Meine elektronische Gesundheitsakte.
Meine Entscheidung!

ELGA GmbH

„ELGA 2.0“ aka elga2

Konzepte zur Weiterentwicklung der ELGA- und eHealth-Zielarchitektur

Datum: 21.03.2023

Version: 1.0

Status: Final

Inhaltsverzeichnis

1 Einleitung

Die eHealth-Welt ist in Bewegung. eHealth-Standards, eHealth-Technologien und eHealth-Großprojekte werden initiiert und vorhandene ausgebaut. Hierfür ist das eHealth-Trends 2022 als Übersicht heranzuziehen.

In dem elga2-Konzept wird eine mögliche ELGA-/eHealth-Gesamtarchitektur (empfohlener Zeithorizont von 5 Jahren), basierend auf aktuellen eHealth-Trends und bereits bekannten Pain-Points des aktuellen Systems [ARK], vorgestellt. Bei der Vision handelt es sich um die Weiterentwicklung der ELGA-Infrastruktur zu einer gemeinsamen Gesundheitstelematik Infrastruktur (GTI).

Die vorgestellte Infrastruktur soll eine „offene“ Plattform ("open-to-the-world“) schaffen, welche die Nutzung von regionalen und nationalen eHealth-Anwendungen ermöglicht. Weiters soll die GTI Digitalisierungs- und eHealth-Bestrebungen der Systempartner unterstützen. Demzufolge wird eine Servicierung von bestehenden Komponenten ("as-a-Service") angestrebt, um eine möglichst serviceorientierte Plattform zu kreieren. Services wie Anbindungsgateway-as-a-Service (AGWaaS), Registry-as-a-Service (REGaaS), Repository-as-a-Service (REPaaS) sollen die Komplexität der derzeitigen ELGA-Gesamtarchitektur vereinfachen und die gemeinsame Nutzung von GTI-Komponenten ermöglichen. Die Bereitstellung dieser Services ist nach Empfehlung der Architekturgruppe [ARK], um die organisatorische Komplexität, die Hand in Hand mit der technischen sowie betrieblichen Komplexität einhergeht, zu reduzieren. Architektur-Themen, welche in der 27. Sitzung der Fachgruppe eHealth hoch priorisiert wurden, sind bereits teilweise im Konzept inbegriffen. Dazu gehören folgende Themen:

- Nutzung der "Plattform-as-a-Service" (PaaS) inkl. der damit einhergehenden technologischen Möglichkeiten zur Reduktion der Betriebskosten und Kapselung von Services
- Bereitstellung einer „AGW-as-a-Service“ zur Optimierung von Betriebsprozessen und damit Reduktion der Aufwände bzw. Komplexität bei den ELGA-Bereichs- und Anwendungsbetreibern.
- Überarbeitung des Kontaktbestätigungsservices zur Reduktion von Clearingaufwänden
- Aufbau einer „Registry-as-a-Service” für ELGA-Bereiche und eHealth-Anwendungen
- Einsatz des CDA-Validators zur Steigerung der Datenqualität

Schwerpunkt des architektonischen Zielbildes ist es, die Eckpunkte von der zukünftigen GTI zu beschreiben und einen Weg zu darzustellen, der die Kompatibilität der existenten

CDA-dokumentbasierten ELGA-Mechanismen mit der möglichen zukünftigen FHIR-basierenden Architektur sicherstellt. Auch die Dualität zwischen zentralen und dezentralen Komponenten soll näher betrachtet werden. Der Vorschlag eines möglichen Zielbildes der ELGA GmbH zielt eben auf diese Dualität, sowohl in Hinblick auf die technischen Schnittstellen als auch auf die semantische Interoperabilität, ab um eine kontinuierliche Betriebsführung zu ermöglichen.

1.1 Ziele

In dem vorliegenden Konzept wird ein Architektur-Zielbild vorgestellt, wie die ELGA-/eHealth-Infrastruktur zukünftig erweitert werden wird. Des Weiteren sind Ergebnisse aus der eHealth Roadmap zukünftig einzubeziehen. Die "Blöcke" in der Gesamtdarstellung sind im nächsten Schritt in Hinblick auf die mögliche Weiterentwicklung zu bewerten und dienen somit primär als Orientierungshilfe.

1.2 Abgrenzung

In der derzeitigen Version ist ein mögliches Architekturbild beschrieben.. Konkrete technische Spezifikationen an die Architektur sind nicht Teil bzw. Fokus dieses Dokumentes. Diese sind erst nach Abstimmung des gemeinsamen Zielbildes zu erarbeiten (in Form von einzelnen Konzepten). Das Erreichen des beschriebenen Zielbildes ist in mehreren Phasen vorgesehen, Näheres dazu ist im Migrationskonzept (noch in einer frühen Arbeitsversion) vorzufinden. Das beschriebene Zielbild kann mithilfe von modularen Erweiterungen an die bestehende Architektur oder durch eine komplette Neuimplementierung erreicht werden.

Kernthema dieses Dokument ist nicht die Sekundärdatennutzung (Zugriffsmöglichkeiten, etc.). Um dieses Thema ist ein separates Dokument vorzusehen und es ist auf Spezifikationen von EHDS abzuwarten.

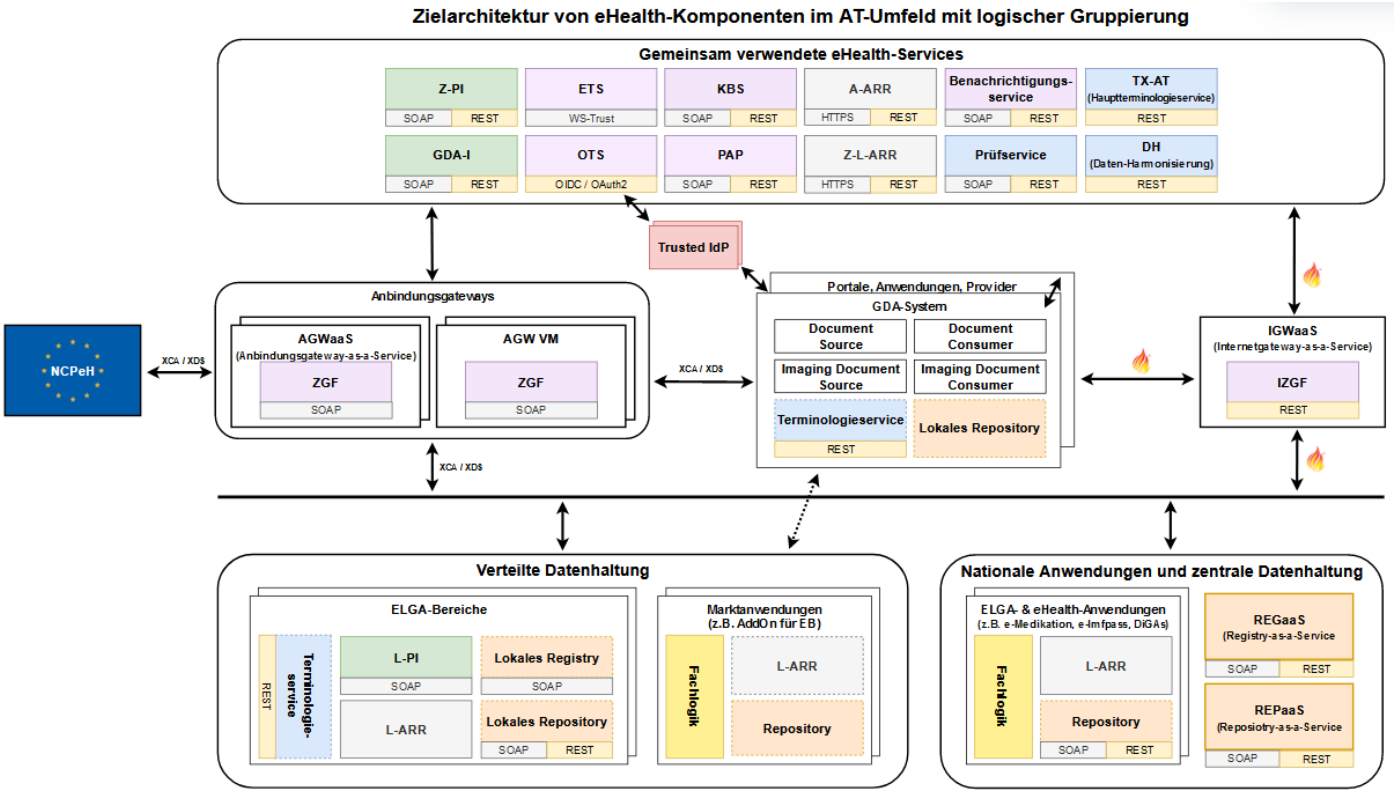
Das kommende Gesundheitstelematikgesetz (GTelG) ist nach Finalisierung entsprechend zu berücksichtigen.

Das technische Verhalten des derzeitigen Systems ist im Wesentlichen in folgenden Dokumentationen beschrieben:

- ELGA Berechtigungssystem / A-ARR Pflichtenhefte für V4.5b
- ELGA Gesamtarchitektur V2.30
- eHealth Gesamtarchitektur V1.2

2 Kontext und Umfang

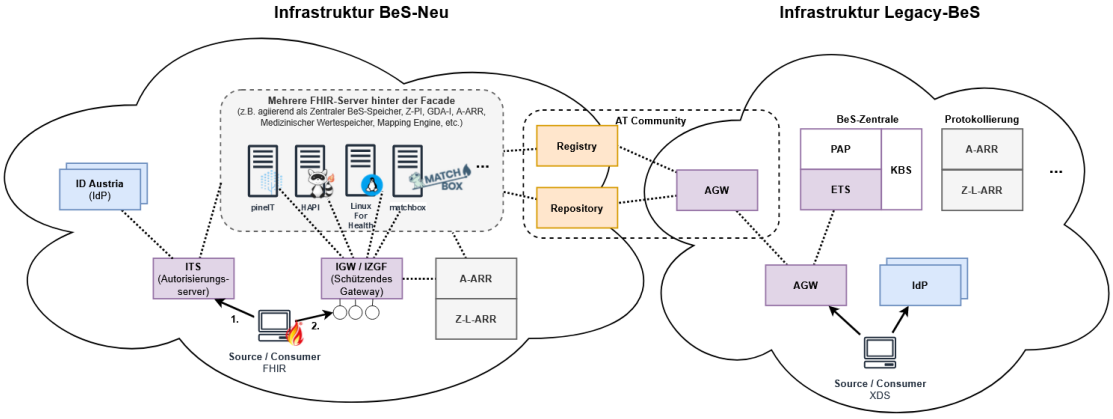
Die nachfolgende Abbildung gibt einen schematischen Überblick der möglichen eHealth-/ELGA-Infrastruktur (aus der Vogelperspektive) und zeigt die Dualität zwischen den SOAP/IHE- und REST/FHIR-Webservices.



Legende:
lila: Berechtigungssystem; grün: Index; orange: Datenhaltung; grau: Protokollierung; blau: Semantische Interoperabilität; gelb: Fachlogik; rot: Identity Provider; strichlierte Linien: optional

Des Weiteren ist im Zielbild direkt eine Servicierung ("as-a-Service") von bestehenden Komponenten zu erkennen. Die Service-Herangehensweise kommt vor allem nach Empfehlung der Architekturgruppe (u.a. für AGW-as-a-Service und Registry-as-a-Service).

Die Dualität der beiden Systeme wird in der folgenden Abbildung noch weiter hervorgehoben:



In der linken Wolke sind die Komponenten des neuen Systems zu sehen. Neue Anwendungen (in der linken Wolke als FHIR-Server eingezeichnet), die auf den neuen Technologien und Systemen basieren, könnten weiterhin über die derzeit etablierten Zugriffswege (rechte Wolke, SOAP/IHE) genutzt werden. Nach einer zu definierenden Zeitspanne soll das alte System (rechte Wolke) kontrolliert außer Betrieb genommen werden. Die Empfehlung der ELGA GmbH und der Architekturgruppe ist es, diese Dualität durch ein „Proof of Concept“-Entwicklungsprojekt nachzuweisen, bevor größere Investitionen getätigt werden.

Die nachfolgende Tabelle schafft einen Überblick der verschiedenen Begriffe aus der Gesamtübersicht. Neue bzw. stark überarbeitete Komponenten werden in Kapitel 5 näher beschrieben.

Begriff	Abkürzung	Beschreibung
Zentraler Patientenindex	Z-PI	Gewährleistet die eindeutige Identifikation von ELGA- und eHealth-Teilnehmer. Der eindeutige Personenschlüssel ist das bPK-GH.
Gesundheitsdiensteanbieter-Index	GDA-I	Dient der eindeutigen Identifikation von ELGA- und eHealth-GDA (sowie OBST) und ermöglicht Abfragen von rollenspezifischen Attributen in ELGA/eHealth
ELGA-Token-Service	ETS	Stellt Authorization-Assertions (SAML Tickets) für ELGA- und eHealth-Benutzer aus, die identitäts-, rollen- sowie weitere

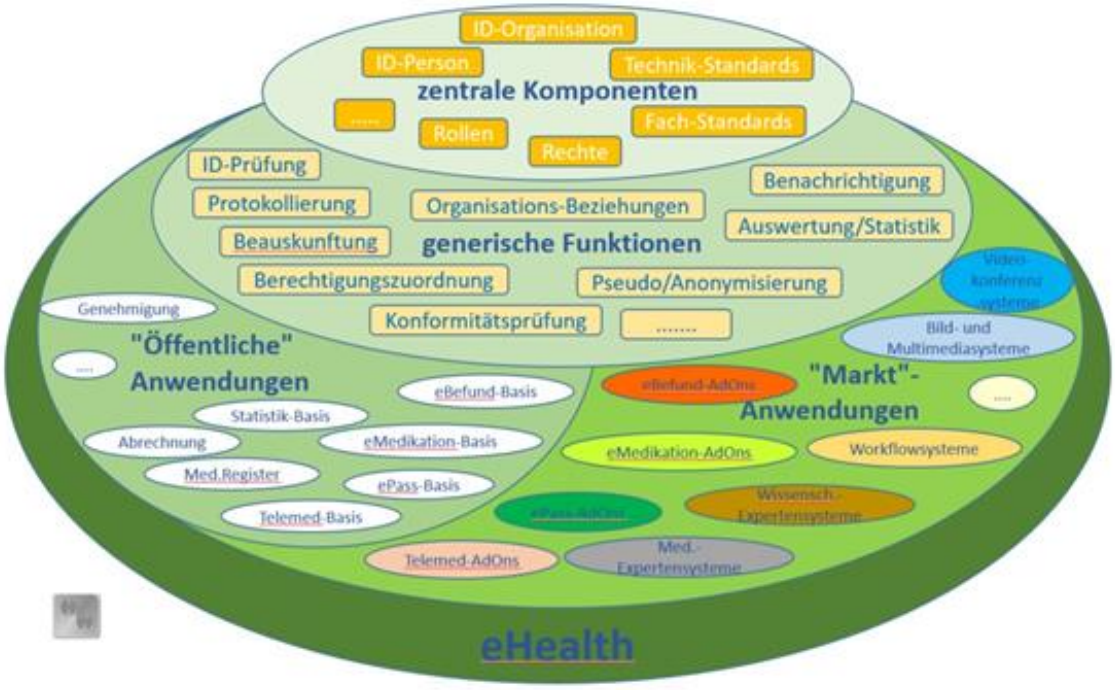
Begriff	Abkürzung	Beschreibung
		autorisierungsbezogene Attribute in einer standardisierten Form elektronisch abbilden
OAuth2 Token Service	OTS	Autorisierungsserver, welcher OAuth2 und OIDC Tokens ausstellt Das Service als Ausbaustufe vom bestehenden Internet Token Service (ITS) zu sehen.
Kontaktbestätigungsservice	KBS	Verwaltet Kontaktbestätigungsmeldungen
Policy Administration Point	PAP	Erlaubt es, die Zugriffsberechtigungen/Policies von ELGA- und eHealth-Benutzer zu speichern und zu warten
Aggregiertes Audit Record Repository	A-ARR	Aggregiert die dezentral anfallenden Protokollnachrichten und sthellt relevante Auszüge für die Anzeigefunktion am ELGA-Portal bereit
Lokale Audit Record Repositories der zentralen Komponenten	Z-L-ARR	Stellt eine zentrale Instanz eines Lokalen Audit Record Repository für alle ELGA-Zentralkomponenten (BeS-seitig) dar. Hier knüpfen beispielsweise auch Services wie die Betriebskennzahlendatenbank an.
FHIR Engine	-	Hierbei handelt es sich um einen FHIR Server, welcher FHIR/REST API für den Austausch von Gesundheitsdaten implementiert. Unterstützt somit die Aufbewahrung von FHIR-Ressourcen (FHIR Store → z.B. für Metadateneinträge, Befunde, Diagnosen, Laborergebnisse etc.) aber auch gewisse FHIR-Operationen. Die FHIR Engine ist als erweiterbar zu sehen und kann somit mit Fachlogik und Adaptern ergänzt werden.
Terminology Exchange Austria (Hauptterminologieservice)	TX-AT	Spezieller FHIR Store nur für Terminologien (CodeSystem, ValueSet, ConceptMap, ...) im österreichischen Gesundheitswesen. Wird

Begriff	Abkürzung	Beschreibung
		benötigt für FHIR Stores mit Ressourcen, die Terminologien verwenden. Wird innerhalb des österreichischen eHealth-Terminologie-Services automatisch befüllt. Über dieses können Stakeholdern des österreichischen Gesundheitswesens eigene Terminologien zusätzlich bereitstellen, siehe https://termgit.elga.gv.at/. Technologisch basiert das österreichische eHealth Terminologie-Service auf TerminoloGit, welches zentralisiert die organisationsübergreifende Terminologie-Arbeit, Terminologie-Recherche, Terminologie-Download in verschiedenen Formaten, usw. ermöglicht (siehe https://termgit.elga.gv.at/arch_and_setup_de.html). Für den dezentralen Einsatz wird TerGi entwickelt.
Terminologieserver	-	Eine vereinfachte lokale Terminologieserver-Instanz (auch unter TerGi bekannt), welche sich in gewissen Intervallen mit einem TerminoloGit-Service oder TerGi-Service synchronisiert.
Daten-Harmonisierungskomponente	DH	Führt CDA- und FHIR-Transformationen durch, anonymisiert ELGA-Daten und wandelt sie ins OMOP Common Data Modell um
Anbindungsgateway	AGW	Wird von den Teilnehmern im Gesundheitsnetzwerk für die Kommunikation mit den Services verwendet
Zugriffsteuerungsfassade	ZGF	Schützt Ressourcen aus dem Gesundheitsnetzwerk und setzt allgemeine und individuelle Berechtigungen um
Internetgateway	IGW	Wird von Teilnehmer im Internet für die Kommunikation mit Services verwendet

Begriff	Abkürzung	Beschreibung
Internet-Zugriffsteuerungsfassade	IZGF	Schützt Internet-Ressourcen und setzt allgemeine und individuelle Berechtigungen um
Lokaler Patientenindex	L-PI	Lokaler Patientenindex, welcher die LPIDs der ELGA-Teilnehmer führt
Lokale Audit Record Repositories	L-ARR	Stellt eine dezentrale Instanz eines Lokalen Audit Record Repository für einen ELGA-Bereich dar
Registry	-	Enthält Metadateneinträge von CDAs
Repository	-	Aufbewahrungsort für CDAs
Anbindungsgateway-as-a-Service	AGWaaS	Gemeinsam genutztes AGW für SOAP/IHE-Clients, welches als Service bereitgestellt werden kann
Internetgateway-as-a-Service	IGWaaS	Internet-Gateway für REST/FHIR-Clients, welches als Service bereitgestellt werden kann
Registry-as-a-Service	REGaaS	Gemeinsam genutztes Verweisregister für ELGA- und eHealth-Metadateneinträge, welches als Service bereitgestellt werden kann
Repository-as-a-Service	REPaaS	Gemeinsam genutzter Aufbewahrungsort (für ELGA- und eHealth-Daten generell), welcher als Service bereitgestellt werden kann.
GDA-System, Portal, Anwendung	GDA-System, EBP, DiGA	Hierbei sind alle Clients zu sehen, auch WIST, OBST und DiGAs (Digitale Gesundheitsanwendungen) beispielsweise Portale sind zu differenzieren: • Gesundheitsportal.at • ELGA-Bürgerportal (EBP) • Länderportale • Private Portale (z.B. Radiologie, HSM-Doku) • etc.

Begriff	Abkürzung	Beschreibung
National Contact Point eHealth Austria	NCPeH-AT	Ein Gateway, das den technisch und semantisch interoperablen Austausch von medizinischen Daten in der EU ermöglicht
Identity Provider	IdP	Komponente des Authentifizierungsprozesses (z.B. ID-Austria). Verifiziert und bestätigt die elektronische Identität eines ELGA-/eHealth-Benutzers mittels elektronisch signierten Tokens
Nationale Anwendung	-	“Zentrale” Anwendung wie z.B. e-Impfpass und e-Medikation. Für diese muss es eine Rechtgrundlage geben.
Fachlogik	-	Fachlogik übernimmt die Transaktionen von der vorgeschalteten AGW/ZGF und bearbeitet diese. Diese übernimmt das „Fachwissen“ und ist für die Inhalte zuständig. Eine Fachlogik kann passiv (responding) oder aktiv-passiv (initiating & responding) agieren. Darüber hinaus sind Workflows als Teil der Fachlogik zu sehen.
Prüfservice	-	Technische Prüfung von ELGA- und eHealth-Befunden, bevor diese eingestellt werden (u.a. mittels CDA-Validator)
Research Stores	-	Ein Aufbewahrungsort für die Verarbeitung/Nutzung von "harmonisierten" anonymisierten/pseudonymisierten Daten für Forschungszwecke. Diese können beispielsweise über REPaaS und REGaaS gehosted werden. Research Stores sind auch unter den Begriffen Micro Data Repositories bzw. Clinical Data Repositories bekannt.

Beim Entwurf des architektonischen Zielbildes wurde das bereits beschlossene Zielbild 2023 berücksichtigt. Das logische Zielbild ist in der nachfolgenden Abbildung zu sehen.



Abgebildete Komponenten wie das Prüfservice, DH, Benachrichtigungsservice, AGWaaS etc. sind nach dem logischen Zielbild als generische (gemeinsam genutzte) Funktionen zu sehen. Weiters zielt die Architektur darauf ab, dass das Andocken von öffentlichen Anwendungen und Marktanwendungen (sprich DiGAs) an die GTI mit den neu zu etablierenden Services wie AGWaaS bzw. IGWaaS und REPaaS ermöglicht bzw. generell vereinfacht werden soll.

3 Lösungsstrategie

Eine Zusammenfassung und Erläuterung der grundlegenden Entscheidungen und Lösungsstrategien, welche die Grundzüge der vorgestellten eHealth-/ELGA-Infrastruktur bestimmen bzw. beeinflussen. Das primäre Ziel ist es mit einer erweiterten Architektur die Verfügbarkeit, Performance, Qualität und Betreibbarkeit von ELGA- und eHealth-Anwendungen (u.a. DiGAs) deutlich zu steigern und gleichzeitig Betriebs- und Entwicklungskosten zu reduzieren (bei mindestens gleichbleibender Sicherheit sowie Datenschutz). Mithilfe der vorgestellten Lösungsstrategien soll ELGA zukunftssicher aufgestellt und in Richtung GTI weiterentwickelt werden.

Die elga2-Weiterentwicklung sieht u.a. folgende Schwerpunkte vor:

Ziel	**Ansatz**
Zugriff auf fein-granuläre Ressourcen/Werte ermöglichen	Medizinische Inhalte neben CDA auch mittels FHIR-Ressourcen abbilden. Verschiedene Herausforderung werden noch auf Standardsseite gelöst (Zugriffe auf Werte und das Zusammenspiel zw. CDA und FHIR)
Gemeinsam verwendete Komponenten bzw. Gesamtarchitektur vereinfachen	Aufteilung des derzeitigen BeS in mehrere Microservices Bei einer Microservices-Architektur werden einzelne generische Anwendungen aus vielen lose aneinander gekoppelten und unabhängig voneinander einsetzbaren kleineren Services zusammengesetzt. Servicierung von bestehenden Komponenten ("as-a-Service") → Verteilte Komponenten, welche die gleichen Geschäftsfälle unterstützen, sollen gemeinsam verwendet werden (z.B. AGWaaS, REGaaS und REPaaS). Die Aufteilung der aggregierten Protokollierung ist zu überdenken (z.B. beim Umstieg auf AGWaaS bzw. auf IGW).
Wesentliche Verkürzung der Release-Zyklen & Innovationszyklen für neue Anwendungen	Implementierung von Micro-Service SW-Architektur (u.a. das BeS)
Betriebsaufwand reduzieren und Betreibbarkeit vereinfachen	Umstieg auf eine PaaS Umgebung und ihre Vorteile nutzen (→ führt u.a. zur einfacheren Etablierung von

Ziel	Ansatz
	Kollaborationsplattformen / Umgebungen, CI/CD Pipeline etc.)
Abhängigkeiten für Entwicklung auflösen	Open-Source Lösungen für zukünftige Neuentwicklungen, damit verschiedene Softwarehersteller beauftragt werden können Gemeinsamen Entwicklungskasten mit Systempartnern schaffen (→Programmcode im ELGA Besitz, Entwicklung von verschiedenen Partnern, Referenz-Implementierungen)
Bestehende GDA-Systeme unterstützen	Abwärtskompatibilität hinsichtlich bestehender Daten (CDAs sowie administrative Daten) und Schnittstellen (SOAP) Migrationspfad bereitstellen
Anbindungen von DiGAs und weiteren Clients an eHealth-Infrastruktur vereinfachen	REST/FHIR-Protokoll für effiziente, rasche und kostengünstige Anbindungen (→ "developer friendly") Demzufolge IZGF erweitern, um Anbindungen mittels REST/FHIR zu ermöglichen Mobile Zugänge über das Internet schaffen (abseits vom Gesundheitsnetz)
Übergreifende Suche vereinfachen	Vereinfachung mittels gemeinsamen Suche-Index (zentrale statt verteilte Abfrage)
Qualitätssicherung der Infrastrukturkomponenten (u.a. IdP, Web-Portale) und GDA-Systeme	End-2-End-Test, Connectaton, Projectathon, Zertifizierung

Ausgangssituation von der derzeitigen Architektur:

- Steigende Komplexität führt zu höheren Betriebs- und Wartungskosten
- Hohe Durchlaufzeiten und lange Produkt Release-Zyklen
- Verteilte XDS-Architektur und verschiedene Berechtigungsregimen (regionale Anwendungsfälle können schwer über ein zentrales Berechtigungssystem gesteuert werden)
- Die langfristige vertragliche Bindung an einen dedizierten SW-Hersteller (Beispiel ELGA-BeS)
- Keine Möglichkeit Daten nach Anonymisierung/Pseudonymisierung freizugeben
- Dokumente als kleinste Informationseinheit

- Zugriff primär über geschlossene Gesundheitsnetzwerke
- Keine einfache Anbindung von DiGAs zu ELGA möglich (derzeit nur über IZGF/ITS mit MHD)
- Prototyping und MVP-Zyklus mit der derzeitigen Architektur (aus ELGA GmbH Sicht) nicht möglich (u.a. Changes werden zu langsam umgesetzt, kein Zugriff auf Source Code)

Zu erwartende Herausforderungen bei der Etablierung einer überarbeiteten Architektur:

- Migrationspfad bereitstellen mit maximaler Stabilität für vorhandene Services und Etablierung neuer Services
- Paradigmenwechsel von CDA-Dokumenten auf einzelne FHIR-Ressourcen und weiterführend auf OMOP (Entwicklungen seitens EHDS dazu sind zu berücksichtigen)
- Gegebene technische Grundlagen für die Anbindung von DiGAs
- ELGA-Daten entsprechend den gesetzlichen Vorgaben für Forschung öffnen (Anonymisierung für Statistiken bzw. Pseudonymisierung für Forschung)
- Verschlüsselungskonzept berücksichtigen
- Harmonisierung von ELGA-Bereichen (neben den Komponenten und Schnittstellen sind die internen Prozesse, z.B. SOO & KBS-Fallartwechsel, bestmöglich zu vereinfachen)

Annahmen, welche einen Einfluss auf die Konzeption der erweiterten eHealth-Architektur haben:

- Der Betrieb von einzelnen ELGA Komponenten wird auf PaaS umgestellt
  - 2022 wird das Zentrale BeS (inkl. A-ARR) in die PaaS migriert
  - 2023 werden manche der dezentralen AGWs in die PaaS migriert (zumindest BRZ-seitig)
- REST/FHIR-Schnittstellen werden immer beliebter bei Entwicklern und werden laufend in neuen Gesundheitsanwendungen adaptiert
- CDAs werden auch in der Zukunft weiterhin relevant bleiben und nicht unmittelbar durch FHIR ersetzt
- Im österreichischen Gesundheitswesen verfügen nicht alle Clients über eine Internetverbindung (z.B. manche Krankenhäuser sind nur über Gesundheitsnetzwerke angebunden)
- Immer mehr Portale und Third-Party Apps (u.a. von Smartphones und Smartwatches) beinhalten hilfreiche Behandlungsdaten

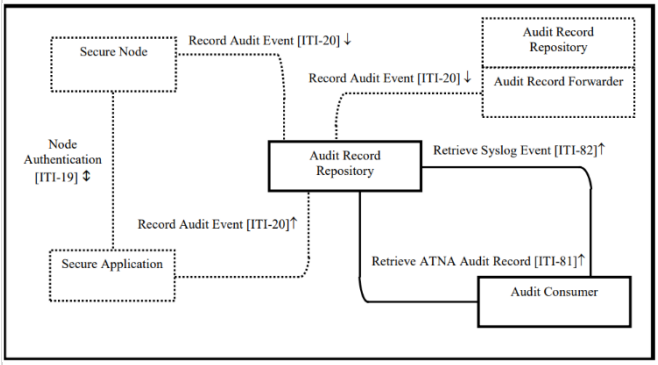
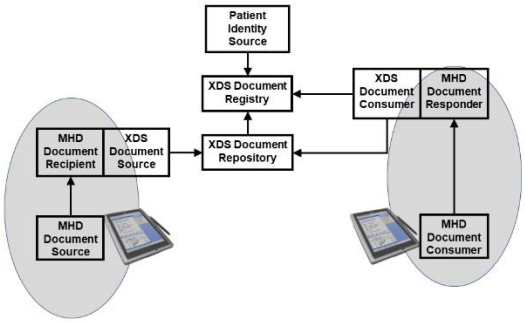
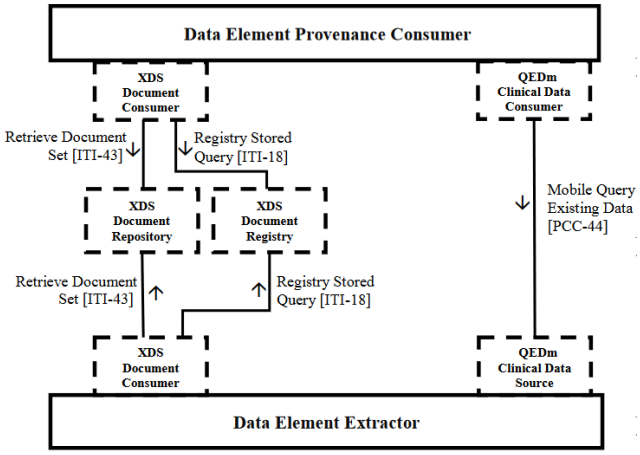
4 Technologien und Standards

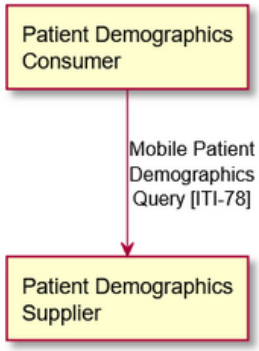
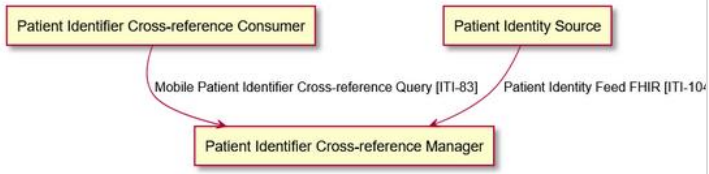
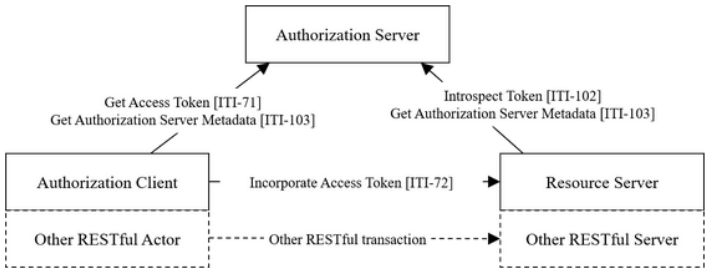
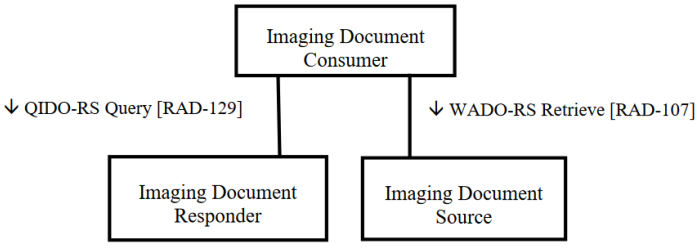
Die aktuellen eHealth-Trends (in Bezug auf eHealth-Standards, eHealth-Technologien und eHealth-Großprojekte) wurden bereits in eHealth-Trends 2022 näher erläutert. In dieser Sektion werden Technologien und Standards sowie IHE-Profile aufgelistet, welche für die Umsetzung der erweiterten eHealth-Architektur in Betracht gezogen werden sollen. Diese Auflistung ist als rein informativ (und nicht als vollständig) zu sehen. Details sind dem SetOfStandards (SoS) zu entnehmen. Nicht alle hier genannten Technologien und Standards sind zwingend erforderlich für die Umsetzung der skizierten Ziel-Architektur. Das Ziel ist, dass bereits vorhandene Lösungen (in Form von verfügbaren Produkten bzw. in Form von etablierten Standards und Technologien), welche sich im Markt erfolgreich durchgesetzt haben, verwendet werden. Demzufolge ist jedoch anzumerken, dass es nicht die Erwartungshaltung geben darf, dass ein bereits vorhandenes Produkt out-of-the-box die spezifischen Anforderungen der ELGA-Architektur und Anwendungsfälle erfüllen wird.

Auflistung von möglichen Technologien und Standards für die Etablierung der erweiterten eHealth-Infrastruktur:

Technologie / Standard	**Anwendung**
HL7 FHIR	Abbildung von medizinischen und administrativen Informationen in einer fein-granularen und standardisierten Form (u.a. mittels Ressourcen)
REST	http-Protokoll mit den bekannten Anfragemethoden (PUT, POST, GET, DELETE, etc.) → FHIR API basiert auf REST
OHDSI OMOP CDM	Standardisierte Ausgangsbasis für ein mögliches Persistenz-Schema (Fokus auf Verarbeitung medizinischer Daten zu Forschungszwecken)
OAuth2	Industrie-Standard Protokoll für Autorisierung im www
OIDC	Authentifizierungsschicht, die auf OAuth2 basiert (ID Austria ist beispielsweise ein OIDC-IdP-Provider)
HEART	Health Relationship Trust Profile for OAuth 2.0

Zusätzlich werden relevante IHE-Profile gelistet, welche im Zuge der zu erweiternden Infrastruktur zu analysieren sind:

IHE-Profil	Anwendung	Grafische Übersicht
REST ATNA	Erweitert die Funktionalitäten des ATNA-Profils durch die Einführung von REST-Operationen und das HL7 FHIR Datenformat, die für die Übermittlung und den Abruf von Audit-Datensätzen verwendet werden können	
MHD	Hauptsächlich um mobile Clients mittels REST-Requests an bestehende XDS/XCA-Infrastrukturen anzubinden (bereits mit IZGF/ITS eingesetzt)	
QEDm	Unterstützt dynamische Abfragen für klinische Datenelemente (Ressourcen)	
mXDE	Bietet die Möglichkeit, auf Datenelemente zuzugreifen, die aus gemeinsam genutzten strukturierten	

IHE-Profil	Anwendung	Grafische Übersicht
	Dokumenten extrahiert wurden	
PDQm	Definiert eine leichtgewichtige REST-Schnittstelle zu einem Anbieter von demografischen Patientendaten	
PIXm	Definiert eine leichtgewichtige REST-Schnittstelle zu einem Patient Identifier Cross-Reference Manager	
IUA	Übermittelt Benutzeridentität, Attribute und Berechtigungen an einen REST-Dienst, um die Durchsetzung von Sicherheits- und Vertraulichkeitsrichtlinien zu ermöglichen	
WIA	Definiert Methoden für den Austausch von Bildern und die interaktive Betrachtung von Bildgebungsstudien unter Verwendung von RESTful-Diensten wie WADO-RS und QIDO-RS.	

Diese Liste ist nicht vollständig und die laufenden IHE-Profile werden beobachtet (d.h. z.B. ob diese implementiert und umgesetzt werden), siehe https://wiki.ihe.net/index.php/Profiles.

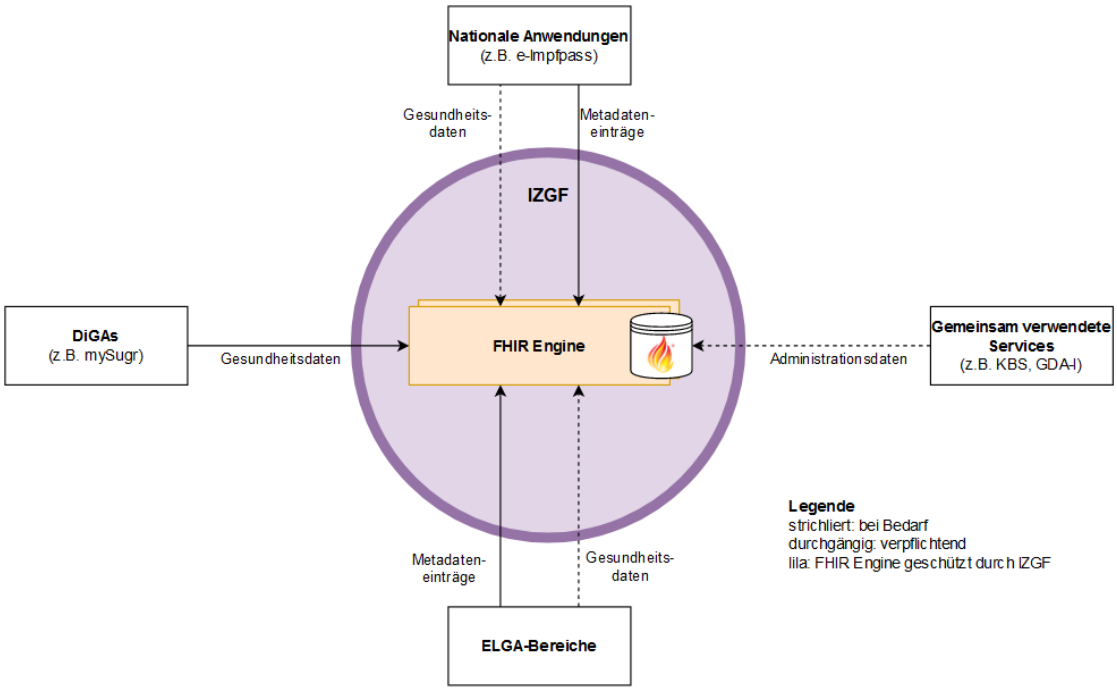
5 Komponenten der erweiterten eHealth-/ELGA-Gesamtarchitektur

In den nachfolgenden Sektionen werden neu zu etablierende bzw. stark zu überarbeitende Services beschrieben, welche für die Erweiterung der eHealth-Architektur eine große Bedeutung haben. Nach Abstimmung und Finalisierung des Zielbildes ist für jede einzelne Komponente zukünftig ein eigenes Konzept mit genaueren Details (u.a. technische Architekturbeschreibung, Anforderungen etc.) vorzusehen. Schlussendlich wird in dieser Sektion versucht, die Grundzüge der erweiterten eHealth-/ELGA-Gesamtarchitektur zu beschreiben. Die Authentifizierungsmöglichkeiten von eGovernment (u.a. ID Austria) werden berücksichtigt.

5.1 Gemeinsam verwendete FHIR Engines agierend als Registry und Repository

Eine essenzielle Rolle in der zukünftigen eHealth-Architektur sollen ELGA/eHealth FHIR-Engines übernehmen (in IHE-Profilen als Resource Server definiert), welche gemeinsam von allen GDA-Systemen verwendet werden können. Hierbei handelt es sich um FHIR-Server, welche eine Ressourcen-basierte Speicherung ermöglichen müssen und die FHIR/REST APIs implementieren. Die FHIR-Engines unterstützen FHIR-Operationen und sind als erweiterbar zu sehen und können somit mit Fachlogik und Adaptern ergänzt werden. Die grundlegenden Gedanken sind, dass diese FHIR Engines u.a. im Zuge folgender Services einzusetzen sind: Registry-as-a-Service und Repository-as-a-Service. An dieser Stelle ist anzumerken, dass die Funktionalitäten theoretisch auch mithilfe eines einzigen, mandantenfähigen FHIR-Servers angeboten werden könnten. Demzufolge würde eine FHIR-Engine gleichzeitig als gemeinsam genutzte Registry und Repository fungieren. Die techn. Optionen des Datenmanagements sind vorallem auch den Blickwinkeln des Datenschutz und des Betriebes (IT-Sicherheit, SLA) zu betrachten. Eine Multi-Domain FHIR-Architektur (kaskadierende FHIR-Server) ist jedenfalls zu unterstützen.

Schematische Darstellung des Datenstroms in Richtung gemeinsam verwendete FHIR Engines:



Grundsätzlich müssen FHIR Engines vom BeS geschützt werden. Daher sind Zugriffe auf die FHIR Engines nur über die AGW bzw. IGW (vorgeschaltete Zugriffsteuerungsfassaden → Policy Enforcement) zu ermöglichen. Ein direkter Zugriff auf FHIR Engines darf nicht gestattet sein.

5.1.1 Registry-as-a-Service

Eine wesentliche Rolle in der erweiterten eHealth-Infrastruktur soll zukünftig ein gemeinsames Register übernehmen, welches als Service angeboten werden soll (→ Registry-as-a-Service, REGaaS). Beim Register handelt es sich in weiterer Folge um eine FHIR Engine, welche die CDA-Metadaten (Metadaten von e-Befunde, e-Medikation, e-Impfpass etc.) mittels FHIR-Ressourcen (DocumentReference-Ressourcen) abbilden und Ressourcen-orientierte (FHIR) Anfragen (für den Abruf von Metadaten) unterstützen würde. Demzufolge können in der finalen Ausbaustufe des gemeinsamen Registers die vorhandenen Metadaten von allen verfügbaren ELGA-Dokumenten (inkl. e-Impfpass) zu einem Patienten (Anm.: Policies sind zu berücksichtigen) anhand einer einzigen HTTP GET Abfrage. Dies wäre als Alternative zu den bestehenden SOAP Query-Transaktionen für e-Befunde, e-Medikation etc. zu sehen. Die XCA-Query-Abfrage von eHealth-/ELGA-Anwendungen muss somit zukünftig nicht mehr separat getriggert werden. Auf Basis der Inhalte aus den abgerufenen Ressourcen würden im nächsten Schritt alle CDAs weiterhin lokal von den

ELGA-Bereichen bzw. von den zentralen Anwendungen (u.a. e-Medikation und e-Impfpass) angefordert werden.

Hinweis:
Es sind weitere Überlegungen notwendig, wie das Register mit Ressourcen aus REPaaS umgehen soll und wie diese bei zukünftigen Suchanfragen miteinbezogen werden sollen (z.B. nur Composition-Ressourcen, etc.).

Eine gemeinsame Registry war eine Maßnahme aus dem Evaluierungsbericht zur Reduzierung der Komplexität der ELGA-Architektur (siehe Pain-Point 2.11 von [ARG]), der Erreichung der notwendigen SLA des Gesamt-Systems sowie der Steigerung der Performance der Such-Anfragen. Ein zentrales Verweisregister (XDS Registry) ist gleichzusetzen mit der Migration und der Zusammenführung der derzeit verteilten ELGA-Bereiche (sowie "eHealth-Bereiche", z.B. e-Impfpass) in eine gemeinsame, österreichweite XDS Affinity Domain mit verteilten Datenspeichern. Ein gemeinsam verwendetes Verweisregister lässt sich prinzipiell entweder durch intrusive, bzw. direkte Maßnahmen errichten, oder schleichend (non intrusiv) im Hintergrund. Die unterschiedlichen Maßnahmen (intrusive vs. schleichend) werden im Migrationskonzept genauer beschrieben.

Da es sich bei REGaaS um eine FHIR Engine handelt, wird diese bereits vom Anfang an mit entsprechenden FHIR-Schnittstellen ausgestattet sein (für den Abruf von Metadaten). Darüber hinaus werden SOAP-Clients anhand eines zusätzlichen SOAP/IHE-Adapters mit der zentralen (gemeinsam verwendeten) Registry kommunizieren können. Dieser Adapter würde die klassischen SOAP/IHE-Anfragen und die Responses von der FHIR Engine entsprechend umwandeln. Das zentrale Verweisregister hat damit zwei unterschiedliche Zugänge. Einmal die klassische SOAP/IHE-Schnittstelle und darüber hinaus auch eine FHIR/REST-Schnittstelle. Für das Mapping der Metadaten von FHIR-Ressourcen auf XDS DocumentEntry ist das bereits implementierte Mapping in der IZGF (als Grundlage wurde das IHE MHD Profil eingesetzt) als Ausgangsbasis heranzuziehen.

Des Weiteren sind bei der Errichtung der REGaaS Sicherheitsaspekte und die Zugriffssteuerung zu berücksichtigen. Zum Beispiel sind manche Metadaten-Einträge nicht für alle Rollen (bzw. GDAs) lesbar (z.B. dürfen nur e-Impfpass Metadaten-Einträge an Amtsärzte übermittelt werden) und müssen daher (mithilfe von s.g. Security-Labels beispielsweise) rausgefiltert werden. Gewisse Berechtigungsinformationen sind der Fachlogik zu übergeben.

Mit einer zentralen Registry würden sich u.a. folgende Vorteile anbieten:

- Vereinfachung der ELGA-Architektur (→ keine Notwendigkeit für dezentrale Registries und ZGF-Caches)
- Reduktion von Transaktionen (d.h. es entfällt in der letzten Ausbaustufe die Notwendigkeit von verteilten Registry Stored Query Operation, Reduktion von PIX-Anfragen an Z-PI, etc. → ermöglicht somit schnellere Suchanfragen)
- Steigerung der Verfügbarkeit von Best Effort bis zur Hochverfügbarkeit
- Schnellere Verfügbarkeit (d.h. schnellere Abfragen nach vorhandenen Dokumenten z.B.)
- Verbessertes Informationsmanagement über den Patientenpfad hinweg (mit einer Abfrage alle Metadaten abholen)
- Rasche Bereitstellung von neuen eHealth-Anwendungen (→ wichtiges Element in der Anbindung von DiGAs und weiteren ELGA- und eHealth-Anwendungen)

REGaaS führt infolgedessen zur Erhöhung der Effizienz und der Stabilität des Gesamtsystems, mit einer mittelfristigen Kostenreduktion des Betriebes.

Informativ:
Im Jahr 2021 hat die Architekturgruppe die Anzahl der Transaktionen und Systemübergänge (Netzwerk Hops) für ausgewählte Aktionen mittels einem Werkzeug darstellen lassen [ARG]. Für die exemplarische Darstellung wurde der Dokumentenabruf (eine Standardaktion) ausgewählt. Der Dokumentenabruf (Dokumente in 3 Bereichen vorhanden) führte zu insgesamt 112 Transaktionen und 25 Systemübergänge. Eine Realisierung des REGaaS in Kombination mit REPaaS würde die Anzahl der internen Transaktionen und Systemübergänge dramatisch reduzieren, da die dezentrale Komplexität wegfallen würde (PIX-Anfragen an Z-PI, verteilte Dokumente etc.).

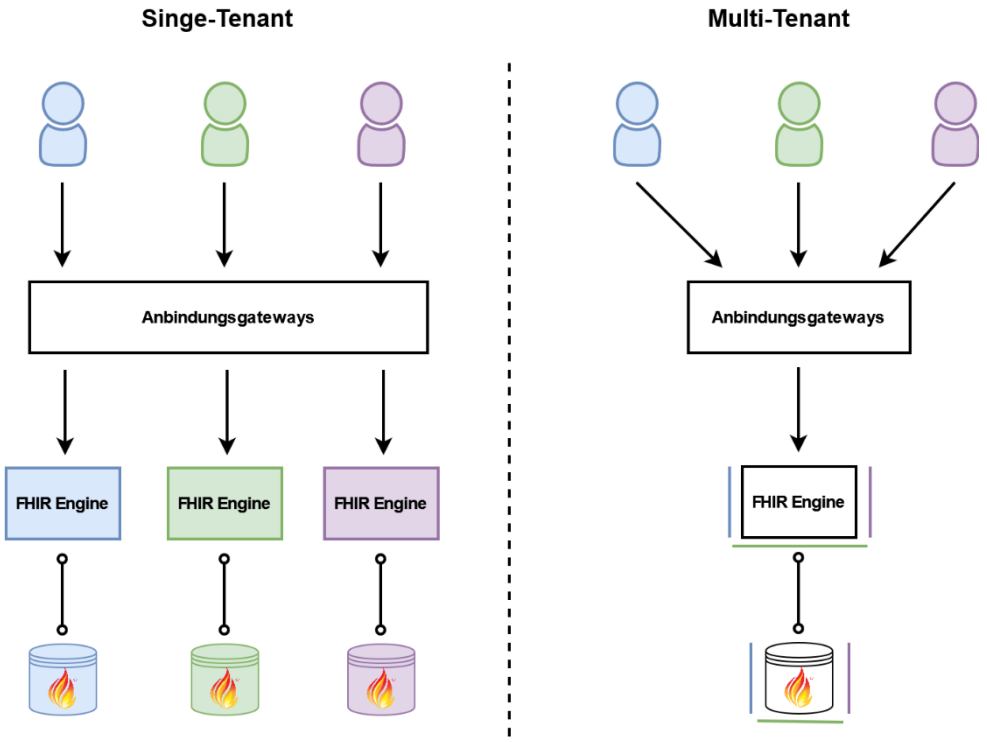
5.1.2 Repository-as-a-Service

Mit REPaaS soll ELGA-Bereichen sowie generell allen Clients (vor allem DiGAs) die Möglichkeit optional gegeben werden, ihre Dokumente (v.a. CDAs) bzw. ihre Gesundheitsdaten (-> FHIR-Ressourcen) auf einer zentralen (gemeinsam verwendeten) ELGA/eHealth FHIR Engine zu persistieren. Dies ist als zusätzliches Service zu sehen - die ELGA-Bereiche werden ihre regionalen Daten nach wie vor dezentral in ihren Repositories verwalten können.

Der Grundgedanke dieses Services ist, dass in der ersten Phase CDA-Dokumente als Ganzes auf die FHIR Engine gespeichert werden (mittels Binary- bzw. Bundle-Ressourcen). Eine komplette Abbildung mittels FHIR (sprich das Dokument wird mittels mehrerer einzelner Ressourcen abgebildet → Composition-Ressource mit Verweise auf

die einzelne Ressourcen) kann erst erfolgen, nachdem die DH-Komponente eine Umwandlung von CDA auf FHIR verlustfrei durchführen kann. Wie anfangs erwähnt, kann REPaaS auch für die Aufbewahrung von Daten aus regionalen und nationalen Anwendungen bzw. DiGAs (mHealth-Daten aus Wearables und Smartphones) genutzt werden.

Anwendungen (u.a. DiGAs), welche ihre Daten im FHIR Store hosten, können anfangs nur auf ihre eigenen Daten lesend bzw. schreibend zugreifen. Demzufolge ist ein wichtiger Aspekt der FHIR-Engine die Mandantenfähigkeit ("Multi-Tenant", siehe z.B. https://hapifhir.io/hapi-fhir/docs/server_plain/multitenancy.html), die Gruppen von Nutzern bedienen kann, ohne dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung und Ähnliches haben. Bürger werden jedoch die Möglichkeit haben, den Apps Zugriff auf weitere Daten aus dem FHIR Store zu gewähren. Die nachfolgende Abbildung stellt den Unterschied zw. Single-Tenant und Multi-Tenant grafisch dar.



Weiters wäre es auch möglich (bei Bedarf), dass in die FHIR Engine administrative Daten aus zentralen Services (z.B. Z-PI, GDA-I, A-ARR, PAP und KBS) gespeichert bzw. gespiegelt werden (in Form von Patient-, Organization-, AuditEvent-, Consent-, Encounter-Ressourcen, etc.). Des Weiteren sind die aktuellen Serviceänderung rund um das Aufkündigen der SAP-ISH (Ende 2027) zu berücksichtigen. In dem Zusammenhang sind Änderungen betreffend KA-ORG vorzusehen.

Clients werden weiters die Option haben, granulare Daten (z.B. spezifische Werte aus vorhandenen FHIR-Ressourcen) mithilfe von FHIR-Operations oder FHIRPath zu extrahieren. Darüber hinaus können diverse Default FHIR-Operations (siehe https://www.hl7.org/fhir/operationslist.html) angeboten werden. Der Abruf von allen Ressourcen eines Patienten kann beispielsweise als Default FHIR-Operation verstanden werden. Es könnten auch zusätzliche Operationen definiert werden, wie z.B. zum Generieren eines Patient Summaries (auf Basis von nur strukturierten Inhalten).

Mit einem zentralen Repository würden sich u.a. folgende Vorteile anbieten:

- Vereinfachung der ELGA-Architektur für eine raschere Bereitstellung von einem sicheren Datenspeicher für eHealth.Anwendungen (→ wichtiges Element in der Anbindung von DIGAs und weiteren ELGA- und eHealth-Anwendungen, da die Daten zentral gehostet werden könnten)
- Steigerung der Verfügbarkeit bis zur Hochverfügbarkeit (z.B. weniger Abhängigkeit von dezentralen Repositories)
- Komponente für die Migration von Daten zw. ELGA-Bereichen (z.B. beim Zusammenlegen von Bereichen, nachdem einer deaktiviert wird → das Repository würde somit zusätzlich auch für den Export und Import von Gesundheitsdaten genutzt werden)
- Datenspeicher für Daten, die ggf. der Bürger bereitstellen will (-> Hinterlegung eines Benutzer-Profils)

Informativ:

Für die verlustfreie Umwandlung von ELGA-CDA auf FHIR und zurück muss zuerst ein Logisches Modell von dem österreichischen CDA-Schema in FHIR abgebildet werden, weiters muss der Allgemeine CDA Implementierungsleitfaden überarbeitet werden, um eine Dualität zu ermöglichen und letztendlich wird jeder spezielle ELGA Implementierungsleitfaden angepasst werden auf den neuen allgemeinen Implementierungsleitaden. Diese neuen ELGA Implementierungsleitfäden definieren CDA wie auch FHIR, und lassen dem Implementierer die Möglichkeit, eines der beiden Standards mit all den Vor- und Nachteilen für denselben Inhalt zu implementieren.
Damit Third-Party Apps die zentrale FHIR Engine nutzen können, sind gewisse Voraussetzungen zu erfüllen. Dafür ist weiters ein spezieller ELGA Leitfaden für DiGAs zu definieren, welche möglicherweise keine CDA-Abbildung führen kann. Für die wird es mindestens notwendig sein, dass diese mit dem österreichischen HL7 FHIR Core-Implementierungsleitfaden konform sind.
Alle Ressourcen der REGaaS sind verpflichtend mit Security Labels (siehe https://www.hl7.org/fhir/security-labels.html) zu versehen, damit das BeS mithilfe der Labels Berechtigungsentscheidungen treffen kann.

5.2 Erweitertes Berechtigungssystem für bestehende Clients und für native FHIR-Clients

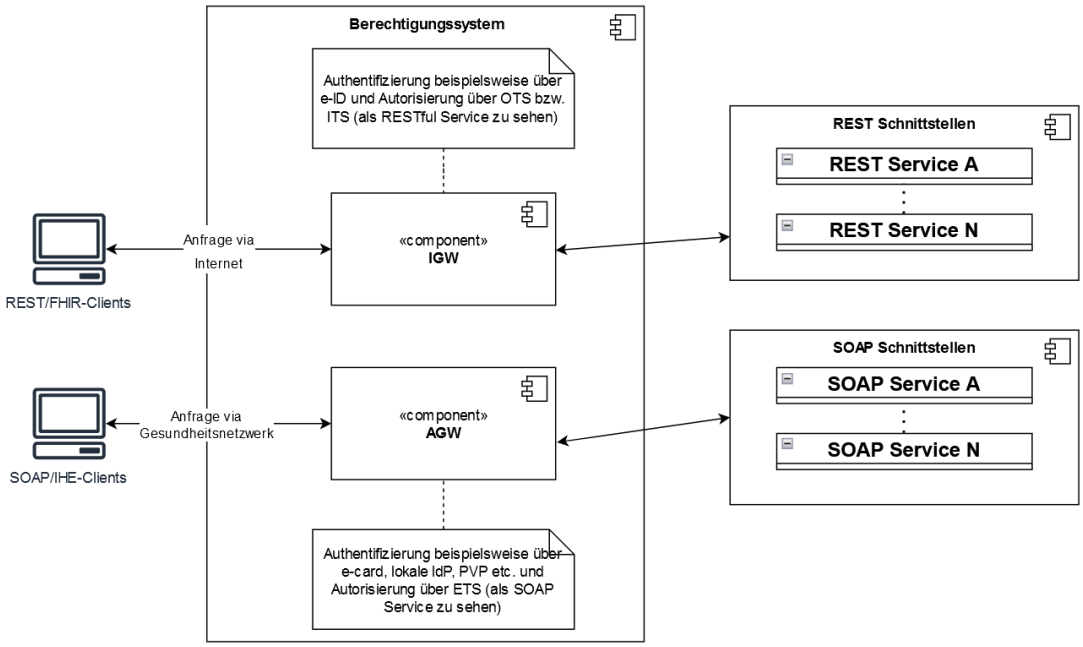
Basierend auf dem vorgestellten Zielbild muss für eine noch zu definierende Zeitspanne die ELGA-/ eHealth-Gesamtarchitektur weiterhin in der Lage sein SOAP zu unterstützen. Darüber hinaus müssen zukünftig REST/FHIR-Clients ("native FHIR") zusätzlich unterstützt werden. Daher muss das gesamte ELGA-BeS in der Lage sein mit beiden Protokollen (SAML und OAuth2/OIDC) umzugehen und Berechtigungen entsprechend umzusetzen bzw. zu exekutieren. Die vorgestellte Architektur sieht vor, dass SOAP-Clients über eine zentrale (gemeinsam verwendete) AGW mit den bestehenden Services kommunizieren (→ AGWaaS) und FHIR-Clients kommunizieren ausschließlich über das Internetgateway (IGW) mit den Services. Demzufolge ist das IGW ebenfalls als ein zentrales Service zu sehen (→ IGWaaS). Es wird angenommen, dass im Kernbereich (abgeschottete eHealth Netzwerke) weiterhin via SOAP und WS-Trust Protokolle kommuniziert wird. REST- und OIDC-Protokolle sind hingegen für die Kommunikation im Internet vorzusehen. In dem Konzept wird davon ausgegangen, dass es in der Zukunft zu einer Reduzierung der Anzahl von dezentralen AGWs/ZGFs führen wird. Eine IGW kann auch im abgeschotteten Gesundheitsnetzwerk aufgestellt werden. Voraussetzung ist, dass zumindest ein IdP OAuth2/OIDC im Gesundheitsnetzwerk unterstützt. Derzeit ist ID-Austria der einzige OAuth2/OIDC IdP und ist nur über das Internet erreichbar.

Es ist hinzuweisen, dass eine erste Version des "Internet-BeS" im Rahmen des e-Impfpasses bereits realisiert wurde und kann als Ausgangsbasis für Erweiterungen herangezogen werden. Dieses wurde im Zuge der mobilen Immunisierungseintragung (e-Impfdoc) entwickelt und besteht im Wesentlichen aus den Komponenten ITS (fungiert als Open ID Connect Authorization Server) und IZGF (überprüft die vom Client eingebetteten JWT-Tokens und leitet Anfragen Richtung MHD-Komponente, welche die REST Business-Transaktionen auf SOAP IHE bzw. WS Trust übersetzt). Die derzeitige IZGF-Implementierung ist für eine "native FHIR" Kommunikation weiterzuentwickeln. Schlussendlich wurden mit dem bestehenden Internet-BeS die grundlegenden Hauptfunktionalitäten (für Authentifizierung und Autorisierung) bereits erfolgreich erprobt. Demzufolge kann das "native FHIR BeS" aufbauend auf das bereits vorhandene Fundament (IZGF und ITS) realisiert werden. Eine nähere Architekturbeschreibung zu IZGF und ITS (sowie Beschreibung zu notwendigen Adaptierungen) ist in [EHA] vorzufinden.

Für die Etablierung der erweiterten eHealth-Infrastruktur ist zusätzlich ein geringfügiger Umbau und eine Weiterentwicklung von bestehenden Kernkomponenten des BeS vorzusehen, indem die zentralen Komponenten des BeS mit FHIR/REST-Schnittstellen

ausgestattet werden. Das Ziel ist, dass die IGW mit der bestehenden Infrastruktur kommuniziert, indem die REST/FHIR-Schnittstellen von den einzelnen Komponenten angesprochen werden. Es ist anzumerken, dass jegliche aus dem Internet kommende FHIR-Anfragen auch natürlich über die MHD-Brücke geleitet werden könnten, dies ist jedoch nicht wünschenswert. Über die SOAP- und REST/FHIR-Schnittstellen muss jedenfalls auf die gleichen Daten zugegriffen werden können.

Die nachfolgende Abbildung stellt Anfragen Richtung erweitertes BeS sehr vereinfacht dar:



Darüber hinaus sind erprobte Konzepte aus dem bestehenden BeS zu analysieren, ob diese auch für das Internet-BeS eingesetzt werden können. Als Beispiel sind die Application Container (AC) zu nennen, welche eine leichte Anbindung von Anwendungen/Fachlogiken ermöglichen, indem über Konfiguration Endpunkte sowie Basis-Einstellungen (berechtigte GDAs, erlaubte Transaktionen, OptIn-Modell, etc.) eingestellt werden können.

5.2.1 BeS-Komponenten für SOAP/IHE-Clients

Informativ:
Unter BeS-Komponenten für SOAP/IHE-Clients sind KBS, PAP, ETS, A-ARR, Z-L-ARR, AGW/ZGF und das zu etablierende AGWaaS zu verstehen.

Wie bereits in der Einleitung angeschnitten, ist das BeS derzeit monolithisch (im Sinne von funktional miteinander verstricktem und abhängigem Quellcode) aufgebaut. Das

heißt, dass BeS-Services wie KBS, PAP, etc. aus der BeS-Zentrale aufzubrechen sind, damit sie ihre Dienste autark und ohne gegenseitige Abhängigkeiten erfüllen und als Microservices in einer PaaS agieren können. Für das Splitting der Services aus der derzeitigen BeS-Zentrale ist Quellcode-Refactoring nötig. Das hat den Vorteil, dass BeS-Erweiterungen besser lokalisiert und einzelne Services unabhängig voneinander aufgefrischt (installiert) werden können. Auf diese Weise würden Release-Zyklen dramatisch gekürzt und vereinfacht werden.

Das ETS ist jedenfalls nicht für REST (bzw. OIDC/OAuth2) zu verwenden, da dieses weiterhin nur von SOAP-Clients (für die Ausstellung von Assertions) einzusetzen ist. Für die Ausstellung von Tokens im Internet wird analog dazu das OTS bzw. ITS verwendet. Des Weiteren sind BeS-Services, welche für GDA-/Bürger-Anwendungsfälle relevant sind, mit REST/FHIR-Schnittstellen auszustatten, damit Client/GDA-Systeme REST kommunizieren können. Alternativ können die BeS-Kernkomponenten für das FHIR-BeS von Anfang an als komplett neue Service implementiert werden, anstatt dass die bereits vorhandenen Komponenten mit zusätzlichen Schnittstellen ausgestattet werden. Wichtig ist, dass in beiden Fällen auf den gleichen Datenbestand zugegriffen wird.

Eine essenzielle Rolle für SOAP/IHE-Clients soll in der erweiterten Architektur das AGWaaS übernehmen. Nähere Details dazu sind in der nachfolgenden Sektion zu finden.

5.2.1.1 Anbindungsgateway-as-a-Service

Unter AGW-as-Service (AGWaaS) ist eine zentrale AGW zu verstehen, welche von SOAP/IHE-Clients für den Zugriff auf die ELGA-/eHealth-Infrastruktur verwendet werden soll. Mit dieser sollen die derzeit dezentral verteilten AGWs harmonisiert werden. Demzufolge ist die Idee, dass zukünftig alle SOAP/IHE-Clients über die AGWaaS mit dem eHealth-Gesamtsystem kommunizieren (anstatt über die dezentral liegenden AGWs).

AGWaaS wurde entsprechend den Bemühungen zur Reduzierung der Komplexität der derzeitigen ELGA- und eHealth-Architektur eingeleitet. Die Einführung der AGWaaS führt konsequent zu einer erwünschten Ziel-Architektur, welche lokal betriebene AGW (als virtuelle Maschinen) nicht mehr erfordern würde. Den ELGA-Bereichen (darunter sind auch die bereits vorhandenen ELGA- und eHealth-Anwendungen zu sehen, da sie als XDS Affinity Domains aufgestellt sind) würde somit eine Möglichkeit bereitgestellt werden, lokale AGWs auszulagern. Aktuell sind über 200 AGWs auf mehrere Instanzen (über diverse Test-Umgebungen) im Einsatz. Daraus ergibt sich dementsprechend eine hohe Komplexität und ein hoher Ressourcenbedarf für Wartung und Test (vor allem für die ELGA-Bereiche).

Derzeit existieren drei unterschiedliche AGW-Arten, die zwar alle Quellcode-Ident sind, jedoch per Konfiguration unterschiedlichen Anforderungen dienen:

1. **Initiating AGWs:** Eine Reihe der AGWs bedient sich ausschließlich des initiierenden ZGF-Teils. Diese AGWs schützen keine lokalen Daten oder Services. Folgende AGWs gehören zu dieser Subgruppe:
    a. EBP
    b. WIST
    c. ROZ
2. **Responding AGWs:** Diese Gruppe von AGWs bietet lediglich vorgeschaltete antwortende (passiven) Fassaden für den Schutz von Anwendungen und Daten an:
    a. e-Medikation
    b. e-Impfpass
3. **Initiating & responding AGWs:** In den ELGA-Bereichen werden derzeit Standard (STD) AGWs betrieben, welche sowohl einen initiierenden wie auch einen antwortenden ZGF-Teil aufgeschaltet haben.

AGWaaS würde bestenfalls alle drei AGW-Arten in eine einzige Instanz zusammenfassen. Es wird empfohlen, AGWaaS stufenweise aufzubauen. Im ersten Schritt für AGWaaS würden nur die initiating AGWs und responding AGWs (Punkt 1 und 2 oben) zentralisiert werden, da diese weniger Komplexität aufweisen. Im letzten Ausbauschritt würden die Bereichs-AGWs harmonisiert werden.

<u>Mit einer gemeinsamen AGW würden sich folgende Vorteile anbieten:</u>

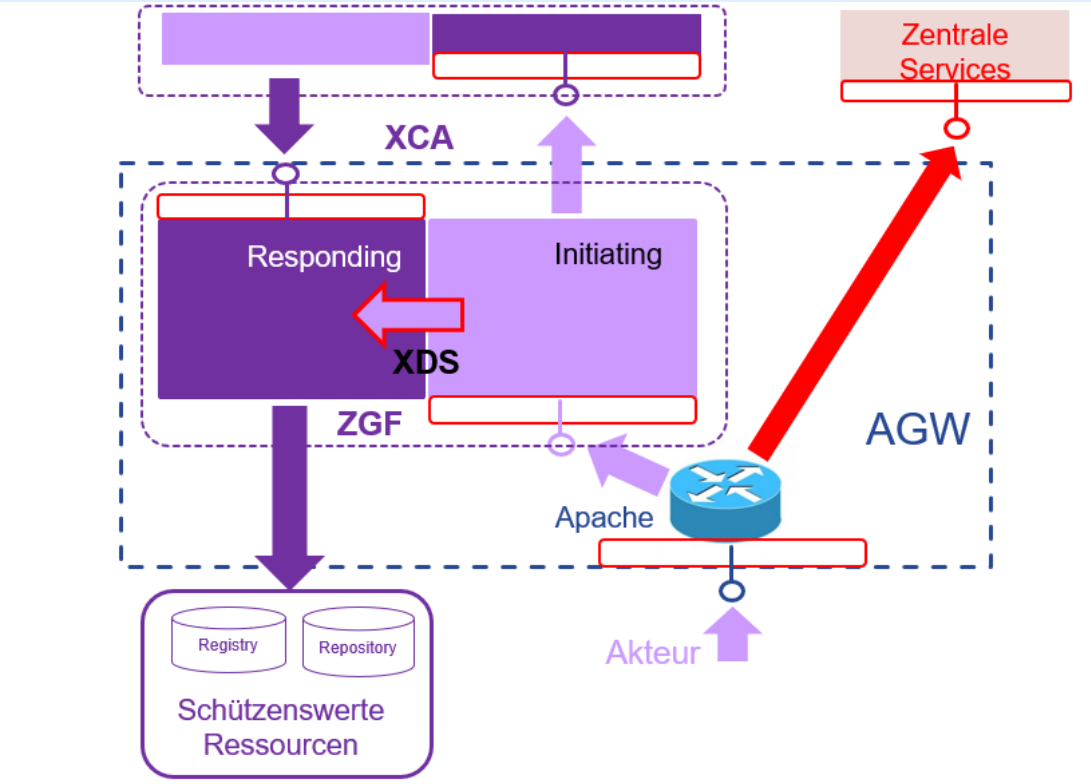
- Vereinfachung der ELGA-Architektur (→ keine Notwendigkeit für dezentrale AGWs)
- Steigerung der Verfügbarkeit von Best Effort bis zur Hochverfügbarkeit
- Reduktion der Aufwände bei den ELGA-Bereichs- und Anwendungsbetreibern (Monitoring etc.)
- Durch die Zentralisierung reduzieren sich auch die Netzwerkstrecken und es gibt Vereinfachungen im Zertifikatsmanagement

<u>Mit einer gemeinsamen AGW sind folgende Nachteile zu berücksichtigen / zu Kenntnis zu nehmen:</u>

- Zusätzliche Hops zu erwarten und keine Point-to-point Kommunikation: Die Vorteile der AGW-to-AGW Kommunikation sind gleichzeitig auch die Nachteile jeglicher Service Cloud-Lösung. Insbesondere bei der Übertragung von großen Datenmengen mit erhöhten Bandbreitenbedarf (DICOM-Objekte) ist eine direkte Point-to-Point Verbindung von Source zum Konsumenten ausgesprochen vorteilhaft. In einer Cloud-Lösung (AGWaaS) müssen die zur Übertragung bestimmten Dateien zuerst in die Cloud geladen werden und erst danach ist überhaupt möglich diese zum Consumer weitertransportieren. Diese Überlegung stellt das Konzept von AGWaaS zumindest für bestimmte

Anwendungsfälle in Frage. Insbesondere im Falle der Bereichs-AGW, wo die abzuholenden Dateien verteilt, in den lokalen Repositorien vorliegen.

Informativ:



Zum besseren Verständnis werden hier die einzelnen Bestandteile einer AGW erklärt. In der nachfolgenden Abbildung ist ersichtlich, dass die AGW prinzipiell aus einem Apachen und einer ZGF aufgebaut ist. Die Apache-Komponente dient lediglich als Drehscheibe, indem entgegengenommene Anfragen entweder an den zentralen Services (KBS, ETS, PAP, Z-PI, etc.) oder an die ZGF weiterleitet werden. Die ZGF selbst ist zweigeteilt, bestehend aus einem initiierenden und einem antwortenden Bestandteil.

Diskussionspunkt

Auch denkbar, dass nur die Initiating und die Responding AGWs als AGWaaS bereitgestellt werden → STD könnten unverändert beibehalten werden (bzw. bei Bedarf in der PaaS betrieben werden)

5.2.2 BeS-Komponenten für REST/FHIR-Clients

Informativ:
Unter BeS-Komponenten für REST/FHIR-Clients sind IZGF (in Form von IGWaaS) und OTS bzw. ITS zu verstehen.

5.2.2.1 Internet Token Service bzw. OAuth2 Token Service

In der derzeitigen eHealth-Architektur existiert bereits ein Autorisierungsserver auf Basis von OpenID Connect, nämlich das ITS. In diesem Dokument wird dieser Dienst teilweise auch als OTS bezeichnet. Im Kern ist ein Autorisierungsserver einfach eine Komponente zum Ausstellen von OpenID Connect- bzw. OAuth 2.0-Tokens (u.a. Access Token und Refresh Token). Das ITS ist als das ETS des Internet-BeS zu sehen. Das ITS wurde bereits für die Unterstützung von der mobilen Immunisierungserfassung (e-Impfdoc) umgesetzt. Der Autorisierungsprozess beginnt mit einer anonymen Anfrage an den entsprechenden Endpunkt des ITS-Autorisierungsservers (→ Code-Flow). Neben ID Austria sind auch weitere Authentifizierungsprovider (z.B. GINS: Gesundheits-Informations-Netz-Service) in Betracht zu ziehen.

Der Autorisierungsserver wird verwendet, um rollenbezogene Berechtigungen und generelle Zugriffsrichtlinien (Policies vom PAP) durchzusetzen und im Access Token einzubetten. Das BeS für die REST/FHIR-Clients soll somit Benutzern weiterhin Rechte über Policies und Rollen gewähren. An dieser Stelle ist anzumerken, dass weitere Überlegungen notwendig sind, ob ITS nur generelle Policies (u.a. entsprechende Rolle) durchsetzen soll und das IZGF im nächsten Schritt die individuellen Policies (z.B. GDA-Sperre, Opt-Out, etc.) sowie Kontaktüberprüfung durchsetzen soll. Theoretisch wäre es möglich, wenn das ITS die zweite Überprüfung (individuelle Policies und Kontakt) ebenfalls durchführt, hierzu sind jedoch zusätzliche Analysen notwendig.

Bei der Erweiterung dieser Komponente sind zusätzlich Weiterentwicklungen des SMART Standard zu beobachten. Es ist jedoch anzumerken, dass die ELGA- und eHealth-Anwendungsfälle mit SMART nicht abdeckbar sind. In SMART sind aber beispielsweise Basis Scopes definiert (z.B. Patient/Observation.*, damit eine App Observations für Bürger schreiben/lesen darf), welche auch im ELGA-Kontext eingesetzt werden können. Des Weiteren sind mit Scopes lediglich die Rechte des Clients / der App allgemein abgebildet.

Nähere Details zur ITS Komponente sind [EHA] zu entnehmen. In der folgenden Sektion ist eine Definition von IGWaaS zu finden.

5.2.2.2 Internet-Zugriffssteuerungsfassade

Wie das ITS wurde auch die IZGF bereits für die Unterstützung von der mobilen Immunisierungserfassung (e-Impfdoc) umgesetzt. Demzufolge ist das IZGF entsprechend zu erweitern, dass alle Business-Transaktionen, auch über das REST-Protokoll durchgeführt werden können. Business-Transaktionen betreffend das Dokumentenmanagement werden in der derzeitigen Lösung nur für e-Impfpass unterstützt und das IZGF dient primär als Übersetzungskomponente zw. REST auf SOAP IHE (→ MHD). Die IZGF setzt individuelle Berechtigungen/Policies (z.B. GDA-Sperre, Ausblenden von spez. Docs) durch und übernimmt die Kontaktüberprüfung, bei REST/FHIR Business-Transaktionen betreffend das Dokumentenmanagement. Schlussendlich ist die Policy Enforcement Point (PEP) Komponente hier eher vorzusehen als im ITS. Bei PEP handelt es sich um eine logische Komponente, welche die individuellen Berechtigungsregeln (u.a. individuelle Policies und Kontaktüberprüfung) exekutiert und direkt durchsetzt (Allow oder Deny Entscheidung).

Die IZGF ist als ein Teil der IGW zu sehen. Darüber hinaus muss die IGW als API-Gateway für "native FHIR" Anfragen dienen und Logging-Funktionalitäten (u.a. für Problemanalysen und -lösungen) inkludieren. API-Aufrufe von Client-Anwendungen sollen somit von der IGW entgegengenommen werden und REST Business-Transaktionen sind an das entsprechende Service weiterzuleiten. Abhängig vom angesprochenen Endpunkt wird dementsprechend der Service Kontext (z.B. zu einer FHIR Engine) abgebildet. Die sicherheitsrelevanten Aufgaben im Kontext OAuth2 werden jedoch von der IZGF übernommen. Diese schützt dahinterliegende Ressourcen und Services.

Diskussionspunkt

Security Labels in Ressourcen sind vorzusehen, jedoch sind diese aufgrund der Performance nicht direkt bei der Abfrage zu überprüfen bzw. durchzusetzen.

Das IGW ist als zentrale AGW zu sehen, wie das zu etablierende AGWaaS, welches für die Harmonisierung der dezentralen AGWs dienen soll. Demzufolge wird eine zentrale AGW für SOAP/IHE-Clients (im Gesundheitsnetzwerk) angeboten und eine zweite für REST/FHIR-Clients (im Internet).

Nähere Details zur IZGF sind von [EHA] zu entnehmen.

5.3

5.3 Umwandlungskomponente für die Daten-Harmonisierung

Die Daten-Harmonisierungskomponente (DH) ist für das Mapping zwischen CDA und FHIR vorgesehen, kann aber auch für weitere Zwecke (z.B. für die Pseudonymisierung und Anonymisierung von ELGA-Daten) eingesetzt werden. Infolgedessen übernimmt die DH-Komponente die Rolle der Mapping Engine.

5.3.1 Umwandlungen zwischen CDA und FHIR

In erster Linie soll diese Komponente für die Umwandlung von medizinischen Daten zw. CDA und FHIR verwendet werden (z.B. CDA-Dokument als ClinicalDocument bzw. Bundle Ressource abbilden, oder über Composition-Ressource mit Verweisen auf einzelne granulare Ressourcen). Anhand dieser Komponente wird den Clients die Möglichkeit gegeben werden, Transformationen zw. CDA und FHIR durchzuführen. Die Komponente soll eingesetzt werden, sobald Clients CDAs über die SOAP-Schnittstelle der FHIR Engine einbringen wollen. Auf diese Weise werden CDAs ins FHIR-Format umgewandelt, bevor sie in die FHIR Engine persistiert werden. Bei dem Abruf von CDA-Dokumenten über die FHIR Engine wird die Komponente ebenfalls eingesetzt, damit die FHIR-Dokumente ins CDA-Format überführt werden, bevor sie an Clients retourniert werden.

Hinweis:
An dieser Stelle ist hinzuweisen, dass eine Migration von CDA auf FHIR in Österreich grundsätzlich möglich sein sollte, würde aber eine Adaptierung des Allgemeinen CDA Implementierungsleitfadens voraussetzen, damit Unterschiede zw. den Standards abgeglichen werden (unterschiedlicher Umgang mit nullFlavors etc.) und eine verlustfreie Umwandlung ermöglicht wird.

5.3.2 Pseudonymisierung und Anonymisierung für Secondary Use & Datenauswertungen

Mit der derzeitigen Architektur besteht keine Möglichkeit Daten nach Anonymisierung/Pseudonymisierung freizugeben. Um medizinische und ggf. auch administrative Daten aus dem Routine-Betrieb für weitere Datenauswertungszwecke zur Verfügung zu stellen, wird ausgehend von current best-practices vorgesehen diese in eine separate Analyse-Datenbank ("Research Stores", nicht in der Gesamtübersicht abgebildet), die als standardisiertes Datenbank-Schema das *Common Data Model* (CDM) der *Observational Medical Outcomes Partnership* (OMOP) Initiative nutzt, zu überführen. Grundsätzlich ist vorzusehen, dass alle Daten in der Analyse-Datenbank

anonymisiert (z.B. für Statistiken) und pseudonymisiert (z.B. für tatsächliche Forschung) vorgehalten werden. Demzufolge können produktive Daten über die DH-Komponente pseudonymisiert bzw. anonymisiert werden, damit diese für Forschungszwecke genutzt werden können. Die Research Stores können von berechtigten Forschungsanwender ausgewertet und analysiert werden. Je Forschungszweck ist ein eigener Research Store vorzusehen.

Im Wesentlichen umfasst die Datenharmonisierung von CDAs und FHIR-Ressourcen in die Analyse-Datenbank folgende Verarbeitungsschritte:

1. strukturelle und inhaltliche Validierung
2. Validierung der korrekten Patienten-Referenz innerhalb der Ressourcen
3. Pseudonymisierung/Anonymisierung von Ressourcen Id's und Patienten Id's sowie aller Referenzen zwischen den Ressourcen. Im Falle von CDA betrifft dies Id's der sections und entries
4. "Date-shifting" als weitere Sicherheitsmaßnahme, Preserving temporal relations in clinical data while maintaining privacy" (Hripcsak, 2016b)
5. Übernahme spezifischer CDA/FHIR-Ressourcen Inhalte in die OMOP-Tabellen via XPath/FHIR-Path whitelist-Filtern
    a. OMOP unterstützt die Terminologien SNOMED-CT, LOINC und RxNorm. Dementsprechend sind codable concepts von CDA/FHIR-Ressourcen auf diese Standard-Terminologien zu mappen. Im Kontext der Weiterverarbeitung auf nationaler Ebene können die OMOP Terminologien um weitere, in Österreich standardisierte und verwendete Terminologien ergänzt werden. Ein Terminologie-Mapping ist nur erfolgreich, wenn eine 1:1 Relation besteht. Ambiguitäten führen zu Fehlern und müssen anhand der Logdateien durch Domänen-Experten reviewed werden.

Diskussionspunkt

Die Analyse-Datenbank ermöglicht Forschern die explorative Datenanalyse und Datenauswertung. Sofern die Analyse ergibt, dass für eine spezifische Forschungsfrage geeignete Daten vorliegen, werden diese aus der Analyse-Datenbank in eine eigene virtuelle Maschine (VM) transferiert. Diese VM steht dem anfragenden Forscher über einen Web-Browser für alle weiteren detaillierten Analysen zur Verfügung. Damit wird der Ansatz "bring the analysis to the data, not the data to the analysis" verfolgt.

5.3.3 Extrahierung von FHIR-Ressourcen aus ELGA-CDAs

Die DH-Komponente kann bei Bedarf weiter ausgebaut werden, um FHIR-Ressourcen (z.B. AllergyIntolerance, Condition, Observation, etc.) aus ELGA-CDAs zu extrahieren und würde infolgedessen die Rolle eines "Data Element Extractors" (basierend auf das IHE mXDE-Profil) übernehmen. Darüber hinaus werden Links zu den Quell-Dokumenten

in Form von Provenance-Ressourcen erstellt. Über die Verlinkung wird der klinische Gesamtkontext geliefert, in welchem das extrahierte Datenelement aufgezeichnet wurde. Das Mapping muss auf der Grundlage des spezifischen CDA-Dokumentinhalts und der verwalteten Datenelemente manuell erstellt werden. Es existiert kein allgemeingültiges Mapping, welches die Extraktion von allen CDA-Typen unterstützt. Demzufolge sind für die Umsetzung des mXDE-Profils hohe Mappingaufwände zu erwarten und es würde voraussetzen, dass alle CDAs einen "Level 3" Strukturierungsgrad aufweisen.

5.3.4 Software assembled Patient Summaries

Mithilfe der DH-Komponente könnten zusätzlich Patient Summaries automatisch (software assembled) generiert werden. In https://gitlab.com/elga-gmbh/partner-projekte/elga2ips bzw. https://ebooks.iospress.nl/volumearticle/59476 wurde bereits prototypisch ein exekutierbares Mapping (mittels FHIR Mapping Language) für die Generierung von International Patient Summaries (IPS) im FHIR Format (als Bundle Ressource) aus ELGA-Daten etabliert. Bei IPS handelt es sich um die HL7 Spezifikation eines Patient Summaries, welche für den grenzüberschreitenden Datenaustausch vorgesehen ist. Des Weiteren kann ein solches Mapping auch für das ELGA Patient Summary erstellt werden (vorausgesetzt es existiert ein normativer Implementierungsleitfaden dazu). Es ist anzumerken, dass das ELGA Patient Summary auf Basis des IPS-Leitfadens erstellt wurde und infolgedessen eine ähnliche Struktur aufweist.

Im Gegensatz zur software assembled Variante können Patient Summaries auch natürlich von GDAs (human assembled) erstellt werden. Dieser Ansatz würde aber langfristig mehr Kosten verursachen (u.a. aufgrund zusätzlicher GDA Aufwände) und sollte daher nicht in Betracht gezogen. Patient Summaries können abschließend auch hybrid erstellt werden. Hierbei wird das Patient Summary automatisch erstellt und infolgedessen von einem GDA vervollständigt. Eine hybride bzw. software assembled Variante würde unter das Medizinproduktegesetz fallen.

Folgende Herausforderung und Rahmenbedingungen sind zu berücksichtigen, falls eine automatisierte Generierung eines Patient Summaries in ELGA (über die DH-Komponente) tatsächlich implementiert werden würde:

- Das Patient Summary muss immer On-Demand generiert werden, da GDAs unterschiedliche Berechtigungen haben (Amtsarzt darf z.B. kein Zugriff auf abgeleitete Inhalte aus e-Befunde haben).
    - Bei dem software assembled Ansatz müsste ein Verweis auf die verwendeten ELGA CDAs/Ressourcen gesetzt werden.

    - Für die automatisierte Generierung sind explizit Level 3 ELGA CDAs/Ressourcen zu verwenden.
- Im IPS Kontext sind ggf. unterschiedliche Terminologien zu berücksichtigen (ELGA vs. IPS).

5.4 Prüfservice für Qualitätssicherung von Gesundheitsdaten

Das Prüfservice ist vorgesehen für die Prüfung von ELGA- und eHealth-Befunden, bevor diese eingestellt werden (u.a. Schema/Schematron-Konformität und Metadaten-Check). Dieses Service würde demnach jedes Dokument vor dem Einstellen prüfen. Bei dem Prüfservice handelt es sich um einen CDA bzw. FHIR Validator, welcher von der FHIR Engine angeboten wird.

5.5 Vereinfachung der Bereichskomponenten

Verteilte Komponenten, welche die gleichen Geschäftsfälle unterstützen, sollen zukünftig gemeinsam verwendet werden (z.B. AGWaaS, REGaaS und REPaaS). Daher sind zukünftig lokale AGWs und ELGA-Registries nicht mehr zwingend als Teil des Zielbildes zu sehen. Registries für eHealth-Zwecke können nichtsdestotrotz weiterhin lokal beibehalten werden (→ Entscheidung ist jedem Bereich überlassen). Auch lokale ELGA-Repositories können optional weitergeführt werden können.

5.6 Weitere Anforderungen

Weitere Themen bzw. Anforderungen, welche in der 27. Sitzung der Fachgruppe eHealth hoch priorisiert wurden:

- Herstellung der Netzneutralität auch unter Verwendung des Internets
- Überarbeitung des Kontaktbestätigungsservices zur Reduktion von Clearingaufwänden
- Umsetzen von Streaming zur Übertragung großer Datenmengen, insb. Bilddaten
- Einsetzen eines Z-PI Cachings zur Reduktion des Transaktionszeiten und Entlastung des Z-PI
- Aktivierung der Kompression bei der Datenübertragung zwischen AGWs zur Reduktion der notwendigen Netzwerkbandbreite
- Workflowunterstützung
- Umsetzung von National Contact Point eHealth (NCPeH) für den sicheren grenzüberschreitenden Datenaustausch

Zusätzlich sind Themen wie Asynchrone Protokollierung ("Fire & Forget Prinzip") und Benachrichtigungsservice im Zuge der Neukonzeption zu berücksichtigen.

6 Migration

In einem separaten Migrationskonzept sind bereits erste Überlegungen enthalten, welche Schritte notwendig sind, um zentrale (gemeinsam verwendete) FHIR Engines in Form von REGaaS und REPaaS sowie AGWaaS in der eHealth-Infrastruktur zu etablieren.

7 Referenzen

[ARK] Robert Feitscher. HMP Ergebnisdokumentation. 2021.

[EHA] ELGA GmbH. eHealth Gesamtarchitektur. 2022.

[EHT] ELGA GmbH. eHealth Trends. 2022.

[EMK] ELGA GmbH. elga2 Migrationskonzept. 2022.

8 Reviews

Version	Vorgelegt am	Review durch	Freigegeben am/von Kommentar
v0.1		Architekturgruppe	
V0.9		Architekturgruppe	

9 Ansprechpartner (Projektteam)

Name	Rolle	Organisation	E-Mail
Alexander Dimitrov	Architekt	ELGA GmbH	Alexander.Dimitrov@elga.gv.at
Stefan Repas	Architekt	ELGA GmbH	Stefan.Repas@elga.gv.at
Nikola Tanjga	Architekt	ELGA GmbH	Nikola.Tanjga@elga.gv.at
Peter Breyer	Architekt	ELGA GmbH	Peter.Breyer@elga.gv.at
Oliver Kuttin	Architekt	ELGA GmbH	Oliver.Kuttin@elga.gv.at
Andreas Schuler	Architekt	ELGA GmbH	Andreas.Schuler@elga.gv.at