen (Anwendungsfall ET.1.3)

18.5.1. Allgemeines

Jeder ELGA-Teilnehmer hat die Möglichkeit zusätzlich zu den voreingestellten generellen Zugriffsberechtigungen weitere individuelle Zugriffsberechtigungen zu definieren. Folgende, als Beispiele zu betrachtende, individuelle Zugriffsberechtigungen können festgelegt werden:

- Opt-Out bzw. Opt-Out Widerruf erklären. Ab dem Zeitpunkt der Opt-Out Festlegung ist die Veröffentlichung weiterer ELGA-CDA-Dokumente des betroffenen ELGA-Teilnehmers in ELGA nicht mehr möglich. Bereits vorhandene Verweise auf ELGA-CDA-Dokumente werden für alle ELGA-Benutzer gelöscht (soweit die Dokumente explizit und ausschließlich für ELGA zur Verfügung standen). Mit dem Zeitpunkt der Festlegung eines Opt-Out Widerrufs ist die Veröffentlichung und Einsicht von Verweisen auf medizinische Dokumente des betroffenen ELGA-Teilnehmers wieder zulässig.
- Einzelne Dokumente ausblenden. Diese sind durch GDA somit nicht mehr einsehbar.
- Einzelne Dokumente löschen. Die konkrete Vorgehensweise hierfür ist davon abhängig, ob das Dokument (die Dokumente) ausschließlich für ELGA Zwecke veröffentlicht wurde. Zumindest jedoch muss der Verweis vom betroffenen ELGA-Verweisregister entfernt werden.
- Die Gültigkeitsdauer eines existierenden Behandlungszusammenhangs festlegen. Ein gültiger Behandlungszusammenhang stellt die Voraussetzung für Zugriffe auf personenbezogene medizinische Dokumente durch GDA dar.

Es ist wesentlich, sicherzustellen, dass eine möglichst einfache und effiziente Vergabe von individuellen Zugriffsberechtigungen auf medizinische Dokumente des ELGA-Teilnehmers in ELGA unterstützt wird. Dies wird erzielt mittels

- einer übersichtlichen Darstellung von ELGA CDA Dokumenten, die durch den Bürger selbst bestimmbar ist. Nach individuellen Ansprüchen können Dokumente einerseits frei gewählt und gruppiert oder gemäß parametrierbarer Kriterien (z.B. zeitliche Einschränkung, Dokumentenklasse, Aufnahme, Einrichtung) sortiert bzw. gefiltert werden.
- einer übersichtlichen Darstellung der GDA-Kontakte (Behandlungszusammenhänge).

Die entsprechende Benutzeroberfläche (GUI, Graphical User Interface) wird seitens des ELGA-Portals bereitgestellt. Resultierende Zugriffsberechtigungen werden vom Berechtigungssystem gemäß der *eXtensible Access Control Markup Language (*XACML) in

formale Policies (=Zugriffsberechtigungen) übersetzt und durch den zentralen Policy Administration Point (PAP, entspricht einem Policy Access Point) persistiert.

Der Bürger kann mit Hilfe des ELGA-Portals individuelle Zugriffsberechtigungen erstellen. Die Festlegung der individuellen Zugriffsberechtigungen wird formal durch ein digital signiertes *Consent Document* (PDF, kein IHE BPPC) im PAP hinterlegt, welches durch den Bürger jederzeit einsehbar und ausdruckbar ist. Dieses signierte Dokument enthält auch Verweise (Signierter Hashwert) auf die technische Repräsentation der XACML-Policies.

18.5.2. Ergebnisse bei Erfolg

Eine XACML-Policy wurde definiert oder verändert. Entsprechende Festlegungen pro futuro zu einer definierten oder geänderten Policy (Consent Document) werden historisiert gespeichert. Zur Sicherstellung einer lückenlosen Nachvollziehbarkeit werden alle Aktionen betreffend der Policies protokolliert.

18.5.3. Vorbedingungen und Voraussetzungen

- BP01a: *ELGA User I Assertion* wurde erfolgreich durchgeführt oder Bürger hat sich gegenüber einer Widerspruchs- oder Ombudsstelle identifiziert und diese schriftlich beauftragt in seinem Namen individuelle Zugriffsberechtigungen zu erstellen bzw. zu ändern.
- Um medizinische Dokumente auszublenden wurde BP08c: Dokumentenabruf durch ELGA-Teilnehmer erfolgreich durchgeführt.

18.5.4. Auslöser/Trigger

Der Bürger will individuelle Zugriffsrechte in ELGA definieren oder ändern.

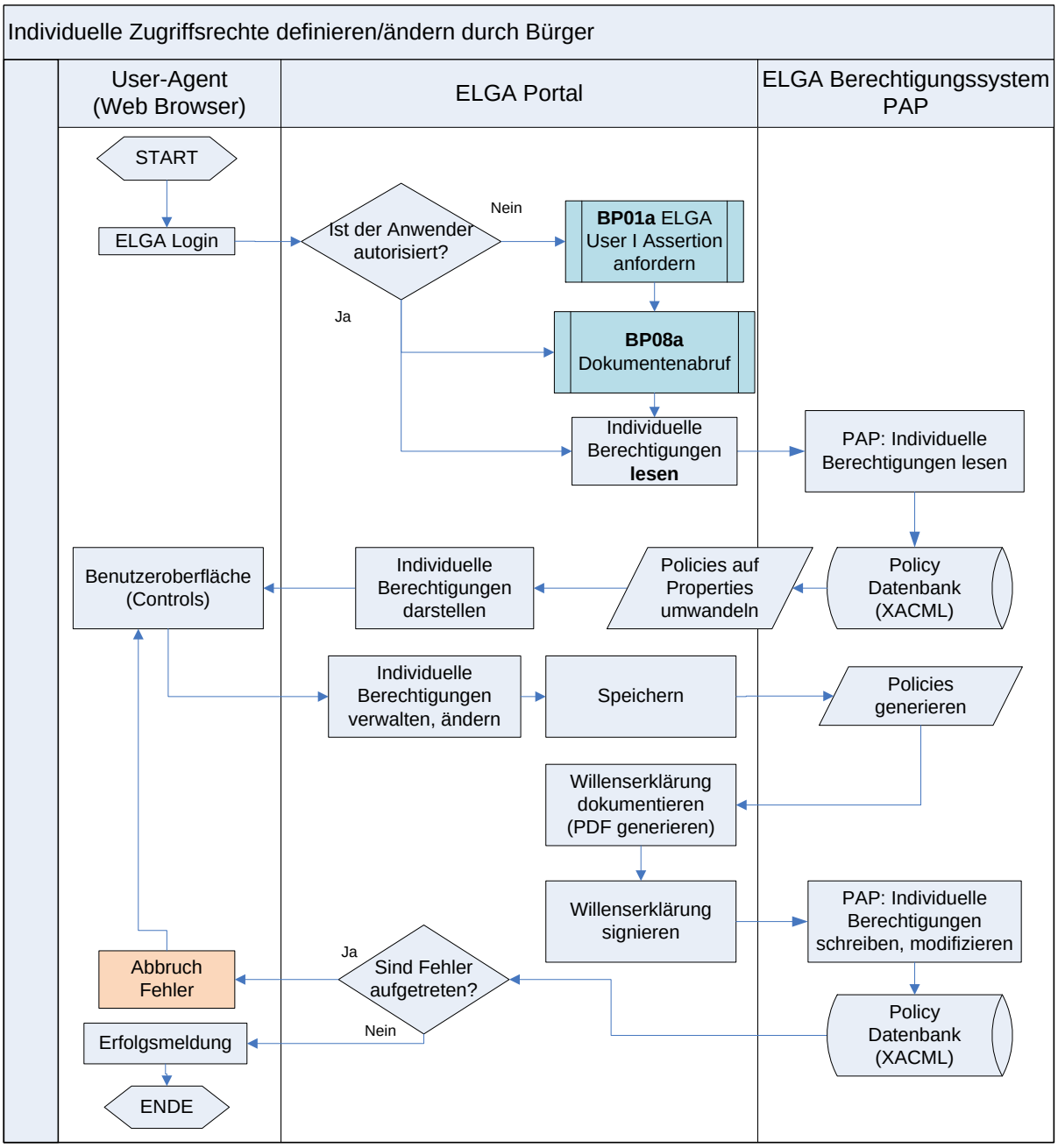
18.5.5. Szenario

1. Der ELGA-Teilnehmer öffnet am ELGA-Portal jene Seite (Page, Tab oder View), auf der Zugriffsrechte verändert werden können.
2. Der Bürger wartet seine individuellen Zugriffsrechte. Er vergibt oder entzieht Zugriffsrechte auf einzelne Dokumente, bestimmt ein generelles Opt-Out/Opt-Out Widerruf, legt die zulässige Zugriffsdauer für GDA fest.
3. Die Festlegung des Bürgers zu einer oder mehreren individuellen Policies (Satz von Policies) wird dokumentiert. Das dadurch entstandene Consent Document wird digital signiert und zentral im PAP gespeichert. Das so signierte Dokument enthält die definierten Regel und Berechtigungen (bzw. Richtlinien) in verbaler Textform, deutlich und eindeutig

artikuliert bzw. ausgedrückt. Die damit verbundenen exakten XACML-Policies müssen serverseitig (zentral vom Berechtigungssystem) generiert werden und die eindeutigen Verweise auf diese Policies (etwa in Form von Hash-Werten) in das Dokument eingebettet werden.

4. Das ELGA-Portal übermittelt die auf der Benutzeroberfläche betätigten Eingaben des ELGA-Teilnehmers an den Policy Administration Point (PAP) in dem das entsprechende Web Service des PAP kontaktiert wird. Der PAP generiert in der Folge eine oder mehrere XACML Policies bzw. XACML-Regeln und prüft auf Plausibilität. Das kontaktierte PAP Web Service sendet die XACML-Policies dem ELGA-Portal zurück. Das ELGA-Portal erzeugt einen eindeutigen Verweis (Hash-Wert) auf die erhaltenen Policies und generiert das entsprechende Zustimmungs-Dokument (PDF) in das der Verweis eingebettet wird. Dies ist im Pflichtenheft detailliert auszuarbeiten. Das signierte Dokument wird anschließend dem PAP gesendet und dort mit den dazugehörigen XACML-Policies gespeichert. Anhand des erwähnten Hash-Wertes ist es jederzeit möglich die Verbindung zwischen technischer Repräsentation und PDF-Dokument herzustellen und zu überprüfen.
5. Alle Zugriffe auf das Web Service des PAP sind ausnahmslos *via ELGA User I Assertion autorisiert*.

Der zeitliche Ablauf wird durch Abbildung 75 deutlich.



7209

7210 *Abbildung 75: Darstellung des Anwendungsfalls BP06 (ET.1.3)*

7211 **18.5.6. Alternativszenario**

7212 Hat der Bürger keine Möglichkeit Zugriffsberechtigungen zu definieren oder zu ändern (z.B.
7213 kein Internetzugang), kann er sich persönlich an eine Ombudsstelle oder Widerspruchstelle
7214 wenden, die nach Bestätigung seiner Identität die entsprechenden Änderungen durchführen
7215 kann.

18.5.7. Ergebnisse bei Fehler

Bei Ungültigkeit oder verletzter Plausibilität wird dem ELGA-Portal ein entsprechender Fehler retourniert. Die Benutzeroberfläche ist für deren anwenderfreundliche Aufbereitung zuständig. Hierfür ist in das entsprechende Pflichtenheft vdes ELGA-Portals (in Bearbeitung) Einsicht zu nehmen.

18.6. BP07: Generelle Zugriffsrechte definieren/warten

18.6.1. Allgemeines

Im Kontext des Berechtigungssystems werden generelle Zugriffsberechtigungen betreffend GDA in Abhängigkeit ihrer Rolle auf entsprechende Dokumentenklassen definiert. Die für ELGA relevanten Dokumentenklassen werden im Rahmen fortschreitender Normierungsprojekte anhand von Implementierungsleitfäden spezifiziert. Zugriffsrechte werden in Form von XACML Policies auf dem zentralen Policy Administration Point (PAP) hinterlegt. Diese Policies bilden die generellen Berechtigungen ab. Die Policies müssen im Vorfeld mit der aktuellen Version der Berechtigungssystemsoftware entsprechend getestet werden (ist hier nicht abgebildet). Erst danach kann dieser Schritt erfolgen.

18.6.2. Ergebnisse bei Erfolg

Eine oder mehrere XACML Policies (oder XACML-Rules bzw. PolicySets) wurden definiert oder verändert. Diese Syntax ist detailliert im Pflichtenheft auszuarbeiten.

18.6.3. Vorbedingungen und Voraussetzungen

- Policies wurden im Vorfeld getestet und administrativ (etwa durch Gesetz oder Erlass/Verordnung) sind diese freigegeben worden
- Ein ELGA Regelwerkadministrator hat sich am Administrationsinterface des Policy Administration Point angemeldet.
- ELGA Service-Assertion anfordern wurde erfolgreich durchgeführt.

18.6.4. Auslöser/Trigger

Ein ELGA Regelwerkadministrator möchte generelle Policies definieren oder ändern.

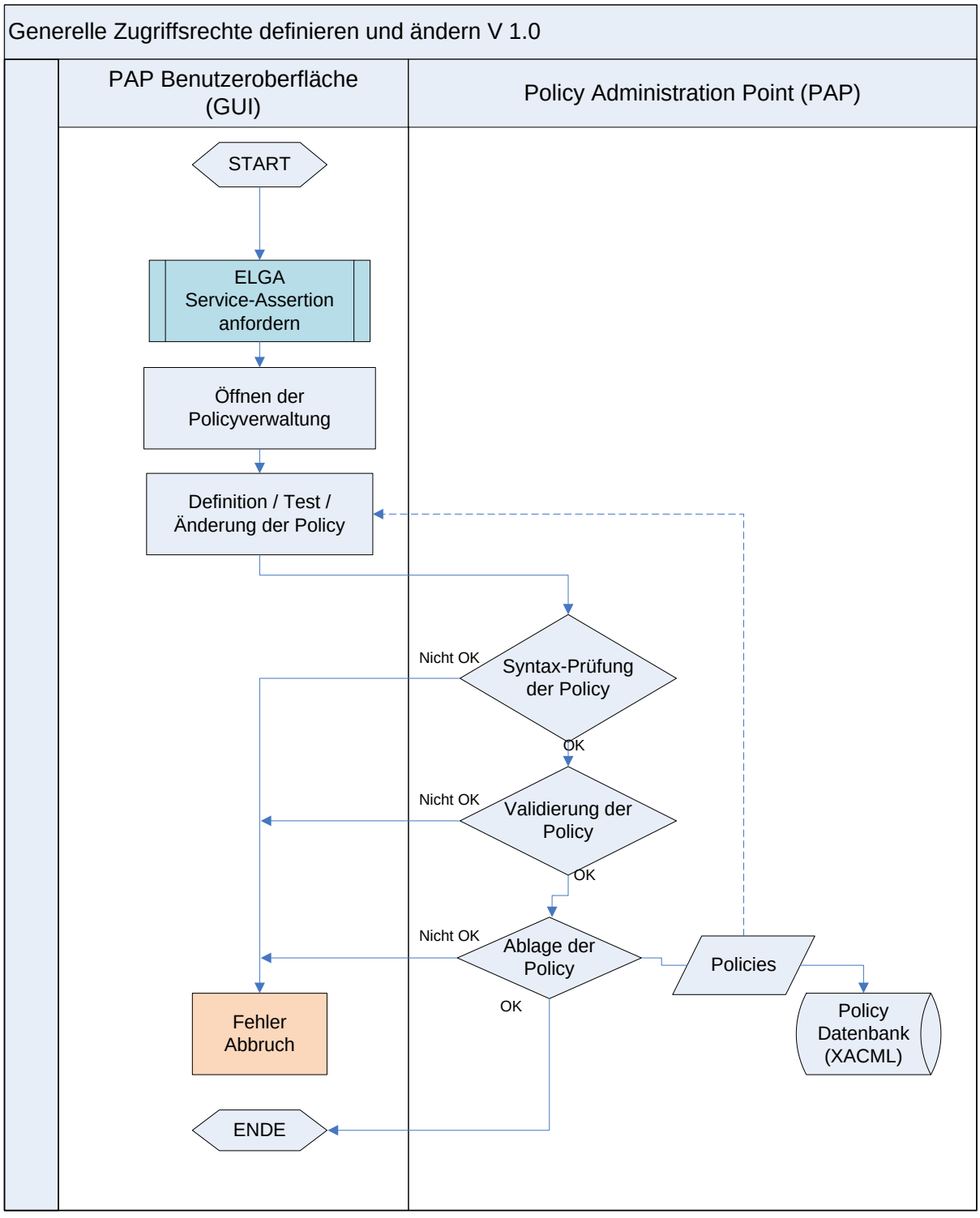
18.6.5. Szenario

1. Ein ELGA-Service-Mitarbeiter ausgestattet mit einer ELGA-Regelwerkadministrator Berechtigung meldet sich in ELGA an. Eine ELGA Service-Assertion in entsprechender

Form autorisiert den Benutzer, generelle Berechtigungsregeln zu pflegen (Berechtigungen zu definieren, ändern oder warten).

2. Der ELGA-Regelwerkadministrator öffnet auf Administrationsoberfläche des Policy Administration Point (PAP) jenen Bereich, in dem Policies definiert oder verändert werden können.
3. Der ELGA-Regelwerkadministrator definiert oder ändert die Regeln bzw. die entsprechende Richtlinien. Die Tätigkeit des Administrators wird mitprotokolliert. Wichtig ist zu beachten, dass die Rolle ELGA-Regelwerkadministrator keinen Zugriff auf die aufgezeichneten Protokolle hat.
4. Die XACML-Policy wird am Policy Administration Point auf Gültigkeit und Plausibilität geprüft, eingestellt und abgelegt.
5. Ein Vieraugenprinzip ist hier zumindest organisatorisch zu implementieren. PAP-Zugangspasswort könnte beispielsweise zweigetrennt werden.

Abbildung 76 veranschaulicht den genaueren Ablauf.



7265

7266

7267 *Abbildung 76: Darstellung des Anwendungsfalls BP07 (entspricht RADM.6.2)*

18.6.6. Ergebnisse bei Fehler

Bei Ungültigkeit oder Verletzung der Plausibilität wird ein entsprechender Fehler an den ELGA Regelwerkadministrator zurückgemeldet.

18.7. BP08: Zugriffsautorisierung umsetzen

18.7.1. Allgemeines

Es ist unbedingt sicherzustellen, dass GDA nur jene Dokumente einbringen, suchen und abrufen können, für die sie aufgrund ihrer Rolle autorisiert sind. Zusätzlich können durch den Willen des ELGA-Teilnehmers individuelle Zugriffsberechtigungen für seine Dokumente festgelegt werden. Die Prüfung der Zugriffsberechtigung erfolgt, indem verglichen wird, was jemand machen „darf“ (Sollwert), mit dem, was jemand tun möchte (Istwert). In den Anwendungsfällen „BP06: Individuelle Zugriffsberechtigungen definieren und ändern“ und „BP07: Generelle Zugriffsberechtigungen definieren und ändern“ wurde die Festlegung entsprechender individueller und genereller Zugriffsberechtigungen durch den ELGA-Teilnehmer bzw. den ELGA-Regelwerkadministrator beschrieben. Die Zugriffsberechtigungen werden technisch als XACML-Policies durch den zentralen PAP bereitgestellt und repräsentieren, entsprechend kombiniert, in der Zugriffsberechtigungsprüfung den Sollwert. Die beabsichtigte ELGA-Transaktion eines ELGA-Benutzers samt Identitäts- und Rollenbestätigung stellen den Istwert dar. Die Entscheidung darüber, ob und in welcher Art und Weise ein zulässiger Zugriff stattfinden darf, wird am jeweiligen *Policy Decision Point* (PDP) als Teil der Zugriffssteuerungsfassade dezentral getroffen. Der Vollzug dieser Entscheidung, also das Durchlassen, Filtern oder Verweigern einer ELGA Transaktion wird durch den sogenannten *Policy Enforcement Point* (PEP), ebenfalls Teil der ZGF, umgesetzt.

18.7.2. Ergebnisse bei Erfolg

Eine ELGA Transaktion, initiiert durch einen ELGA-Teilnehmer bzw. GDA, wird durchgelassen, gefiltert oder verweigert. Über gefilterte Informationen wird keine Rückmeldung an den GDA erstattet.

18.7.3. Vorbedingungen und Voraussetzungen

Im Fall Zugriff durch ELGA-Teilnehmer:

- BP01a: *ELGA User-Assertion I* und BP01d: *ELGA User-Assertion II* wurden erfolgreich durchgeführt.
- Eine ELGA Transaktion wurde initiiert.

Im Fall Zugriff durch GDA:

- BP01b: *ELGA HCP-Assertion* anfordern wurde erfolgreich durchgeführt.
- Eine ELGA Transaktion, welche die Vorgaben in Kapitel 3.18 erfüllt, wurde initiiert
- BP05: *ELGA Treatment-Assertion* ausstellen wurde erfolgreich durchgeführt.

Im Fall Zugriff durch Bevollmächtigten:

- BP01c: *ELGA Mandate-Assertion I* ausstellen wurde erfolgreich durchgeführt.
- Eine ELGA Transaktion, welche die Vorgaben in Kapitel 3.18 erfüllt, wurde initiiert.
- BP01e: *ELGA Mandate-Assertion II* ausstellen wurden erfolgreich durchgeführt.

Im Fall Zugriff durch ELGA-Regelwerk- bzw. Sicherheitsadministrator

- *ELGA Service-Assertion* ausstellen wurde erfolgreich durchgeführt.
- Eine (nicht IHE) Transaktion wurde initiiert.

Im folgenden Szenario wird die Autorisierung von Zugriffen unabhängig vom konkreten ELGA-Benutzer erläutert. Es wird daher der Oberbegriff *ELGA Authorisation-Assertion* für die ELGA-Benutzer spezifische User-, Treatment-, Mandate- bzw. Service-Assertion verwendet.

18.7.4. Auslöser/Trigger

Die ZGF eines ELGA-Bereichs empfängt eine Anfrage entweder aus einer entfernten Domäne (ELGA-Bereich) oder aus dem eigenen Bereich.

18.7.5. Szenario

1. Eine ELGA Transaktion wird bereichsintern bzw. bereichsübergreifend durch den ELGA-Benutzer initiiert und an die bereichseigene ZGF übermittelt.
2. Der PRP als Teil der, dem eigenen ELGA Initiating Gateway vorgeschalteter, Zugriffssteuerungsfassade (Intermediary) empfängt die Transaktion und agiert im Weiteren im Namen des Anwenders. Der PRP übernimmt die im Request vorhandenen HCP-/Patient- bzw. User-/Mandate-Assertion I und veranlasst über das ETS entweder *ELGA Treatment-Assertions* oder *ELGA User-/Mandate-Assertion II* zu generieren. Als Nächstes wird die Transaktion bereichsintern bzw. bereichsübergreifend (XCA) weiterverarbeitet.
3. Der PEP als Teil der, dem entfernten ELGA Responding Gateway vorgeschalteter, Zugriffssteuerungsfassade (Intermediary) nimmt die Transaktion entgegen und prüft auf Vorhandensein einer *ELGA Authorisation-Assertion*. Die ELGA Authorisation-Assertion bildet identitäts- und rollenbezogene Informationen des zugreifenden ELGA-Benutzers sowie kontextabhängige generelle bzw. individuelle Zugriffsberechtigungen in einer strukturierten Art und Weise ab. Optional finden sich auch generelle

Zugriffsentscheidungen, welche bereits im Rahmen der Authentifizierung festgelegt werden konnten, wieder.

4. Der PEP setzt ggf. bereits festgelegte generelle Zugriffsentscheidungen um
5. PEP extrahiert aus der Transaktion sowie der ihr beigefügten *ELGA Authorisation-Assertion* für das Zugangskontrollsystem relevante Teile (z.B. Identität des anfordernden GDAs, dessen Rolle, Identität des Patienten, Art des Zugriffs, Dokumentenklasse). Der PEP delegiert die Entscheidung an den Policy Decision Point (PDP) weiter.
6. Der PDP verarbeitet die empfangenen Informationen (Claims, Attribute, Richtlinien, Berechtigungen, Regeln, etc.) und entscheidet generell über den Zugriff. Das Ergebnis der Zugriffsautorisierung wird dem PEP übermittelt.
7. Der PEP setzt diese Entscheidung um und leitet diese bei generell zulässiger Anfrage an ein ELGA Verweisregister bzw. Repository weiter. Bei fehlender Berechtigung erfolgt eine entsprechende Fault-Meldung an den aufrufenden ELGA-Benutzer. Hierfür ist, wie bereits angemerkt, eine *Access Violation* (SOAP-Fault) vorgesehen.
8. Das ELGA-Verweisregister bzw. Repository empfängt und verarbeitet die Transaktion. Die resultierende Antwort wird an die bereichseigene Zugriffssteuerungsfassade übertragen.
9. Der PEP als Teil der Zugriffssteuerungsfassade nimmt die Antwort entgegen, extrahiert daraus für das Zugangskontrollsystem relevante Teile (z.B. Dokumenten ID) und leitet diese gemeinsam mit den Autorisierungsattributen, zwecks einer Entscheidungsfindung an den PDP weiter.
10. Der PDP trifft basierend auf den durch den PEP übermittelten Autorisierungsinformationen und Zugriffsberechtigungen die Zugriffsentscheidung und teilt diese dem PEP mit.
11. Der PEP setzt die Zugriffsentscheidung um, indem die Antwort entsprechend geblockt bzw. ungefiltert oder gefiltert an die Zugriffssteuerungsfassade des anfragenden ELGA-Bereichs weitergeleitet wird.
12. Die Zugriffssteuerungsfassade des anfragenden ELGA-Bereichs empfängt die Antwort und leitet diese an den anfragenden ELGA-Benutzer weiter.
13. Der anfragende ELGA-Benutzer empfängt die zulässige Antwort auf die von ihm initiierte ELGA Transaktion.

Es wird davon ausgegangen, dass ein konkreter Dokumentenabruf immer eine zeitnahe Dokumentensuche bedingt. Daher beschreiben die nächsten Flussdiagramme sowohl Dokumentensuche als auch -abruf aus der Perspektive eines ELGA-Teilnehmers bzw. durch

diesen Bevollmächtigte und eines GDAs. Dokumentensuche und –Abruf beschränkt sich hierbei auf XDS Objekte SubmissionSet sowie DocumentEntry. XDS Folder werden nicht unterstützt und bei Verwendung eine Fehlermeldung „XDSRegistryMetadataError“ bei [ITI-18, ITI-42] bzw. „XDSRepositoryMetadataError“ bei [ITI-41] an den Aufrufer retourniert. Der Ablauf der Zugriffsautorisierung bleibt unabhängig von der Aktion ident.

18.7.5.1. Anwendungsfall BP08a: Dokumentensuche durch ELGA-Teilnehmer

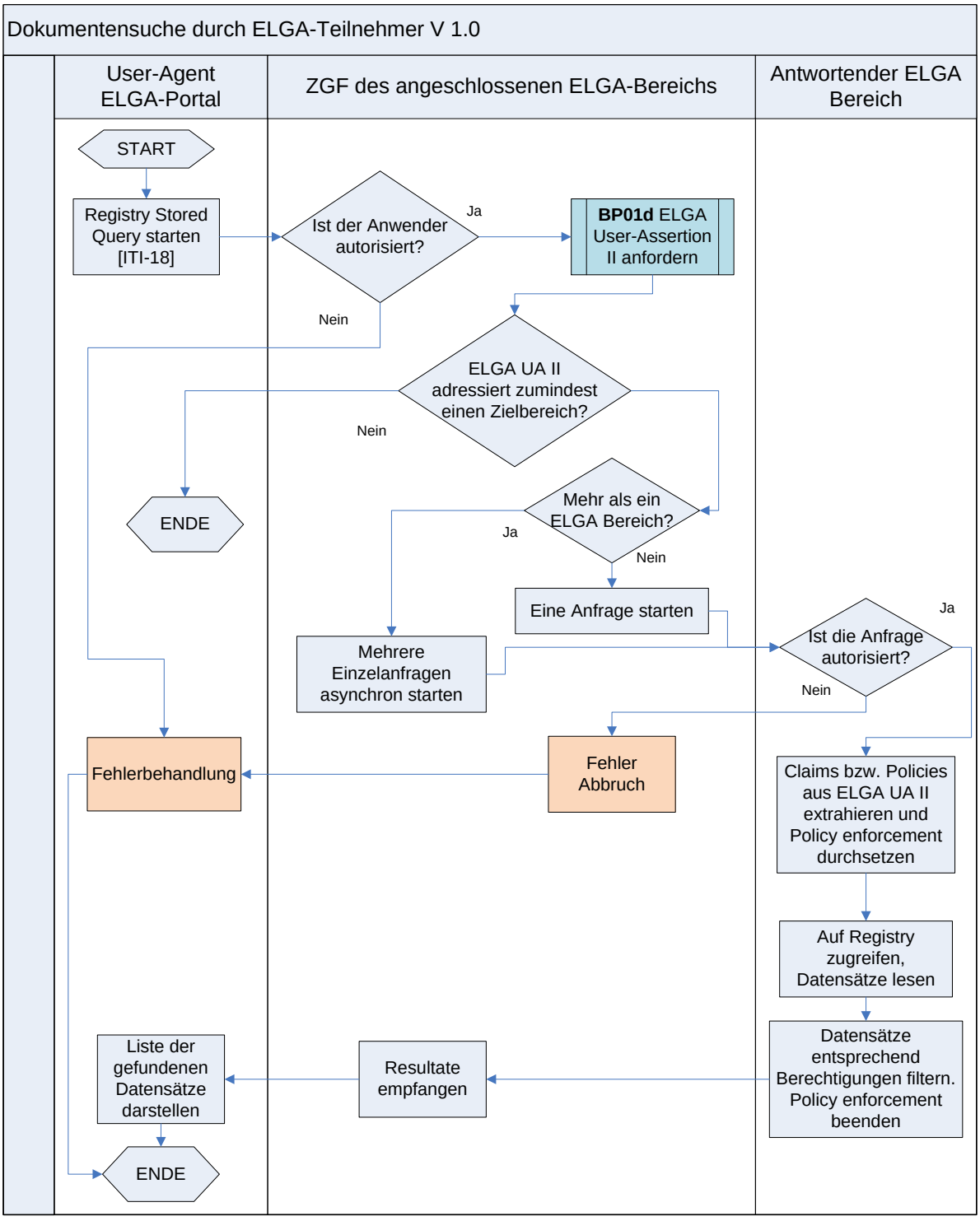
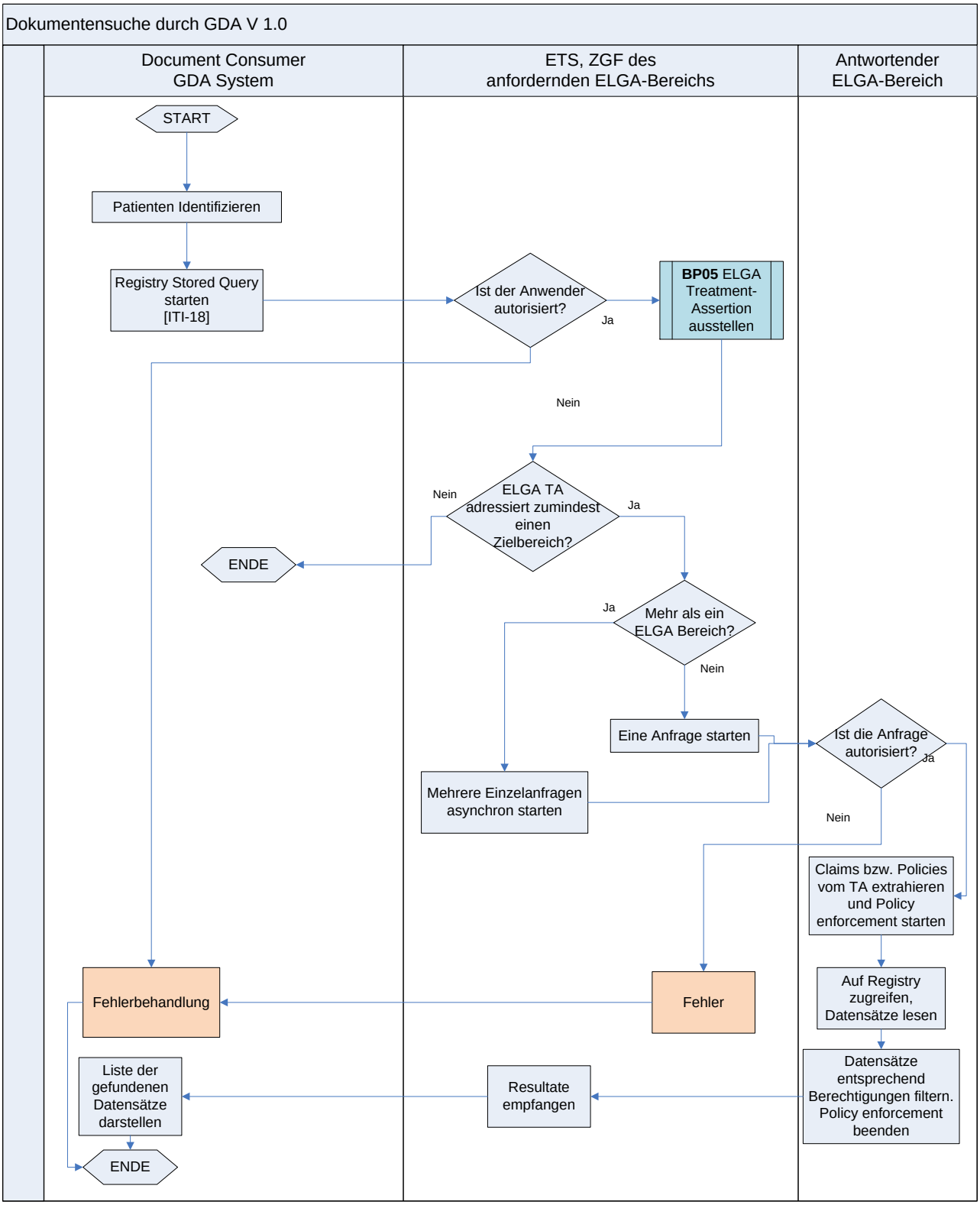


Abbildung 77: Darstellung des Anwendungsfalls BP08a mit der Annahme, dass ein Login bereits stattgefunden hat. Entspricht ET.1.8

7378

18.7.5.2. Anwendungsfall BP08b: Dokumentensuche durch GDA



7382 *Abbildung 78: Darstellung des Anwendungsfalls BP08b mit der Annahme, dass ein Login*
7383 *bereits stattgefunden hat. Entspricht GDA.3.9*

18.7.5.3. Anwendungsfall BP08c: Dokumentenabruf durch ELGA-Teilnehmer

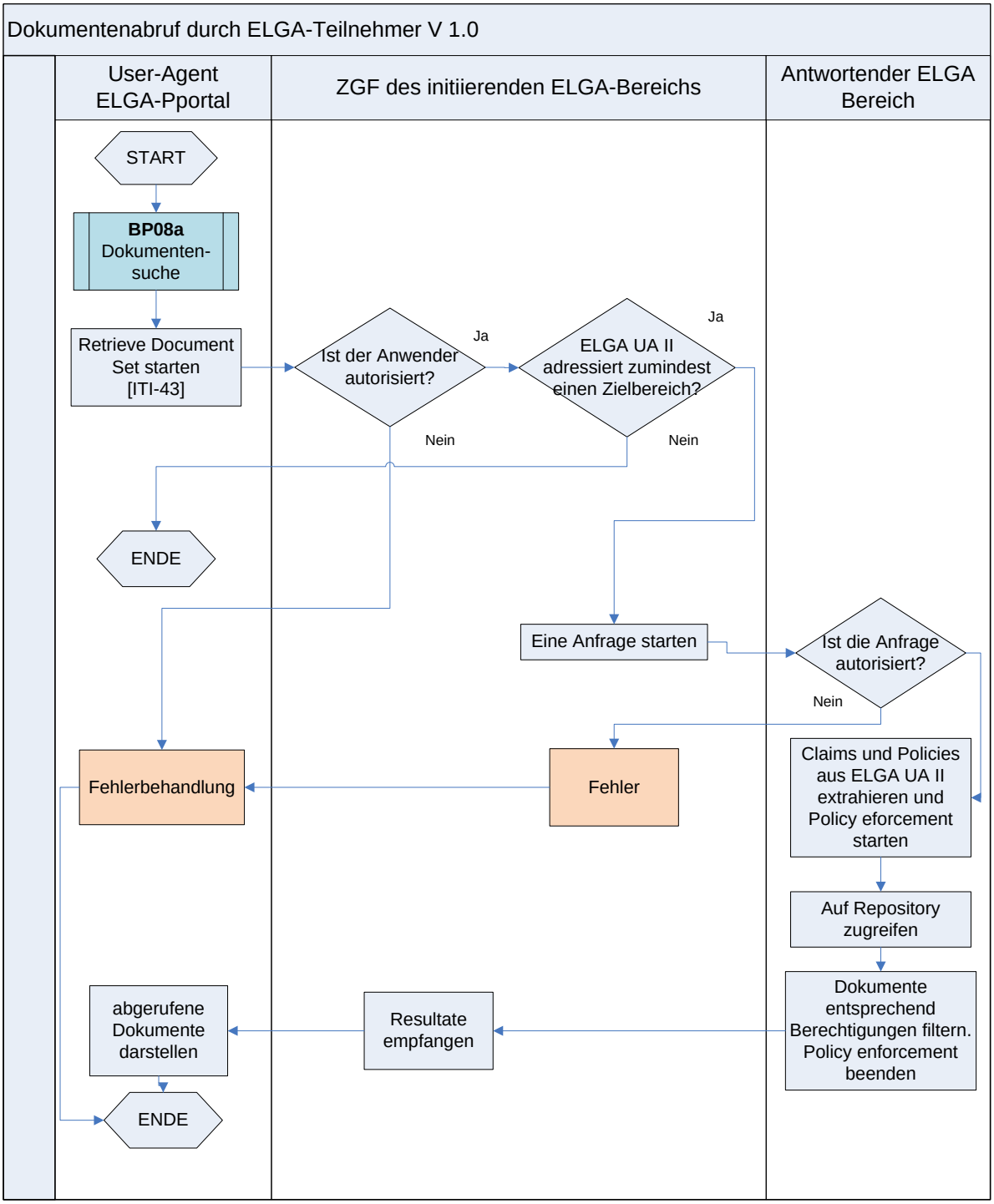


Abbildung 79: Darstellung des Anwendungsfalls BP08c mit der Annahme dass ein Login bereits stattgefunden hat. Entspricht ET.1.9

18.7.5.4. Anwendungsfall BP08d: Dokumentenabruf durch GDA

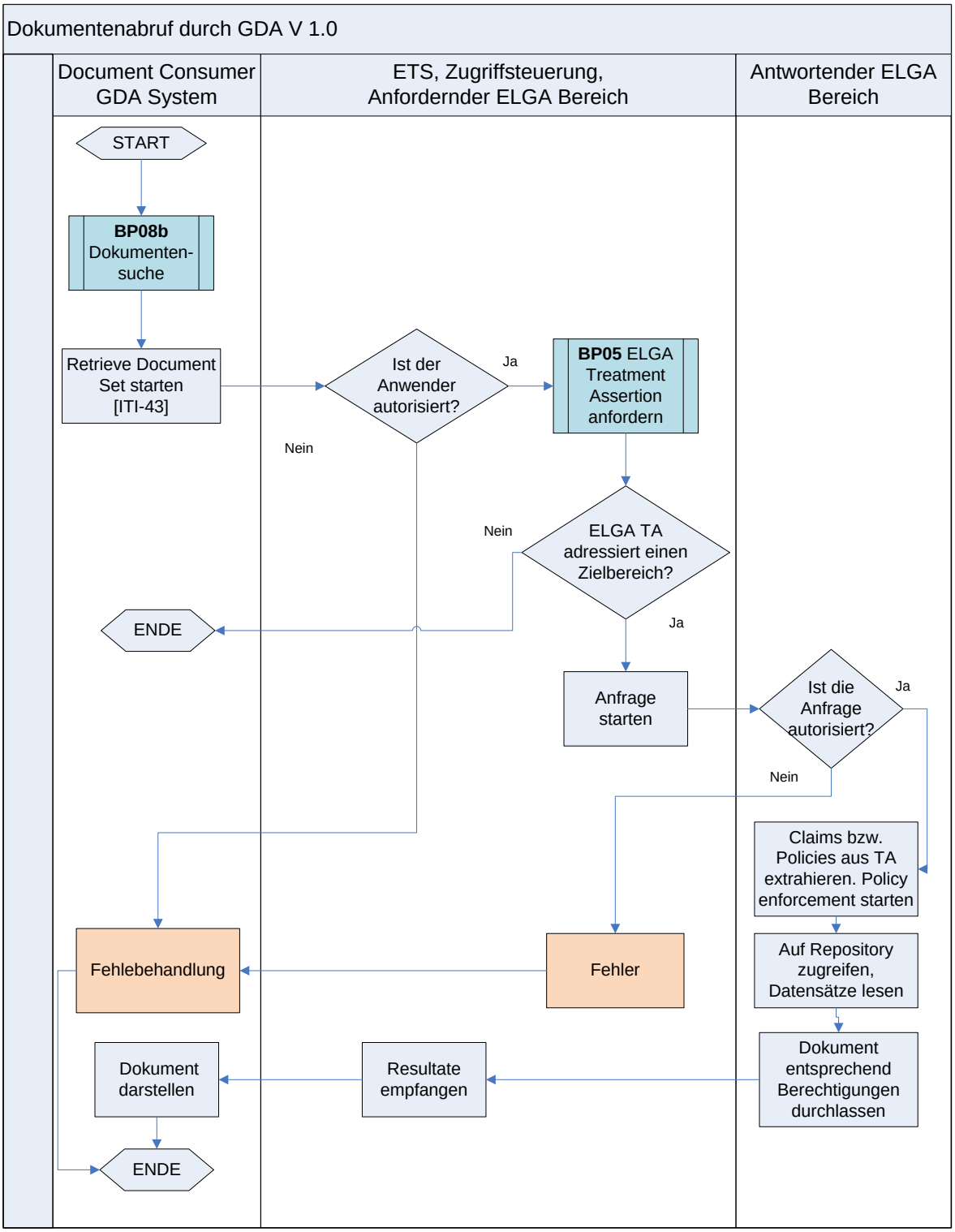


Abbildung 80: Darstellung des Anwendungsfalls BP08d mit der Annahme, dass ein Login bereits stattgefunden hat. Entspricht GDA.3.10

18.7.6. Ergebnisse bei Fehler

- Auftretende Fehler müssen zum Abbruch der Transaktion führen. Hierfür sind SOAP-Faults sowie Fehlercodes zu erwarten und zu bestimmen (Pflichtenheft).
- Bestimmte Fehlermuster, die auf einen Angriff des Systems hindeuten (DOS Attacke, Brute Force Attacke, etc.), müssen zur Sperre des Zugriffs und in wiederholtem Fall zur Sperre der ELGA Komponente führen. Das Problem ist an den zuständigen Administrator zu eskalieren.
- Die Definition von Systemangriffen sowie die Beschreibung entsprechender Gegenmaßnahmen erfolgt im Rahmen des ELGA ISMS.

18.8. BP09: GDA Zugriffe protokollieren

18.8.1. Allgemeines

Sinn der Protokollierung ist die lückenlose Nachvollziehbarkeit aller Aktionen innerhalb ELGA. Dies umfasst insbesondere Operationen im ELGA-Kernbereich (ELGA-Core) und zwar verändernde Zugriffe auf Willenserklärungen der ELGA-Teilnehmer, GDA-Zugriffe auf Dokumente/Befunde, Bilder und Verweise auf diese Informationsobjekte. BP09 bezieht sich ausschließlich auf Protokollierung der GDA-Zugriffe (siehe GDA.3.21).

Jeder ELGA-Bereich führt ein lokales *Audit Record Repository (L-ARR).* Die ZGF hat die Aufgabe alle stattgefundenen (XDS/XCA-) Transaktionen in den von den ELGA-Bereichen zur Verfügung gestellten L-ARR zu protokollieren. Darüber hinaus wird auch in A-ARR kontinuierlich protokolliert. Protokollnachrichten können von dafür zuständigen und einberufenen Sicherheits-Administratoren bei Bedarf eingesehen werden. A-ARR Einträge müssen für ELGA-Teilnehmer am Portal in einer verständlichen Art und Weise aufbereitet werden.

18.8.2. Ergebnisse bei Erfolg

Die Protokollierung einer mit exakter Transaktionsnummer identifizierbaren ELGA Transaktion ist erfolgt. Datum und Zeitstempel basierend auf NTP garantieren die zeitliche Kausalität der Aktionen nachvollzuziehen (GDA.3.21).

18.8.3. Vorbedingungen und Voraussetzungen

- Anwendungsfall BP01: ELGA-Benutzer authentifizieren wurde erfolgreich durchgeführt.
- ELGA Transaktion findet statt.

- Kommunizierende ELGA Komponenten sind mittels Server-Zertifikaten gegenseitig authentifiziert (siehe ATNA Secure Nodes).

18.8.4. Akteure

Das Berechtigungssystem, ETS, ZGF, L-ARR, A-ARR

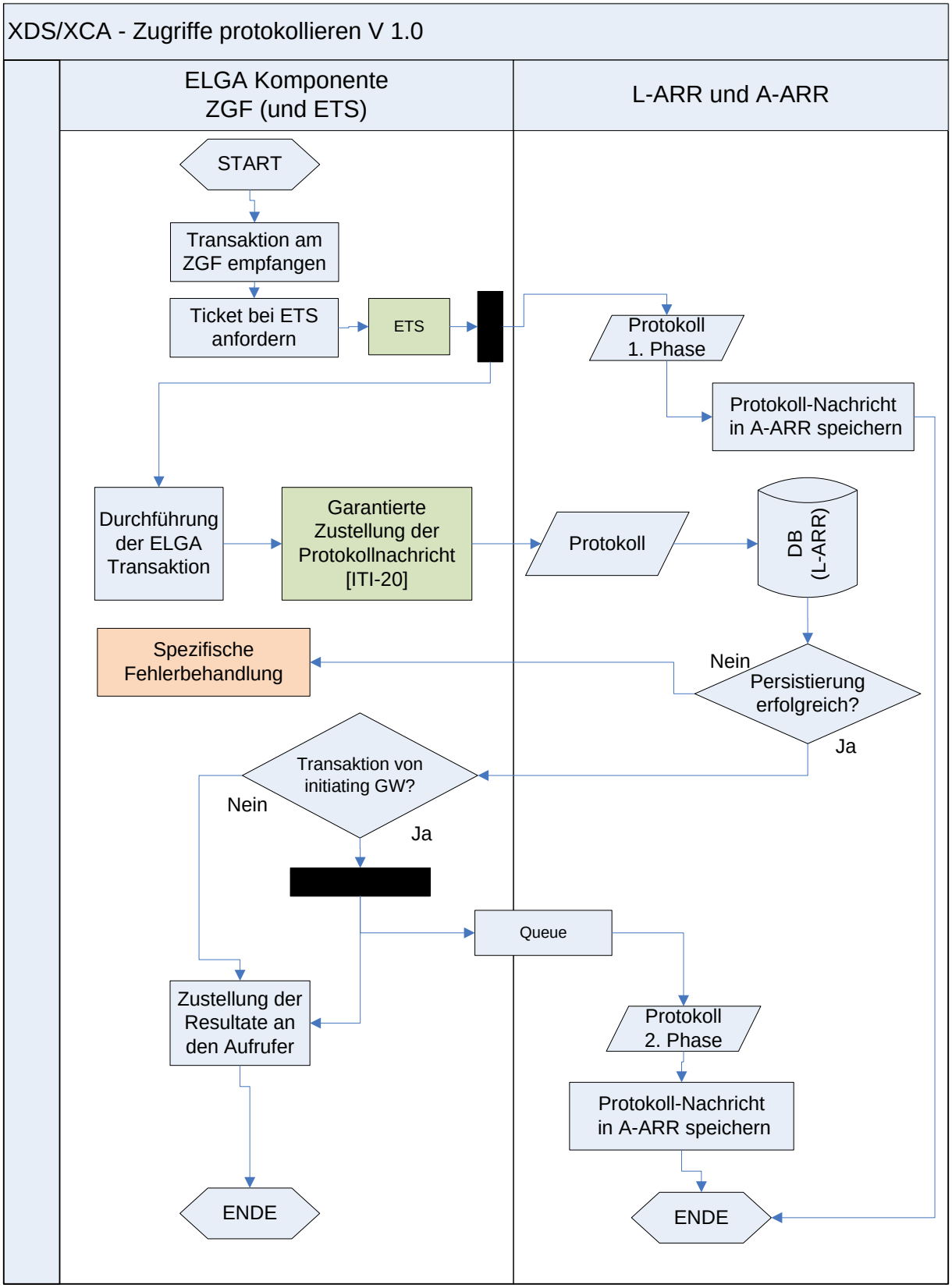
18.8.5. Auslöser/Trigger

Eine oder mehrere initiierte ELGA Transaktionen, die von der Zugriffsteuerungsfassade überwacht und empfangen werden.

18.8.6. Szenario

1. Ein ELGA-Benutzer initiiert eine Transaktion.
2. Der AGW/ZGF empfängt die initiierte Transaktion und fordert von ETS eine Assertion dafür an.
3. Das ETS entscheidet über die Durchführung der Transaktion und sendet bei Zustimmung entsprechende Protokollnachricht an das A-ARR.

   Anmerkung: Im zentralen A-ARR wird auch alles mitprotokolliert, wird aber im Workflow nicht dargestellt
4. ZGF sendet eine entsprechende Protokollnachricht ([ITI-20]) an das angeschlossene L-ARR des jeweiligen ELGA-Bereichs, dem diese ELGA Komponente zugehörig ist (siehe Abbildung 81).
5. Die gesendeten Nachrichten (nach L-ARR) müssen garantiert zugestellt werden. Das BeS-Pflichtenheft [18] muss hierfür Details anführen.
6. Das L-ARR empfängt und bestätigt den erfolgreichen und vollständigen Empfang der Protokollnachricht.
7. Die Zugriffssteuerungsfassade übermittelt eine abschließende Protokollnachricht an das *Aggregierte Audit Record Repository* (A-ARR) soweit diese Transaktion von einem GDA *Document Consumer* oder GDA *Document Source* Akteur ausgelöst wurde. Details der Übermittlung des Resultates der Transaktion sind im Pflichtenheft ausführlich zu definieren.



7453
7454

7455 *Abbildung 81: Darstellung des Anwendungsfalls BP09 (entspricht GDA.3.21)*

18.8.7. Ergebnisse bei Fehler

Protokollnachrichten dürfen nicht verloren gehen. Wenn Protokollnachrichten nicht an das L-ARR geschickt werden können oder L-ARR nicht in der Lage ist, diese zu empfangen (Fehlermeldung), so muss der betroffene ELGA-Bereich bis zur Wiederherstellung der Funktionstüchtigkeit von L-ARR deaktiviert werden und die nicht protokollierte verändernde Transaktion rückgängig gemacht werden. Bei nichterfolgter Zustellung seitens A-ARR werden die Nachrichten in der dafür vorgesehene Queue zwischengepuffert. Läuft die Queue voll, die ZGF muss den ELGA-Bereich abschalten.

18.9. BP10: Zugriffsprotokolle einsehen

18.9.1. Allgemeines

Der ELGA-Teilnehmer hat das Recht, in die lückenlose Protokollierung aller erfolgten Zugriffe auf seine medizinischen Dokumente in ELGA Einsicht zu nehmen. Dies erfolgt über das ELGA-Portal. Dabei kann er nachvollziehen, wer wann auf welche Daten zugegriffen hat. Die zusammenfassende Darstellung liefert im Wesentlichen eine Übersicht der erfolgten Zugriffe hinsichtlich folgender Aspekte:

- Zeitpunkt und Art des Zugriffs
- Vor-/Nachname der zugreifenden Person sowie Bezeichnung und Rolle des GDAs
- Informationsobjekt (CDA Dokument), auf das zugegriffen wurde

Protokolle sind innerhalb ELGA gemäß der gesetzlich definierten Aufbewahrungspflicht 3 Jahre lesbar und verfügbar zu halten. Außerdem ist auf Anfrage des Bürgers Einsichtnahme zu gestatten.

Aus betriebstechnischen Gründen wird es für ELGA-Sicherheitsadministratoren (siehe SADM.7.2 und SADM.7.3) notwendig sein, das Protokoll einzusehen. Entsprechende Möglichkeiten sind in den lokalen Administrationsmasken der L-ARR vorzusehen.

18.9.2. Ergebnisse bei Erfolg

Protokolle durch ELGA-Teilnehmer, bevollmächtigten Vertreter, Ombudsstelle eingesehen (ET.1.6, BET.2.6, OBST.5.6).

18.9.3. Vorbedingungen und Voraussetzungen

Für den Fall Einsicht durch ELGA-Teilnehmer:

- BP01a: *ELGA User-Assertion I* ausstellen wurde erfolgreich durchgeführt.

Für den Fall Einsicht durch Ombudsstelle:

- ELGA-Teilnehmer hat sich gegenüber der Ombudsstelle identifiziert und diese beauftragt, in seinem Namen Zugriffsprotokolle einzusehen.
- BP01c: *ELGA Mandate-Assertion I* ausstellen wurde erfolgreich durchgeführt.

Für den Fall Einsicht durch ELGA-Sicherheitsadministrator:

- Der zuständige Administrator wurde explizit autorisiert.
  - Zugang wurde genehmigt.
- Vieraugenprinzip könnte organisatorisch als zusätzliche Sicherheitsmaßnahme implementiert werden (soweit ELGA-SIKO dies befürwortet).

18.9.4. Auslöser/Trigger

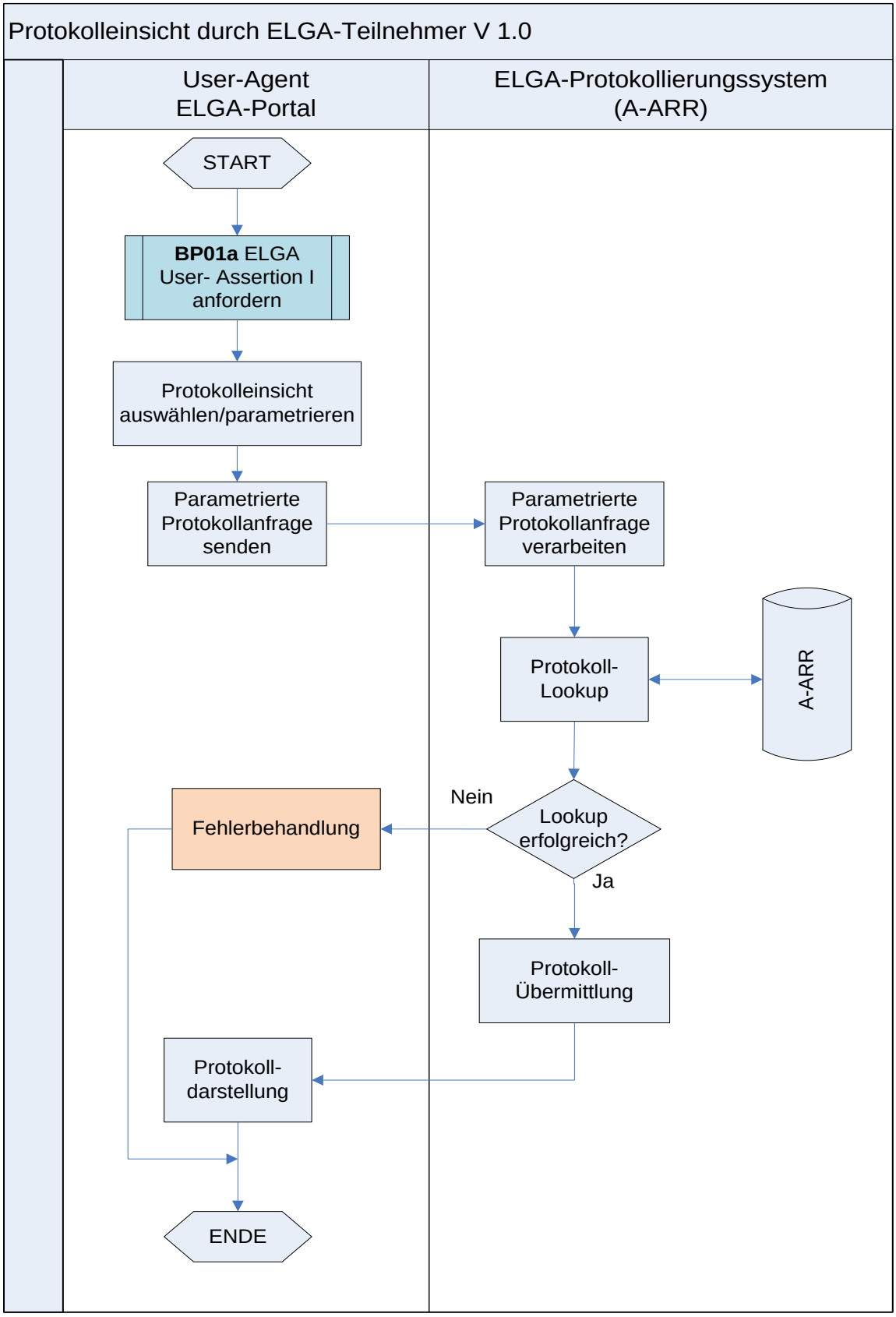
Aufruf des Bereichs zur Einsichtnahme in die ELGA-Protokollierung am ELGA-Portal bzw. für zuständige Administratoren über die entsprechende Benutzeroberfläche.

18.9.5. Szenario

Im Folgenden wird das Szenario der Protokolleinsicht aus der Perspektive des Bürgers und/oder der Ombudsstelle angemeldet in Vertretung eines ELGA-Teilnehmers dargestellt. Anwendungsfall BP10a: Protokolleinsicht durch ELGA-Teilnehmer (ET.1.6)

1. Bürger öffnet am ELGA-Portal den visuellen Bereich zur Einsichtnahme in die Protokollierung.
2. Bürger parametriert die Protokolleinsicht z.B. zeitlich (von bis Einschränkung).
3. Parametrierte Protokollanfrage wird durch das ELGA-Protokollierungssystem anhand des Protokollspeichers (A-ARR) verarbeitet. Die Ergebnisse der Anfrage werden dem Aufrufer übermittelt.
4. Resultate der Protokollanfrage werden am ELGA-Portal für den Bürger aufbereitet und dargestellt.

Abbildung 82 verdeutlicht den zeitlichen Ablauf.



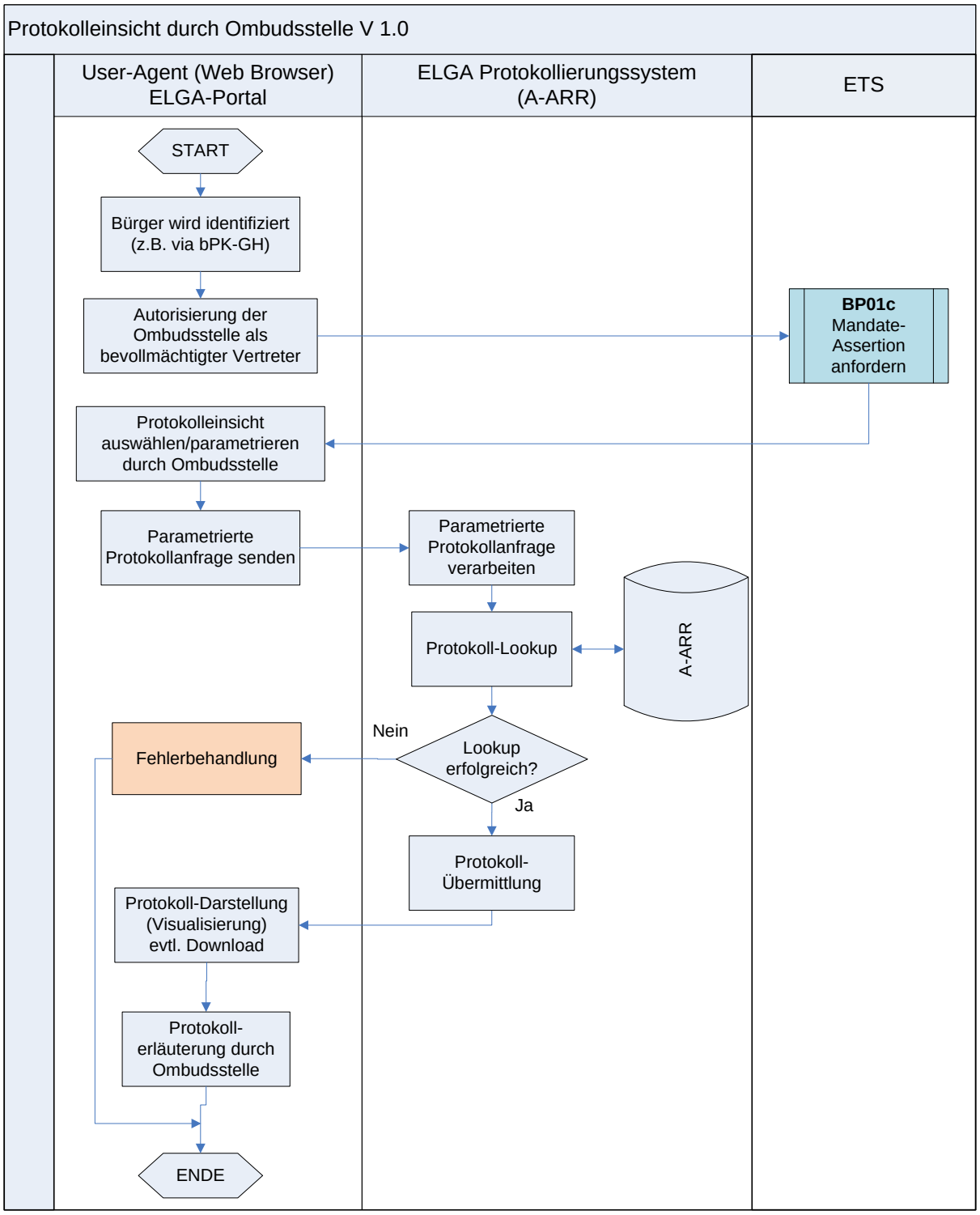
7511

7512 *Abbildung 82: Darstellung des Anwendungsfalls BP10a (entspricht ET.1.6)*

18.9.5.1. Anwendungsfall BP10b: Protokolleinsicht durch Ombudsstelle (OBST.5.6)

1. Bürger identifiziert sich selbst gegenüber der Ombudsstelle.
2. Ombudsstelle meldet sich beim ELGA-Berechtigungssystem als bevollmächtigter Vertreter des Bürgers an.
3. Das ETS autorisiert den Zugriff.
4. Ombudsstelle parametriert die Protokolleinsicht gemäß den Anforderungen des Bürgers z.B. zeitlich.
5. Parametrierte Protokollanfrage wird durch das ELGA-Protokollierungssystem anhand des Protokollspeichers (A-ARR) verarbeitet.
6. Resultate der Protokollanfrage werden am ELGA-Portal inhaltlich aufbereitet (Identifier aufgelöst), um eine lesbare und verständliche Darstellung für den Bürger zu erzielen.
7. Protokolldaten können für den Bürger (als PDF) heruntergeladen werden.
8. Die Ombudsstelle erläutert die Protokolldarstellung für den Bürger.

Abbildung 83 verdeutlicht den zeitlichen Ablauf.



7527

7528

7529 *Abbildung 83: Darstellung des Anwendungsfalls BP10b (entspricht BET.2.6 und OBST.5.6)*

7530

19. Anhang C – Berechtigungssteuerung bei e-Befunden

19.1. Präambel

Die ELGA-Anwendung e-Befunde stellt für jeden ELGA-Teilnehmer über Dokumentenverweise den Zugriff auf dezentral gespeicherte Dokumente bereit. Der ELGA-Teilnehmer kann über das ELGA-Portal Dokumente ansehen, ausdrucken oder lokal abspeichern (nur PDF mit eingefügter persönlicher Kennung).

Der ELGA-GDA kann direkt aus seiner Softwareumgebung, entsprechend seiner Rolle und Berechtigung, auf die Dokumentenliste und auf Einzeldokumente via standardisierter Schnittstellen zugreifen (suchen, filtern, sortieren ist möglich).

19.2. Berechtigungssteuerung

Der Zugriff auf die ELGA-Anwendung e-Befunde erfolgt ausschließlich über die ELGA-Zugriffsteuerung (ZGF). D.h. die ZGF setzt die generellen und individuellen Berechtigungen für den Datenzugriff lt. ELGA-G um. Folgende Regeln können über das ELGA-Portal durch den ELGA-Teilnehmer festgelegt werden:

- **Genereller Widerspruch**/ Opt-Out aus allen ELGA-Anwendungen (derzeit: e-Befund und e-Medikation)
  - Für alle ELGA-GDA ist weder das Schreiben noch das Lesen von Dokumenten oder Medikationsdaten möglich. Bei einem Opt-Out werden alle Dokumentenverweise unwiderruflich gelöscht.
- **Partieller Widerspruch**/ Opt-Out aus einer – oder mehreren – ELGA-Anwendungen
  - Für alle ELGA-GDAs ist weder das Schreiben noch das Lesen der betreffenden Daten möglich. Bei einem Opt-Out werden alle Dokumentenverweise unwiderruflich gelöscht.

Darüber hinaus kann der Bürger vor Ort beim GDA situativ spezifisch für diesen Kontakt/Besuch widersprechen:

- **Situativer Widerspruch**/ Opt-Out:
  - Der ELGA-Teilnehmer kann bei einem Besuch bei einem GDA der Registrierung von Dokumenten situativ widersprechen. Der Widerspruch kann mündlich erfolgen, es wird empfohlen, den Widerspruch schriftlich zu bestätigen. Der Widerspruch gilt für ALLE Dokumente dieses Besuches („Falles“).
  - NUR dem Schreiben kann widersprochen werden.
  - Dem Lesen kann situativ NICHT widersprochen werden.
  - Ein situativer Widerspruch kann nicht rückgängig gemacht werden.

- **Standardzugriff für GDA**
  - Der GDA kann nach erfolgter Kontaktbestätigung (KB) und innerhalb der standardmäßig vorgesehenen Frist von 28 Tagen (Apotheken: 2 Stunden) Dokumente in ELGA abrufen und registrieren. Nach Ablauf der Frist ist kein Zugriff – weder lesend noch schreibend – möglich (Außer wegen Recht auf Richtigstellung).
  - Bei stationären Aufenthalten beginnt diese Frist ab dem Entlassungsdatum.
  - Updaten von nicht gelöschten Dokumenten ist möglich.
- **Delegation einer Kontaktbestätigung**
  - Ein GDA kann einen anderen GDA in die Behandlung des Patienten miteinbeziehen, ohne dass der Patient zu dem miteinbezogenen GDA gehen muss (beispielsweise Labor-GDA, nur die Blutprobe kommt ins Labor). Damit dieser miteinbezogene GDA die ELGA verwenden kann, ist es erforderlich, die GDA-Patienten-KB zu delegieren. Der beauftragte GDA kann innerhalb der regulären Frist (z.B. 28 Tage) lesend und schreibend zugreifen.
  - Delegierte Zugriffe gelten immer als ambulante Kontakte.
  - Delegierte KB erhalten immer die reguläre Zugriffsdauer des Empfängers (Defaultwert für Rolle des Empfängers). Die individuellen Zugriffseinstellungen, die der ELGA-Teilnehmer für den delegierenden GDA vorgenommen hat (der den anderen GDA miteinbezieht) wirken sich NICHT auf die delegierte KB aus.
  - Wenn ein ambulanter Kontakt delegiert wird, errechnet sich die Dauer des Zugriffes für den Empfänger ab dem Zeitpunkt des Kontakts des Auftraggebers.
  - Wenn ein stationärer Kontakt[2] delegiert wird, errechnet sich die Dauer des Zugriffes für den Empfänger ab dem Zeitpunkt der Delegation.
  - Der Patient kann individuelle Regeln für den Auftragsnehmer-GDA treffen, in diesem Fall übersteuern sie die Default-Frist.
- **Zugriffszeit für ELGA-GDA verkürzen** (d.h. nach einem GDA-Besuch wird die Lese-Zugriffszeit auf 1-27 Tage gesetzt)
  - Bei jeder weiteren Kontaktbestätigung (Besuch) beginnt die eingestellte Zugriffsdauer erneut.
  - Bei stationären Aufenthalten gilt die verkürzte Frist nach der Entlassung

[2] Als „stationäre Kontakte“ gelten Aufenthalte in Krankenanstalten oder Pflegeeinrichtungen über mehrere Tage (mindestens über eine Nacht). Auch eine vertraglich definierte Hauskrankenpflege über einen längeren Zeitraum wird zu den stationärer Kontakten gerechnet.

- **GDA sperren (verkürzen auf 0 Tage,** nach einem GDA-Besuch wird die Lese-Zugriffszeit auf 0 Tage gesetzt)
  - Die Defaultzugriffsdauer wird auf 0 gesetzt. Das bedeutet, dass der betroffene GDA die ELGA dieses Patienten ab diesem Zeitpunkt trotz gültiger KB weder zum Lesen noch zum Schreiben verwenden kann. Das gilt auch für stationäre Aufenthalte (Sperre gilt ab sofort, nicht erst ab Entlassung).
- **Zugriffszeit für ELGA-GDA verlängern**
  - Der Bürger darf beliebige niedergelassene Ärzte oder Apotheken als „Vertrauens-GDA“ definieren (nicht Krankenanstalten!), diesen kann der Zugriff auf ELGA Gesundheitsdaten (lesend und schreibend) bis zu 365 Tage gewährt werden.
  - Die individuelle Verlängerung ist über das ELGA-Portal möglich, wenn der GDA in der Kontaktliste aufscheint. Voraussetzung ist, dass der GDA der Verlängerung zugestimmt hat.
  - Die Verlängerung wirkt (rückwirkend) ab letzter Kontaktbestätigung[3].
  - Bei jeder neuen Kontaktbestätigung (Besuch) beginnt die individuell eingestellte Zugriffsdauer neu.
- **Dokumente sperren**
  - Das Sperren und Entsperren von Dokumenten ist für den ELGA-Teilnehmer am ELGA-Portal möglich.
  - Das Ausblenden einzelner Abschnitte in Dokumenten ist nicht möglich.
  - Die Sperre von Dokumenten gilt ausnahmslos für alle ELGA-GDA, das Lesen von einem gesperrten Dokument ist nicht möglich.
  - Ein Update von gesperrten Dokumenten ist möglich (siehe Recht auf Richtigstellung).
- **Dokumente löschen**
  - Das unwiderrufliche Löschen von Dokumenten ist für den ELGA-Teilnehmer am ELGA-Portal möglich.
  - Der Zugriff auf gelöschte Dokumente ist weder für den ELGA-Teilnehmer noch für den GDA möglich.
  - Ein Update von gelöschten Dokumenten ist nicht möglich.

[3] Die neue Frist errechnet sich aus der Differenz zwischen der Zeitspanne seit der letzten Kontaktbestätigung und der neuen Zugriffsdauer

20. Glossar

Bezeichnung	Abk.	Erläuterung
Actor (oder Akteur)		Ein Akteur agiert, produziert und/oder verwaltet Informationen gemäß eines IHE Integrationsprofils
Assertion		Als Assertion werden elektronisch strukturierte und digital signierte XML-Strukturen bezeichnet (meistens identitätsbezogene). Betreffend relevante Standards für die Umsetzung in ELGA wird auf OASIS SAML referenziert.
Audit Record Repository	ARR	Protokoll Speicher. Jeder ELGA-Bereich führt ein Audit Record Repository. Das Audit Repository ist ein Akteur im IHE-Profil ATNA.
Audit Trail and Node Authentication	ATNA	Audit Trail and Node Authentication. IHE Integration Profile, das Vorgaben betreffend Inhalt, Struktur und Kommunikation von Protokollnachrichten zusammenfasst.
Basic Patient Privacy Consent	BPPC	Basic Patient Privacy Consent. Integration Profile, das Mechanismen hinsichtlich der Dokumentation von Willenserklärungen sowie deren Einsatz im Rahmen einer Zugriffssteuerung umfasst.
Behandlungs-zusammenhang		Eine mit Zeitstempel versehene elektronische Bestätigung eines Behandlungsverhältnisses zwischen Arzt (GDA) und Patienten. Synonym Kontaktbestätigung.
Benutzer-authentifizierung		Digital signierte elektronische Bestätigung der elektronischen Identität einer natürlichen oder juristischen Person.
Berechtigungsregel (Policy / Richtlinie)		Im Rahmen von ELGA wird mit *Policy* (Richtlinie) häufig die maschinell bearbeitbare Repräsentation der Berechtigungsregeln (Zugriffsrechte) bezeichnet.

Bereichsspezifisches Personen-kennzeichen	bPK	Eindeutiges Identifikationsmerkmal natürlicher Personen, das für spezifische Verfahrensbereiche (z.B. Gesundheit) existiert. Das e-Government-Gesetz definiert die Begriffe Stammzahl und bereichsspezifisches Personenkennzeichen (bPK).
Bürgerkarten-umgebung	BKU	Bei der Bürgerkartenumgebung handelt es sich um eine Software, die für die Verwendung von österreichischen Bürgerkarten (und Handysignatur) benötigt wird.
Business Logic	BL	**Geschäftslogik** (auch **Anwendungslogik**) ist ein abstrakter Begriff in der Softwaretechnik, der eine Abgrenzung der durch die Aufgabenstellung selbst motivierten Logik eines Softwaresystems von der technischen Implementierung zum Ziel hat.
Certificate Authority	CA	In der Informationssicherheit ist eine Zertifizierungsstelle (englisch Certificate Authority), eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.
Certificate Revocation List	CRL	Eine Zertifikatsperrliste ist eine Liste, die die Ungültigkeit von Zertifikaten beschreibt. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.
XCA-Community		Eine Gemeinschaft (Community, ELGA-Bereich) die an einem Community- (oder Bereichs-) übergreifenden Datenaustausch gemäß IHE-Profil teilnimmt.
Cross Enterprise User Assertion	XUA	IHE-Profil, ermöglicht es, Akteure (z.B. ELGA-Benutzer) über Unternehmens- und Organisationsgrenzen hinaus zu authentifizieren (bzw. verifizieren), um aufgrund dessen in weiteren Folge Entscheidungen über deren Zugriffsberechtigungen zu treffen.

Cross-Community Access	XCA	Ein Community-übergreifender Zugriff auf Gesundheitsdaten gemäß dem genannten IHE-Profil.
Cross-Enterprise Document Sharing	XDS	Ein bereichsinterner (cross-enterprise) Austausch von Gesundheitsdaten gemäß dem genannten IHE-Profil.
Cross-Enterprise Document Sharing for Imaging	XDS-I	Ein bereichsinterner Austausch von Bilddaten (meistens Radiologie) gemäß dem genannten IHE-Profil. In neueren Dokumentationen auch als XDS-I.b bezeichnet.
Datenintegrität		Sicherheitsanforderung, dass unautorisierten Änderungen von signierten Daten einen technischen Riegel vorschiebt und solche Versuche verhindert.
Digital Imaging and Communications in Medicine	DICOM	Ein TCP/IP basierendes Standardprotokoll für den weltweiten Austausch, die Verwaltung und Kommunikation von medizinischen und radiologischen Bildern und deren textliche Beschreibung in der Telemedizin.
Document Consumer	DC	IHE Akteur im XDS Profil. Umfasst Schnittstellen betreffend Suche und Abruf von medizinischen Dokumenten.
XDS Document Source		Akteur im Integration Profile XDS, der die Quelle für die in ELGA anzuzeigenden Dokumente darstellt. Aus Sicht der Software kann dies z.B. ein Adapter sein, der im Verbund mit dem lokalen Gesundheitsinformationssystem diese Schnittstellen implementiert.
ELGA-Anbindungsgateway	AGW	Bezeichnet eine komplette gehärtete Virtuelle Maschine (VM) mit Proxy-Funktionalität (Apache Server), Web Appplication Firewall (WAF) und eingebetteter Zugriffssteuerungsfassade (ZGF)
ELGA-Verweisregister		Registry Akteur im Integration Profile XDS. Verwaltet einen Verweis auf die gespeicherten Dokumente mit Metadaten und bietet eine Abfragefunktion.

ELGA-Authorisation-Assertion		Ein SAML2 Ticket ausgestellt durch das ELGA-Token-Service (ETS). Eine digital signierte Bestätigung eines Sachverhalts bezüglich Identitätsattribute, Rollenattribute, Zugriffsart und Zugriffsberechtigungen.
ELGA-Berechtigungssystem	BeS	Dient der Autorisierung von ELGA-Benutzern und derer Umsetzung beim Zugriff auf vertrauliche Informationen im Rahmen der bereichsinterner und gemeinschaftsübergreifender Kommunikation (XDS/XCA).
ELGA-Bereich		Eine konkrete Ausprägung einer auf dem IHE XDS Profil basierenden Affinity Domäne auch im Sinne von XCA (bereichsübergreifend) aufzufassen.
XCA-Gateway	XCA-GW	Akteur entsprechend dem IHE Profil XCA. Unter einem XCA Gateway versteht man die Hard- und Software, um die Netze von verschiedenen Gemeinschaften (Bereiche) miteinander einheitlich zu verbinden. Ermöglicht die Dokumentensuche und den Dokumentenabruf zwischen XDS-basierten Communities.
ELGA-Gateway		Akteur entsprechend dem Integration Profile XCA. Unter einem ELGA-Gateway versteht man ein spezialisiertes XCA-Gateway, die Hard- und Software, um die Netze von verschiedenen ELGA-Bereichen miteinander einheitlich zu verbinden. Ermöglicht die Dokumentensuche und den Dokumentenabruf zwischen einzelnen ELGA-Bereichen.
ELGA-Healthcare Provider-Assertion	ELGA-HCP-Assertion	Eine konkrete Ausprägung der ELGA-Authorisation-Assertion, ausgestellt ausschließlich für ELGA-GDA. Eine föderierte Identität eines GDA im ELGA.
ELGA-Identity-Assertion	IDA	Elektronische Identitätsbestätigung von ELGA-Benutzer ausgestellt für ELGA von einem externen vertrauenswürdigen Identity Provider.

ELGA-Mandate-Assertion		Eine konkrete Ausprägung der ELGA-Authorisation-Assertion, ausgestellt für bevollmächtigte ELGA-Teilnehmer. Eine föderierte Identität eines Vertreters im ELGA.
ELGA-Portal		Web-Portal zu ELGA für ELGA-Teilnehmer erreichbar über das Internet.
ELGA-Protokollierungssystem		Dient der Protokollierung von Zugriffen in ELGA gemäß IHE ATNA-Profil.
ELGA-Service-Assertion		Eine konkrete Ausprägung der ELGA-Authorisation-Assertion, ausgestellt an ELGA-Service. Berechtigt nicht für Zugriffe auf Gesundheitsdaten.
ELGA-Token-Service	ETS	ELGA-Token-Service ist eine konkrete (spezielle) Ausprägung eines Security Token Services (STS). Autorisiert ELGA-Benutzer via ausgestellten ELGA-Authorisation-Assertions (sog. SAML-Assertions).
ELGA-Treatment-Assertion	E-TA	Konkrete Ausprägung der ELGA-Authorisation-Assertion, ausgestellt für delegierte XCA-Zugriffe im Namen von ELGA-GDA. Beinhaltet ELGA-Teilnehmer spezifische individuelle Zugriffsberechtigungen.
ELGA-User-Assertion	E-UA	Eine konkrete Ausprägung der ELGA-Authorisation-Assertion, ausgestellt für ELGA-Teilnehmer, die sich am ELGA-Portal via Bürgerkarte anmelden. Eine föderierte Identität eines ELGA-Teilnehmers in ELGA.
ELGA-Benutzer		Bezeichnet gesamthaft die verschiedenen Akteure wie ELGA-Teilnehmer, d.h. Bürger bzw. dessen Bevollmächtige und gesetzliche Vertreter und ELGA-GDA als Person oder Organisation sowie ELGA-Service-Mitarbeiter.

ELGA-Gesundheitsdienste-anbieter	ELGA-GDA	ELGA-Gesundheitsdiensteanbieter, die in die Behandlung oder Betreuung eines ELGA-Teilnehmers eingebunden sind und die Voraussetzungen für die Teilnahme an ELGA erfüllen.
ELGA-Komponenten		Sind jene Komponenten aus denen sich ELGA zusammensetzt. Sie werden eingeteilt in „logisch“ zentrale Komponenten (Z-PI, GDA-I, Berechtigungssystem, Protokollierung, Portal) und dezentral zur Verfügung zu stellende Komponenten (ELGA-Bereiche mit ihren Gateways, ihrer Einbindung ins Berechtigungssystem und die Protokollierung, L-PI, Verweisregister, Repositories).
ELGA-Teilnehmer		Natürliche Personen, die die Teilnahmevoraussetzungen erfüllen und für die daher elektronische Verweise auf sie betreffende ELGA-Gesundheitsdaten aufgenommen werden dürfen (gemäß § 15 Abs. 1 GTelG 2012).
eXtensible Access Control Markup Language	XACML	eXtensible Access Control Markup Language. Ein OASIS Standard für die Zugriffssteuerung im Kontext verteilter, serviceorientierter Architekturen.
generelle Zugriffsrechte		Im Kontext des Berechtigungssystems werden generelle Zugriffsberechtigungen betreffend GDA in Abhängigkeit ihrer Rolle auf entsprechende Dokumentenklassen definiert.
Gesundheitsdienstea nbieter	GDA	Anbieter von Gesundheitsdiensten im österreichischen Gesundheitssystem.
Gesundheitsdienstea nbieter-Index	GDA-I	Zur Überprüfung der Identität von ELGA-Gesundheitsdiensteanbietern ist von den ELGA-Systempartnern ein Gesundheitsdiensteanbieterindex einzurichten und zu betreiben.
Gesundheitsinformati onsnetz-Adapter	GINA	Eigenständiger kleiner Computer, der dem GDA die Nutzung des e-card Systems ermöglicht.

Health Level 7	HL7	Standard für den Datenaustausch im Gesundheitswesen
Security Token Service	STS	Ein vertrauenswürdiges Sicherheitsservice, welcher entweder primär das Authentisieren von Anwendern durchführt und/oder Ressourcenzugriffe in Form von ausgestellten signierten SAML-Tickets autorisiert.
Identitätsföderation		Identity Federation ermöglicht es Unternehmen und Organisationen, vertrauenswürdige Identitäten anderer Organisationen, wie zum Beispiel von Partnern oder Zulieferern, zu akzeptieren. Das Ziel von Federation ist es, Informationen von Identitäten über Unternehmensgrenzen hinweg zu integrieren, um Geschäftsprozesse zu vereinfachen.
Identity Provider	IdP	Komponente des Authentifizierungsprozesses. Verifiziert und bestätigt die elektronische Identität eines ELGA-Benutzers mittels elektronisch signierten Tokens (SAML Assertions)
Identity Providing Gateway	IdpGW	Komponente eines lokalen Informationssystems zur nahtlosen Unterstützung von Authentifizierungen und/oder Identitätsföderationen.
IHE-Akteur		Ein Akteur im Sinne der IHE ist eine Funktion bzw. eine Rolle einer EDV Applikation, die die Vorgaben für einen IHE-Akteur gemäß eines IHE-Profils implementiert.
Individuelle Zugriffsrechte		Der ELGA-Teilnehmer hat die Möglichkeit zusätzlich zu den voreingestellten generellen Zugriffsberechtigungen weitere individuelle Zugriffsrechte via ELGA-Portal online oder über Widerspruchstelle und/oder Ombudsstelle zu definieren.
Integrating the Healthcare Enterprise	IHE	Amerikanische Initiative von GDA und Herstellern im Bereich der Medizin, Bildgebung und Kommunikation. Ziel ist die Förderung und erhöhte Interoperabilität verteilter

		Gesundheits-informationssysteme durch den Einsatz existierender Standards (siehe www.ihe.net).
KA-Nummer		Krankenanstalten-Nummer
Lokale Patienten-ID	L-PID	Mittels einer L-PID werden Personendaten innerhalb des L-PI eines ELGA-Bereichs eindeutig identifiziert. Eine L-PID kann mehrere GDA-PIDs zusammenfassen, welche dieselbe Person identifizieren.
Lokaler Patientenindex	L-PI	Ein lokaler Patientenindex (L-PI) ist ein Bestandteil eines ELGA-Bereichs. Er ermöglicht die eindeutige Identifizierung von Patienten innerhalb eines (z.B. Krankenhaus-) Verbunds. Im Rahmen von ELGA stellt er somit einen Index dar, der die Patientenstammdaten (z.B. demographische Daten, lokale Patienten-ID (L-PID)) eines ELGA-Bereichs an den Zentralen Patientenindex weiterleitet und, falls gewünscht, von diesem über Datenänderungen der Linkgruppe informiert wird.
OASIS	OASIS	Die Organization for the Advancement of Structured Information Standards (OASIS) ist eine internationale, nicht-gewinnorientierte Organisation, die sich mit der Weiterentwicklung von e-Business- und Webservice-Standards beschäftigt.
Cross-Enterprise Security and Privacy Authorization	XSPA	Eine Ansammlung von OASIS Standards bzw. Profilen bestimmt für gemeinschaftsübergreifende Autorisierung im Gesundheitsbereich. Zu dem XSPA-Profil gehören u.a. die OASIS Standards WS-Trust, SAML und XACML.
Object Identifier	OID	Die OID dient zur eindeutigen Bezeichnung von Informationsobjekten in offenen Systemen und bietet ein hierarchisch organisiertes Ordnungssystem, dessen Verwaltung dezentral erfolgt. OIDs sind weltweit eindeutige Kennungen für Objekte und in ISO/IEC 9834-1 und ÖNORM A 2642 (1997, 2011) normiert. Siehe auch: http://www.hl7.org/oid/index.cfm

Ordinationskarte	o-card	Die Ordinationskarte des Arztes ist eine PIN-geschützte Karte autorisiert für Zugriffe auf das e-card-System.
Patient Demographics Query	PDQ	Eine IHE-Abfrage (Transaktion) zur Abfrage von demografischen Personendaten und Fachschlüsseln.
Patient Identifier	Patient ID	Patienten-Identifikationsschlüssel zur eindeutigen Zuordnung von Personendaten zu einem bestimmten Patienten.
Patient Identifier Cross Referencing Query	PIX	Das IHE PIX Integrationsprofil beschreibt detailliert den Umgang mit Patientenidentifikatoren in großen Gesundheitsinstitutionen mit heterogenen Informationssystemen und Nummernkreisen.
Patient Identity Feed	PIF	IHE-Transaktion, dient der Einmeldung bzw. Änderungsmeldung von Patientendaten an einen lokalen oder zentralen Patientenindex.
Policy Decision Point	PDP	Funktionale Komponente für die Umsetzung von Zugriffssteuerungsmechanismen gemäß OASIS XACML. Verarbeitet Zugriffsberechtigungen mit dem Ziel der Bestimmung von Zugriffsentscheidungen.
Policy Enforcement Point	PEP	Eine logische Komponente, die die Berechtigungsregeln (Richtlinien) exekutiert und direkt durchsetzt (Fachbegriff im XACML Standard von OASIS).
Policy Information Point	PIP	Eine Komponente für die Unterstützung der Umsetzung von Zugriffssteuerungsmechanismen. Akquiriert autorisierungsrelevante Attribute, welche nicht direkt aus dem Zugriffskontext ableitbar sind.
Policy Push		Ein Verfahren welche die Richtlinien eines autorisierten Akteurs (z.B. individuelle Berechtigungen) in den ausgestellten SAML-Token in Form von sog. Claims (Behauptungen) integriert.

Policy Retrieval Point	PRP	Eine funktionale Komponente des Berechtigungssystems für den Bezug von Zugriffsberechtigungen gemäß RFC 2904 *AAA Authorization Framework*.
Protokoll Data-Warehouse	P-DWH	Zur bereichsübergreifenden Erkenntnisgewinnung bezüglich Betrieb, Angriffsmuster und Abwehrsystematiken ist ein Protokoll-Data-Warehouse System geplant. Die Übermittlung von Protokoll-Metadaten der lokalen Repositories an das Protokoll Data-Warehouse soll kontinuierlich erfolgen.
Public Key Infrastructure	PKI	Ein auf Kryptologie basiertes System (inklusive Instanz und Infrastruktur), das digitale Zertifikate verwalten, ausstellen, verteilen, prüfen und zurückziehen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden etwa zur Absicherung von digitaler Kommunikation verwendet.
Verweisregister bzw. Registry		Ein IHE-Akteur, logische Komponente zur Veröffentlichung von Metadaten gespeicherter Gesundheitsdaten (CDA-Dokumente)
Repository		Ein IHE-Akteur, Komponente zum Speichern von Gesundheitsdaten (CDA-Dokumente)
Request Security Token	RST	Ein Protokoll definiert in WS-Trust Standard. Dient zur Anfrage eines Tokens beim zuständigen Token-Service.
Rolle		Klassifizierung von GDA nach der Art ihres Aufgabengebietes, ihrer Erwerbstätigkeit, ihres Betriebszweckes oder ihres Dienstleistungsangebotes.
Root-OID		Siehe Wurzel-OID.
Schützenswerte Informationen		Informationen, deren Missbrauch die Menschenwürde, die persönliche Integrität und Sicherheit sowie das Vermögen der Patienten, der Mitarbeiter, Vertragspartner und sonstiger Dritter und die Wahrung von Geschäfts- und Betriebsgeheimnissen gefährdet.

Secure Node		Ein durch digitale Zertifikate identifizierter sicherer Akteur im ATNA-Profil.
Security Assertion Markup Language	SAML	Ein OASIS Standard, der die Strukturierung von authentifizierungs- und autorisierungsrelevanten Attributen, welche für die Umsetzung von Zugriffssteuerungsmechanismen erforderlich sein können, ermöglicht.
Single Sign On	SSO	Single-Sign-On (SSO) ist eine Universalstrategie für einen Login, bei dem der Benutzer nur eine Einzelbenutzer-ID benötigt um sich den Zugang zu Rechnern, Anwendungen, Services oder Programmen im Netzwerk zu verschaffen. Single-Sign-On hat für Benutzer die Vorteile, dass sie ihre Passwörter nicht mehr pflegen und sich nicht mehr diverse, teilweise unsichere Passwörter, sondern nur noch ein Passwort merken müssen. Teilnehmer können nach einmaliger Authentifizierung ohne weitere Abfrage auf für sie freigegebene Ressourcen zugreifen.
Smart Open Services for European Patients	epSOS	EU-Projekt mit dem Ziel den Austausch grundlegender Patientendaten und elektronischer Verschreibungen zwischen Europäischen Gesundheitssystemen zu ermöglichen [epSOS].
Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft mbH	SVC	Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft mbH
Stammzahlenregister	STZR	Im österreichischen E-Government erfolgt die eindeutige Identifikation von natürlichen Personen durch eine geheime Stammzahl.
Transaktion		Im Sinne von IHE stellt eine Transaktion einen Informationsaustausch zwischen IHE Akteuren dar. Dieser

		kann eine oder mehrere Nachrichten (Messages) umfassen.
Transaktionsnummer	TAN	Eine weltweit (oder Systemweit) eindeutige Nummer zur Identifikation und Autorisierung von Transaktionen
Uniform Ressource Locator	URL	Internetadresse oder Webadresse.
Uniform Ressource Name	URN	Dauerhafte, ortsunabhängige Bezeichner für eine Ressource
Universal Unique Identifier	UUID	Standard für eindeutige Identifikatoren aus Zufallszahlen
Vertragspartner-nummer	VPNR	Die Vertragspartnernummer identifiziert eine Krankenanstalt bzw. eine Verrechnungseinheit einer Krankenanstalt. Der Ordnungsbegriff Vertragspartnernummer wird vom Hauptverband der österreichischen Sozialversicherungsträger verwaltet.
Web Access to DICOM Persistent Objects	WADO	Eine Erweiterung des DICOM Standards mit der Bilddaten (Images) auch über Web-Interfaces (HTTP) zur Verfügung gestellt werden können.
Web Service	WS	Allgemein ein Dienst, oder X-Service-Provider, der im Internet oder Intranet durch standardisierte Web-Protokolle (http, SOAP, REST, usw.) erreichbar ist und für gewöhnlich für entfernte Clients (Requestor) Mehrwert produziert.
X-Service Provider		IHE Akteur (Web-Service) gemäß XUA Integration Profile. Stellt im Kontext von ELGA-CDA Dokument-Metadaten bzw. ELGA-CDA-Dokumente authentifizierten ELGA-Benutzern zur Verfügung.
X-Service User		Ein autorisierter IHE-Akteur (Client oder Requestor) gemäß XUA Integration Profile, der Dienste eines X-Service-Providers nutzt.

Cross-Enterprise Security and Privacy Authorization	XSPA	Ein OASIS Sammelprofil bestehend aus mehreren spezialisierten Profilen, die der Vereinheitlichung der bereichsübergreifenden Berechtigungssteuerung dienen.
Zentrale Partnerverwaltung des Hauptverbandes der österreichischen Sozialversicherungsträger	ZPV	Wird in ELGA als Quelle für Identifikationsdaten von Bürgern verwendet.
Zentraler Patientenindex	Z-PI	Der Zentrale Patientenindex ermöglicht die eindeutige verbund-übergreifende Identifizierung von Patienten. Ein Synonym für Master Patient Index (österreichweit versteht sich).
Zentrales Melderegister	ZMR	Das Zentrale Melderegister ist ein System des Bundesministeriums für Inneres (BMI) zur Erfassung und Speicherung von u.a. Adressdaten.
Zugriffsprotokolle		ELGA-Transaktionen werden lückenlos gemäß IHE ATNA Profil protokolliert. Die Protokolle werden lokal in Audit Record Repositories (L-ARR) geführt und gespeichert. Zugriffsprotokolle können zentral via A-ARR (zukünftig Protokoll Data-Warehouse) zusammengefügt, um mittels Data-Mining auf verdächtige Muster (Intrusion) analysiert zu werden.
Zugriffssteuerungs-fassade	ZGF	Dezentraler Teil des ELGA-Berechtigungssystems. Eine ZGF ist in einer Virtuellen Maschine (VM) eingebettet. Schützt die Ressourcen eines ELGA-Bereichs. Die Zugriffssteuerungsfassaden setzen typischerweise die allgemeinen und individuellen Berechtigungen um. Nicht zu verwechseln mit einem ELGA-Anbindungsgateway.
Single Sign On	SSO	Einmalanmeldung. Bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung in einer bestimmten Domäne in der Folge auch auf Dienste einer anderen

		(vertrauenswürdigen) Domäne ohne eine zusätzlich erforderliche Authentifizierung zugreifen kann.
Service Information Manager	SIM	Verteilte ELGA-Komponente mit SOAP-Schnittstelle zur Abfrage von Versions- und Release-bezogenen Informationen

7624

7625

21. Abbildungen

22. Tabellenverzeichnis

23. Literaturverzeichnis

No.	Bezeichnung des referenzierten Dokumentes
[1]	ELGA Lastenheft Gesamtarchitektur Version 1.0 vom 1.6.2008
[2]	ELGA CDA-Implementierungsleitfäden (entsprechend über das Gesundheitsportal öffentlich zugänglicher Dokumentation)
[3]	ZPI_Anforderungsdokument_20091222_v1.3.pdf
[4]	IHE IT-Infrastructure White Paper Access Control by Jörg Caumanns, Raik Kuhlisch, Oliver Pfaff, Olaf Rode, September 28, 2009
[5]	On secure implementation of an IHE XUA-based protocol for authenticating healthcare professionals by Massimiliano Masi, Rosario Pugliese, and Francesco Tiezzi
[6]	e-Government Bund-Länder-Gemeinden; Online-Vollmachten-Spezifikation mis-1.0.0
[7]	ELGA-Leitfäden; Implementierungsleitfaden XDS Metadaten V2.06 oder höher
[8]	ELGA-Leitfäden; Allgemeiner CDA-Implementierungsleitfaden V2.06 oder höher
[9]	IHE Radiology Technical Framework Volume 1 (IHE RAD TF-1) Integration Profiles
[10]	IHE Radiology Technical Framework Supplement; Cross-Community Access for Imaging (XCA-I) Trial Implementation
[11]	IHE ITI Technical Framework Volumes 1, 2a, 2b, 2x, 3 (**Revision 12**)
[12]	Security analysis of the SAML single sign-on browser / artifact profile, IEEE 2004, Thomas Gross, IBM Zurich Res. Lab., Ruschlikon, Switzerland, Print ISBN: 0-7695-2041-3
[13]	Proving WS-Federation passive requestor profile with a browser model, Thomas Groß, 2005 Workshop on Secure Web Services, ISBN:1-59593-234-8

[14]	Anforderungsdokument ELGA-Portal V2.0 (AD_EBP_V2.docx) und entsprechende Pflichtenheftdokumentation (laufend)
[15]	e-Medikation; Bündel der Pflichtenheftdokumentation (laufend) inklusive: • PH_014_EMEDAT_Hauptdokument und Architektur • PH_014_EMEDAT_Anwendung • PH_014_EMEDAT_SS_eMedikation • PH_029_SS_XDS_und_PHARM_Transaktionen
[16]	ELGA Service Levels v1.0 oder höher
[17]	GDA-Index Servicehandbuch Version 1.1 oder höher
[18]	CSC/TIANI; ELGA BeS Pflichtenheft V2.2 oder höher
[19]	CSC/TIANI; ELGA A-ARR Pflichtenheft Version 2.0 oder höher
[20]	OBST Konzept, Anforderungsdokument und Pflichtenhefte (laufend)
[21]	WIST Konzept, Anforderungsdokument und Pflichtenheft (laufend)
[22]	Z-PI_Schnittstelle_ITI-44,45,46,47 ab Version 2.6 oder höher
[23]	Architektur der bereichsübergreifenden Bilddatenübertragung in ELGA (laufend)
[24]	Rahmenbedingungen für ELGA Releases und Releases von Umfeld-Komponenten V1.0 oder höher
[25]	Pflichtenhefte von ELGA-Proxy in aktuellen Version
[26]	Pflichtenhefte des Vertretungsmoduls (VEMO) der Sozialversicherung in aktueller Version

24. Dokumentenhistorie bis Version 1.3

Die geschichtliche Entwicklung der Gesamtarchitektur von Version 1.0 bis 1.3 ist textuell in den hier folgenden Kapiteln detailliert und umfangreich zusammengefasst. Die Änderungen ab Version 1.3 sind tabellarisch im Anhang (Tabelle 34: Änderungen in tabellarischer Form) einzusehen.

24.1. Vergleich der ELGA-Gesamtarchitektur in der Versionen 1.0 und 1.3

Die derzeit aktuelle Version der ELGA-Gesamtarchitektur basiert auf der ersten Version der ELGA-Gesamtarchitektur, datiert am 1. Juni 2008. Die aktuelle Version ist eine natürliche Weiterentwicklung, moderate Überarbeitung und Anpassung der vor vier Jahren aufgestellten Konzepte im Hinblick auf den aktuellen Stand der technischen Entwicklung insbesondere im Bereich der Standardisierung. In den weiteren Kapiteln wird ausführlich erklärt, welche

Konzepte unangetastet geblieben sind und wo und vor allem warum die Änderungen und Erweiterungen notwendig geworden sind.

24.1.1. Zusammenfassung der unveränderten Bereiche

Dieser Kapitel fokussiert sich auf jene Konzepte der Originalarchitektur, welche unverändert geblieben sind. Dies betrifft im Wesentlichen beinahe alle grundlegenden Prinzipien der Gesamtarchitektur. Anbei die Übersicht aufgrund der Kapitel-Struktur der Originalversion.

24.1.2. Management Summary

Die Darstellung der ELGA-Gesamtarchitektur ist im Wesentlichen unverändert (siehe Abbildung 1 der Version 1.0). Im ELGA-Kontext existieren weiterhin all jene zentrale Services, die hier abgebildet sind, namentlich der Zentrale Patientenindex, der GDA-Index, das Bestätigungsservice (derzeit ELGA-Token-Service mit dem Policy Administration Point), die Protokoll-Aggregation (derzeit Zentraler Audit Record Repository) und das Portal. Unverändert ist das Grundkonzept der virtuellen Gesamtregister, welche die Summe aller lokalen in den einzelnen ELGA-Bereichen liegenden Register zusammenfasst. Der hier dargestellte Aufbau der einzelnen ELGA-Bereiche ist weiterhin gültig. In den ELGA-Bereichen sind unverändert all jene Komponenten vorhanden, die hier explizit dargestellt sind: ELGA-Verweisregister, Lokaler Patientenindex, ELGA-Gateway und das ELGA-Berechtigungs- und Protokollierungssystem. Auch die Anbindung der GDA-Systeme ist unverändert.

24.1.3. Darstellung der Gesamtarchitektur

Die in diesem Kapitel dargestellte Verwendung von Cross-Enterprise Document Sharing (XDS) und Cross-Community Access (XCA) sowie die ELGA-Bereiche (Affinity Domains) sind unverändert. Auch die zentralisierte Funktion des Zentralen Patientenindex (Z-PI) ist unangetastet, auch wenn „kosmetische“ Änderungen in Bezug auf die Record Locator Service (RLS) Funktionalität vorhanden sind (siehe Kapitel mit den Änderungen). Nach wie vor ist das XCA Gateway jene Instanz, welche die bereichsübergreifende Kommunikation mit allen anderen ELGA-Bereichen übernimmt. Änderungen sind wiederum in einigen wenigen Details vorgenommen worden, die im nächsten Kapitel ausführlich erläutert werden.

Unverändert vorhanden sind alle hier aufgelisteten zentralen ELGA-Komponenten. Das ELGA-Token-Service stellt die einzelnen Assertions (SAML-Tokens) für autorisierte Zugriffe aus und verkörpert dadurch das zentrale Herzstück des ELGA-Berechtigungssystems.

Auch die Verteilung der Daten (Kapitel 2.5) und die Anforderungen an die ELGA-Bereiche (Kapitel 3.8 und weitere) behalten ihre Gültigkeit und die Konzepte lassen sich in der aktualisierten Version wiederfinden.

Alle Definitionen und Anforderungen hinsichtlich Service Orientierter Architektur (SOA) und der Nutzung der WS* Standards sind unverändert. Dies betrifft auch die Hervorhebung der HL7 Version 3 als Basis für ELGA. Unverändert ist die Anforderung zur Einführung einer eindeutigen ELGA-Transaktionsnummer bei allen IHE Transaktionen.

24.1.4. Patientenindex

Das Konzept eines zentralen Patientenindexes wie dies in der Version 1.0 der Gesamtarchitektur vorgesehen, bleibt aufrechterhalten. Für Änderungen siehe das nächste Kapitel.

24.1.5. GDA-Index

Die Rolle des GDA-Index als zentralisierter Service bleibt relevant und gültig, auch wenn bestimmte Änderungen und Erweiterungen vorhanden sind. Siehe das nächste Kapitel.

24.1.6. ELGA-Verweisregister / Dokumentenaustausch

Auch wenn Änderungen, insbesondere im Bereich von XDS-I und DICOM bzw. WADO stattgefunden haben (siehe Kapitel mit aufgelisteten Änderungen), sind die wesentlichen Eckpunkte unverändert geblieben, etwa die Organisation der Dokumentregister und das damit verbundene Policy Enforcement.

24.1.7. ELGA-Berechtigungs- und Protokollierungssystem

Die Mehrheit der Änderungen der neuen Version sind gerade diesem Bereich zuzuordnen. Es existieren jedoch unverändert die ELGA-Benutzerbestätigung (in der neuen Version ELGA-User-Assertion) und die ELGA-Patienten Token (in der neuen Version ELGA-Patient-Assertion) welche als SAML-Assertions laut der entsprechenden OASIS Standards strukturiert sind. Unverändert ist die Anforderung hinsichtlich ATNA – Secure Nodes sowie die Anforderung des ATNA Consistent Time Profils (CT).

24.1.8. Portal

Die Definition und Beschreibung eines ELGA-Portals ist in den Grundzügen unverändert, auch wenn in den einzelnen Details Anpassungen und wesentliche Erweiterungen stattgefunden haben.

24.1.9. Mengengerüst

Dieses Kapitel wurde unverändert übernommen.

24.1.10. Antwortzeiten

Dieses Kapitel ist teilweise unverändert geblieben, teilweise sind Änderungen eingeflossen. Veränderungen sind vor allem in den Begriffsdefinitionen vorgenommen worden, etwa statt Kontakt Service spricht man in der neuen Version über einen Behandlungszusammenhang. Weitere Details zu den Neuigkeiten sind im weiteren Kapitel erörtert.

24.1.11. Betriebsanforderungen

Die hier aufgestellten Anforderungen, wie Hochverfügbarkeit, sind nur erweitert und präzisiert worden und der hier präsentierte Inhalt wurde restlos übernommen.

24.2. Übersicht der wesentlichen Änderungen und Erweiterungen in der Version 1.3

Die Veränderungen und Erweiterungen der neuen Version der Gesamtarchitektur (gemeint ist ausschließlich die Version 1.3) werden nicht kapitelweise erörtert sondern themenschwerpunktorientiert aufgelistet. Der Grund für die Änderungen sind einerseits entsprechende Änderungen im ELGA-Gesetz und andererseits das Erscheinen von neuen Standards, insbesondere nach dem 2008 Jahr.

24.2.1. Authentifizierung, Autorisation und Standards

Die umfangreichsten und wesentlichen Änderungen der gegebenen Architektur sind in den folgenden Bereichen anzusehen:

- Authentifizierung der ELGA-Benutzer und Identity Provider
- Neue OASIS Standards WS-Trust und WS-Federation
- Erweitertes IHE XUA++ Profil und dadurch das Eibeziehen des OASIS XSPA (Cross-Enterprise Security and Privacy Authorization Profile) Standards

24.2.1.1. Authentifizierung

Die neue Version der Gesamtarchitektur definiert alle ELGA-Benutzer. ELGA grenzt sich jedoch von der Authentifizierung der Benutzer ab, indem diese wichtige und essentielle Aufgabe an vertrauenswürdige externe Identity Provider delegiert wird. ELGA beschäftigt sich daher weniger mit der Authentifizierung der Benutzer als mit der Aufgabe des **Föderierens** von existierenden und angemeldeten digitalen Identitäten und fokussiert sich vor allem auf die Aufgabe der **Autorisierung** der föderierten Identitäten. Wichtig ist hier die Aussage, dass ELGA sich das Recht vorbehält, bestimmten Identity Provider zu vertrauen oder eben dieses Vertrauen zu verweigern, soweit bestimmte (z.B. gesetzliche) Grundvoraussetzungen nicht eingehalten werden. Vertraut wird jedenfalls der authentischen Bürgerkartenumgebung, die

mit den dafür bestimmten MOA-ID Komponenten umgesetzt wird. Die Frage der Vertretungen ist auch gänzlich an das e-Government ausgelagert.

24.2.1.2. Profile, Standards und XSPA

Das IHE XUA Profil ist für komplexe Autorisierungen nicht ausreichend. Hierfür sieht IHE ein erweitertes XUA++ Profil vor. XUA++ (derzeit Trial Implementation) verweist auf das OASIS XSPA Profil. Dieses Profil wurde erst nach der Veröffentlichung der ersten Version der ELGA-Gesamtarchitektur erweitert, indem das „*WS-Trust for Healthcare*“ Profil fix in die Sammlung der XSPA Profile integriert wurde. Dieses Profil beruht auf dem OASIS Standard WS-Trust. Somit haben sich die Protokollvorgaben bezüglich der Anforderung (Request), Erneuerung (Renewal) bzw. Abbruch (Cancel) von SAML-Tickets von den ursprünglichen SAML-Protokollen in Richtung WS-Trust Protokolle verschoben.

Es ist wichtig zu vermerken, dass die Vorgabe von SAML-Tickets beibehalten wurde, da die WS-Trust Protokolle assertion-agnostisch (unabhängig) sind. Neu in dieser Hinsicht sind die Protokolle Request Security Token (RST) und Request Security Token Response (RSTR) und weitere. WS-Trust definiert ja die Interaktion von vertrauenswürdigen aktiven Komponenten.

Bemerkung: Web-SSO Profil basierende SAML-Protokolle unterstützen ausschließlich passive Clients (Web-Browser).

24.2.1.3. Autorisierung

Eine große Änderung ist bezüglich der Weitergabe der generellen und individuellen Berechtigungen gemacht worden. Die erste Version der Gesamtarchitektur hat hier einen sog. Policy-Pull Mechanismus vorgesehen, indem der Policy Enforcement Point (PEP) bei Bedarf eine remote Rückfrage nach den Berechtigungen des Anfragenden an das Zentrale Bestätigungsservice startet und selbst dadurch aktiv wird (siehe Abbildung 24 und die dazugehörige Erklärung in der Version 1.0, Seiten 68/69). Diese Vorgehensweise hat den Nachteil, dass XCA-Anfragen, die bereits remote initiiert worden sind, remote für Informationen Rücksprache halten müssen, obwohl bereits zum Zeitpunkt der Initiierung der IHE Transaktion die Antworten bekannt gewesen wären.

Die neue Version berücksichtigt das Vorgehensmodell des OASIS WS-Trust Standards und verwendet Policy-Push eingebettet in die SAML-Token (sog. Claims). Die Idee dabei ist, XACML Policies, die zum Zeitpunkt der Initiierung der Anfrage (IHE-Transaktion) bekannt sind, sofort mitzugeben und dadurch einen zusätzlichen Remote-Callback der Relying-Party (oder PEP) zu verhindern. Dies erhöht die Stabilität und die Performance und vereinfacht die Implementierung der Komponenten.

Es gibt neue SAML-Tokens, und neu ist auch die damit verbundene Klassenhierarchie: Die einzelnen Assertion-Klassen der neuen Version der ELGA-Gesamtarchitektur unterscheiden

zwischen ELGA-User-Assertion (für ELGA-Teilnehmer), ELGA-HCP-Assertion (für GDA), ELGA-Patient-Assertion (Patientenkontext), ELGA-Treatment Assertion (eingebettete Berechtigungen), ELGA-Mandate-Assertion (Vertretungen) und ELGA-Service-Assertion (Betriebspersonal).

24.2.2. Anwendungsfälle

Neu ist das Auflisten der wichtigsten Anwendungsfälle sowohl seitens der ELGA-Teilnehmer wie auch seitens der ELGA-GDA, sowie Ombudsstelle und Widerspruchstelle. Auch die Vertreter-Anwendungsfälle sind neu.

24.2.3. ELGA-Kernbereich

Neu ist die Bestimmung bezüglich eines Hochsicherheitsbereiches, sog. ELGA-Kernbereiches innerhalb der ELGA-Basis. Ein ELGA-Kernbereich unterscheidet sich vom gewöhnlichen ELGA-Basisbereich dadurch, dass zusätzlich zu den ATNA Secure Nodes Vorgaben, alle Zugriffe explizit autorisiert werden müssen. Egal, von welchem Consumer auch immer kommend, ein gültiger SAML-Token muss immer präsentiert werden. Ansonsten wird der Zugriff verweigert.

24.2.4. ELGA-XCA-Gateway

Das Konzept der ELGA-XCA Gateways wurde präzisiert und erweitert. Neu ist die gewählte Strategie der Erkundung der ELGA-Zielbereiche. IHE XUA++ definiert ja nur die Frameworks (XSPA) zur Realisierung der Autorisierungsanforderungen. Details der Implementierung werden vorerst nicht präzisiert.

IHE sieht vor, dass ein beliebiges Initiating Gateway die anzusprechenden Zielbereiche eruiert. Hinsichtlich der Tatsache, dass XCA **Responding**-Gateways entsprechende ELGA-Autorisierung verlangen (SAML-Token), müssen bereits die XCA **Initiating** Gateways die einzelne Tokens vom ELGA-Token-Service (ETS) verlangen. Folglich muss das ETS PIX-Anfragen an den Z-PI stellen. Das ETS sendet somit dem Initiating Gateway eine Liste mit den jeweiligen gültigen Tickets (RSTRC - Request Security Token Response Collection).

Die neue Version der Gesamtarchitektur sieht ein kompaktes ELGA-XCA Gateway mit integrierten Komponenten vor. Neben einem Policy Retrieval Point (PRP) sind im Gateway ein Policy Enforcement Point (PEP), ein Policy Information Point (PIP) und ein Policy Decision Point (PDP) inkludiert.

Die PEP-PIP-PDP Komponenten sind dem ELGA-Verweisregister und dem Repository vorgeschaltet, um sensitive Inhalte zu schützen. Es muss auch die Gesetzesanforderung erfüllt werden, wonach für ELGA-Teilnehmer, die „opt-out“ gewählt haben, keine neuen Gesundheitsdaten in ELGA eingepflegt werden dürfen. Hierfür ist eine Schnittstelle im ELGA-XCA-Gateway entworfen worden, um das Veröffentlichen von CDA-Dokumenten (ITI-42) in den ELGA-Verweisregistern für opt-outed ELGA-Teilnehmer zu verhindern oder zuzulassen (je nachdem ob die Policy „opt-out“ gültig ist).

24.2.5. Patientenindex (Z-PI)

Änderungen gibt es durch das Einführen der Verwendung des bereichsspezifischen Personenkennzeichens (bPK-GH) lt. ELGA-Gesetz.

Der Patientenindex bietet kein Record Locator Service (RLS) mehr an. Statt RLS liefert der Z-PI bei einer PIX-Anfrage jene potentiellen ELGA-Bereiche zurück, wo der Patient zumindest eine lokale ID zugeordnet hat. Hierfür muss es nicht gewährleistet werden, dass auch Gesundheitsdaten im identifizierten ELGA-Bereich vorliegen, lediglich die Tatsache wird ausgewiesen, dass der Patient im Bereich administrativ aufgenommen wurde.

24.2.6. GDA-Index

Die Beschreibung des GDA-Indexes in der Version 1.0 der Gesamtarchitektur ist allgemein gehalten und spezifiziert die Umsetzungsdetails nicht. Diese Version hat auch noch die Integration des E-Health-Verzeichnisdienstes (eHVD) in den GDA-Index vorgesehen (siehe Abbildung 13 der Version 1.0) und folglich die Lieferung von Ordinationsadressen sowie E-Mail Adressen. Die neue Version der Gesamtarchitektur sieht nun die im eHVD gespeicherten Informationen vom GDA-I getrennt. Der GDA-I ist die Quelle von eindeutigen Object IDs (OID) und Rollen von GDA. Aktuelle Auskunftsdaten bezüglich Ordinationsadressen, Telefonnummer oder Ordinationszeiten sowie E-Mail Adressen sind hier nicht vorgesehen.

Es wurde erwogen, den GDA-Index laut IHE Healthcare Provider Directory (HPD) Schema aufzubauen und entsprechend via IHE Transaktion Provider Information Query [ITI-58] abzufragen. Die neue Version der Gesamtarchitektur begründet die Entscheidung einen Kompromiss zu wählen, und den Index soweit wie möglich HPD-Konform aufzubauen und über eine spezifische serviceorientierte Web-Service Schnittstelle anzubinden.

24.2.7. NAV Profil

Dieses Profil wurde in der neuen Version nicht aufgenommen. Ein wesentlicher Grund wurde bereits im vorherigen Kapitel GDA-Index angedeutet. Das NAV-Profil braucht die Verwaltung von E-Mail Adressen, welche aber im GDA-Index nicht mehr vorhanden sind und vorerst vom eHVD nicht übernommen werden. Somit besteht zurzeit keine Möglichkeit, ohne Zusatzaufwand die für das NAV-Profil notwendigen E-Mail Adressen zur Verfügung zu stellen.

Andererseits ist das Versenden und Empfangen von E-Mails immer mit einem gewissen nicht zu vernachlässigenden Sicherheitsrisiko verbunden. Etwa Phishing Attacken, Cross Site Scripting (XSS) und/oder Cross Site Request Forgery (XSRF) können von einer bösartigen Quelle unternommen werden, um nur einige wenige zu nennen.

24.2.8. Offline Betrieb der ELGA-Bereiche

In der neuen Version wurde der offline Betrieb der ELGA-Bereich näher spezifiziert und mögliche Szenarien genauer betrachtet und auch klassifiziert sowie die notwendigen Maßnahmen und Bedingungen für die genannten offline Modi spezifiziert.

24.2.9. Gesundheitsapplikationen

Eine Minimaldefinition von sog. Gesundheitsapplikationen ist in der neuen Version angeführt und die Patientenverfügung wurde als ein entsprechendes Beispiel für eine ELGA-Applikation beschrieben.

Die Beschreibung der e-Medikation wurde nicht mehr in die neue Version der Gesamtarchitektur aufgenommen, weil die Pilotapplikation nicht IHE konform gestaltet war. Sollte die in der neuen Version verfasste Definition von ELGA-Applikationen eine breite Zustimmung bekommen, muss die e-Medikation dem entsprechend in ELGA integriert werden. Auch die IHE Pharmacy Trial Implementation wäre zu berücksichtigen.

24.2.10. DICOM und WADO

Die erste Version der ELGA-Gesamtarchitektur sieht den Zugriff auf Bilder in Bildarchiven via DICOM bzw. Web Access DICOM (WADO) vor. Hierfür sind bei den Zugriffen sog. WADO-Gateways vorgesehen (siehe Abbildung 17 in der Version 1.0). Cross Enterprise Imaging basiert auf DICOM Application Entity Title (AET), der vom Consumer auf eine URL zu verlinken ist. Dieses Konzept unterstützt nur Web-Browser basierende Applikationen (via http). Die neue Version der ELGA-Gesamtarchitektur schlägt vor, den IHE Radiology Technical Framework Supplement XDS-I.b und XCA-I zu berücksichtigen und neben XCA ELGA-Gateways auch die Implementierung von XCA-I ELGA-Gateways zu erwägen. Dieses Konzept unterstützt nicht nur passive Clients (Web-Browser) sondern auch im Sinne von WS-Trust beliebige aktive Komponenten.

24.2.11. ELGA-Portal

Die Konturen und Anforderungen der Service Orientierten Architektur (SOA) bezüglich des ELGA-Portals sind viel schärfer gezogen. Die Portalapplikation ist demnach ein sog. „Mash-Up“ mit einer graphischen Oberfläche (GUI) welche bestimmte vordefinierte Hintergrundservices (WS) bündelt und konsumiert. Somit verlagern sich wesentliche Teile der Geschäftslogik in den Bereich der zu konsumierenden Web-Services. Auch die Grenze zwischen IHE und non IHE Welt wurde scharf gezogen, um die Anforderungen für den Bau des Portals so klar und deutlich wie möglich vorgeben zu können.

24.2.12. Betriebsanforderungen

Die Betriebsanforderungen sind erweitert bzw. präzisiert worden. Dies betrifft die Punkte Verfügbarkeit und Skalierbarkeit. Die Anforderungen hinsichtlich Datensicherheit sind entsprechend des Datenschutzgesetzes aufgeschnürt und neu zusammengefasst worden.

25. Dokumentenhistorie ab Version 1.3

Version	Datum	Autor (Editoren)	Beschreibung der Änderungen
1.3	07.10.2011	Stefan Repas	Erweiterungen gegenüber Version 1.0 sind im vorherigen Kapitel detailliert dargestellt.
1.42	08.03.2012	Stefan Repas	• Management Summary erweitert • Anwendungsfälle eingefügt • ELGA-Systemgrenzen präzisiert • Bezeichnung Record Locator Service (RLS) wird nicht mehr verwendet • Abbildungen präzisiert und überarbeitet • Offline Szenarien der ELGA-Bereiche präzisiert und erweitert • Neues Kapitel *Vertrauensverhältnisse* • Neues Kapitel *Replikationen des zentralen GDA-Index* • ELGA-Gateway (Pipelines) Beschreibung erweitert • Kapitel XDS-I überarbeitet • Fehler in der ELGA-Authorisation-Assertion Struktur behoben • Portal überarbeitet samt Abbildungen • Definition Gesundheitsapplikationen (ELGA-Applikationen) präzisiert • Patientenverfügung umgearbeitet • Mengengerüst in Tabellen übernommen • Betriebsanforderungen, Annahmen und Datensicherheit überarbeitet • Glossar eingefügt • Dokumentenhistorie eingefügt • Kapitel der offenen Punkte eingefügt
1.43	14.03.2012	Andrea Klostermann	• Korrektur und Anpassungen im Sinne von Feedbacks bis 12.03.2012
1.50	30.12.2012	Oliver Kuttin, Stefan Repas	• Überarbeitete Version basierend auf Beschlüsse der Architektur Workshops • Änderungen bis zur Version 1.3 eingefügt • Aufstellung des ELGA-Portals über das eigene XCA Gateway • Kontaktbestätigungsservice Varianten neu eingefügt • Auflassen der Bezeichnung EGVB (ELGA Grundversorgungsbereich) • Interne Version (nicht ausgeschickt)
2.00	06.01.2013	Stefan Repas	• Korrektur der Inhalte
2.01	11.01.2013	Günter Rauchegger	• Inhaltliche Korrektur (Vorabversion)
2.02	05.05.2013	Stefan Repas	• Erkenntnisse eingearbeitet, die bei den Expertenmeetings zum

			Berechtigungssystem und zur Protokollierung gewonnen werden konnten (Kapitel 2.13, 7) • Ergänzungen der Liste der offenen Punkte • Ergänzt um Kapitel 2.14 • Ergänzt durch Anhang der Anwendungsfälle, Kapitel 14.
2.03	12.09.2013	Stefan Repas	• Ergänzungen, Fehlerbehebungen aus dem Technologiebeirat-Review eingearbeitet
2.04	30.11.2013 Bis 31.04.2014	Stefan Repas	• Überarbeitung und Anpassung jeglicher Beschreibungen der Kontaktbestätigungen. • ELGA Patient-Assertion wird nicht mehr verwendet • Subject Confirmation Method „sender-vouches“ wird eingeführt • Policy-Anbindung an Dokumenten ID • e-Medikation in der aktuellen Version eingearbeitet • laufende Präzisierungen, die im Rahmen der Realisierung des Berechtigungssystems erarbeitet wurden eingepflegt. • aktuelle Abstimmungsergebnisse zum Netzwerk eingepflegt.
2.10	21.05.2014	Stefan Repas	• Terminologieserver eingearbeitet • Zugelassene XDS-Anbindungsvarianten • CDA löschen und Registry-Signatur • A-ARR • PAP Geschäftslogik
2.11	03.06.2014	Stefan Repas, Andrea Klostermann	• Kommentare von SVC bezüglich Kontaktbestätigungsservice eingearbeitet • Löschen von Gesundheitsdaten aufgrund Expertenabstimmergebnis präzisiert • ELGA Bürgerportal durch ELGA-Portal gemäß PR-Entscheidung ersetzt
2.12	30.07.2014	Stefan Repas, Andrea Klostermann	• Es wird nun auf IEH ITI TF Revision 10 referenziert • Das XUA++ Profil wird nicht mehr erwähnt (weil in die Revision 10 integriert) • Feedbacks und Anmerkungen sind eingearbeitet worden
2.13	15.09.2014	Stefan Repas, Andrea Klostermann, Carina Seerainer	• Überarbeitung aufgrund der Rückmeldungen der ELGA Errichtungspartner
2.14	24.09.2014	Stefan Repas, Andrea Klostermann	• Entfernung aller Hinweise auf PDWH • Aufgelassenes Konzept der lokalen Replikate • Einarbeitung der Beschlüsse der Kommission für Interpretation des ELGA-Gesetzes (Update von Dokumenten)

2.15 (draft only)	23.01.2015	Stefan Repas Carina Seerainer Oliver Kuttin Johannes Hell	• Festlegungen zur Notation • UML-Klassendiagramm der Architektur • UML-Komponentendiagramme • A-ARR Zwei-Phasen Protokollierung • OID Werte der entsprechenden Code-Listen eingetragen • Strukturelle Reorganisation • GDA-Browser vom Portal entfernt. Das Setzen von Policies ohne Kontaktbestätigung ist nicht möglich (wird nicht unterstützt) • Änderungen, vor allem Präzisierungen entlang der Erkenntnisse aus dem Fraunhofer FOKUS-Review • Neues Kapitel 15.3 Restore (by Johannes Hell)
2.16	01.03.2015	Stefan Repas	• Arbeitsversion für Review (sonst keine Änderungen)

2.17	05.05.2015	Stefan Repas	• Einarbeitung der Review-Feedbacks von
			  ○ ITSV
			  ○ SVC
			  ○ AUVA
			  ○ ITH icoserve
			  ○ x-tention
			  ○ BRZ
			  ○ KAV-Wien
			  ○ KAGes-Stmk
			  ○ Fraunhofer FOKUS
			• Geänderte der Zugangskontrolle von Z-PI/PDQ (HCP-Assertion erforderlich)

2.20	28.05.2015	Stefan Repas	• Freigegebene Version
2.21	14.07.2015 bis 01.10.2016	Stefan Repas	• Dies ist eine Arbeitsversion/Draft • Referenz auf IHE Revision **12** • Explizite Regeln für KBS im Kapitel 3.14 • Anforderungen bezüglich Suche nach Fachrichtung in GDA-I präzisiert • Alle Texte und Abbildungen dem aktuellen ELGA-Istzustand angepasst • Regeln eingefügt bezüglich Löschen von älteren (> 1Jahr) Kontakten in KBS Kapitel 3.14 • Clearing anhand Abstimmungen mit ITH, NÖ und Tiani ausdefiniert • XAD-PID Link Change Funktion beschrieben • Definition der Bereichsvarianten A und C wurde präzisiert • Verbindliche Einschränkungen bei Verwendung von *NonVersioningUpdate* festgelegt • Neues Kapitel zum Thema Profilierung von ELGA IHE-Transaktionen • Kapitel über Versionierung von Komponenten stark ergänzt • ELGA-Anwendungen mit Interaktionsmuster und dazugehörigen Anwendungsfälle

			• Bearbeitung von offenen Punkten insbesondere mit Rücksicht auf Bilddaten-Erweiterung • ELGA-Proxy Beschreibung eingefügt • VEMO-Beschreibung eingefügt • Service Information Manager und Release Informationen neu definiert
2.30		Stefan Repas	• Freigegebene Version (inhaltlich wie Version 2.21)

8054 *Tabelle 34: Änderungen in tabellarischer Form*

8055 # 26. Reviews

Version	Vorgelegt am	Review und Freigabe durch	Freigegeben am/von Kommentar
2.00	08.01.2013	Martin Hurch	11.01.2013
2.02	22.07.2013	Martin Hurch, Johannes Hell	14.08.2013
2.03	12.09.2013	Martin Hurch, Oliver Kuttin	14.09.2013
2.04	31.04.2014	Martin Hurch, Andrea Klostermann	21.05.2014
2.10	21.05.2014	Martin Hurch	22.05.2014
2.11	04.06.2014	Martin Hurch	12.06.2014
2.12	30.07.2014	Martin Hurch für FOKUS-Review	30.07.2014
2.13	15.09.2014	Martin Hurch für TLB	19.09.2014
2.14	29.09.2014	Martin Hurch für TLB & KAUS	01.10.2014
2.15	26.01.2015	Martin Hurch für BeS	09.02.2015
2.16	09.03.2015	Martin Hurch für Herstellerreview	13.03.2015
2.17	24.04.2015	Martin Hurch für Q-Sicherungsrunde	05.05.2015
2.20	28.05.2015	Martin Hurch	23.06.2015
2.21	12.10.2016	Martin Hurch	Freigabe zum Review an: BRZ, ITSV, SVC, Bereichs-SW Hersteller & Betreiber, Länder: OÖ, K, Stmk
2.30	09.03.2017	Martin Hurch	Freigegeben

8056