ELGA GmbH

Anbindung von DICOM Ressourcen in ELGA

Architektur des bereichsübergreifenden Austauschs von Bilddaten

Datum: 04.09.2023

Version: 2.00f

Inhaltsverzeichnis

1. Architektur des bereichsübergreifenden Bilddatenaustauschs in ELGA

1.1. Einleitung

Entsprechend der Begriffsbestimmungen in der aktuellen Fassung des ELGA-Gesetzes §2.9a sind ELGA-Gesundheitsdaten personenbezogene Daten, die zur weiteren Behandlung von ELGA-Teilnehmer/inne/n wesentlich sein könnten. Diese umfassen unter anderem „medizinische Dokumente einschließlich allfälliger Bilddaten in standardisierter Form". Dementsprechend müssen neben medizinischen Befunden im standardisierten Format der *HL7® Clinical Document Architecture® Rel.2* („CDA")[1] auch Bilddaten in einem geeigneten Standardformat in ELGA bereitgestellt werden. Die Wahl eines geeigneten Standardformats für Bilder wird einerseits durch die gängige radiologische Praxis, und andererseits durch den aktuellen Stand der technologischen Entwicklung beeinflusst. Demnach muss sich das technische Lösungsdesign für den Bilddatenaustausch in ELGA streng an den in unserem Gesundheitssystem vorhandenen und etablierten Lösungen (siehe hierfür DICOM & DICOMweb) orientieren. Üblicher Praxis folgend werden digitale Bilddaten, die im Rahmen bildgebender Verfahren (Digitales Röntgen, CT, PET, MRT etc.) entstehen, in eigens dafür vorgesehenen Systemen, sogenannten *Picture Archiving and Communication Systems* (PACS) verwaltet. Zur Persistenz und zum Austausch der Bilder kommt dabei primär der internationale Standard DICOM[2] (*Digital Imaging and Communications in Medicine,* ISO 12052) zum Einsatz. Auf diesen Systemen aufbauend wird in ELGA eine entsprechende Infrastruktur realisiert, die ausschließlich das Registrieren/Bereitstellen von Verweisen auf Bilddaten sowie das Auffinden und Herunterladen von in den lokalen PACS oder anderen adäquaten Speichersystemen verfügbaren Bilddaten ermöglicht. Aufgaben der Bildgenerierung, -speicherung, und -bearbeitung werden in ELGA nicht unterstützt, sondern müssen weiterhin durch die bewährten PACS, Bildarchivierungs-Systeme und radiologischen Geräte adressiert werden. Darüber hinaus werden Themen wie die Unterstützung von Imaging-Workflows oder gerichtete Kommunikation als Nicht-Ziele festgelegt.

[1] HL7® and CDA® are the registered trademarks of Health Level Seven International and the use does not constitute endorsement by HL7.

[2] DICOM® is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information. DICOM® is recognized by the International Organization for Standardization as the ISO 12052 standard.

1.2. Häufig verwendete Abkürzungen

ACS	Access Control System
AGW	Anbindungsgateway, eine Virtuelle Maschine
A-ARR	Aggregate Audit Record Repository (zentrale ELGA Komponente)
A²R²	Alternativbezeichnung von A-ARR
BeS	ELGA-Berechtigungssystem, erweitert um eHealth-Funktionalitäten
CDA	Clinical Document Architecture® (HL7 Standard)
DICOM	Digital Imaging and Communications in Medicine (DICOM®)
EBP	ELGA-Bürgerportal
ETS	ELGA Token Service (zentrale ELGA Komponente)
FHIR	Fast Healthcare Interoperability Resources (HL7 Standard)
GDA	Gesundheitsdiensteanbieter
HEX-I	eHealth eXchange of Images (ein Projekt zwischen Wien und der Vinzenzgruppe)
IDC	Imaging Document Consumer
IdP	Identity Provider
IDS	Imaging Document Source
IHE	Integrating the Healthcare Enterprise (internationale Initiative und Regelwerk)
ITI	IT Infrastructure (zur Bezeichnung von IHE-Transaktionen)
JPEG	Joint Photographic Experts Group
KH	Krankenhaus
KOS	Key Object Selection Document
L-ARR	Local Audit Record Repository (eine dezentrale Bereichskomponente)
OAuth2	Ein Autorisierungsstandard-Protokoll
OIDC	Open ID Connect (Ein Protokoll für Authentifizierung und Autorisierung)
OTS	OAuth2 Internet Token Service
OZGF	OAuth ZGF (früher als IZGF, Internet Zugriffssteuerungsfassade bezeichnet)
PACS	Picture Archiving and Communication System
PAP	Policy Administration Point (zentrale ELGA Komponente)
PH	Pflegeheim
RAD	IHE Radiology Framework
REST	Representational State Transfer (eine Alternative zum SOAP)
SOAP	Simple Object Access Protokoll (ein W3C-Industriestandard)
WADO	Web Access to DICOM Objects
WIA	Web-based Image Access
QIDO	Query for Imaging DICOM Objects
XDS	Cross Enterprise Document Sharing (IHE Profil)
XDS-I	Cross-enterprise Document Sharing for Imaging (IHE Profil)
XCA	Cross Community Access (IHE Profil)
XCA-I	Cross Community Access for Imaging (IHE Profil)
ZGF	Zugriffssteuerungsfassade (Komponente des BeS, Teil der AGW)
ZGF-I	Zugriffssteuerungsfassade für Imaging (Komponente des BeS)

1.3. Abgrenzungen und wichtige Richtigstellungen

Bei dieser Version des aktuellen Dokumentes handelt es sich um eine komplett überarbeitete Version, welche anhand von Rückmeldungen und Kommentaren zur Version 1.85 erarbeitet wurde.

Dieses Dokument behandelt das Thema der Bilddatenübertragung in ELGA und e-Health vorwiegend aus der Sicht der Imaging Document Consumer Akteure sowie aus der Perspektive des ELGA- und e-Health-Berechtigungssystems (im Weiteren BeS). Siehe diesbezüglich den 4. und 5. Abschnitt (ELGA bzw. e-Health Anwendungen) der aktuellen Fassung des GTelG. Dementsprechend gilt (4. Abschnitt, §13 (4); sowie §28 (2)), dass für Bilddaten aktuell die ELGA-Bestimmungen schlagend sind. Die generelle und spezifische Erarbeitung des Themenkreises (e-Health und Bilddaten) ist jedoch bereits in dafür aufgestellten Fachgremien (Kernteam) früher erfolgt, die Resultate dieser Arbeiten wurden im Dokument *Gesamtkonzept Bilddaten V1.1* „***Organisationsübergreifende Nutzung von Bild- und Multimediadaten im österreichischen Gesundheitswesen***“ [1] erfasst. Dieses Dokument ist auch über die ELGA-Homepage (elga.gv.at/technischer-hintergrund) aufrufbar.

Hierfür ist weiters wichtig zu vermerken, dass der Wirkungsgrad des BeS auf der Ebene der jeweiligen GDA-Organisationseinheiten bzw. AGW/ZGF endet. Darunter bzw. tiefer in der Verarbeitungskette liegt die Verantwortung bzw. die Autorisierungshoheit bei den einzelnen GDA. Authentifizierung der Anwender und Teilnehmer ist entsprechend ELGA-Gesamtarchitektur externalisiert und wird an vertrauenswürdige Identity Provider (IdP) übertragen.

Entsprechend dieser Auslegung sind die in diesem Dokument erörterten, bereichsspezifischen Adapter (auch sonstigen Adapter) sowie Imaging Document Source Akteure, im Wirkungsbereich der einzelnen ELGA-Bereiche und GDA zu sehen. Dieses Dokument beschäftigt sich nicht mit dem Aufbau und Betrieb von solchen Adaptern. Es ist nicht auszuschließen, dass aus der Sicht der Hersteller (PACS) bzw. der Bereichsbetreiber, das Aufstellen oder Einrichten solcher Adapter nicht erforderlich ist. Dies ist insbesondere dann der Fall, wenn ein Archivsystem die vom BeS unterstützen Transaktionen der Bilddatentransfers nativ unterstützt (z.B. mittels DICOMweb).

1.4. ELGA und e-Health

Dieses Dokument beschreibt den Bilddatenaustausch aus der Sicht von ELGA und des ELGA-Berechtigungssystems (BeS). Zukünftig sollen aber auch e-Health Anwendungen im Bereich des Bilddatenaustauschs durch die hier vorgeschlagene ELGA-Architektur unterstützt werden. e-Health wird daher als eine über die „ELGA Opt-Out Policy“ hinausgehende Erweiterung des ELGA-Berechtigungssystems mit autorisierten GDA-Anwendern (die nicht unbedingt auch ELGA-GDA sein müssen) betrachtet. e-Health-Anwendungen nutzen für bestimmte Zwecke (Bilddatenübertragung, e-Impfpass, PVN, …) die ELGA-Komponenten ganz oder teilweise und fallen nicht unter das Regime des 4. Abschnitts des Gesundheitstelematikgesetzes (ELGA, Opt-Out), sondern werden im 5. Abschnitt beschrieben (vgl. e-Impfpass).

1.5. Anforderungen

Die Bereitstellung von Bilddaten in ELGA muss folgenden Kriterien und Anforderungen genügen:

1. Bildarchive (PACS) können auch ohne Duplizierung von deren Inhalten an ELGA angebunden werden, unter der Voraussetzung, dass sie in gesicherten (hoch)verfügbaren Rechenzentren betrieben werden und einen Zugang zu gesicherten Gesundheitsnetzwerken (GIN/eHI bzw. HEALIX) haben.
2. Bilddaten müssen auch im **JPEG-Format** in reduzierter Auflösung/Qualität bandbreitensparend dynamisch (On-Demand) bereitgestellt werden können, zum Beispiel für das Bürgerportal (EBP). Der Zugriff auf Bilder in nativer Qualität darf aber nicht verhindert werden.
3. Das Berechtigungssystem muss folgende existierende Standards und Schnittstellen der anzubindenden Archive berücksichtigen und unterstützen:
    a. **DICOM** im Backend (PACS) als Basis
    b. **IHE XDS-I und XCA-I Profile**
    c. **IHE RAD** Technical Framework Revision 19 (oder höher)
        i. Client-Zugriffe via IHE RAD-69/75 **müssen** bereichsintern (XDS-I) und bereichsübergreifend (XCA-I) unterstützt werden
        ii. Das Registrieren von KOS-Objekten und deren Metadaten **muss** via RAD-68 erfolgen.
    d. DICOM SOAP Web-Services
        i. WADO-WS PS3.18 2016b (SOAP-Messaging) ist nicht mehr Teil der aktuellen DICOM-Spezifikation, wird aber nach wie vor in den IHE

XDS-I und XCA-I Profilen als Transaktion RAD-69 bzw. Rad-75 verwendet.

e. **DICOM REST Web-Services entsprechend PS3.18 (DICOMweb)**

i. QIDO-RS [RAD-129] und WADO-RS [RAD-107] sind entsprechend PS3.18 2021d (oder höher) zu unterstützen unter Berücksichtigung des IHE Integration Profiles Web Based Image-Access (WIA).

4. Dem ELGA GDA muss ermöglicht werden, auf Studien, Serien sowie einzelne Bilder bereichsübergreifend in Originalqualität und im Originalformat (DICOM) zuzugreifen.

   a. Für die Anbindung am AGW (bzw. ZGF und IZGF) sind explizite Endpunkte und dedizierte Services für Bilddatenübertragung vorzusehen.

5. Änderungen in der Bilddarstellung sind Aufgaben der jeweiligen Anwenderoberflächen (UI – User Interface) und können nur im Rahmen der implementierten IHE- und DICOMweb-Profile unterstützt werden.

6. Das ELGA-Berechtigungssystem (BeS) ist entsprechend den gesetzlichen Vorgaben zuständig für die Zugriffsautorisierung.

7. Protokollierung (in den ELGA-Bereichen und für SOAP-basierenden Transaktionen gemäß IHE ATNA) ist für alle teilnehmenden Akteure verpflichtend.

8. Bilddaten werden unter Einsatz von DICOM KOS-Objekten (*Key Object Selection Document*) in ELGA verfügbar und abrufbar gemacht. Als Alternativformat zu DICOM KOS wird eine JSON-Repräsentation beim Anfordern von DICOM KOS unterstützt (entsprechend Anhang F, DICOM JSON Model in DICOM NEMA PS3.18 Dokumentation).

9. Die in ELGA registrierten DICOM KOS-Objekte (inkl. darauf basierende Befunde) müssen in den XDS-Metadaten einheitlich beschlagwortet werden. Hierfür ist der APPC (*Austrian PACS Procedure Code*) zu verwenden.

10. Metadaten für die Registrierung von KOS-Objekten sind entsprechend der in ELGA gültigen einheitlichen Vorgaben (XDS-Metadaten Leitfaden [3] und KOS Leitfaden von DICOM-Austria [4]) zu verwenden. Diese umfassen zudem die Abbildung von Relationen zwischen Radiologie-Befunden (CDA) und zugrundeliegenden Bildverweisdaten, den KOS-Objekten.

1.6. IHE XCA-I Architektur

1.6.1. Allgemeines

IHE-Vorgaben für Bilddatenaustausch (und im Allgemeinen der Austausch von Multimedia-Inhalten) sind zum Zeitpunkt der Erstellung dieses Dokumentes im Wandel. Frühere, ausschließlich auf SOAP-Nachrichten basierende Ansätze sind teilweise nicht mehr zeitgemäß. Mobile Geräte und REST-Protokolle haben im letzten Jahrzehnt das Web erobert, was entsprechende Nachjustierungen und Neudefinitionen bei den Erwartungshaltungen bedarf. Die hier dargestellte Lösungsarchitektur nimmt weitgehend Rücksicht auf diese Tendenzen.

Die bereichsübergreifende Lösungsarchitektur leitet sich somit prinzipiell aus dem IHE XCA-I Modell ab (Abbildung 1), mit dem Ziel, die IHE-Konzepte entsprechend den aufgelisteten ELGA-Anforderungen und Bedürfnissen anzupassen (Abbildung 2).

IHE XCA-I sieht ein eigenes Initiating und Responding Imaging Gateway für den Bildaustausch vor. Dieser Akteur ist in ELGA in Form einer ZGF-I (Zugriffssteuerungsfassade für Imaging) zu realisieren. Bereichsintern (XDS-I.b) kommuniziert die ZGF-I mit den angebundenen PACS/Archiven über einen zwischengeschalteten **bereichsspezifischen** Adapter (siehe Abbildung 2), der lokale Umsetzungsspezifika gegenüber der ZGF-I entkoppelt. Der Adapter wird im Kapitel 1.6.4 spezifiziert.

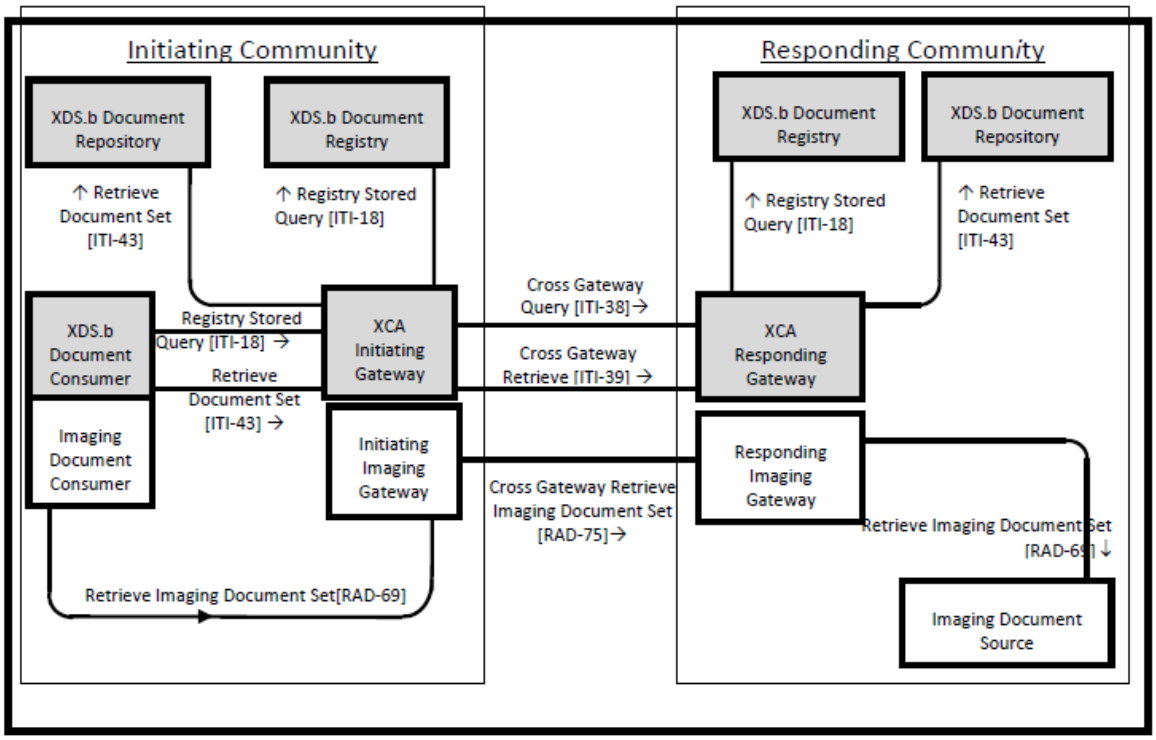
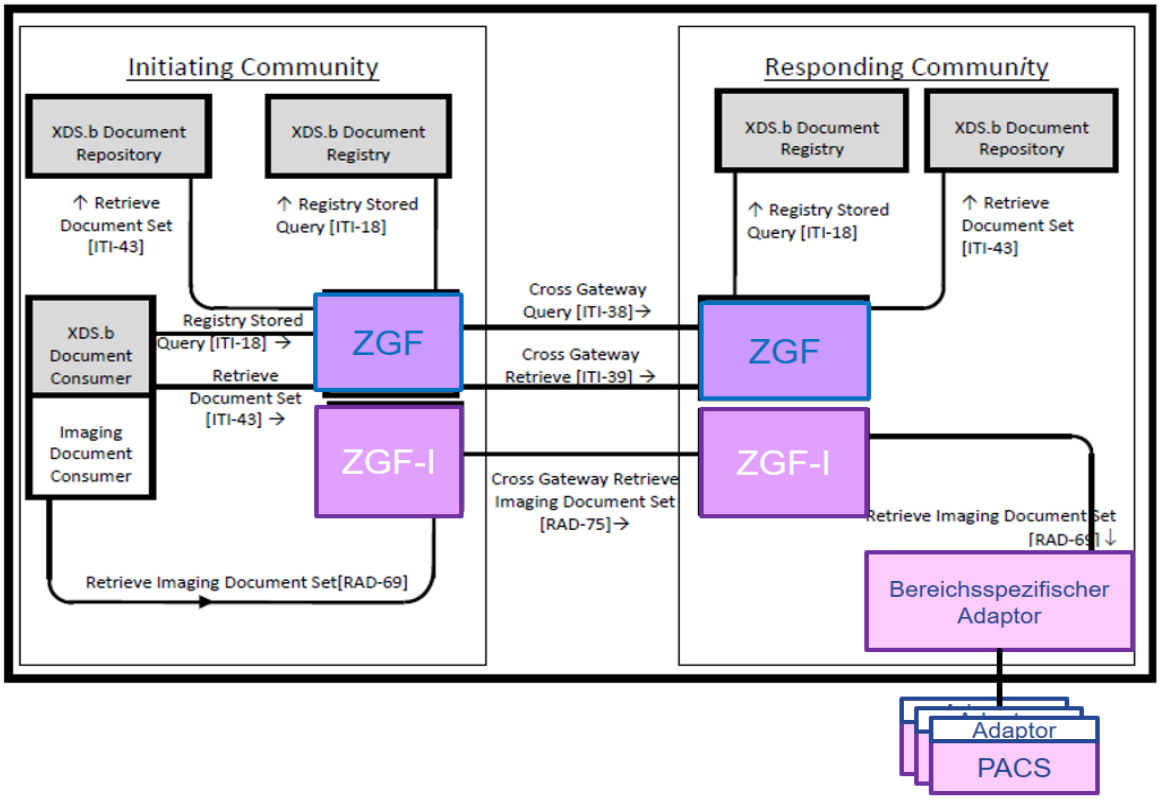


Abbildung 1: XCA-I Konzept von IHE



237

238 *Abbildung 2: ELGA-bereichsübergreifender Bilddaten-Austausch*

239 **1.6.2. Registrieren von Bilddaten in ELGA**

240 Bilddaten müssen in ELGA über ein für ELGA explizit freigegebenes KOS-Objekt (*Key Ob-*
241 *ject Selection Document*) referenziert, angefordert und zugänglich gemacht werden. KOS-
242 Objekte veröffentlicht (in ELGA) der Ersteller möglichst zeitnah zur Fertigstellung der damit
243 zusammenhängenden Studie. KOS-Objekte müssen entsprechend des Leitfadens zu Erstel-
244 lung und Verwendung von KOS-Objekten [4] aufgebaut werden.

245 Ein KOS-Objekt wird mittels [RAD-68] *Provide and Register Imaging Document Set -*
246 *MTOM/XOP* in einem XDS Repository gespeichert und durch dieses anschließend in einer
247 XDS Registry für ELGA registriert (veröffentlicht).

248 Das KOS-Objekt selbst ist nicht Bestandteil der Studie und wird daher nicht aus dem PACS
249 mitausgeliefert werden. Es ist darüber hinaus auch davon auszugehen, dass der Imaging
250 Document Source Actor lokal kein KOS speichert. Das KOS stellt nur den Bildverweis im IHE
251 Repository dar.

252 Für KOS-Objekte ist in ELGA eine Dokumentenklasse definiert (55113-5, *Key images*
253 *Document Radiology*). Darüber hinaus müssen die beim Registrieren eines KOS-Objektes
254 verpflichtend und optional geführten Metadaten den in ELGA gültigen Vorgaben folgen.

Dadurch wird es ermöglicht, ELGA-weit nach KOS-Objekten via [ITI-18] *Registry Stored Query* zu suchen und diese dann in der Folge auch abzurufen.

Es ist legitim, nur ein KOS pro Studie zu erstellen und dieses im Fall von Erweiterungen zu überschreiben (versionieren). Theoretisch können auch mehrere KOS für eine Studie registriert werden. Prinzipiell gilt, dass bereits registrierte KOS per RPLC (replace) erweiterbar sein müssen, damit eine erweiterte Studie veröffentlicht werden kann.

Das Berechtigungssystem verhindert das Abrufen von Bildmaterial, das von bereits als „deprecated“ markierten KOS-Objekten referenziert wird.

Die veröffentlichten KOS-Objekte müssen selbst keinen APPC-Code beinhalten (in den DICOM Daten), bei der Registrierung in ELGA ist die Anreicherung **der Metadaten** mit dem APPC jedoch **verpflichtend**.

Es gilt zu bedenken, dass ELGA standardmäßig ein gesetzlich vordefiniertes Zeitfenster (mehrere Tage/Monate) für die Registrierung der Dokumente vorsieht. Ein ELGA-Dokument kann nur in diesem Zeitfenster nach dem ambulanten Aufenthalt bzw. ab Entlassung erstregistriert werden. Später bearbeitete Bilddaten können aus diesem Zeitfenster fallen und könnten daher in ELGA nicht mehr veröffentlicht werden. Eine Ausnahme stellt das Update unter dem Titel „Recht auf Richtigstellung“ dar.

1.6.3. ZGF-I Spezifikation

1.6.3.1. Funktionale Spezifikation

Der ZGF-I Akteur ist ein Teil des ELGA-Berechtigungssystems, er autorisiert und protokolliert Anfragen entsprechend der in der Gesamtarchitektur [2] erläuterten Prinzipien (basierend auf gesetzlichen Grundlagen). Darüber hinaus erfüllt eine ZGF-I die Bestimmungen und Definitionen eines Imaging Gateways laut IHE RAD TF Vol.1.

Die ZGF-I bietet Schnittstellen und unterstützt Imaging-Protokolle zum Bildaustausch im Umfang des im folgenden Kapitel aufgelisteten Inhalts. Zwischen den initiierenden und antwortenden ZGF-I werden entsprechend XCA-I Profil lediglich SOAP-basierende Protokolle verwendet.

Zusätzlich zu den Anforderungen, die aus den IHE-Profilen resultieren, und die die Auslieferung eine KOS-Objekts als natives DICOM Objekt vorsehen, muss die ZGF-I auch in der Lage sein, ein KOS-Objekt in JSON umzuwandeln und in diesem Format auszuliefern. Der Grund für die explizite Unterstützung von JSON liegt in der Anwendung dieses Formats in gängigen Web-Anwendungen.

1.6.3.2. Schnittstellenspezifikation

Wenn ein Imaging Document Consumer Bilddaten anfordert, durchquert der Datenstrom mehrere Knoten und Schnittstellen. Ein vereinfachtes Bild dieser Übertragungskette ist in Abbildung 3 dargestellt. Ein Imaging Document Consumer sendet die initiierende Anfrage an die Schnittstelle „A“ seiner lokalen initiierenden ZGF-I. Die ZGF-I verarbeitet die Anfrage. Bereichsübergreifend wird die Anfrage über die Schnittstelle „B“ einer antwortenden ZGF-I initiiert. Die entfernte ZGF-I verarbeitet den eingehenden Request und leitet danach die Anfrage über die Schnittstelle „C“ an den bereichsspezifischen Adapter weiter. Der Adapter propagiert via Schnittelle „D“ die Anfragen an die angeschlossenen lokalen Systeme (PACS).

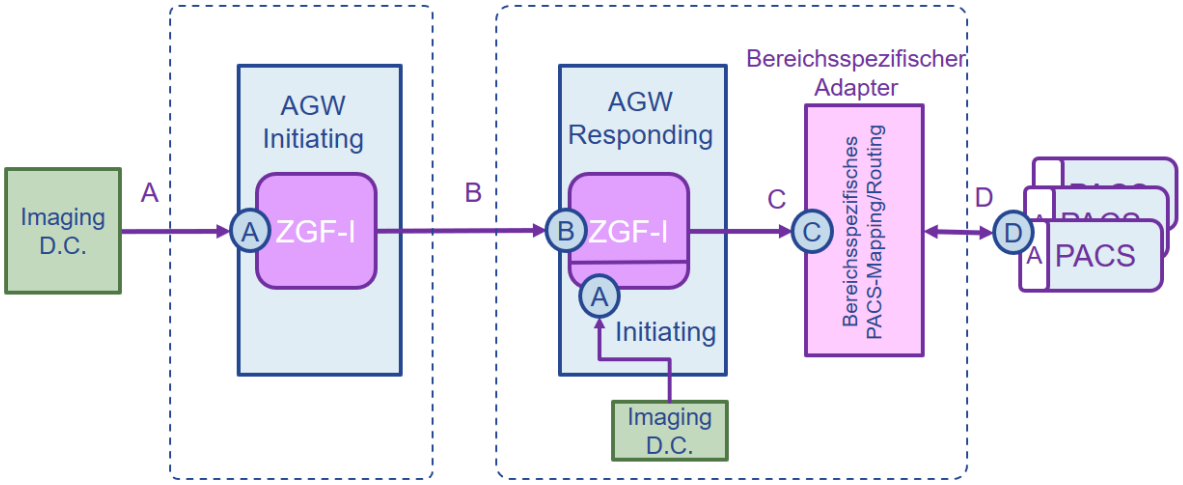


Abbildung 3: Kommunikationswege und Schnittstellen. Ein bereichsspezifischer Adapter ist eine im Bereich zentral aufgestellte Komponente. „A“ rechts im Bild (optionale Komponente) bezeichnet lokale PACS- Adapter, welche http-basierende Protokolle (SOAP und/oder REST) auf DICOM umwandeln.

An den **Schnittstellen „A“** (https://<$AGW_FQDN>:443/XCA/DCMeBefunde) der initiierenden ZGF-I müssen zumindest folgende Schnittstellen und Protokolle unterstützt werden:

- RAD-68 entsprechend IHE RAD Technical Framework: Provide and Register Imaging Document Set
- RAD-69 entsprechend IHE RAD Technical Framework
    - RetrieveImagingDocumentSet

An den **Schnittstellen „B“** (https://<$AGW_FQDN>:443/XCA/DCMeBefunde/respGW) der responding ZGF-I muss entsprechend XCA-I Profil die Transaktion RAD-75 implementiert werden.

An den **Schnittstellen „C“** des Adapters ist RAD-69 vorgesehen. Die antwortende (responding) ZGF-I führt keine Protokollumwandlungen durch. RAD-69 wird als RAD-69 an den bereichsspezifischen Adapter weitergeleitet.

- RAD-69
    - RetrieveImagingDocumentSet

Die **Schnittstelle „D“** liegt nicht im Wirkungsbereich des BeS, demnach kann aus Sicht der vorliegenden Architektur keine Vorgabe definiert oder ausgesprochen werden. Die erwarteten Schnittstellen sind von den spezifischen Fähigkeiten der einzelnen Archive abhängig und mit dem Hersteller des bereichsspezifischen Adapters abzustimmen. Auch hinsichtlich eventuell notwendiger Adapter kann auf dieser Ebene keine Aussage getroffen werden.

Abbildung 4 zeigt die teilnehmenden Komponenten in einer höheren Granularität. Die derzeitige AGW muss neben einer ZGF-Instanz auch eine ZGF-I Instanz integrieren. Beide nehmen an der Abwicklung der Bilddatenübertragung teil, indem über die ZGF das KOS-Objekt angefordert wird und über die ZGF-I die im KOS referenzierten Bilddaten.

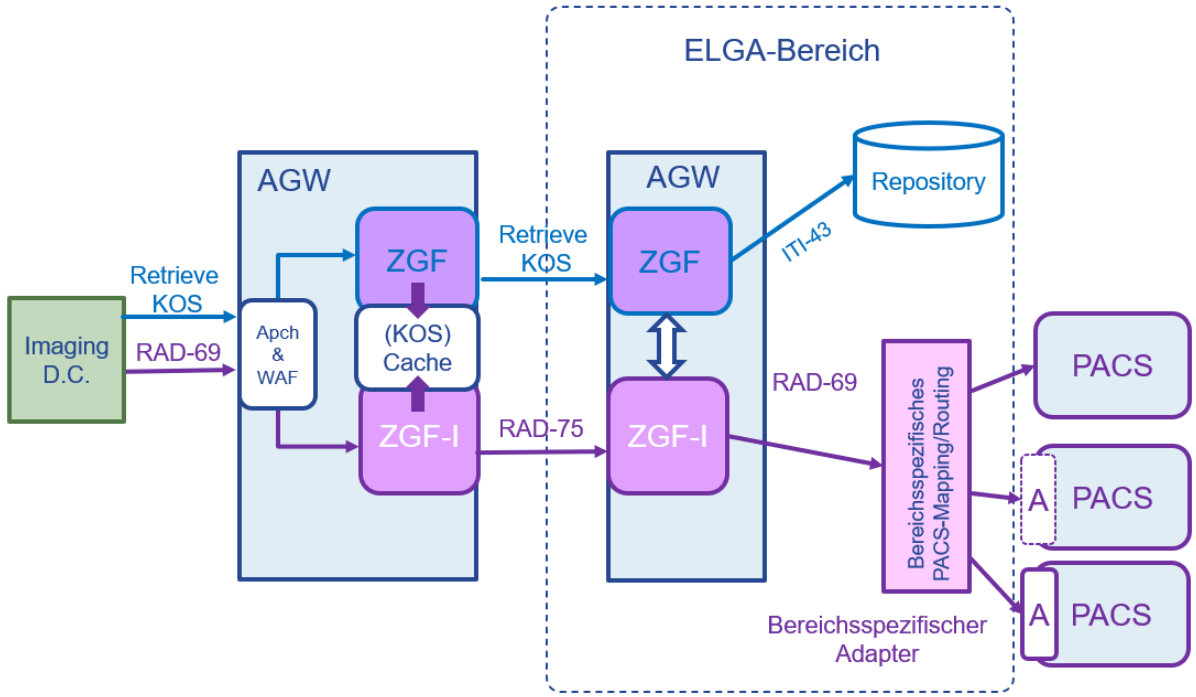


Abbildung 4: ZGF-I Basisarchitektur. „Retrieve KOS“ bezeichnet die Anfrage für ein KOS-Objekt in verschieden Formaten (DICOM und JSON). Die Darstellung der rechts im Bild angeführten Adapter ist symbolisch, da eventuell auch eine direkte Kommunikation mit dem Archiv möglich ist.

1.6.3.3. Netzwerkverbindungen für RAD-69 und https-Streaming

Wie in Abbildung 4 schon deutlich hervorgehoben, kann die eigentliche Bilddatenübertragung über bereits existierende Breitbandverbindungen ermöglicht werden. Dafür muss die dafür derzeit vorgesehene [RAD-69] Transaktion über eigene AGW-Endpunkte geführt werden. Dadurch ergibt sich die Möglichkeit bei Bedarf für diese Übertragungen dedizierte Leitungen zu verwenden. Eine entsprechende Skizze wird in Abbildung 5 dargestellt.

Darüber hinaus müssen für e-Befunde geltende ModSecurity-Größenlimits (derzeit auf 25 Mbyte gesetzt) außer Kraft gesetzt werden. Eine nahtlose Übertragung von größeren Studien/Serien muss via https-Streaming (bei AGW zu AGW) ermöglicht werden. Diese Lösung verspricht keine negativen Auswirkungen bei den Konsumenten, da diese gar nicht wissen müssen, dass das angefragte Bildmaterial gestreamt wird. Nach Einführung (Inbetriebnahme) des AGW-Streamings bedarf der bereichsspezifische Adapter keiner Umbauten. Es ist dennoch empfehlenswert, dass der Adapter selbst diese (Streaming) Fähigkeiten annimmt. Live-Streaming wird jedoch nicht implementiert, sprich der Konsument muss das heruntergeladene Bildmaterial vor der Darstellung komplett empfangen.

Um einen stabilen Betrieb zu gewährleisten, muss die notwendige Bandbreite der Bilddaten-Übertragungswege auf der Grundlage von Erfahrungswerten angepasst werden. Auf Basis bisheriger Erfahrungswerte aus dem HeX-I-Projekt und als Folge der Schätzungen für die künftige Auslastung, werden als Minimum durchgehend (vom Consumer zur Source) zumindest 1Gbit angesehen und erfordert.

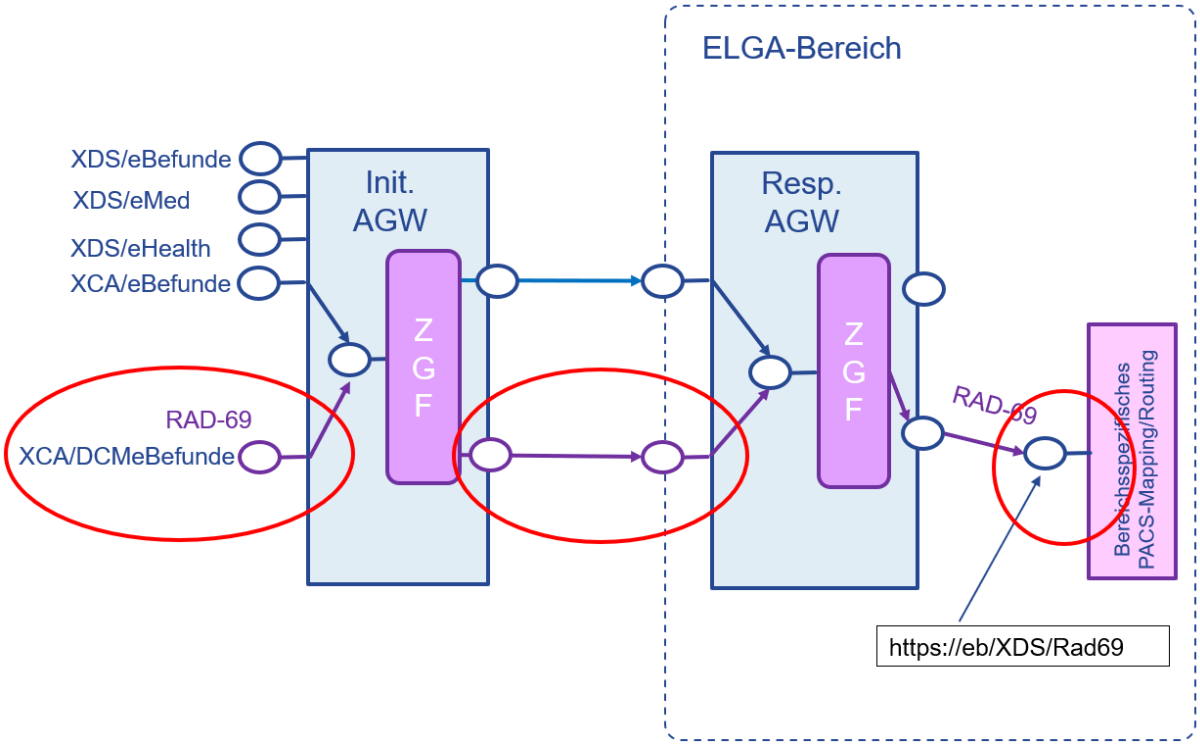


Abbildung 5: Skizze von für RAD-69 angeforderten netzwerktechnischen Verbindungen am initiierenden und antwortenden AGW (rot eingekreist)

1.6.4. Spezifikation des bereichsspezifischen Adapters

Der bereichsspezifische Adapter (eine Komponente pro Bereich) dient als Bindeglied zwischen ZGF-I und den einzelnen angebundenen PACS/DICOM-Archiven. Der bereichsspezifische Adapter ist keine Sicherheitskomponente und darf ausschließlich vom ZGF-I weitergeleitete Nachrichten erhalten und verarbeiten.

Der bereichsspezifische Adapter lokalisiert und adressiert (via Konfiguration) die einzelnen angebundenen PACS/DICOM- Archive. Die primäre Aufgabe eines bereichsspezifischen Adapters ist die Wegfindung (unterstützte Protokolle/Schnittstellen) zu den tatsächlichen Archiven.

1.6.5. Autorisierung, Zugriffseinschränkungen und Protokollierung

1.6.5.1. Allgemeines

Die Autorisierung der ELGA-Zugriffe erfolgt grundsätzlich entsprechend der ELGA-Gesamtarchitektur via WS-Trust Tokens. Dies gilt für alle Imaging-Anfragen. Imaging Document Consumer in ELGA-GDA Rollen müssen verbindlich eine ELGA HCP-Assertion, in der Rolle ELGA-Teilnehmer eine ELGA User-Assertion I (in Vertretung eines ELGA-Teilnehmers eine ELGA Mandate-Assertion I) dem BeS präsentieren.

- SOAP-Zugriffe sind ausnahmslos via ELGA SAML2 Token zu autorisieren.
- Zugriffe der Client-Akteure über FHIR/REST
  - Als Übergangslösung können ELGA SAML2-Tokens im https Authorization-Header transportiert werden. Eine Übergangslösung stützt sich an die existierende WS-Trust Infrastruktur des Berechtigungssystems.
  - Langfristig müssen Autorisierungen über JSON Web Tokens (JWT) erfolgen (Open ID Connect als Richtlinie ist anzuwenden).

Bei XCA-I ([RAD-75]) müssen alle Imaging-Requests über eine ELGA Treatment Imaging-Assertion verfügen. Von der antwortenden ZGF-I zum bereichsspezifischen Adapter sind alle Requests mit einer üblichen ELGA-Community-Assertion auszustatten. Die Autorisierung der Anfragen auf dem weiteren Weg zu den PACS ist interne Angelegenheit des Bereiches.

1.6.5.2. ZGF KOS-Cache

Die initiierende ZGF-I muss gewährleisten, dass nur auf jenes Bildmaterial zugegriffen werden kann, das in einem vorher autorisierten [ITI-43] Abruf eines KOS-Objektes referenziert ist. Dementsprechend muss die initiierende ZGF in Zusammenarbeit mit der initiierenden ZGF-I die im KOS-Objekt enthaltenen Informationen sicher zwischenspeichern (Cache). Ausgehend von der derzeitigen Ausführung der AGW/ZGF kann die Dauer von zwischengespeicherten KOS-Daten auf 30 Minuten (konfigurierbar) beschränkt werden. Um eventuelle Updates, die in diesem Zeitraum stattgefunden haben, abfangen zu können, muss der Imaging Document Consumer eine neue, explizite KOS-Query Anfrage starten, womit die im Cache aufgehobene Informationen mit dem aktuellen Stand überschrieben werden.

Darüber hinaus müssen die zwischengespeicherten Daten des KOS-Objekts an einen eindeutig identifizierbaren ELGA-Token (HCP-Assertion, User-Assertion I bzw. Mandate-Assertion I) gebunden werden. Bilddaten können nur mit derselben Assertion geladen werden, die auch für das Retrieval des KOS-Objektes verwendet wurde. Damit muss die initiierende ZGF-I garantieren, dass nur jener Akteur auf die Bilddaten zugreifen kann, dem zeitnah (im Zeitraum von 30 Minuten – nach Praxiserfordernis konfigurierbar) das entsprechende KOS-Objekt aushändigt wurde. Falls nach Ablauf dieser Frist die Bilder noch nicht geholt wurden, muss der Client einen Refresh anstoßen – also das KOS noch einmal laden – um wieder Zugriff auf die Bilddaten zu erhalten. Die Lebensdauer des Cache muss den Softwareherstellern bekanntgegeben werden, um die entsprechende Logik umzusetzen.

Die Absicherung des KOS-Cache, der Treatment Imaging-Assertion und die Verknüpfung deren Inhalte mit dem entsprechenden ELGA-Token erfordern einen Integritätsschutz durch kryptografische Maßnahmen (Verschlüsselung).

Alle von einem Imaging Document Consumer ausgehenden Zugriffe müssen im Security-Header wie üblich nur eine ELGA Login-Assertion (HCP-Assertion, User-Assertion I bzw. Mandate-Assertion I) mitführen. Der initiierende Teil der ZGF-I entscheidet basierend auf dieser Grundlage, ob die Anforderung rechtmäßig ist. Die präsentierte ELGA-Assertion muss mit jener im gesicherten KOS-Cache mitgeführten übereinstimmen. Diese Maßnahme soll verhindern, dass durch unbeabsichtigte oder bewusste Weitergabe von Informationen, die in einem KOS-Objekt enthalten sind, nicht autorisierte Benutzer auf die Bilddaten zugreifen können.

Sollte der ELGA-Teilnehmer das KOS-Objekt ausgeblendet oder gelöscht haben, kann der GDA das im KOS-Objekt referenzierte Bildmaterial nicht anfragen. Die ZGF-I muss all jene Anfragen abweisen, die ohne zeitnah erfolgreich abgeholtes KOS-Objekt erfolgen.

Dadurch ist der KOS-Cache neben den regulären ELGA-Tokens (wie einer HCP-Assertion) ein unentbehrliches Mittel zur Umsetzung der Zugriffsautorisierung. Der Zugang zu den Bilddaten ist für ein vertretbares Zeitfenster limitiert. Sollte ein Imaging-Zugriff außerhalb des angeführten Zeitlimits erfolgen, signalisiert die ZGF-I das Fehlen entsprechender Autorisierungsinformationen im KOS-Cache. Der Imaging Document Consumer muss in diesem Fall das zugrundeliegende KOS-Objekt erneut anfordern.

1.6.5.3. ELGA Treatment Imaging-Assertion

KOS-Objekte referenzieren prinzipiell auf eine durch Serien und Studien zusammengefasste Menge von Bilddateninstanzen. Einem Akteur steht frei, die Instanzen entweder blockweise oder auch einzeln abzufragen. Nach derzeitigem Stand der ELGA-Architektur, muss jeder einzelne Request basierend auf einer ELGA Treatment-Assertion autorisiert werden. Das Ausstellen eines Tokens ist eine zeitaufwendige kryptografische Operation. WS-Trust erlaubt hingegen einen bestehenden Token im Rahmen dessen Gültigkeit wiederzuverwenden. Hierfür muss die ZGF-I beim ersten berechtigten Zugriff auf das KOS-Objekt vom ETS auch eine der HCP-Assertion entsprechende ELGA Treatment Imaging-Assertion anfordern. Die Gültigkeit der Treatment Imaging-Assertion muss mit dem KOS-Cache korrespondieren. Wenn der Gültigkeitszeitraum des KOS-Cache 30 Minuten beträgt, dann muss die ZGF die Treatment Imaging-Assertions vom ETS für 30 Minuten beantragen. Die angeforderte Assertion muss im Cache durch kryptografische Maßnahmen gesichert, für nicht berechtigte unerreichbar, aufgehoben werden.

1.6.5.4. Confidentiality & Integrity

Zwischengespeicherte Treatment Imaging-Assertions müssen kryptografisch gesichert werden. Die Assertions sind ausnahmslos verschlüsselt in der ZGF-I zu halten bzw. zwischen den geclusterten ZGF-I Instanzen zu synchronisieren. Der symmetrische AES-Schlüssel

muss mit einem asymmetrischen Verschlüsselungsverfahren anhand des von der Core-PKI bezogenen Zertifikats geschützt werden. Der Integritätsschutz des KOS-Cache (via Message Authentication Code) muss ebenfalls auf Grundlage von Core-PKI Zertifikaten erfolgen. Die Implementierung dieser Mechanismen erfolgt innerhalb der AGWs.

Optional, je nach Entscheidung der Betriebsführung und der Bereichs-CISOs, sind Schlüsselmaterial und Zertifikate mit HSM-Modulen zu schützen. Nur dem BeS ist es erlaubt, diese Hardwarestores zu lesen.

1.6.5.5. Protokollierung

Sämtliche KOS-Objekt- und Imaging-Zugriffe sind in den bereichsspezifischen L-ARR entsprechend IHE ATNA-Profil zu protokollieren. Zugriffe auf KOS-Objekte sind auch im A-ARR zu vermerken. Dadurch sind etwaige GDA-Zugriffe auf Bilddaten für ELGA-Teilnehmer transparent zu halten. Zugriffe auf einzelne, innerhalb der KOS-Objekte referenzierte Instanzen der Bilddaten müssen im A-ARR nicht protokolliert werden:

1. Der Anker für den Zugriff auf Bilddaten ist das KOS-Objekt. Wird das KOS-Objekt dem GDA zugänglich gemacht, kann im KOS-Objekt referenziertes Bildmaterial uneingeschränkt angefordert werden.
2. ELGA-Teilnehmer können den Zugang zu Bildmaterial durch das Ausblenden bzw. Löschen von KOS-Objekten steuern.
3. Die potenziell große Anzahl der im KOS-Objekt referenzierten Bilddaten würde die Protokollierung für den ELGA-Teilnehmer unübersichtlich gestalten, ohne dabei einen essenziellen Mehrwert zu liefern.

Um dennoch RAD-69 Zugriffe zu protokollieren, müsste wie folgt vorgegangen werden:

- Für RAD-68 muss ein neuer **BeS** Event-Code eingeführt werden „Bilddaten veröffentlicht“. Beim Einlesen (Laden via ITI-43) von KOS-Objekten muss ein weiterer neuer Event-Code eingeführt werden „Bilddaten abgerufen“.
- Bei RAD-69 müssen zwei neue **BeS** Event-Codes eingeführt werden
  - DICOM Zugriff gestartet – beim ersten RAD-69 Zugriff im aktuellen KOS-Kontext
  - DICOM Zugriff fortgesetzt – beim zweiten RAD-69 Zugriff in aktuellen KOS-Kontext
  - Weitere RAD-69 Zugriffe im gleichen KOS-Kontext müssen zentral nicht protokolliert werden. Dies wird dadurch begründet, dass anhand der im KOS angeführten Studien/Serien theoretisch auch hunderte und tausende Zugriffe erfolgen, welche protokolltechnisch eher lokal (L-ARR) und auf der DICOM-Ebene zu verfolgen sind
- Im lokalen L-ARR müssen alle Transaktionen (RAD-68, 69) entsprechend bisher geltenden Protokollierungsrichtlinien (siehe in [2] und [5]) protokolliert werden.

- Im zentralen Z-L-ARR wird entsprechend BeS-Pflichtenheft ([5]) RAD-68 und RAD-69 (beim Ausstellen der Imaging Treatment-Assertion) protokolliert.
- Im A-ARR wird nur RAD-68 mitprotokolliert, nicht aber RAD-69.

Anmerkung: Es gibt noch laufende Diskussionen zur Protokollierung der Bildzugriffe. Aktuell ist nur die Protokollierung auf Ebene der KOS-Objekte implementiert.

1.6.6. Beispielhaftes Veröffentlichen von DICOM-Studien/Serien in ELGA

Es wird angenommen, dass ein ELGA-Teilnehmer mit Mitteln der bildgebenden Diagnostik untersucht wird. Es wurde bereits eine Kontaktbestätigung ins KBS geschickt. Im Rahmen der Untersuchung entsteht eine DICOM-Studie, die mehrere DICOM-Serien umfasst und im dafür bestimmten lokalen PACS-Archiv gespeichert wird (außerhalb von ELGA). Das Archiv ist via bereichsspezifischen Adapter (Abbildung 4) an eine ELGA ZGF-I angeschlossen. Anschließend wird ein DICOM KOS-Objekt erstellt.

Sofern der ELGA-Teilnehmer über den Z-PI eindeutig identifiziert wurde und keine individuelle Policy dies verhindert, kann das KOS-Objekt in ELGA veröffentlicht werden. Dies erfolgt manuell oder automatisch als Teil einer eventuellen Batch-Prozedur. Hierfür muss das zuständige KIS/RIS/PACS-System (GDA) via RAD-68 das KOS-Objekt in ein ELGA-Repository speichern und registrieren.

Für die Veröffentlichung eines KOS-Objekts in ELGA sind eine gültige ELGA HCP-Assertion und eine Kontaktbestätigung notwendig. Für die Registrierung des KOS-Objekts sind bestimmte Metadaten verbindlich anzugeben. Insbesondere (siehe auch XDS-I Metadaten für Bilddaten in [3] und [4]):

- Verschlagwortung entsprechend APPC-Codesystem

Die eigentliche Registrierung in ELGA erfolgt, wie für Befund-CDA bereits etabliert, im angebundenen ELGA-Bereich. Sollten individuell gesetzte Berechtigungen der Veröffentlichung widersprechen, wird das Speichern (Bereichsvariante **A**) bzw. das Registrieren (Bereichsvariante **C**) in ELGA zurückgewiesen.

Nachdem das Registrieren des KOS-Objektes in ELGA erfolgreich abgeschlossen wurde, können die darin referenzierten Bilddaten in ELGA abgerufen werden.

Wenn das Registrieren des KOS-Objektes in ELGA erfolgreich abgeschlossen ist, wird für weitere beispielhafte Szenarien angenommen, dass die Befundung bei einem anderen ELGA-GDA stattfindet. Für diesen, in die Behandlung einbezogenen ELGA-GDA, wird ein Kontakt des ELGA-Teilnehmers delegiert.

1.6.7. Beispiel Sequenz „DICOM Studie herunterladen“

Die Befundung des im Beispiel oben angeführten Bildmaterials erfolgt durch einen anderen GDA in einem zweiten ELGA-Bereich. Hierzu delegiert der GDA des ersten ELGA-Bereichs seine Kontaktbestätigung für den betroffenen ELGA-Teilnehmer an den GDA des zweiten ELGA-Bereichs. Die Studie ist zum Beispiel nicht älter als 10 Tage (für dieses Szenario willkürlich gewähltes Zeitfenster).

Anmerkung: Dieses Szenario könnte nicht funktionieren, wenn der Patient eine individuelle Einschränkung (z.B. GDA ist gesperrt) eingebracht hat.

Der GDA des zweiten ELGA-Bereichs ist authentifiziert und in ELGA angemeldet. Das entsprechende KIS-System besitzt eine gültige ELGA HCP-Assertion. Er sucht nach Dokumenten in ELGA (via KIS-System), wobei als Suchkriterien die konkrete Dokumentenklasse des KOS-Objektes und ein Erstellungszeitraum für die letzten 10 Tage, entsprechend des vorab dem GDA mitgeteilten Wissens, festgelegt wird (siehe Abbildung 6).

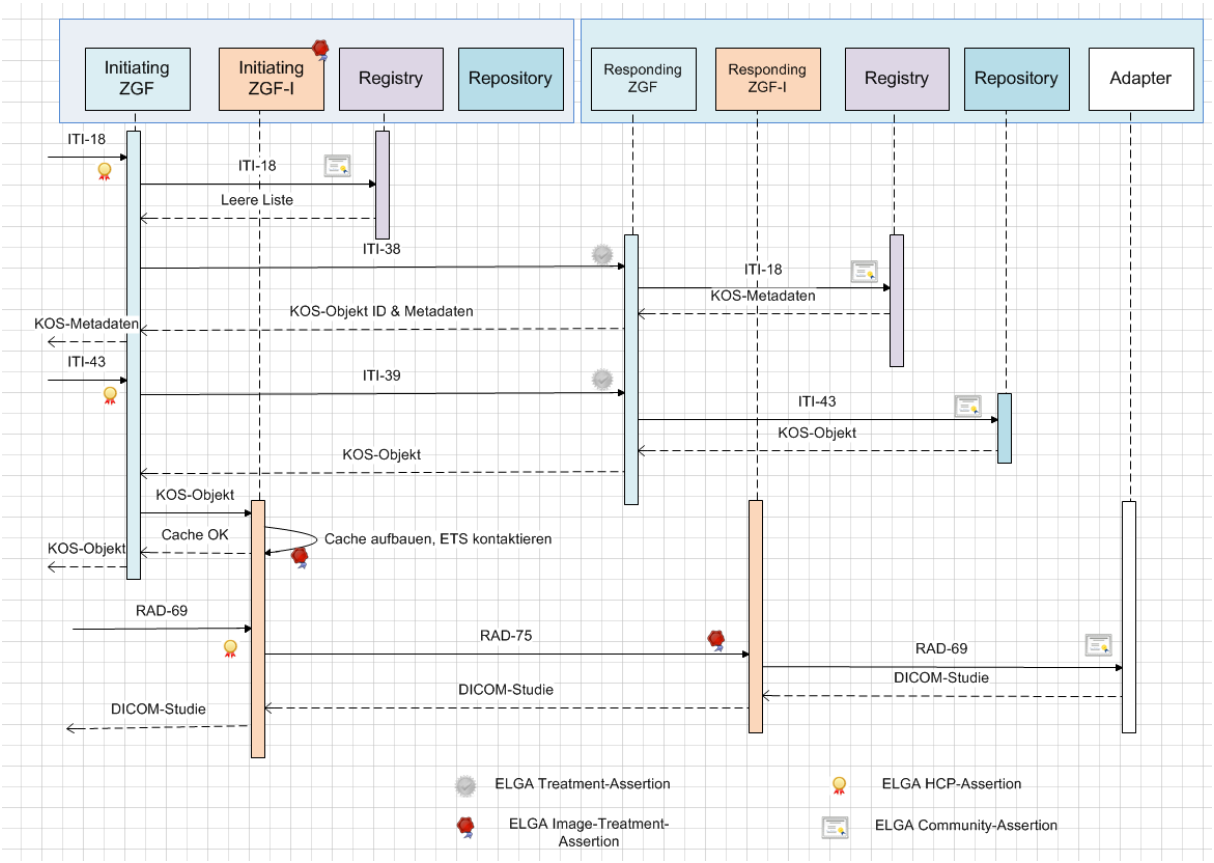


Abbildung 6: Zugriff auf eine DICOM-Studie

1. Der GDA setzt (via KIS-System) ein *Registry Stored Query* ([ITI-18]) mit obigen Suchkriterien ab. Die Anfrage wird anhand einer gültigen HCP-Assertion autorisiert. Die Anfrage wird über das bereichseigene AGW der initiierenden ZGF weitergeleitet.
2. Die initiierende ZGF erhält - kommunizierend mit dem ETS - die Community IDs und Treatment-Assertions für jene ELGA-Bereiche, die potenziell Gesundheitsdaten des ELGA-Teilnehmers führen.
3. Die initiierende ZGF stellt Anfragen **bereichsintern** sowie **bereichsübergreifend** an die Registries der entsprechenden ELGA-Zielbereiche. Die Antworten der einzelnen ELGA-Bereiche werden (durch die Responding ZGFs) entsprechend der individuellen Berechtigungen des ELGA-Teilnehmers (XACML Response-Policies) gefiltert. Im Folgenden wird angenommen, dass das gesuchte KOS-Objekt in einem **entfernten** ELGA-Bereich gefunden wurde und es in ELGA weder ausgeblendet noch gelöscht wurde.
4. Die initiierende ZGF sendet nun basierend auf den Suchkriterien des GDAs entsprechende Dokument-Metadaten (des KOS-Objekts) dem KIS-System zurück (siehe Rückgabe von *KOS-Objekt-ID* in der Abbildung 6).
5. Ausgehend von Informationen der erhaltenen Dokument-Metadaten fordert der GDA das DICOM KOS-Objekt im Originalformat via *Retrieve Document Set* ([ITI-43]) an. Hierfür ist im Security-Header eine HCP-Assertion eingebettet. Die initiierende ZGF setzt die Anfrage als *Cross Gateway Retrieve* ([ITI-39]) um und versieht den Security-Header wie üblich mit einer ELGA Treatment-Assertion.
6. Die antwortende ZGF verifiziert die Treatment-Assertion und holt das KOS-Objekt vom entsprechenden Repository. Sind laut Assertion keine individuellen Berechtigungsregeln anzuwenden, die dies untersagen, übersendet die antwortende ZGF das angeforderte KOS-Objekt der initiierenden ZGF.
7. Die initiierende ZGF übermittelt nun das KOS-Objekt an die ZGF-I, um die Informationen im KOS-Cache integritätsgeschützt abzulegen. ZGF-I berechnet und erstellt ein Message Authentication Code (MAC) über den KOS-Cache-Kontext der mit der HCP-Assertion des GDA fest verbunden wird. Es wird zusätzlich eine Treatment Imaging-Assertion zur bekannten HCP-Assertion angefordert und sicher (verschlüsselt) im Cache abgelegt.
8. Der GDA empfängt als Resultat der *Retrieve Document Set* Abfrage das DICOM KOS-Objekt. Das KIS-System identifiziert und selektiert aus dem KOS-Objekt die gewünschte Studie/Serie.

9. Der GDA setzt nun eine RAD-69 Anfrage über die bereichsinterne AGW an die initiierenden ZGF-I ab. Im Security-Header ist wie üblich eine ELGA HCP-Assertion angeführt.
10. Die initiierende ZGF-I empfängt die RAD-69 Anfrage und verifiziert die HCP-Assertion. Die Anfrage darf nur auf jene Image-Instanzen referenzieren, die im KOS-Cache bereits vermerkt sind und im Kontext der gegebenen HCP-Assertion sind. Dadurch wird sichergestellt, dass nur jene GDA die Anfrage stellen dürfen, an die das KOS-Objekt geliefert wurde.
11. Die initiierende ZGF-I sucht im internen Cache nach einer korrespondierenden ELGA Treatment Imaging-Assertion. Die ZGF-I erstellt nun anhand des zwischengespeicherten Patientenkontexts eine bereichsübergreifende RAD-75 Anfrage an die Responding ZGF-I des Zielbereichs. Die RAD-75 wird via ELGA Treatment Imaging-Assertion autorisiert.
12. Die antwortende ZGF-I empfängt die RAD-75 und verifiziert die Assertion gemäß der in ELGA allgemein gültigen Verifizierungsregeln. Im Unterschied zu sonstigen regulären ITI-Anfragen, greifen im Falle von RAD-75 die individuellen Policies nicht. Dies entfällt aufgrund der bereits im Vorfeld (beim Abholen des KOS-Objekts) rigoros durchgeführten Auswertung der individuellen Berechtigungen.
13. Die antwortende ZGF-I münzt nun RAD-75 auf RAD-69 um und schickt die Anfrage, versehen mit einer Community Imaging-Assertion, an den zuständigen bereichsspezifischen Adapter.
14. Der bereichsspezifische Adapter empfängt die RAD-69, und verbindet sich mit dem per Vorkonfiguration eingerichteten lokalen PACS-Adapter. Der Request ist wie vorher mit einer ELGA Community-Assertion ausgestattet. Das angesprochene PACS-Archiv retourniert die angefragten Daten an den Adapter.
15. Die antwortende ZGF-I sendet das Resultat entweder synchron oder in Form eines kontinuierlichen Streams zurück.

1.6.8. Kopplung von Befunden mit Bilddaten

Es wird davon ausgegangen, dass im Allgemeinen jegliche Bilddaten (KOS-Objekte und Befunde/CDA) via *referenceIdList* aufeinander referenzieren können, und zwar in einer N:M Beziehung.

Die Referenzierung wird über die Accession Number hergestellt. Der Datentyp entspricht CXi und enthält keine *Home Community ID*.

- **Accession Number** mit dem Datentyp: urn:ihe:iti:xds:2013:accession

Es muss davon ausgegangen werden, dass Befund und KOS auf unterschiedliche Wege und zu unterschiedlichen Zeitpunkten entstehen und referenziert werden können. Es muss aber bei der Veröffentlichung von KOS-Objekten (via RAD-68) in die *referenceIdList* des KOS die *Accession Number* eingefügt werden. Das BeS muss eine Überprüfung durchführen, und wenn die *Accession Number* in den Metadaten *referenceIdList* fehlt, muss die RAD-68 Transaktion abgelehnt werden.

Darüber hinaus muss vermerkt werden, dass mehrere KOS-Objekte die gleiche *Accession Number* haben können. Ein e-Befund CDA kann somit gesehen auf 0 bis n beliebige KOS zeigen (referenzieren).

Um die Suche nach referenzierten Dokumenten zu erleichtern bzw. im Sinne der Effizienz sollte das BeS die *Registry Stored Query* [ITI-18] Option *FindDocumentsByReferenceIdList* unterstützen (derzeit nicht umgesetzt).

1.6.9. Versionierung

Für die **Versionierung** von KOS-Objekten wird die bisherige Praxis beibehalten. Im CXi-Wert wird *ownDocument_setId* geführt, sowie *Home Community ID*. Es ist jedoch wichtig anzumerken, dass im KOS keine *setId* vorhanden ist (wie etwa bei CDA). Daher ist eine andere eindeutige ID zu verwenden.

1.6.10. APPC

Es muss davon ausgegangen werden, dass Befund und KOS auf verschiedenen Wegen und zu verschiedenen Zeiten entstehen. Der APPC wird unter Umständen von verschiedenen Instanzen ermittelt, daher ist es möglich, dass KOS und Befund nicht die gleichen APPCs enthalten.

Bei der Veröffentlichung (via RAD-68) von KOS-Objekten muss jedoch in den Metadaten *eventCodeList* entsprechend Metadaten-Leitfaden [3] bzw. [4] zumindest ein APPC-Code eingefügt werden. Das BeS muss den APPC prüfen und wenn kein APPC in *eventCodeList* eingefügt ist, dann muss die RAD-68 Transaktion vom BeS abgelehnt werden. Es können auch mehrere APPC angeführt werden.

1.7. Erweiterung der Architektur

Die technologische Entwicklung und das Fortschreiten der Standardisierung erlauben neue Bilddaten-Übertragungskonzepte. Hierbei ist insbesondere das IHE WIA-Profil [6] hervorzuheben, das, wie im Titel auch erfasst, das Internet (das Web) für die Übertragung postuliert. Dennoch kann diese Technologie auch in den gesicherten Gesundheitsnetzen genutzt werden. In den weiteren Abschnitten wird die daraus folgende Architektur erörtert.

1.7.1. Fragmentierte Natur der Gesundheitsnetzwerke

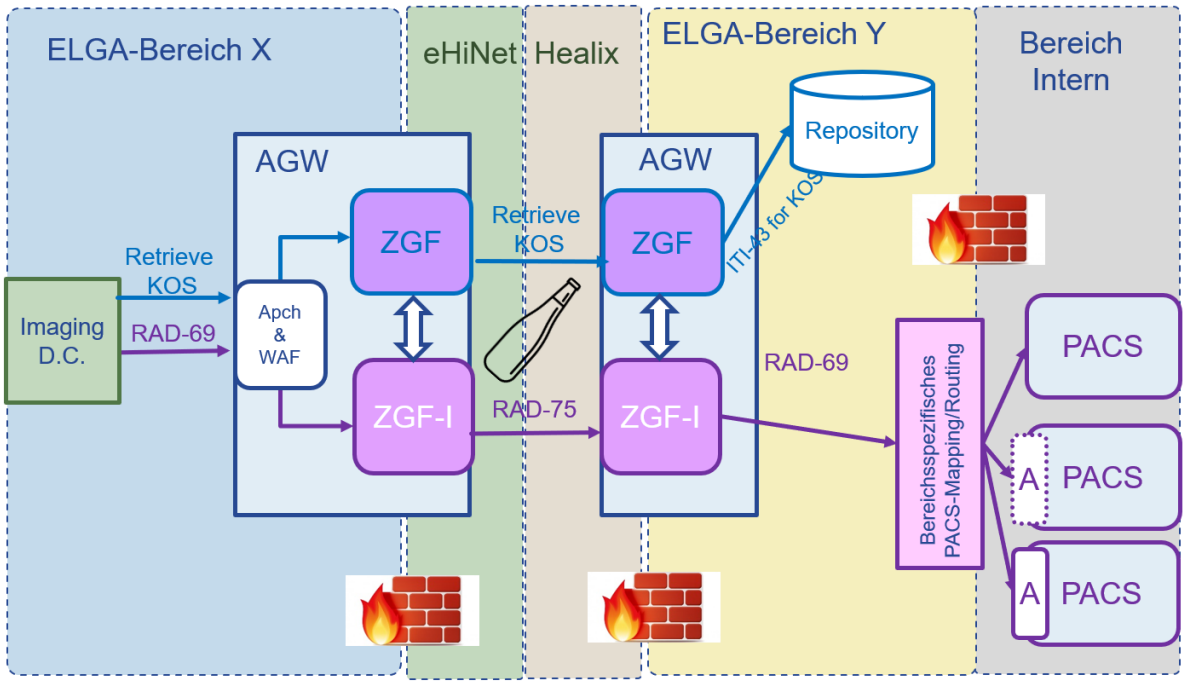


Abbildung 7: Fragmentierte Gesundheitsnetzwerke

Wie obige Abbildung hervorzuheben versucht, ist die historisch gewachsene Fragmentierung der Gesundheitsnetzwerke zu berücksichtigen, da diese Landschaft eine große Herausforderung für die Einführung von Point-to-Point Internet-Protokollen (REST), darstellt. Insbesondere für den Übergang zwischen eHi-Net und HEALIX waren bisher keine großen Bandbreiten notwendig – das ändert sich mit der Übertragung von Bilddaten.

Einen potenziellen „Flaschenhals“ (siehe Abb. 7) stellt die Kopplung zwischen den Gesundheitsnetzen am Peering Point dar, der aktuell mit ca. 500 Mbit/s synchron ausgebaut ist. Da trotz Pilotierungen in verschiedenen Szenarien belastbare Zahlen zur erwartbaren Gesamtlast fehlen, muss man sich in Hinblick auf tatsächlich benötigte Bandbreiten annähern. Als Ausgangsbandbreite wird aus den Erfahrungen der bisherigen Pilotierungen 1Gbit/s als erforderliche Bandbreite für Bilddatenübermittlung an der Kopplung der Gesundheitsnetze (eHI, HEALIX) definiert. Zusätzlich ist an Netzübergängen bzw. vom Document-Consumer

bis zur Document-Source ein abgestimmtes und durchgängiges QoS (Quality of Service) zu etablieren, um anderen Netzwerktraffic im Falle von Kapazitätsengpässen entsprechend den Anforderungen zu bewerkstelligen. Pakete mit Bilddaten werden Netzwerktechnisch entsprechend markiert. An den Netzkopplungen obliegt die Verantwortung der Implementierung den Betreibern der Gesundheitsnetze.

Auf der Last-Mile ist der GDA dafür verantwortlich, diese QoS durch seinen Provider implementieren zu lassen. Auch die Anschlussbandbreite der Last-Mile obliegt dem Document-Consumer bzw. der Document-Source in Abhängigkeit zu seinen konsumierten bzw. angebotenen Diensten.

Es ist bekannt, dass das REST-Protokoll, das sowohl dem FHIR-Standard von HL7 als auch dem DICOMweb-Standard zugrunde liegt, nur bei direkten Punkt-zu-Punkt-Verbindungen sein volles Potenzial entfalten kann (siehe hierfür auch die IHE WIA-Profile [6]). Der Einsatz dieses Protokolls in fragmentierten Netzwerken, insbesondere mit AGW-Bausteinen, stellt eine Herausforderung dar und beinhaltet einige Hindernisse bei den einzelnen Netzübergängen (etwa verpflichtende TLS-Terminierungen, Mapping von Endpunkten). Es spricht jedoch nichts gegen eine alternative Implementierung in den gesicherten Gesundheitsnetzwerken ohne die herkömmlichen AGW. Siehe weitere Ausführungen in den nachfolgenden Kapiteln.

1.7.2. Gründe für die Erweiterung auf IHE WIA

Zusätzlich zu den netzwerktechnischen Überlegungen, führt auch die Tatsache, dass RAD-69 ausschließlich die Übertragung von Bilddaten in originaler Qualität und im DICOM-Format zulässt, zu weiteren Herausforderungen. In Anwendungsfällen, wo kein DICOM-Viewer bereitsteht (z.B. bestimmte Zuweiser, oder das ELGA-Bürgerportal), stellt RAD-69 keine realistische Option dar.

2017 wurde der erste Draft des IHE Integrationsprofils Web-based Image Access (WIA) veröffentlicht. Ziel dieses Profils ist, den einrichtungsübergreifenden Zugriff auf Bilddaten über DICOMweb niederschwellig zu ermöglichen. Eine Übertragung von komprimiertem Bildmaterial in Formaten, die auch in einem Standard-Browser dargestellt werden können, ist per Default vorgesehen. Passenderweise für ELGA, wurde im Zuge der Weiterentwicklung des Integrationsprofils auch ein Anwendungsfall detailliert, der im Backend eine XDS-I Infrastruktur verortet. Darauf aufbauend beschreibt das nächste Kapitel die Erweiterung der Architektur.

1.8. IHE WIA Architektur im abgesicherten Netzwerk

Eine alternative Lösungsarchitektur in den abgesicherten Gesundheitsnetzen (siehe Abbildung 8) beruht auf der Wiederverwendung der bereits existierenden und etablierten Autorisierungsprotokolle von WS-Trust via SAML2 und ETS. Die Abfrage des Bildmaterials läuft entsprechend WIA-Profil Use Case #4 [6].

Im ersten Schritt setzt der Imaging Document Consumer (IDC) Akteur (GDA) eine QIDO-RS Abfrage an einen zentralen QIDO-RS Endpunkt (siehe 1.8.2) und holt sich damit **indirekt**, mittels QIDO-as-a-Service Komponente (QIDOaaS), ein oder mehrere KOS ab. QIDOaaS muss die in den KOS-Objekten enthaltenen Informationen nachbearbeiten (formatieren) und die erreichbaren WADO-RS Endpunkte in die Antwort einfügen. Die vom QIDOaaS abgeholten KOS-Objekte werden zusätzlich in einem zentralen KOS-Cache (vgl. 1.6.5.3) aufgehoben (Studien, Serien, SOP-Instance ID) und für spätere WADO-RS Anfragen der WADO-Service-Facade (WADO-SF) zur Verfügung gestellt. Bei einem nachfolgenden WADO-RS Zugriff wird nämlich die Zulässigkeit der Abfrage mit dem im KOS-Cache vorhandenen Informationen abgeglichen (exakt wie bei XCA-I). Nur jene SOP-Instanzen dürfen abgefragt werden, die in den im KOS-Cache aufgehobenen KOS-Objekten auch gelistet sind.

Die UML-Sequenz der Zugriffe ist in der Abbildung 9 dargestellt. Vorbedingung für die Durchführung der QIDO-RS und WADO-RS Abfragen ist der Besitz einer gültigen HCP-Assertion. In der abgebildeten Zugriffs-Variante beantragt die QIDOaaS eine entsprechende Treatment-Assertion mit der gültigen HCP-Assertion.

1.8.1. QIDO Service Facade (QIDO-SF)

Eine QIDO-SF ist ein dezentral laufender Teil des Berechtigungssystems und dient als vorgeschalteter Schutz vor der entsprechenden QIDOaaS-Komponente (siehe 1.8.2). Sie validiert herankommende QIDO-RS Anfragen und deren Authorization-Assertions auf Gültigkeit. Anonyme Anfragen oder Anfragen mit ungültigen SAML-Assertions müssen abgewiesen werden.

Wenn im Authorization-Header der Anfrage eine gültige und validierte HCP-Assertion (oder User I Assertion) angeführt ist, dann wird die Anfrage an die QIDOaaS-Komponente weitergeleitet. Im Authorization-Header wird die empfangene HCP-Assertion eingebettet. Die QIDOaaS-Komponente verwendet sie und setzt damit eine WS-Trust Issue RST an ETS für eine ELGA Treatment-Assertion ab (um nachfolgende [ITI-18/43] Transaktionen ausführen zu können).

1.8.1.1. Protokollierung

QIDO-SF protokolliert entsprechend der bereits bekannten Regeln einer initiierenden AGW, und zwar in L-ARR und A-ARR. Nachdem aber QIDO-SF zentral aufgestellt und ein Cloud-Dienst ist, kann L-ARR mit dem Z-L-ARR (zentrale L-ARR) ersetzt werden.

1.8.2. QIDO-as-a-Service (QIDOaaS)

QIDOaaS ist ein auf Cloud-Technologie basierender, zentraler Service (Dienst) mit einer vorgeschalteten Service Facade (Abbildung 8), die wiederum als dezentral laufender Teil des Berechtigungssystems zu verstehen ist. Die Hauptaufgabe der zentralen QIDOaaS-Komponente ist es, QIDO-RS Anfragen zu beantworten und sekundär wie ein Service-Discovery Dienst (für WADO-RS Endpunkte) zu dienen.

QIDOaaS muss zuerst vom ETS eine oder mehrere ELGA Treatment-Assertions anfordern. QIDOaaS präsentiert hierfür die bei der Initialanfrage (QIDO-RS) übermittelte HCP-Assertion (oder User I Assertion), die durch die dezentrale Berechtigungssystemkomponente (die QIDO Service Facade) übergeben wurde.

Soweit ETS (nach Validierungen und Policy Überprüfungen) die ELGA Treatment-Assertions (laut PIX-Query) ausstellen konnte, muss die QIDO-RS Abfrage auf SOAP-basierende IHE Transaktionen übersetzt werden. Es wird zuerst eine Registry Stored Query [ITI-18] für KOS-Objekte abgesetzt und danach müssen die zutreffenden KOS-Objekte geladen werden [ITI-43].

Darüber hinaus muss eine Vorgehensweise etabliert werden, indem die zu den Studien/Serien passenden WADO-RS Endpunkte ermittelt werden und in die RESTful-Antwort [RAD-129] eingebettet werden (laut Bestimmungen des Richardson Maturity Models, siehe bei Martin Fowler[3]). Hierfür sind die dafür prädestinierten KOS-Attribute (Retrieve URL, Retrieve AET, Retrieve Location UID) zu konsultieren und weitere (organisatorische) Maßnahmen heranzuziehen (etwa tabellarische Erfassung bekannter WADO-RS Endpunkte als Teil der Systemkonfiguration). Anschließend muss QIDOaaS die geladenen KOS-Objekte im eigenen zentralen Cache für eine gewisse vorkonfigurierte Zeit (30 Minuten) aufheben.

Zuletzt muss QIDOaaS die Antwort formatieren, mit DICOM-Metadaten (vom KOS und anhand der ELGA Metadaten) entsprechend der Spezifikation anreichern und zurücksenden.

[3] https://www.martinfowler.com/articles/richardsonMaturityModel.html

1.8.2.1. Protokollierung

Die QIDOaaS-Komponente protokolliert entsprechend der bereits bekannten Regeln einer initiierenden AGW, und zwar in L-ARR und A-ARR. Nachdem aber QIDOaaS zentral aufgestellt und ein Cloud-Dienst ist, kann L-ARR mit dem Z-L-ARR (zentrale L-ARR) ersetzt werden.

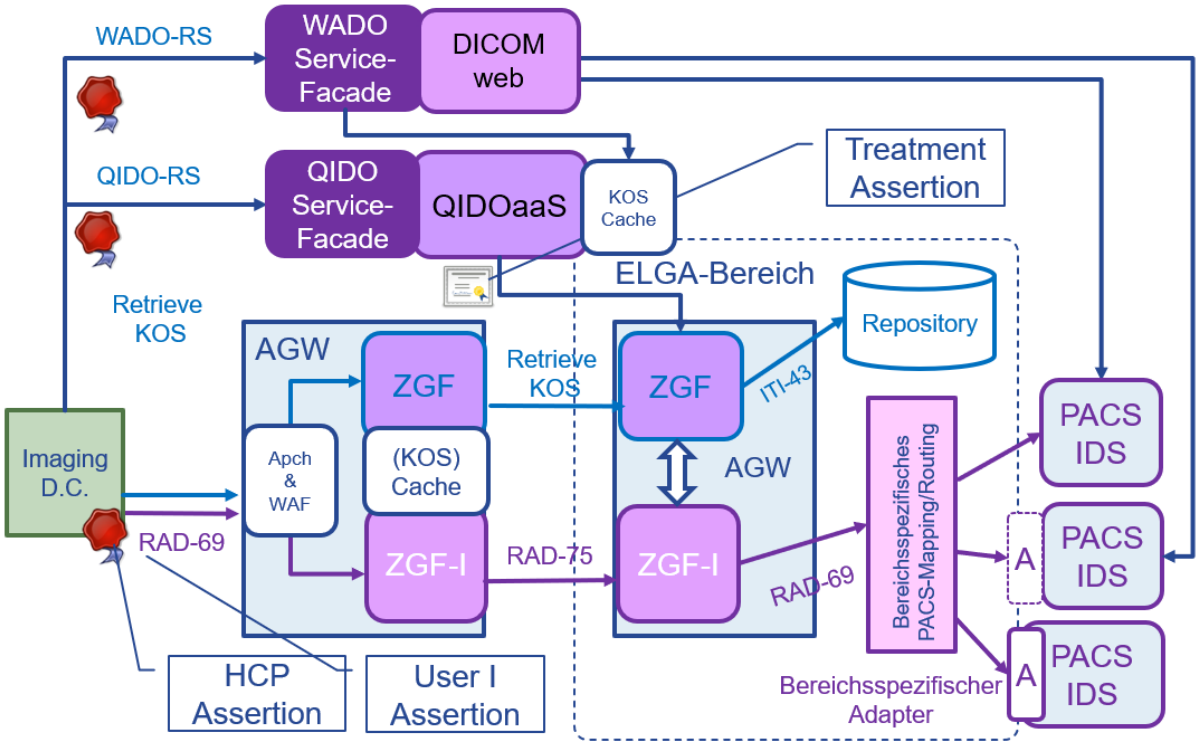


Abbildung 8: Alternative Implementierung des WIA-Profils mit WS-Trust und SAML2-Autorisierung. Die roten Stempel bezeichnen eine existierende und gültige HCP-Assertion. Die QIDO-Service-Facade und die WADO-Service-Facade sind dezentrale Teile des Berechtigungssystems.

1.8.3. WADO Service Facade (WADO-SF)

Eine WADO-SF ist ein dezentral laufender Teil des Berechtigungssystems und dient als vorgeschalteter Schutz vor einem entsprechenden DICOMweb-Service, welcher WADO-RS Anfragen umsetzt. Sie empfängt und validiert herankommende WADO-RS Anfragen. Die WADO-SF kann einen herankommenden WADO-RS Request an den DICOMweb-Service nur dann weiterleiten, wenn

1. Im Authorization-Header der Anfrage eine gültige (validierte) HCP-Assertion (oder User I Assertion) angeführt ist
2. Die in der WADO-RS Anfrage angeführten Studien/Serien und SOP-Instanzen im KOS-Cache der QIDOaaS-Komponente mit dem GDA-OID des Imaging Document

Consumers (GDA) verknüpft sind und damit erlaubt sind. Hierfür ist eine zusätzliche Anfrage an den KOS-Cache der QIDOaaS-Komponente abzusetzen.

Die wie oben angeführt validierte Anfrage wird in der Folge an das DICOMweb-Service entweder mit einem JWT Community-Token oder mit einer ELGA Community Assertion (konfigurierbar) im Authorization-Header weitergeleitet.

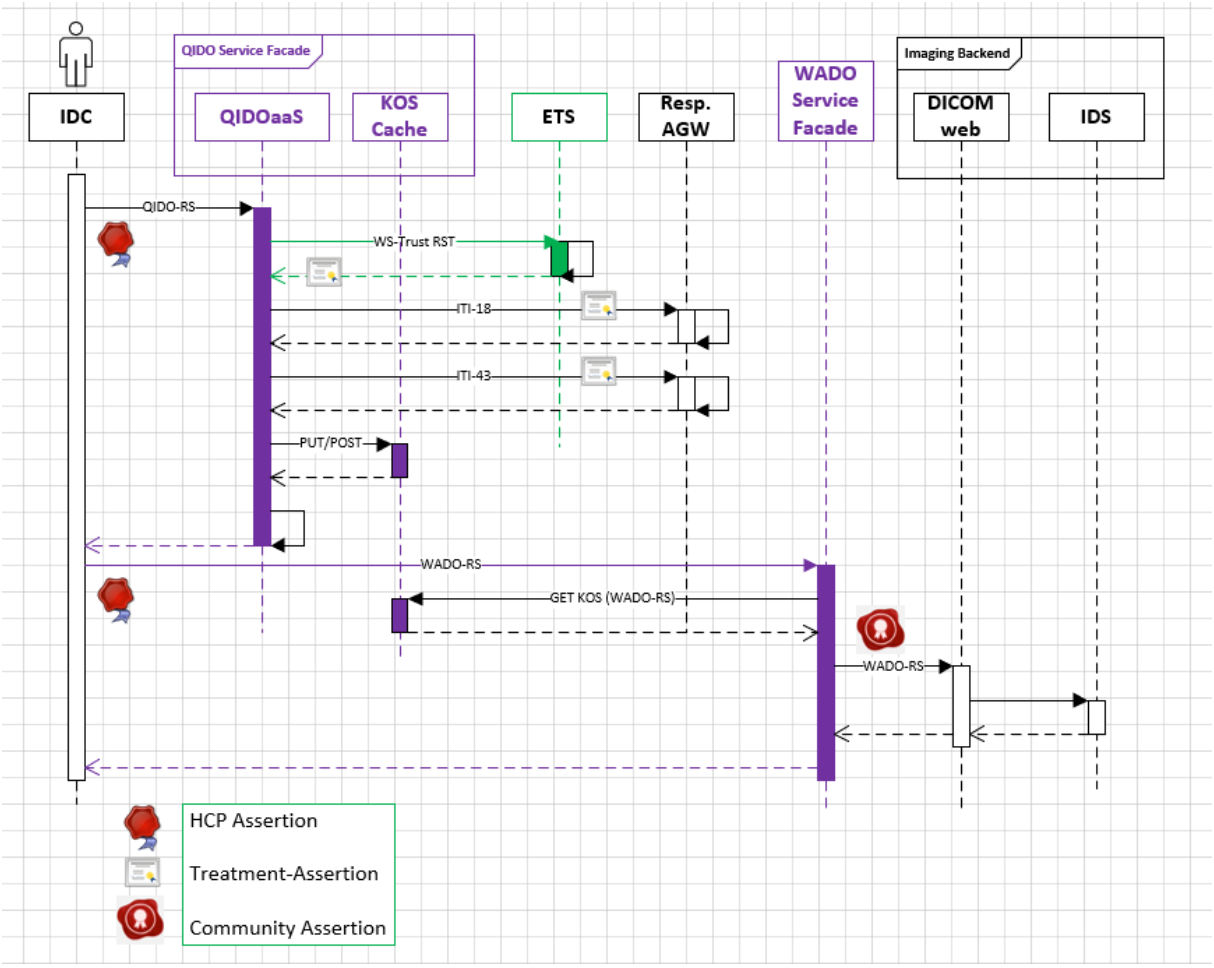


Abbildung 9: UML-Sequenz für Bilddaten-Zugriffe in den Gesundheitsnetzwerken

1.8.3.1. Protokollierung

WADO-SF kann entsprechend der bereits bekannten Regeln einer initiierenden AGW protokollieren, und zwar in L-ARR und A-ARR. Der jeweilige Betreiber von WADO-RS Komponente muss dafür Sorge tragen, dass ein entsprechendes L-ARR (Syslog-Server) zur Verfügung gestellt wird. Wie die WADO-RS Anfragen im A-ARR protokolliert werden, ist noch nicht spezifiziert.

1.8.4. Ablauf und GDA-Kommunikation

Entsprechend Abbildung 9 startet die Abfrage der Bilddaten in den gesicherten Gesundheitsnetzwerken wie folgt:

1. GDA ist bereits authentifiziert und mit einer gültigen HCP-Assertion angemeldet
2. GDA IDC sendet eine RAD-129 (QIDO-RS) Anfrage an die zentral aufgestellte QIDO-SF. Im Authorization-Header ist eine gültige HCP-Assertion eingefügt
3. QIDO-SF empfängt die Anfrage und validiert sie. Die HCP-Assertion wird entsprechend der gültigen ELGA-Richtlinien validiert.
4. Wenn die Nachricht und HCP-Assertion valide sind, wird die Nachricht inklusive der HCP-Assertion an die QIDOaaS-Komponente weitergeleitet.
5. QIDOaaS fragt bei ETS mit WS-Trust Issue RST eine entsprechende Anzahl von ELGA Treatment-Assertions ab.
6. QIDOaaS verhält sich wie eine initiierende ZGF und mit den erhaltenen ELGA Treatment Assertions startet sie parallele ITI-18 FindDocuments Queries (Filter auf KOS-Dokumentenklasse) an die adressierten ELGA-Bereiche.
7. QIDOaaS lädt die per vorherigen Query erhaltenen KOS-Objekte via ITI-43 Anfragen. KOS-Objekte werden nun im Cache für gewisse Zeit (30 Minuten) zwischengespeichert.
8. QIDOaaS extrahiert von den KOS-Objekten die für die QIDO-RS Antwort notwendige Informationen und formatiert sie. Entsprechend der Vorgaben müssen valide WADO-RS Endpunkte in die Antwort eingefügt werden, soweit solche vorhanden sind. Falls kein Endpunkt verfügbar ist, z.B. weil die IDS noch nicht DICOMweb-fähig ist, muss der IDC stattdessen den XCA-I Weg mit RAD-69 gehen.
9. QIDOaaS sendet die Antwort über die QIDO-SF dem GDA IDC.
10. QIDOaaS protokolliert die Events in Z-L-ARR und A-ARR
11. QIDOS-SF protokolliert die Events in Z-L-ARR
12. GDA IDC empfängt die QIDO-RS Antwort und baut daraus eine WADO-RS Anfrage auf.
13. GDA IDC sendet WADO-RS Anfrage [RAD-107] an den angeführten (in der QIDO-RS Antwort) WADO-RS URL inklusive HCP-Assertion im Authorization-Header.
14. WADO-SF empfängt die Anfrage und validiert sie, inklusive HCP-Assertion.

15. WADO-SF muss die GET-Query analysieren und die adressierten Studien, Serien, SOP-Instanzen über eine spezifische Anfrage mit dem KOS-Cache abgleichen. Enthält der KOS-Cache die in der Anfrage angeführten Studien, Serien und SOP-Instanzen verbunden mit dem GDA-OID des anfragenden IDC, dann kann die Anfrage an den DICOMweb-Service weitergeleitet werden.
16. WADO-SF leitet die WADO-RS Anfrage je nach Konfiguration entweder mit einer ELGA Community-Assertion oder mit einer JWT Community-Token weiter.
17. WADO-SF protokolliert die Events in Z-L-ARR. Analog zur RAD-69 (XCA-I/XDS-I) wird zum jetzigen Zeitpunkt in A-ARR nicht protokolliert.

1.9. IHE WIA Architektur im Internet

Eine technische Lösung über das Internet ist in der Abbildung 10 dargestellt. Hierfür ist es notwendig allen betroffenen Imaging Document Consumer (IDC) Akteure einen entsprechenden sicheren Internetzugang auf die DICOMweb-Service Endpunkte zu gewähren. Die Endpunkte sind durch die fürs Internet gehärteten Alternativvarianten der antwortenden AGW/ZGF in Form von vorgeschalteten Autorisierungsfassaden (QIDO-SF/WADO-SF) geschützt.

Auch in dieser Architekturvariante (Abbildung 10) ist davon auszugehen, dass die Abfrage des Bildmaterials entsprechend WIA-Profil Use Case #4 [6] ablaufen wird. Die Akteure agieren weitgehend analog zur IHE WIA Architektur in Gesundheitsnetzen.

Anmerkung: Die Internet-Lösung befindet sich noch in der Konzeptionsphase und erhebt keinen Anspruch auf Vollständigkeit. Die Beschreibung in diesem Dokument dient als Ausblick auf die künftige Ausrichtung. Technische Details können sich noch ändern.

1.9.1. QIDO Service Facade (QIDO-SF)

Die QIDO-SF ist ein dezentral laufender Teil des Berechtigungssystems. Sie autorisiert und schützt die QIDOaaS-Komponente vor nicht zulässigen Zugriffen. Sie stellt einen zentralen QIDO-RS Endpunkt (URL) zur Verfügung. Die Autorisierung der [RAD-129] Anfragen erfolgt im Sinne der OAuth2-Protokolle. Die Anfrage ist entweder innerhalb einer bereits aufgebauten Session autorisiert oder es muss anhand des Code-Token (im Authorization-Header) eine neue Session zum anfragenden Clienten (IDC) aufgebaut werden. Hierfür fragt die QIDO-SF im Back-Channel vom OTS einen entsprechenden Access-Token ab. Wenn der Access-Token den Zugriff erlaubt, dann initiiert QIDO-SF damit eine Abfrage für eine HCP-Assertion (oder User I Assertion). Anschließend wird die Anfrage inklusive HCP-Assertion im Authorization-Header an die QIDOaaS-Komponente weitergeleitet.

1.9.2. QIDO-as-a-Service (QIDOaaS)

Der QIDO-RS Endpunkt der QIDOaaS-Komponente ist mit einer vorgeschalteten QIDO-SF geschützt. Über eine QIDO-RS [RAD-129] Query, wie vom WIA-Profil vorgesehen, wird **indirekt** ein oder mehrere KOS abgefragt und die Antwort entsprechend nachjustiert und formatiert. Die tatsächliche KOS-Abfrage erfolgt via SOAP-basierten XDS/XCA-Anfragen [ITI-18/43]. Netzwerk- und Protokollwechsel, wie abgebildet (vom Internet in die Gesundheitsnetzwerke), ist entsprechend IHE MHD-Profil vorzusehen. Die von der QIDO-SF empfangene Anfrage muss eine HCP-Assertion (oder User I Assertion) im Authorization-Header haben. Die QIDOaaS-Komponente als vertrauenswürdige Einheit, beantragt damit eine oder mehrere ELGA Treatment Assertions. Die QIDO-RS Anfrage wird auf [ITI-18/43] Transaktionen umgewandelt.

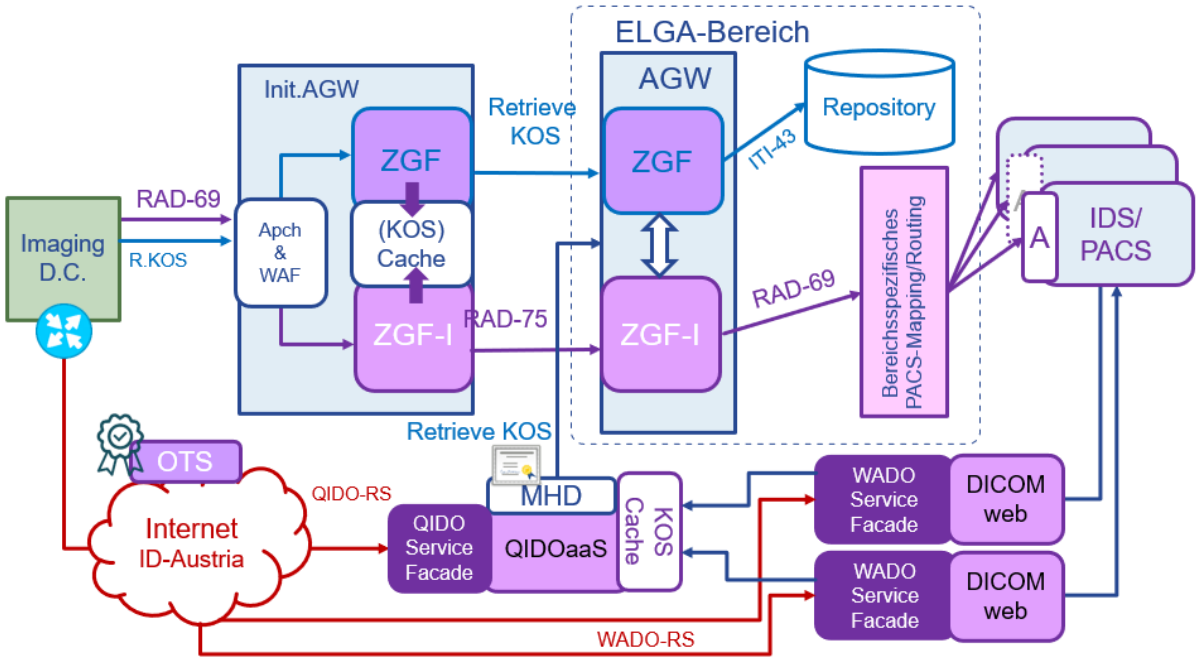


Abbildung 10: QIDO- & WADO-RS Implementierung über das Internet. OTS (OAuth2 Token Service) sowie QIDO-SF und WADO-SF sind neue Komponenten des ELGA/e-Health Berechtigungssystems. IDS = Imaging Document Source (eventuell auch ein Kurzzeitarchiv)

In der REST-Antwort von der QIDOaaS-Komponente muss immer der jeweils zuständige WADO-RS Endpunkt [RAD-107] sog. „retrieve URL“ (entsprechend Richardson Maturity Model[4]) angeführt werden (soweit bekannt).

[4] https://www.martinfowler.com/articles/richardsonMaturityModel.html

1.9.3. WADO Service Facade (WADO-SF)

Die im Kernbereich (Gesundheitsnetzwerke) geltenden Regeln „ohne KOS kein Bildmaterial“ wird auch hier (mit den Mechanismen des Berechtigungssystems) nahtlos umgesetzt. Anders gesagt, vor einem WADO-RS Aufruf muss zeitnah eine entsprechende QIDO-RS Transaktion durchgeführt werden. Die QIDO-RS Antwort gibt eindeutige Anhaltspunkte, auch bezüglich des Vorhandenseins von WADO-RS Endpunkten. Wenn in der Antwort kein „retrieve URL“ angeführt ist, kann das Bildmaterial nur klassisch (XDS-I/XCA-I) in den Gesundheitsnetzwerken abgeholt werden.

Der WADO-RS Endpunkt der WADO-SF ist daher nur dann sinnvoll anzusteuern, wenn der IDC vorher bereits eine erfolgreiche QIDO-RS Antwort erhalten hat. Die initiale WADO-RS Anfrage ist mit einem Code-Token (ausgestellt vom OTS) anzusteuern. WADO-SF nimmt den Code-Token entgegen und fragt im Back-Channel vom OTS den eigentlichen Access-Token ab. Wenn der Access-Token gültig ist und den Zugriff erlaubt, dann wird eine Session zum IDC aufgebaut. Zusätzlich macht WADO-SF eine entsprechende KOS-Cache Abfrage, um die inhaltliche Zulässigkeit der WADO-RS Anfrage zu prüfen. Erst wenn diese Prüfung erfolgreich ist, kann die Anfrage mit einem Community JWT-Token an den nachgeschalteten DICOMweb-Service weitergereicht werden. Siehe auch Kapitel 1.9.5 für detaillierte Ausführung des Kommunikationsablaufes.

1.9.4. Authentifizierung und Zugriffsautorisierung

Das Internet bedingt geeignete Authentifizierungs- und Autorisierungsprotokolle wie Open ID Connect bzw. OAuth2 (Version 2.1 oder höher). Darüber hinaus sind zusätzliche Maßnahmen und Empfehlungen für Sicherheit bei Umgang mit dem OAuth2-Framework, z.B. [8], zu berücksichtigen.

1.9.4.1. Authentifizierung

Die Authentifizierung der Anwender und Teilnehmer kann ausschließlich an vertrauenswürdige Identity Provider (IdP) ausgelagert werden, die OIDC/OAuth2 unterstützen. Im Internetumfeld ist derzeit nur ID-Austria als vertrauenswürdiger IdP anzusehen. Nach einer erfolgreichen Authentifizierung wird die elektronische Identität der Person (Anwender) durch eine bPK-GH im e_id Token bestätigt.

Der OAuth2 Internet Token Service (OTS) ist für die Autorisierung zuständig. OTS stellt Access-Tokens im Sinne von OAuth2 aus. Darüber hinaus steuert OTS einen entsprechenden „Authorization Code Grant Flow“ (siehe OpenID Connect [9]), soweit ein anonymer Request den dafür zuständigen Endpunkt des OTS erreicht. OTS leitet demnach eine hereinkommende anonyme Anfrage an die zuständige Authentifizierungsstelle (z.B. ID-Austria/Digitales Amt) um.

Um eine bereits im ELGA-Umfeld authentifizierte Personen (Anwender/Teilnehmer) zu autorisieren (bzw. zu föderieren), muss eine Verknüpfung (bzw. Mapping) des bereits bestätigten bPK-GH zu einem im GDA-Index geführten GDA-OID gewährleistet sein. Diese Verknüpfung ist daher eine grundlegende Voraussetzung für eine erfolgreich abschließbare Authentifizierung von Anwendern und Teilnehmern.

Alternative IdP im Internetumfeld müssen die entsprechenden standardisierten Protokolle OIDC/OAuth2 umsetzen und für einen Internetbetrieb gehärtet (und zertifiziert) sein (z.B. e-Card-System).

1.9.4.1.1. Authentifizierung im Internet ohne ID-Austria

Wenn ein Anwender (GDA) bereits in den Gesundheitsnetzwerken authentifiziert ist und eine gültige HCP-Assertion besitzt, dann kann gemäß RFC 7522 der Richtlinie der OAuth Working Group „SAML 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants“ ein JWT-Access-Token vom OTS angefordert und damit föderiert werden. Der vom OTS ausgestellte Access-Token ermächtigt die Anwender (und Teilnehmer) für reguläre QIDO-RS und WADO-RS Zugriffe.

1.9.4.2. Autorisierung

Autorisierung der QIDO/WADO-Zugriffe erfolgt entsprechend geltenden GTelG Vorgaben. Die Umsetzung wird durch eine zentrale OTS-Instanz (als Authorization Server im Sinne von OAuth2) und durch vorgeschalteten Service Facaden durchgeführt (siehe Abbildung 10 sowie Kapitel 1.9.2 und 1.9.3). Im Access-Token, der vom OTS ausgestellt wird, werden alle Zugriffsrechte der Anwender aufgelistet. Die vorgeschalteten Service Facaden überprüfen, ob im Access-Token, der gerade angesprochene URL-Service Endpunkt angeführt und gestattet ist. Wenn der Zugriff erlaubt ist, reichen die Service Facaden die Anfrage unverändert an die zuständigen Services (QIDOaaS oder DICOMweb) weiter. Im Authorization-Header wird zusätzlich und ausschließlich für Informations- und Protokollierungszwecke ein Community-Token gesetzt (entspricht inhaltlich der bekannten Community-Assertion).

1.9.4.3. KOS/QIDO-Spezifika

Die Zugriffsautorisierung für Bilddaten erfolgt im Fall von XDS-I/XCA-I auf Basis des berechtigten Besitzes des entsprechenden KOS-Objektes, welches für die Dauer von 30 Minuten im lokalen Cache der initiierenden AGW/ZGF aufgehoben wird. Nachfolgende RAD-69 Zugriffe über die AGW/ZGF werden erst nach Abgleich mit dem im Cache gespeicherten KOS erlaubt. Anders gesagt, wenn ein GDA berechtigt ist, auf ein KOS zuzugreifen und dieses abzurufen, wird das ELGA-BeS auch die nachfolgenden RAD-69 autorisieren und zulassen, sofern nur im KOS angeführte SOP-Instanzen adressiert sind.

Eine entsprechende Alternativlösung über das Internet muss mithilfe der QIDOaaS Komponente vorgesehen werden. In diesem Szenario muss zuerst eine QIDO-Abfrage (WIA-Profil) erfolgen. Nach einem erfolgreichen Zugriff hebt das QIDOaaS die so eingelesenen und an eine GDA-OID/bPK-GH Pärchen gebundenen KOS und deren Metadaten im eigenen Cache auf (siehe Abbildung 11, UML-Sequenz). Bei nachfolgenden WADO-RS Zugriffen mit demselben GDA fragt die zuständige WADO-SF das im zentralen QIDO-Cache gehaltene KOS ab (Studien/Serien/SOP-Instanzen). Der WADO-RS Zugriff wird nur dann erlaubt, wenn die in der Abfrage angeführten SOP-Instanzen im entsprechenden KOS (Cache) beinhaltet sind.

1.9.4.4. Das „Retrieve URL“ (0008,1190) Problem

Prinzipiell kann davon ausgegangen werden, dass die QIDO-Antwort auf einem dazu passenden KOS-Objekt beruht. Anders gesagt, um eine QIDO beantworten zu können, muss ein entsprechendes KOS gelesen/gefunden werden (siehe Abbildung 10, Abbildung 11). Wird daher für QIDO ein KOS herangezogen, dann muss das im KOS vorhandene „retrieve URL“-Attribut eventuell überprüft und bearbeitet werden. Nachdem das Attribut „retrieve URL“ optional ist, gibt es keine Garantie, dass diese Information vorhanden ist. Somit gesehen müssen organisatorisch und technisch Alternativ-Wege (Attribut AE-Title oder RetrieveLocationUID) gefunden werden, um den tatsächlichen WADO-RS Endpunkt (URL) zu eruieren. Fest steht jedoch, dass das im KOS angeführte „retrieve URL“ Attribut nicht automatisch und ungeprüft für Zugriffe entsprechend WIA-Profil anzuwenden sind.

1.9.5. Ablauf und GDA-Kommunikation mit DICOMweb-Services im Internet

Prinzipiell muss das so genannte "*Authorization Code Grant*" Verfahren gemäß OIDC/OAuth2 Standards [7] implementiert werden. Konkret wird von folgendem Szenario ausgegangen (UML-Sequenz siehe in der Abbildung 11 weiter unten):

1. Die Authentifizierung von GDA IDC startet durch einen anonymen Request an den entsprechenden Endpunkt des OTS. Damit beginnt der Prozess eines *Authorization Code Grant Flows* (grün umrahmter Bereich links oben in der Abbildung 11). Der anonyme Request wird automatisch an ID-Austria umgeleitet, wo die tatsächliche Authentifizierung stattfindet. Am Ende des Prozesses stellt OTS für den GDA-Akteur einen „Code2“-Hash Token aus (weil „Code1“ von ID-Austria ausgestellt wird).
2. GDA IDC kontaktiert mit „Code2“ den QIDO-RS Endpunkt von QIDO-SF und baut eine Session auf
3. QIDO-SF fragt mit „Code2“ (im *Back-Channel*) den Access-Token vom OTS ab und wenn der Token gültig und der Zugriff autorisiert ist, beantragt sie bei ETS via WS-Trust Issue RST Anfrage eine ELGA HCP-Assertion (oder User I Assertion). Danach

leitet sie die QIDO-RS Anfrage mit der HCP-Assertion im Authorization-Header an die QIDOaaS-Komponente weiter.

4. QIDOaaS arbeitet wie eine initiierende ZGF und anhand erhaltener HCP-Assertion beantragt bei ETS eine (oder mehrere) ELGA Treatment-Assertion. Danach holt sie damit ein oder mehrere KOS vom Kernsystem ab [ITI-18/43]. Hierbei kommt eine Protokollumsetzung via IHE MHD-Profil zum Zug.
5. QIDOaaS speichert die gelesenen KOS-Objekte, Studien, Serien, SOP-Instanzen im eigenen zentralen KOS-Cache (verknüpft mit dem GDA.OID des IDC) für gewisse Zeit (etwa 30 Minuten). Die QIDO-RS Antwort wird formatiert, mit DICOM-Metadaten aus dem KOS angereichert (inklusive „Retrieve URL“) und an QIDO-SF weitergeleitet.
6. QIDOaaS protokolliert in Z-L-ARR und in A-ARR
7. QIDO-SF sendet die Antwort an den GDA IDC.
8. QIDO-SF protokolliert in Z-L-ARR
9. GDA IDC erkennt (identifiziert) in der erhaltenen QIDO-Antwort den notwendigen WADO-RS Endpunkt.
10. GDA kontaktiert mit noch gültigem „Code2" den WADO-RS Endpunkt (WADO-Service-Facade).
11. WADO-Service-Facade holt mit „Code2“ im Back-Channel vom OTS den gültigen Access-Token.
12. Wenn der Access-Token den Zugriff prinzipiell genehmigt, kontaktiert die WADO-Service-Facade den beim QIDOaaS eingerichteten KOS-Cache (entsprechender Endpunkt), um die Autorisierung des angefragten Bildmaterials zu vervollständigen. Wenn der Zugriff nur auf im KOS-Cache aufgehobenen Studien/Serien/SOP-Instanzen beschränkt ist, dann wird die Anfrage an den DICOMweb-Service weitergeleitet.
13. Es wird darüber hinaus zwischen GDA und WADO-SF eine Session aufgebaut.
14. WADO-SF leitet die WADO-RS Anfrage an den dahinterstehenden DICOMWeb-Service mit einer Art JWT "Community-Token" im Authorization-Header weiter. Der „Community-Token“ dient als Information für ein eventuelles Auditing.
15. WADO-SF protokolliert die Ereignisse (Events) im zur Verfügung gestellten L-ARR
16. WADO-Service-Facade muss die WADO-RS Anfrage ablehnen, wenn im entsprechenden Scope des KOS-Caches die angeforderten Bilddaten (Studien/Serien oder SOP-Instanzen) nicht geführt (nicht erlaubt) sind.

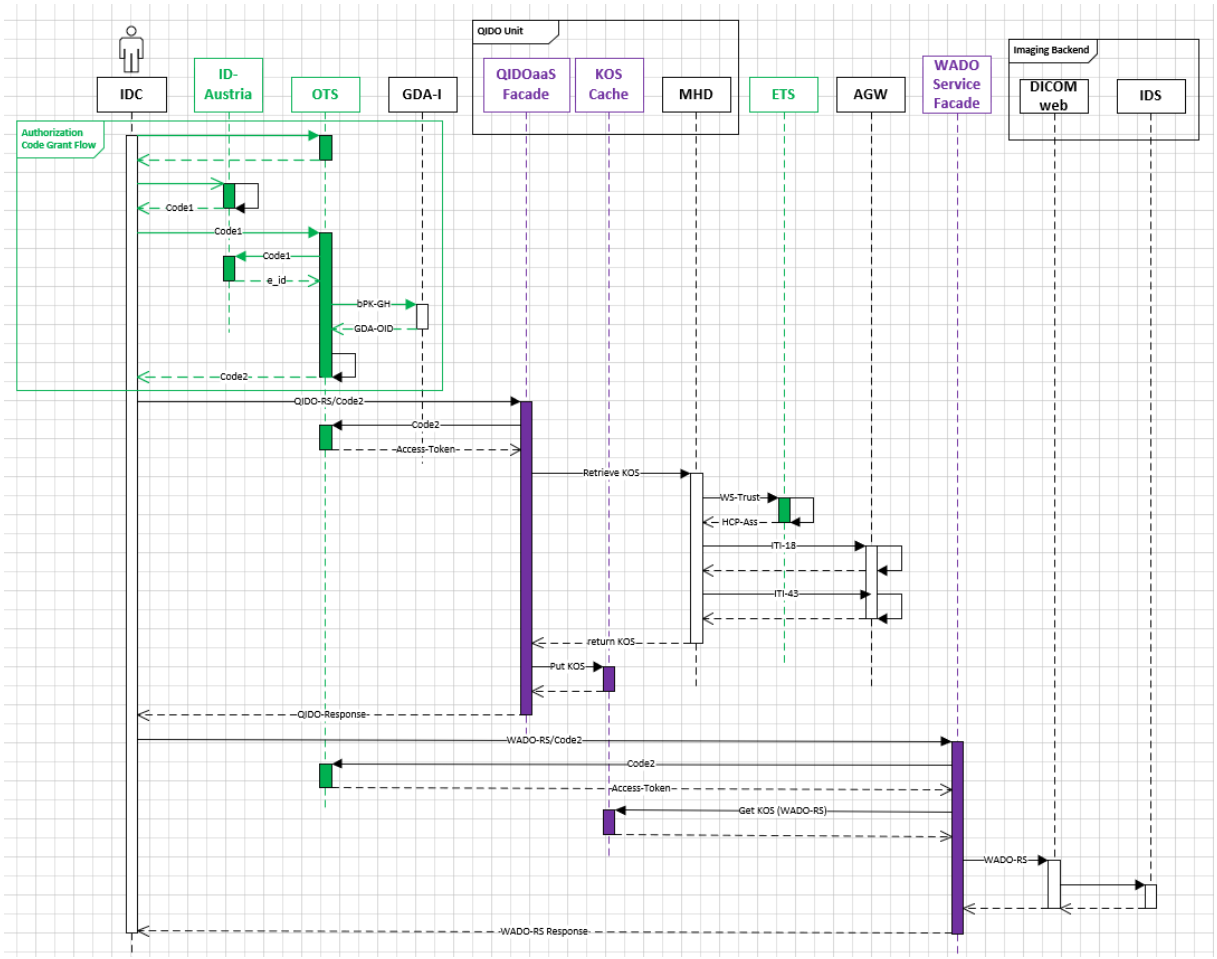
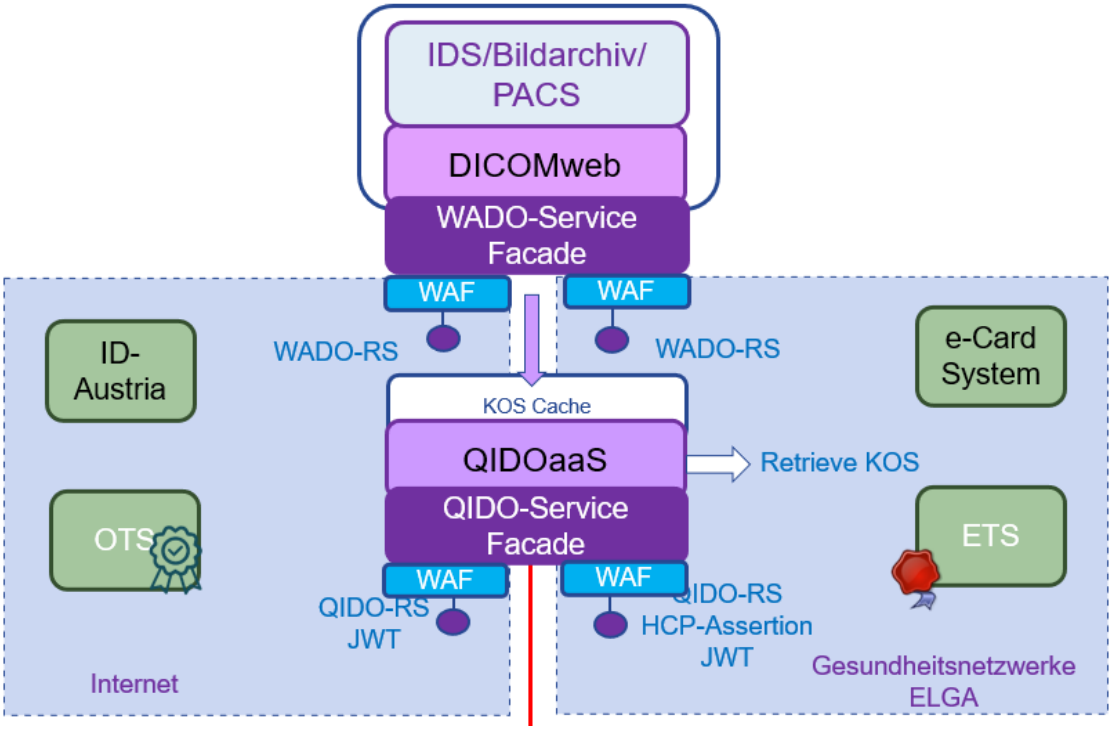


Abbildung 11: UML-Sequenz für Bilddaten-Zugriff im Internet. Grün markiert sind explizite Authentifizierung- und Autorisierungs-Verläufe entsprechend OAuth2/OIDC. Mit lila sind Abläufe hinsichtlich QIDO/WADO markiert.

1.10. Hybrides Szenario

In diesem Szenario geht man davon aus, dass es für einen IDS-Anbieter von keiner wesentlichen Bedeutung ist, ob die angebotenen DICOM-Objekte über das Internet oder über die Gesundheitsnetzwerke abgerufen werden, soweit die sichere, gesetzmäßige und korrekte Autorisierung der Zugriffe und Übertragung der Daten gewährleistet ist. Diese Vorstellung ist in der Abbildung 12 verdeutlicht. Unabhängig davon, ob es sich um Internet oder Gesundheitsnetzwerke handelt, müssen in beiden Fällen die gleichen Funktionalitäten (wie etwa QIDOaaS, KOS-Cache, vorgeschalteten Autorisierungskomponenten, WIA-Profil) angeboten und implementiert werden. Lediglich die Endpunkte und die dahinterliegenden Autorisierungsszenarien (Autorisierungsprotokolle) unterscheiden sich in den einzelnen Netzwerken.



994

995 *Abbildung 12: IHE WIA Architektur, Hybrides Szenario*

996 Die Hauptaufgabe der Service Facaden ist die Zulassung von autorisierten Zugriffen bzw.
997 eine binäre Entscheidung zu treffen, ob IDC zugreifen darf (JA), oder nicht (NEIN). Zusätz-
998 lich sind diese Komponenten angehalten, die vorgeschriebenen Protokolle zu führen, und
999 zwar in A-ARR und in L-ARR (oder Z-L-ARR).

1000 Die im Internet angebotenen Endpunkte der Service Facaden unterstützen nur OIDC Autho-
1001 rization Code Grant Flow und OAuth2. Die in den Gesundheitsnetzwerken aufgestellten End-
1002 punkte müssen auch WS-Trust und SAML2 Assertions unterstützen.

2. Anwendungsfälle

Die Anwendungsfälle des bereichsübergreifenden Bilddatenaustauschs in ELGA sind entsprechend der bereits **in der ELGA-Gesamtarchitektur** (V2.30) beschriebenen, allgemeinen Anwendungsfälle zu definieren, und zwar mit der dort angeführten Nummerierung. Das hinter den Nummerierungen angeführte „.i“ deutet explizit auf einen Imaging-Anwendungsfall hin.

Grundsätzlich kann man zwischen folgenden Anwendungsszenarien unterscheiden:

1) Das Bereitstellen von Bilddaten durch ELGA-GDA.
2) Das Abrufen von Bilddaten durch ELGA-GDA mit Verwendungszweck „Ansicht“ und „Befundung“. Während für die Befundung eine komplette Studie in voller Qualität abgerufen werden können soll, muss es für die „Ansicht“ auch möglich sein, nur eine Teilmenge der Bilddaten oder eine reduzierte Bildqualität abzufragen.
3) Das Abrufen von Bilddaten durch den Bürger am ELGA-Bürgerportal. Hier wird aufgrund der Datenmenge optional eine begrenzte Bildqualität verfügbar gemacht. Die Originalqualität wird auch weiterhin angeboten bleiben.

Diese Anwendungsszenarien werden in den folgenden Kapiteln auf konkrete technische Anwendungsfälle abgebildet:

2.1. Anwendungsfälle von ELGA-Teilnehmern bzw. deren Vertretern

Akteur / User-Agent	No.	Anwendungsfall	Anmerkung / Beispiel
ELGA-Teilnehmer	ET.1.8.i	Liste ausgewählter KOS-Objekte abrufen	Selektion via Filter (z.B. Datum, Kategorie, GDA, etc.) einschränken
	ET.1.9.i	Ein bestimmtes KOS-Objekt im JSON-Format auswählen, öffnen	KOS-Objekt inhaltlich verständlich darstellen (Studien, Serien)
	ET.1.11.i	Ein bestimmtes Bildmaterial bzw. Studie/Serie auswählen, öffnen	HTML5 freundliche Darstellung am Portal. Eventuelle Anwendung von Open Source Viewer (z.B. OHIF)
	ET.1.12.i	Vorversionen eines KOS-Objektes im JSON-Format abrufen	Ausgehend von einer geöffneten aktuellen Version
	ET.1.13a.i	Ein bestimmtes Bild als PDF herunterladen (oder drucken)	Adobe/PDF-Bedingungen am Client sind zu prüfen. Ausbau der EBP-Funktionalität ist erforderlich,
	ET.1.13b.i	Ein oder mehrere Bilder als JPEG herunterladen (bzw. drucken)	Das Portal bietet dem ELGA-Teilnehmer das Herunterladen der eigenen Bilder in voller oder reduzierter Qualität an. Ausbau der EBP-Funktionalität ist erforderlich.

Tabelle 1: ELGA-Teilnehmer Anwendungsfälle

2.2. GDA-Anwendungsfälle (XDS-I & XCA-I)

Akteur / User-Agent	No	Anwendungsfall	Anmerkung / Beispiel
GDA	GDA.3.9.i	Alle KOS-Objekte zu einem Patienten abrufen	Registry Stored Query wird ausgelöst. FindDocuments mit Filter auf KOS-Dokumentenklasse 55113-5
	GDA 3.9.i.2	KOS-Objekte selektiv suchen	Registry Stored Query wird ausgelöst. FindDocuments mit Filter auf KOS-Dokumentenklasse 55113-5 und eventCodeList auf APPC
	GDA.3.10.i	KOS-Objekt(e) zu einem Patienten abrufen. Original DICOM oder JSON-Formate sind zu unterstützen	Retrieve Document Set wird ausgelöst. Das KOS-Objekt wird lokal zwischengespeichert. Vorbedingung: GDA 3.9.i oder GDA 3.9.i.2
	GDA.3.14.i	Instanzen (Studien / Serien/ SOP-Instanzen) der bildgebenden Diagnostik abrufen (derzeit nur in vollständiger Qualität)	Retrieve Imaging Document Set wird ausgelöst. Eventuelles Speichern im lokalen Bereich ist vom BeS nicht unterstützt
	GDA.3.15.i	Befunde mit KOS verbinden	Via Metadaten. In „referenceIdList“ “accessionNumber“ einfügen
	GDA.3.16.i	Registrieren (freigeben) eigener KOS-Objekte in ELGA	RAD-68 wird ausgelöst
	GDA.3.17.i	Update von KOS durchführen (neue Version veröffentlichen)	Neue Version des KOS in die Registry einbringen
	GDA.3.18.i	Storno von KOS-Objekten	KOS-Objekte stornieren und dadurch unzugänglich machen

Tabelle 2: GDA-Anwendungsfälle (immer verpflichtend Patientenbezogen)

2.3. GDA-Anwendungsfälle (via WIA-Profile)

Akteur / User-Agent	No	Anwendungsfall	Anmerkung / Beispiel
GDA	GDA.3.9.w	Vollständige Liste aller Studien/Serien zu einem Patienten abrufen	QIDO-RS wird ausgelöst. QIDOaaS implementiert GDA.3.9.i
	GDA 3.9.w.2	Nur in abgesicherten Gesundheitsnetzwerken! Bestimmte Studien/Serien zu einem Patienten suchen (um WADO-URL zu erhalten)	Im Vorfeld via XCA-I/XDS-I GDA 3.9.i oder GDA 3.9.i.2 und anschließend GDA 3.10.i durchführen. QIDO-RS selektiv mit Studie/Serie-ID auslösen.
	GDA.3.14.w	Instanzen (Studien / Serien/ SOP-Instanzen) der bildgebenden Diagnostik abrufen (Unterstützung bzw. Abfrage von Bilddaten in reduzierter Qualität)	WADO-RS wird ausgelöst. Vorbedingung ist eine zeitnahe QIDO-RS Abfrage. Speichern im lokalen Bereich ist vom BeS nicht unterstützt.
	GDA.3.15.w	Befunde mit Instanzen der bildgebenden Diagnostik verbinden	Umsetzung derzeit nur in den Gesundheitsnetzen möglich. Siehe GDA.3.15.i

Tabelle 3: GDA Internet Anwendungsfälle (immer verpflichtend patientenbezogen)

3. XDS-I Metadaten für Bilddaten

Dieser Abschnitt wird ausgelassen, weil die Beschreibung ab Version 3.0 (XDS Metadaten Leitfaden) separat auf der Homepage der HL7-Austria (https://wiki.hl7.at/) veröffentlicht ist.

4. Abbildungsverzeichnis

5. Literaturverzeichnis

[1] ELGA GmbH, „Organisationsübergreifende Nutzung von Bild- und Multimediadaten im österreichischen Gesundheitswesen," V1.1, 2022

[2] ELGA GmbH, „ELGA Gesamtarchitektur V2.30," ELGA GmbH, Wien, 2017.

[3] ELGA GmbH, „XDS Metadaten Guide," V3.0.1, 2021.

[4] DICOM Austria, „KOS Implementierungsleitfaden", V1.0, 2022.

[5] TIANI Spirit, „ELGA BeS Pflichtenheft V4.5a," CSC/TIANI, Wien, 2022.

[6] IHE Int., „IHE RAD TF Supplement: Web-based Image Access (WIA)," Rev.1.3, 2023.

[7] Hardt, D., „The OAuth 2.0 authorization framework. No rfc6749", 2012.

[8] Lodderstedt, T., et al., „OAuth 2.0 Security Best Current Practice", 2023-06-05.

[9] OpenID Foundation, https://openid.net/developers/specs/, 2023

6. Dokumentenhistorie (Auszug)

Version	Datum	Autoren	Änderungen
V.01	30.03.2016	Stefan Repas	Initialversion/Draft
V.06	08.06.2016	Stefan Sabutsch	XDS Metadaten und Anwendungsfälle eingefügt
V1.1	22.12.2017	Stefan Repas	WADO-WS wurde aus der Spezifikation entfernt (von NEMA nicht mehr unterstützt)
V1.5	3.12.2018	Martin Hurch	Endredaktion vor Weitergabe
V1.51	3.01.2019	Stefan Repas	Feedback zur Version 1.5 eingearbeitet
V1.54	27.11.2019	Stefan Repas	Protokollierungsanforderungen sind definiert. Vorgehensweise bei KOS Veröffentlichen mit *AccessionNumber* wurde klargestellt
V1.6	24.01.2020	Stefan Repas	Anforderungen an Netzwerkverbindungen für Bildübertragung aktualisiert
V1.62	05.03.2020	Stefan Sabutsch	APPC-Anforderungen korrigiert
V1.63	30.03.2020	Stefan Sabutsch	APPC-EventCodeList Mapping korrigiert
V1.64	01.04.2020	Stefan Sabutsch	Korrekturen in XDS Metadaten: 3.2.1. authorInstitution, 3.2.2. authorPerson, 3.2.5. classCode, 3.2.7. creationTime, 3.2.14. title, 3.2.15. typeCode, 3.2.22. healthcareFacilityTypeCode , Verweise, Zitate, Literaturliste
V1.65	20.04.2020	Stefan Sabutsch Silvia Winkler Emmanuel Helm Stefan Repas	Typos ausgebessert, Präzisierungen. Kapitel 1.4.5.5. und 1.4.10 zusammengeführt (Protokollierung) Kapitel 1.4.8 Kopplung von Befunden mit Bilddaten überarbeitet, Kapitel 1.4.9 Versionierung eingefügt. Korrekturen in XDS Metadaten: 3.2.6. confidentialityCode 3.2.11 serviceStartTime/serviceStopTime 3.2.13. sourcePatientInfo 3.2.17. referenceIdList 3.2.21. formatCode

			Gestrichen: 3.2.24. parentDocumentId
V1.70	12.11.2021	Stefan Repas	Erweiterung des Dokumentes mit Vorschlägen und Konzepten insbesondere RAD-107 & RetrieveRenderedImaging
V1.71	18.11.2021	Stefan Repas	Themen mit Stefan Sabutsch besprochen, Kapitel 3 wurde ausgelagert.
V1.72	24.11.202	Stefan Repas	Asynchrone Kommunikation aufgrund HEX-I Erfahrung thematisiert
V1.73	03.12.2021	Stefan Repas	Anpassungen nach Review von Silvia Winkler (DICOM)
V1.74	14.12.2021	Stefan Repas	QIDO- & WADO-RS und Überarbeitung von Netzwerkinternen RAD-107 konsultierend mit Emmanuel Helm
V1.75	13.01.2022	Stefan Repas	Cross-Enterprise Remote Read Workflow Definition (XRR-WD) wurde in die Liste der Anforderungen aufgenommen
V1.85	06.12.2022	Stefan Repas, Oliver Kuttin	Laufende Anpassungen nach Diskussionen in der DICOM-Austria und gelb unterlegte Änderungen
V2.00a	06.03.2023	Stefan Repas Andreas Schuler Oliver Kuttin	Starke Überarbeitung insbesondere wegen WIA-Profil & DICOMweb-Services Einbindung. Einarbeitung von Feedbacks.
V2.00e	17.04.2023	Stefan Repas	Alternativszenario in den Gesundheitsnetzwerken eingearbeitet
V2.00f	04.09.2023	Stefan Repas, Emmanuel Helm	Einarbeitung der Kommentare aus der Architekturgruppe und von Systempartnern. Verweise auf WADO-URI sind entfernt worden. RetrieveRenderedImaging wurde entfernt.

1076

1077

Ansprechpartner (Projektteam)

Name	Rolle	Organisation	E-Mail
Stefan Repas	Architekt	ELGA GmbH	stefan.repas@elga.gv.at
Stefan Sabutsch	GF	ELGA GmbH	stefan.sabutsch@elga.gv.at
Andreas Schuler	Leiter Architektur	ELGA GmbH	andreas.schuler@elga.gv.at
Emmanuel Helm	Standards	ELGA GmbH	emmanuel.helm@elga.gv.at