

Aus dem Institut für Medizinische Informatik
der Hochschule Mannheim
(Dekanin: Prof. Dr. Miriam Föller-Nord)

Unterstützung von Prozessen der intersektoralen Vernetzung
mit medizinischen Bildern unter Berücksichtigung der
Qualitätssicherung

Inauguraldissertation
zur Erlangung des Doctor scientiarum humanarum (Dr. sc. hum.)
der
Medizinischen Fakultät Mannheim
der Ruprecht-Karls-Universität
zu
Heidelberg

vorgelegt von
Florian Schwind

aus
Speyer am Rhein

2020

Dekan: Prof. Dr. med. Sergij Goerdts

Referent: Prof. Dr. Paul Schmücker (Hochschule Mannheim)

Inhaltsverzeichnis

Abkürzungsverzeichnis	1
1. Einleitung	7
1.1. Zielsetzung und Gegenstand der Arbeit	7
1.2. Aufbau der Arbeit	11
2. Grundlagen / Stand der Technik	13
2.1. Austausch medizinischer Daten	13
2.1.1. DICOM	13
2.1.2. HL7	18
2.1.3. DICOM E-Mail	23
2.1.4. Proprietäre Übertragung via HTTP und HTTPS	30
2.1.5. Patienten-CD	32
2.1.6. DICOM in the Cloud	33
2.1.7. Integrating the Healthcare Enterprise	40
2.1.8. IHE Cross-Enterprise Document Sharing	45
2.2. Modelle der Teleradiologie	51
2.2.1. Netzwerktopologie	51
2.2.2. Datenfluss	55
2.3. Qualitätssicherung	58
2.3.1. Qualitätssicherung in der Softwareentwicklung	58
2.3.2. Monitor-Konstanzprüfung	62
2.3.3. Teleradiologie nach Röntgenverordnung	62
2.4. Zugriff auf Daten für Ärzte und Patienten	64
2.4.1. Zuweiserportale	64

2.4.2. Patientenportale	64
2.4.3. Patientenakten	66
2.4.4. Vendor Neutral Archive	69
3. Material und Methoden / Konzeption und Realisierung	71
3.1. DICOM E-Mail und Qualitätssicherung	72
3.1.1. DICOM E-Mail Service Parts	72
3.1.2. Verwaltung von DICOM E-Mail Adressdaten	75
3.1.3. Verwaltung von DICOM E-Mail Schlüsseldaten	77
3.1.4. Verwaltung von Kontaktdaten	78
3.1.5. Verbindungsupdate	80
3.1.6. Empfangsbestätigung	80
3.1.7. Konstanzprüfung	82
3.1.8. Abfrage des Adressverzeichnisses	84
3.2. Multiknotenstatistik	86
3.2.1. Datentransfer	87
3.2.2. Anforderung der Statistik	92
3.3. IHE XDM und DICOM E-Mail	94
3.3.1. Quality Controlled Image Transfer	95
3.3.2. Übertragung von DICOM- und nicht-DICOM-Daten mittels QCIT	98
3.3.3. Erweiterte Empfangsbestätigung mittels QCIT	101
3.3.4. Teleradiologische Konstanzprüfung mittels QCIT	103
3.4. Intersektorale Vernetzung mit IHE XDS	106
3.4.1. XDS-Adapter für Systeme ohne IHE-Unterstützung	108
3.4.2. Mapping von Metadaten zu XDS Value Sets	111
3.4.3. Imaging Cache als Proxy für beschleunigtes Bildladen	114
3.4.4. Request-Broker für verteilte Bildablage	116
3.5. Mobile Bildbetrachtung und Single-Sign-On mit IHE XDS	118
3.5.1. CHILI/Mobile	119
3.5.2. Single-Sign-On	120

3.5.3. Tokenbasierter Aufruf	123
3.6. Workfloworientierte Vernetzung und Portale	126
3.6.1. Umstellung auf ein aktuelles Web-Framework	128
3.6.2. Integration eines mobilen Bildbetrachters und Uploaders	131
3.6.3. Schnittstellen	131
3.6.4. Workflowsteuerung	133
3.6.5. Zugriffssteuerung und Freigaben	134
3.6.6. Auswertung und Export	134
3.6.7. Protokollierung	135
3.7. Qualitätssicherungswerkzeuge für teleradiologische Systeme	136
3.7.1. Erweiterungen für Performancemessungen und Konstanzprüfung .	137
3.7.2. Datenübertragung	140
3.7.3. Auswertung und Aufbereitung der gesammelten Daten	141
3.8. Umsetzung der beschriebenen Methoden	142
4. Ergebnisse	145
4.1. Administration von DICOM E-Mail Netzwerken	145
4.1.1. Anbindung neuer Nutzer	145
4.1.2. Aktualisierung bestehender Verbindungen	148
4.1.3. Erweiterte Empfangsbestätigungen	149
4.2. Automatisierte Konstanzprüfung in der Teleradiologie	150
4.2.1. Durchführung der Konstanzprüfung	151
4.2.2. Überwachung und Protokollerstellung	152
4.3. Multiknotenstatistik	153
4.4. DICOM E-Mail und IHE XDM	155
4.5. Intersektorale Vernetzung unter Verwendung von IHE-Profilen	157
4.5.1. XDS-Adapter	158
4.5.2. Imaging Cache	160
4.5.3. Request-Broker	163
4.6. Mobile Bildbetrachter für Ärzte, Patienten und den Ad-hoc-Zugriff . . .	164

4.7. Portale für Ärzte und Patienten	166
4.7.1. Teleradiologieportal	167
4.7.2. Zuweiser- und Patientenportal	171
4.8. Überwachung von Teleradiologiesystemen	173
4.8.1. Bandbreitenmessung von Teleradiolgiestrecken	174
4.8.2. Nachverfolgbarkeit von Software	175
4.8.3. Monitoring Dashboard	176
4.9. Zusammenfassung der Ergebnisse	178
5. Diskussion	183
6. Zusammenfassung	199
Literaturverzeichnis	201
Abbildungsverzeichnis	217
Tabellenverzeichnis	221
Listings	222
A. Anhang	225
A.1. Service Part - Beispiel-E-Mail	225
A.2. Service Part - Kontaktupdate	226
A.3. Service Part - Adressanfrage	227
A.4. Service Part - Adressantwort	227
A.5. Statistik Request	228
A.6. Statistik Response	229
A.7. SAML-basierter Aufruf des mobilen Viewers	230
Lebenslauf	231
Danksagung	233

Abkürzungsverzeichnis

@GIT	Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft
ACR	American College of Radiology
AET	Application Entity Title
AIMD	Active Implantable Medical Device
AIM	Annotation and Image Markup
API	Application Programming Interface
APT	Arbeitsgemeinschaft Physik und Technik
AWS	Amazon Web Services
BCP	Best Current Practice
BMBF	Bundesministerium für Bildung und Forschung
BPPC	Basic Patient Privacy Consents
BTRFS	B-tree File System
CDA	Clinical Document Architecture
CR	Computed Radiography
CT	Computed Tomography
DBMS	Database Management System
DICOM	Digital Imaging and Communications in Medicine
DMZ	Demilitarisierte Zone
DR	Digitale Radiographie
DRG	Deutsche Röntgengesellschaft
DX	Digital Radiography
EFA	Elektronische Fallakte
EPA	Elektronische Patientenakte

FHIR	Fast Healthcare Interoperability Resources
GCP	Google Cloud Platform
GDT	Gerätedaten-Transfer
GNU	GNU's not Unix
GPG	GNU Privacy Guard
GZIP	GNU ZIP-Dateiformat
HL7	Health Level Seven
HPD	Healthcare Provider Directory
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IANA	Internet Assigned Numbers Authority
IHE	Integrating the Healthcare Enterprise
IMAP	Internet Message Access Protocol
INFOPAT	Informationstechnologie für die Patientenorientierte Gesundheitsversorgung
ISCL	Integrated Secure Communication Layer
IVDD	Invitro Diagnostik Directive
JPEG	Joint Photographic Experts Group
JSF	JavaServer Faces
JSON	JavaScript Object Notation
JSP	JavaServer Pages
KIS	Krankenhausinformationssystem
KOS	Key Object Selection
LDAP	Lightweight Directory Access Protocol
LIS	Laborinformationssystem
MAC	Media Access Control
MDD	Medical Device Directive
MDN	Message Disposition Notification
MDR	Medical Device Regulation
MIP	Maximumintensitätsprojektion

MLLP	Minimal Lower Layer Protocol
MPG	Medizinproduktegesetz
MPI	Master Patient Index
MPR	Multiplanare Reformatierung
MR	Magnetic Resonance
MRT	Magnetresonanztomographie
MTRA	Medizinisch-technische(r) Radiologieassistent/-in
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
PACS	Picture Archiving and Communication System
PaaS	Platform as a Service
PDF	Portable Document Format
PDI	Portable Data for Imaging
PDMS	Patientendatenmanagementsystem
PEPA	Persönliche Elektronische Patientenakte
PGP	Pretty Good Privacy
PNG	Portable Network Graphic
POP	Post Office Protocol
PS	Presentation State
QC	Quality Control
QCIT	Quality Controlled Image Transfer
QMS	Qualitätsmanagementsystem
QOS	Quality of Service
Q/R	Query/Retrieve
REST	Representational State Transfer
RF	Radio Fluoroscopy
RFC	Request for Comments
RIS	Radiologieinformationssystem

RI	Rechtfertigende Indikation
RSNA	Radiological Society of North America
RöV	Röntgenverordnung
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
SR	Structured Report
SSK	Strahlenschutzkommission
SSL	Secure Sockets Layer
SSO	Single-Sign-On
StrlSchG	Strahlenschutzgesetz
StrlSchV	Strahlenschutzverordnung
SWF	Scheduled Workflow
S/MIME	Secure / Multipurpose Internet Mail Extensions
TF	Technical Framework
TLS	Transport Layer Security
TM	Telemedizin
TR	Teleradiologie
US	Ultraschall
UUID	Universally Unique Identifier
VNA	Vendor Neutral Archive
VPN	Virtual Private Network
VR	Value Representation
WADO	Web Access to DICOM Persistent Objects
WAF	Web Application Firewall
XA	X-Ray Angiography
XaaS	Everything as a Service
XACML	Extensible Access Control Markup Language

XCA	Cross-Community Access
XDM	Cross-Enterprise Document Media Interchange
XDS-I	Cross-Enterprise Document Sharing for Imaging
XDS	Cross-Enterprise Document Sharing
XML	Extensible Markup Language
XUA	Cross-Enterprise User Assertion
ZFS	Zettabyte File System
ZIP	ZIP-Dateiformat

1. Einleitung

Im Gesundheitswesen wird der elektronische Austausch von Daten zwischen professionellen Anwendern wie Ärzten, Pflegekräften oder medizinisch-technischen Assistenten sowie zwischen Ärzten und Patienten immer wichtiger, dennoch ist Kollaborationssoftware in diesem Bereich immer noch nicht großflächig im Einsatz. Welche technischen Voraussetzungen müssen geschaffen werden, um den ärztlichen als auch den nicht-ärztlichen Workflow zu unterstützen beziehungsweise zu verbessern? Kann eine Standardisierung zur Verbesserung der Interoperabilität beitragen? Und wie können Vernetzung, Qualitätssicherung, Daten- und damit auch Patientensicherheit miteinander vereint werden, um eine bessere Behandlung zu gewährleisten?

1.1. Zielsetzung und Gegenstand der Arbeit

Im persönlichen Alltag sind Facebook, WhatsApp und andere soziale Netzwerke als auch Nachrichten- oder Messagingdienste nicht mehr wegzudenken und ein unumgängliches Mittel zur Kommunikation und zum Teilen von Daten geworden. Das Kommunikationsverhalten der Menschen hat sich stark gewandelt. Untersuchungen zeigen, dass sowohl die Gruppe der Jugendlichen und jungen Erwachsenen in Deutschland mit 98% Online-Nutzung bereits fast vollständig online ist und auch bei den über 60-jährigen mehr als 43% das Internet täglich nutzen (Kaczmirek and Chalupa, 2018). Bei mehr als 2,6 Mrd. Nutzern der Plattform Facebook inklusive WhatsApp-Messenger und Instagram sowie mehr als 100 Mrd. versendeten Nachrichten pro Tag wird schnell klar, dass die Vernetzung im persönlichen Bereich bereits mehr als angekommen ist (Roth and Wiese, 2018).

Sicherheitsbedenken oder Datenschutz spielen bei der Online-Kommunikation eine eher untergeordnete Rolle. Wichtig sind der einfache und schnelle Zugang zu Informationen und das mühelose Teilen von Daten zwischen den Anwendern.

Wer heutzutage ein Smartphone besitzt, kann sich weitgehend unabhängig von seinem aktuellen Standort und Netzzugang problemlos mit jedem beliebigen Teilnehmer vernetzen, digital kommunizieren und Bilder oder andere Daten austauschen. Ermöglicht werden diese einfache Vernetzung und die rasche Ausbreitung von Kommunikationsdiensten wie WhatsApp, Telegram oder Threema durch große Plattformen, die jedem Nutzer ihre Dienste zur Verfügung stellen. Hier stellt sich oft die Frage, wieso eine solche einfache Vernetzung nicht auch im medizinischen Bereich möglich ist. Warum kann ein Radiologe nicht problemlos und ad hoc ein kurzes Konsil bei einem Kollegen anfragen? Wieso können Daten nicht einfach online übertragen werden? Wieso kann ein Patient nicht elektronisch an seiner Behandlung teilhaben, seine Bilder einsehen und mit einem Arzt in Kontakt treten, gerade wenn doch die soziale Interaktion die Genesung fördern kann (Smailhodzic et al., 2016; Clark et al., 2017; Hazzam and Lahrech, 2018)?

Dem entgegen steht das hohe Maß an Sicherheit, Datenschutz und Vertraulichkeit, welches beim Teilen von medizinischen Daten eine wichtige, wenn nicht sogar die wichtigste Rolle spielt. Auch wenn Anwender oft mehr Wert auf einen schnellen und unkomplizierten Austausch legen, unterliegen patientenbezogene Daten einem erhöhten, wenn nicht sogar dem höchsten Schutzbedürfnis. Neben der Standardisierung des Austauschformats (wie Digital Imaging and Communications in Medicine (DICOM) und Health Level Seven (HL7)) zwischen unterschiedlichen Geräten, Herstellern und medizinischen Einrichtungen haben sich in den vergangenen Jahren auch in Deutschland immer mehr Initiativen und Netzwerke gebildet, um die Vernetzung grundlegend sicherer und einfacher zu machen. Hierbei wurde auch großen Wert auf die Etablierung von standardisierten Methoden wie DICOM E-Mail oder IHE Cross-Enterprise Document Sharing (XDS) für den Austausch von Daten gelegt.

Das Ausrollen von Patientenakten durch die Krankenkassen wie zum Beispiel die digitale Patientenakte der AOK oder TK-Safe, die Akte der Techniker Krankenkasse, trägt

zur weiteren Digitalisierung im Gesundheitsmarkt bei. Auch die Telematikinfrastruktur verspricht mit ihrer elektronischen Patientenakte (ePA) ab 2021 eine Vernetzung für alle Patienten über die Krankenkassen (Bertram et al., 2019). Neben den Akten der Krankenkassen entwickeln auch Klinikkonzerne Vernetzungslösungen und versuchen durch eigene meist anwendungsfallbezogene Angebote die Patienten enger an ihre Klinik zu binden und so auch schon vor der Aufnahme digital mit ihnen in Kontakt zu treten. Neben diesen im Nutzerkreis beschränkten Akten gibt es auch Vernetzungslösungen von privaten Unternehmen wie zum Beispiel Vivy (<https://www.vivy.com>, 05.09.2019), welche den Anwendern eine Akte für ihre Daten anbieten und eine Vernetzung zu anderen Akteuren im Gesundheitswesen versprechen, auch wenn diese sich in der Vergangenheit leider nicht immer durch ihren souveränen Umgang mit der Datensicherheit hervorgetan haben (Tschirsich, 2018). Ebenso spielen die intersektorale Vernetzung von Kliniken und die Teilhabe von Patienten am Behandlungsprozess eine immer größere Rolle im medizinischen Alltag (Marx et al., 2015; Dockweiler and Hornberg, 2019).

Die meisten neuen Vernetzungslösungen konzentrieren sich auf die Kommunikation mit dem Patienten oder auf die Befundkommunikation zwischen medizinischen Anwendern und bieten wenig Mehrwert für radiologische Anwender und deren Bedürfnisse im Umgang mit den meist großen radiologischen Bildvolumen. In der Radiologie und insbesondere der Teleradiologie spielt neben der Datensicherheit auch die Geschwindigkeit der Datenübermittlung und deren Konstanz eine entscheidende Rolle. Können Anwender sich ad hoc vernetzen, so muss im Übertragungsfall auch eine hohe Erreichbarkeit und Stabilität der Verbindung gewährleistet sein.

In dieser Arbeit werden für den Bereich der teleradiologischen beziehungsweise telemedizinischen Bild- und Befundkommunikation mehrere zusammenhängende und sich ergänzende Lösungsansätze entwickelt und anschließend implementiert.

Das Ziel der Arbeit ist die Verbesserung und Erweiterung der Telemedizin zu umfangreichen einrichtungsübergreifenden und intersektoral vernetzten Lösungen unter Berücksichtigung von Patientenakten, -Portalen, Qualitätssicherung und Mobilität. Konkret bedeuten diese Ziele:

- Verbesserung des Workflows zur Unterstützung der medizinischen und nicht-medizinischen Anwender im Bereich der Teleradiologie und intersektoralen Vernetzung
- Qualitätssicherung im Rahmen von DICOM E-Mail sowie deren Standardisierung mit der Arbeitsgemeinschaft Informationstechnologie (@GIT) der Deutschen Röntgengesellschaft (DRG)
- IHE-konforme Realisierung von teleradiologischen Netzen und die Weiterentwicklung von vorhandenen IHE-Profilen, insbesondere im Bereich DICOM E-Mail und IHE Cross-enterprise Document Media Interchange (XDM)
- Qualitätssicherung in komplexen und heterogenen Teleradiologienetzwerken mit mehreren Übertragungsknoten zwischen Sender und Empfänger
- Verbesserung der Administration und Ad-hoc-Kommunikation in großen Teleradiologienetzwerken
- Intersektorale Vernetzung auf Basis von IHE Cross-Enterprise Document Sharing for Imaging (XDS-I) und Verbesserung der Performance im Bereich des Bildmanagements
- Integration von nicht-XDS-fähigen Komponenten durch Schaffung von Kommunikationsadaptern für die intersektorale Vernetzung
- Integration von Handheldgeräten (wie iPad, iPhone etc.) in teleradiologische Anwendungssysteme sowie die Darstellung von DICOM-Bildern auf diesen Geräten
- Entwicklung von Portallösungen für die Kommunikation zwischen Ärzten und Patienten
- Weiterentwicklung von Überwachungs- und Qualitätssicherungswerkzeugen für teleradiologische Systeme

Um diese Ziele zu erreichen, werden einfache und offene Schnittstellen, Standards sowie robuste und einfach anzuwendende Verfahren benötigt. Das Hauptziel ist hierbei,

die teleradiologischen und telemedizinischen Arbeitsabläufe der Anwender, aber auch der Administratoren in größeren Teleradiologienetzwerken und Installationen zu unterstützen, um hier einen reibungslosen Ablauf gewährleisten zu können. Die entwickelten Lösungen müssen neben ihrer Robustheit einfach erweiterbar als auch gut skalierbar sein, um so mit ihren Anforderungen zu wachsen.

1.2. Aufbau der Arbeit

Im folgenden Kapitel wird zunächst auf die Grundlagen und den aktuellen Stand der Technik eingegangen. Hierbei werden insbesondere die Bereiche der medizinischen Bildkommunikation und Vernetzung mit den unterschiedlichen Standards und Modellen eingehend dargestellt. Neben den Modellen der Teleradiologie wird anschließend auf die Qualitätssicherung bei der Entwicklung von Medizinprodukten und auf die Regelungen für die Teleradiologie nach Röntgenverordnung eingegangen. Das Kapitel endet mit der Darstellung der unterschiedlichen Arten von Patientenportalen und -akten sowie deren Anwendungsgebieten.

Das Kapitel Material und Methoden beschreibt die grundlegend für diese Arbeit entwickelten Techniken und Standards im Bereich der qualitätsgesicherten Bildkommunikation und Vernetzung in der Teleradiologie.

Zunächst werden die im Rahmen dieser Arbeit neu entwickelten Verfahren zur Verwaltung von DICOM E-Mail-basierten Teleradiologienetzwerken behandelt, welche auch den Aspekt der Qualitätssicherung und Konstanzprüfung der Teleradiologiestrecken im Netzwerk umfassen. Das darauf folgende Unterkapitel stellt die Möglichkeiten zur Transferzeitmessung in heterogenen Netzwerken dar und geht über die reine Vernetzung mittels DICOM E-Mail hinaus. Im nächsten Abschnitt wird ein Konzept zur Überführung von DICOM E-Mail in IHE-Workflows dargestellt, welches eine auf IHE orientierte Lösung für bisherige E-Mail-basierte Netzwerke bietet. Das Kapitel zur intersektoralen Vernetzung geht auf die durch den Autor durchgeführten Entwicklungen im Bereich der XDS Kommunikation mit nicht-XDS-fähigen Komponenten ein und stellt Methoden zu

Konnektivitäts- und Performancesssteigerung vor. Anschließend wird in den beiden nächsten Unterkapiteln die workfloworientierte Vernetzung mittels Portalen und die Einbeziehung von mobilen Bildbetrachtern für die Radiologie vorgestellt. Das abschließende Unterkapitel über Qualitätssicherung für Teleradiologiesysteme beendet den Methodenteil mit der Implementierung eines Überwachungssystems für Teleradiologiekomponenten.

Im Kapitel Ergebnisse werden die neu entwickelten Technologien und ihr Einsatz in Routine zum Erreichen der gesteckten Ziele der Arbeit detailliert dargestellt und besprochen.

Im anschließenden Kapitel erfolgt eine Diskussion der Arbeit in Bezug auf die erarbeiteten Methoden und Ziele. Eine kurze Zusammenfassung schließt die Arbeit ab.

2. Grundlagen / Stand der Technik

Im Kapitel Grundlagen wird zunächst der aktuelle Stand der Technik dargestellt und der Weg von der Radiologie über die Teleradiologie bis schlussendlich hin zur Telemedizin dargestellt. Insbesondere wird hier auf die unterschiedlichen Arten und Varianten der Vernetzung und des Datentransfers eingegangen. Der Schwerpunkt liegt dabei auf der Darstellung und der Verteilung von medizinischen Bilddaten. Im Anschluss werden die verschiedenen Varianten der Qualitätssicherung und die rechtlichen Rahmenbedingungen eingehend behandelt.

2.1. Austausch medizinischer Daten

Um medizinische Daten zwischen unterschiedlichen Partnern zu übertragen, haben sich in den vergangenen Jahrzehnten verschiedenste Standards etabliert und durchsetzen können. Standardisierungsbewegungen haben mit unterschiedlichen Ansätzen weitere Neuerungen in den Bereich der medizinischen Bildkommunikation gebracht.

2.1.1. DICOM

Der wohl wichtigste und etablierteste Standard zum Austausch medizinischer Bilddaten, insbesondere in der Radiologie, ist der DICOM-Standard.

Als Erfinder des CT gilt bis heute der englische Ingenieur G. H. Hounsfield (Hounsfield, 1973), der seine Ergebnisse 1973 im *British Journal of Radiology* veröffentlichte. Als 1971 die erste Computed Tomography (CT) eines Menschen erstellt und wenig später 1972 der

erste kommerzielle Kopf-Scanner *EMI Mark I* im Atkinson Morley's Hospital in London aufgestellt wurde (Kalender, 2006), konnten zwar CT-Bilder visualisiert werden, aber von einer standardisierten Speicherung oder Kommunikation war man noch weit entfernt. Die Aufnahmetechnik entwickelte sich in den darauf folgenden Jahren immer weiter, und unterschiedliche Hersteller kamen auf den Markt.

Etwa zeitgleich mit Hounsfield veröffentlichte Paul Christian Lauterbur seine Arbeit zur Bildgebung mittels Magnetresonanztomographie (MRT) (Lautenbur, 1973). Auch im Bereich der Kernspintomographie gab es in den darauf folgenden Jahren zahlreiche Weiterentwicklungen, es etablierten sich verschiedenste Hersteller auf dem Markt.

Bis Anfang der 1980er Jahre war es allerdings für andere als den Hersteller solcher Geräte schwer, die entstandenen Daten zu decodieren, anzuzeigen oder gar zu drucken. Aus diesem Grund schloss sich 1983 das American College of Radiology (ACR) und die National Electrical Manufacturers Association (NEMA) zusammen und bildeten ein Standard-Komitee, um die Interessen und Bedürfnisse von Radiologen, Ärzten und Herstellern zu vertreten und die Entwicklung eines einheitlichen Standards im Bereich der Radiologie voranzutreiben (Pianykh, 2011). 1985 wurde der erste ACR-NEMA Standard (No. 300-1985) veröffentlicht, der vor allem auf die Punkt-zu-Punkt-Übertragung von Bildern einging. Die zweite Version (ACR-NEMA V2.0) wurde 1988 veröffentlicht und 1990 zum ersten Mal auf dem jährlichen Treffen der Radiological Society of North America (RSNA) demonstriert. Die Weiterentwicklung traf auf immer mehr Akzeptanz der Hersteller, und so wurde 1993 die noch heute verwendete Version 3 als DICOM-Standard 3.0 (National Electrical Manufacturers Association, 1993) veröffentlicht, die insbesondere auch auf die Kommunikation der Daten auf Protokollschichten oberhalb von TCP/IP eingeht.

Der DICOM-Standard

Heute (Stand 2020) besteht der DICOM-Standard aus 22 Teilen mit mehr als 6800 Seiten sowie diversen Supplements, die zukünftige Erweiterungen enthalten und nach Etablierung in den Standard einfließen werden.

- Part 1 - Introduction and Overview: Enthält eine Einführung in den Standard sowie einen Überblick über die verschiedenen Teile.
- Part 2 - Conformance: Definiert die Erstellung eines DICOM Conformance Statements, welches die Konformität der Implementierung des jeweiligen Herstellers beschreibt.
- Part 3 - Information Object Definitions: Definiert alle im Standard verwendeten Datenobjekte wie Patient, Studie, Bild sowie deren Entsprechung im *Real World Information Model*.
- Part 4 - Service Class Specifications: Gibt die in DICOM möglichen Serviceklassen wie Storage, Query/Retrieve, Worklist- oder Print-Management und deren Rolle als Service Class Provider (SCP) dem Anbieter eines Dienstes oder als Service Class User (SCU) dem Benutzer eines Dienstes vor.
- Part 5 - Data Structures and Encoding: Beschreibt die Kodierregeln, die zur binären Übertragung von Daten aus Part 3 mit den Diensten aus Part 4 nötig sind.
- Part 6 - Data Dictionary: Definiert alle verfügbaren Datenelemente, die verwendet werden können, um Daten zu repräsentieren. Datenelemente werden in Gruppen zusammengefasst und können anhand ihrer Gruppen- und Elementnummer eindeutig identifiziert werden. Jedes Element hat einen Namen, eine Value Representation (VR) (zum Beispiel String, Integer, Date etc.) und eine Multiplizität. Das DICOM Data Dictionary ist nötig, um Daten richtig interpretieren zu können.
- Part 7 - Message Exchange: Beschreibt den Dienst und das Protokoll des Datenaustauschs.
- Part 8 - Network Communication Support for Message Exchange: Beschreibt die Netzwerkkommunikation auf Basis von TCP/IP.
- Part 10 - Media Storage and File Format for Media Interchange: Legt das Format sowie Speicherung von DICOM-Daten auf austauschbaren Medien wie zum Beispiel CD oder USB-Stick fest.

- Part 11 - Media Storage Application Profiles: Gibt unterschiedliche Anwendungsprofile für den Austausch von Medien vor.
- Part 12 - Media Formats and Physical Media for Media Interchange: Beschreibt die unterstützten Formate und physischen Medien für den Dateiaustausch.
- Part 14 - Grayscale Standard Display Function: Beschreibt die standardisierte Anzeige und den Druck von Graustufenbildern auf DICOM konformen Monitoren oder Druckern.
- Part 15 - Security and System Management Profiles: Definiert die Anwendung verschiedener Standardprotokolle wie DHCP, LDAP, TLS und ISCL zur sicheren Kommunikation sowie Verschlüsselung.
- Part 16 - Content Mapping Resource: Listet alle möglichen Codes und deren Bedeutung in DICOM-Feldern auf.
- Part 17 - Explanatory Information: Enthält weiterführende informative und normative Anhänge.
- Part 18 - Web Services: Beschreibt den Einsatz von Web Services für den Zugriff auf DICOM-Objekte. Hier wird auch Web Access to DICOM Persistent Objects (WADO) beschrieben, welches als Proxy für einen Store SCP eingesetzt werden kann, um DICOM-Kommunikation via HTTP zu ermöglichen.
- Part 19 - Application Hosting: Beschreibt ein Application Programming Interface (API), welches eine Plugin-Schnittstelle zwischen medizinischer Software auf DICOM Basis ermöglicht.
- Part 20 - Imaging Reports using HL7 Clinical Document Architecture: Hier wird auf die Transformation von DICOM Structured Report (SR) in die HL7 Clinical Document Architecture (CDA) eingegangen.
- Part 21 - Transformations between DICOM and other Representations: Dieser Teil beschreibt die Transformation von DICOM-Daten in andere Repräsentationen wie

zum Beispiel NCI Annotation and Image Markup (AIM) in DICOM SR und umgekehrt.

- Part 22 - Real-Time Communication: Beschreibt den real-time Transport von DICOM-Metadaten, insbesondere für Video und Audio.

Die beiden Teile 9 (Point to Point Communication Support for Message Exchange) sowie 13 (Print Management Point-to-Point Communication Support) wurden aus Kompatibilitätsgründen, da sie teilweise im Widerspruch zu anderen Teilen standen, aus dem Standard entfernt und werden heute nicht mehr verwendet.

Objekte und Kommunikation

Obwohl DICOM ursprünglich rein für die Netzwerkkommunikation und das herstellerübergreifende Speichern von Bilddaten konzipiert war, hat sich der Standard über die letzten 25 Jahre extrem weiterentwickelt. Mittlerweile können neben den reinen Bilddaten auch Textbefunde als Structured Reports (SR) oder Encapsulated PDF gespeichert und übertragen werden. Neben den textuellen Erweiterungen sind auch Neuerungen im Bereich der Darstellung eingeflossen. Mit Presentation State (PS) Objekten kann genau beschrieben werden, wie ein Bild nach der Übertragung dargestellt werden soll. Eine Key Object Selection (KOS) erlaubt die herstellerunabhängige Selektion von einzelnen Bildern einer ganzen Serie, um wichtige Inhalte hervorzuheben und mit Zusatzinformationen anzureichern. Weiterhin gibt es Erweiterungen für diverse Nicht-Bild-Modalitäten wie zum Beispiel DICOM ECG (Hilbel et al., 2007) oder das Kodieren von diversen Waveforms, welche heute in Routine verwendet werden können.

DICOM-Daten werden grundsätzlich binär übertragen und auch abgelegt. Jede einzelne Information inklusive den Pixeldaten in einem DICOM-Bild ist durch eine eindeutige ID, bestehend aus Gruppe und Element, wie in *Part 6 - Data Dictionary* beschrieben, festgelegt. Bei einer Kommunikation zwischen zwei Partnern müssen diese zu Beginn die entsprechende Transfersyntax mittels eines Handshake-Verfahrens aushandeln, bevor Daten übertragen werden können. Dies erfordert auf beiden Seiten der Kommunikation einen entsprechenden Parser, der alle Aspekte des DICOM-Standards

berücksichtigen muss. Um die Übertragung und das Handling von DICOM-Daten auch für einfache Anwendungen kompatibel zu machen, wurde der Standard in den letzten Jahren um diverse webbasierte Schnittstellen, wie in *Part 18 - Web Services* beschrieben, erweitert. Hier ist insbesondere die Etablierung von Representational State Transfer (REST)-Schnittstellen (Fielding, 2000) zu nennen, die es nun erlauben, Daten in Extensible Markup Language (XML) oder in der JavaScript Object Notation (JSON) zu übertragen.

Conformance Statement

Da der DICOM-Standard in seinem aktuellen Umfang von mehr als 6600 Seiten kaum noch von einem Hersteller vollständig implementiert und unterstützt werden kann, veröffentlichen die Hersteller das sogenannte DICOM Conformance Statement, welches in Part 2 des Standards definiert wird. Hier beschreiben die Hersteller detailliert, welchen Teil des Standards beziehungsweise welche Rollen, Daten- und Bildtypen sie unterstützen. Heute werden zwar immer mehr Geräte und Hersteller 'DICOM-fähig', welchen Teil des Standards sie aber wirklich abbilden und unterstützen, lässt sich nur ihrem Conformance Statement entnehmen.

2.1.2. HL7

Für die Übermittlung von Nicht-Bilddaten und die Kommunikation zwischen den unterschiedlichen Subsystemen in einem Krankenhaus wie zum Beispiel einem Krankenhausinformationssystem (KIS), Radiologieinformationssystem (RIS) oder Laborinformationssystem (LIS) kommt neben dem DICOM-Protokoll vor allem das HL7-Protokoll zum Einsatz, welches sich im Krankenhaus schon lange etabliert hat.

Die HL7-Organisation wurde 1987 mit dem Ziel, eine Norm für den Austausch von Daten im Gesundheitswesen zu verfassen, in den USA gegründet. Die erste Implementierung des Standards ist auf die *UCSF higher level protocol specification* der University of California at San Francisco zurückzuführen, welche dann bereits im Jahre 1989 als

HL7-Version 2.0 publiziert wurde. HL7 leitet sich von der siebten Schicht des ISO/OSI-Referenzmodells für die Kommunikation (ISO7498-1) ab und beschreibt auf einfache Weise die Kommunikation der beteiligten Partner ausschließlich auf der Anwendungsschicht (Application Layer) zwischen verschiedenen Applikationen. In Deutschland ist die HL7-Organisation seit 1993 ein eingetragener Verein, in welchem Mitglieder sowohl aus der Klinik als auch der Industrie organisiert sind (HL7 Deutschland e.V., 2018).

HL7 v2

HL7 v2 ist heute noch die verbreitetste Version des Standards im Krankenhaus. Das Austauschformat für Nachrichten ist rein textbasiert und menschenlesbar. Die Kommunikation zwischen den Systemen basiert auf dem Konzept eines Ereignistriggers, welcher eine HL7-Applikation dazu bewegt, eine spezifizierte Nachricht in das Krankenhausnetz und damit an ein oder mehrere Empfänger zu senden. Nachrichten sind hierbei einzelne Strings, also Zeichenfolgen, die durch Trennzeichen in Segmente und Felder aufgeteilt werden. Die Struktur der Nachricht ist hierbei durch den Standard festgelegt. Empfangende Applikationen verarbeiten die Nachrichten und führen ihrerseits wieder Trigger aus. Trotz der grundlegenden Spezifizierung der Nachrichten und der festgelegten Übertragung via Minimal Lower Layer Protocol (MLLP) hängt die Verarbeitung der Inhalte stark von der konkreten Implementierung des Senders und Empfängers ab, so dass hier meist eine entsprechende Schnittstellenkonfiguration der Systeme vorgenommen werden muss.

Nachrichtentypen

Häufig verwendete Basis-Nachrichtentypen zur Kommunikation von Patientenstammdaten, deren Änderungen sowie von Befunden in der Radiologie sind:

- ADT: Patientenstammdaten und Aufenthaltsdaten (Admission, Discharge, Transfer)
- ORM: Anforderung einer Untersuchung (Order Message)
- ORU: Befundübermittlung (Observation Result Unsolicited)

- MDM: Übermittlung medizinischer Dokumente und Befunde (Medical Document Management)

Nachrichtensegmente

Die gängigen und meist verwendeten Segmente im Bereich der Radiologie sind:

- MSH: Nachrichtenkopf (Message Header)
- EVN: Nachrichtenart (Event Type)
- PID: Patientenstammdaten (Patient Identification)
- PV1: Falldaten (Patient Visit)
- OBR: Auftragsdetails (Observation Request)
- OBX: Befunde (Observation Result)
- ORC: Allgemeine Auftragsinformationen (Common Order)
- MSA: Quittung (Message Acknowledgment)
- ERR: Fehler (Error)

Die in Listing 2.1 gezeigte vereinfachte HL7-Nachricht ADT^A01 teilt allen Empfängern die Aufnahme eines Patienten im Krankenhaus mit. Das MSH-Segment legt die Kommunikationsdaten (Sender, Empfänger) sowie die Art der Nachricht (ADT) und die verwendete HL7-Version (2.3) fest und das EVN-Segment den Typ beziehungsweise die Struktur (A01) der Nachricht. Die folgenden Segmente beschreiben den Patienten. Das PID-Segment (Patient Identification) beinhaltet die Patientenstammdaten und PV1 (Patient Visit) beschreibt den Grund des Aufenthalts.

Listing 2.1: Minimalbeispiel einer HL7 ADT^A01 Nachricht

```

1 MSH|^~\&|SENDAPP|SENDER|RECAP|RECEIVER|20181123144259||ADT^A01|EI348294998|A|2.3|123
2 EVN|A01|20181123144200||
3 PID|||PID12345|Mayer^Peter||2827612|M||Bahnhofstr. 18^Musterhausen^17189^D|||||
4 PV1||IN|01^6^123^URO|||||||987^Müller Heinz^Dr. med.|||||||123456789|||||||20181123144200

```

Da die einzelnen Systeme nicht immer wissen können, an wen sie ihre Nachrichten senden sollen, und zudem meist eine Steuerung des Nachrichtenflusses vorgenommen werden muss, kommt hier meist zusätzlich ein Kommunikationsserver zum Einsatz. Dieser kann Nachrichten von verschiedenen Systemen empfangen und diese regelbasiert an entsprechende Empfänger weiterleiten. Das Kommunikationssystem übernimmt auch die Aufgabe eines Filters, kann Nachrichten zwischenspeichern und bei Bedarf neu versenden oder eine Nachricht an multiple Empfänger weiterleiten. Eine weitere wichtige Aufgabe eines Kommunikationsservers ist auch die Konvertierung von HL7-Nachrichten zwischen verschiedenen Typen und Versionen, um Geräte mit unterschiedlichen Versionsständen miteinander verbinden zu können. Weiterhin bieten die meisten Kommunikationsserver auch die Möglichkeit, HL7-Nachrichten aufgrund von anderen Ereignis-Triggern zu erstellen. Diese können auch nicht HL7-fähige Subsysteme wie zum Beispiel Arztpraxissysteme, die unter Umständen nur über eine Gerätedaten-Transfer (GDT)-Schnittstelle verfügen, in die Krankenhauskommunikation einbinden.

HL7 v3

Das pragmatische Vorgehen von HL7 v2 brachte zwar eine einfache Möglichkeit zum unkomplizierten Austausch von Nachrichten zwischen verschiedenen Sub-Systemen im Krankenhaus, allerdings auch einen extrem hohen Integrationsaufwand und wachsende Inkonsistenzen der Schnittstellen durch das Fehlen jeglicher Definition von Prozessen und Semantik mit sich. Um diese Schwäche zu beseitigen, wurde bereits 1995 an Version 3 des Standards gearbeitet, welche dann 2005 publiziert wurde. Eines der Hauptziele von HL7 v3 ist das Schaffen eines einheitlichen Kommunikations- und Prozessverständnisses zwischen den Partnern. HL7 v3 legt im Gegensatz zu seinem Vorgänger nicht nur die Syntax, sondern auch die Semantik der Nachrichten fest. Diese Entwicklung folgt dem HL7 Development Framework - ISO/HL7 27931. Nachrichten werden nicht mehr textbasiert, sondern im XML-Format kodiert und ausgetauscht.

Trotz der Vorteile von HL7 v3 gegenüber seinem Vorgänger ist HL7 v2 innerhalb des Krankenhauses immer noch der Standard der Wahl und das gängigste Protokoll

in diesem Bereich. Bei der Kommunikation mit Systemen außerhalb des Krankenhauses und bei der Anbindung von mobilen Geräten und Gesundheits-Apps gewinnt HL7 v3 und insbesondere dessen Nachfolger HL7 FHIR (Fast Healthcare Interoperability Resources) jedoch immer mehr an Bedeutung (Bender and Sartipi, 2013; Hussain et al., 2018).

HL7 FHIR

Der 2014 durch Health Level Seven International ins Leben gerufene Standard FHIR (gesprochen engl. *fire*) gilt als neuer Interoperabilitätsstandard speziell für das Gesundheitswesen und unterstützt wie auch schon seine Vorgänger den Datenaustausch zwischen Softwaresystemen (HL7 Deutschland e.V., 2019). Um den Anforderungen moderner Kommunikationssysteme auch über die Grenzen eines Krankenhauses hinweg gerecht zu werden, wurde FHIR auf Basis moderner Webtechnologien entwickelt und vereint die Funktionen von HL7 Version 2, Version 3 und CDA.

Die Speicherung von Gesundheitsdaten findet immer häufiger online statt. Daten werden nicht mehr in monolithischen Desktop-Anwendungen gespeichert, sondern vermehrt online und On-Demand abgerufen. Aus diesem Grund setzt FHIR auf eine REST-Architektur, deren Endpunkte unter Verwendung von im Internet gängigen Sicherheitsmechanismen abgefragt werden können.

Neben den Konzepten der REST-Architektur kommen etablierte Web-Standards wie zum Beispiel XML, JSON, HTTPS oder OAuth zum Einsatz. Bei der Implementierung wurde außerdem darauf geachtet, dass die Inhalte jederzeit auch menschenlesbar dargestellt werden können. Auf eine binäre Codierung der Daten wie beispielsweise bei DICOM wurde verzichtet.

FHIR ist nicht die Lösung aller Interoperabilitätsprobleme und bildet nicht alle Workflows im Gesundheitswesen komplett ab. Der Fokus des Standards liegt viel mehr auf der einfachen Implementierbarkeit für Softwareentwickler und der Unterstützung gängiger Anwendungsfälle. Um hier dennoch ungewöhnliche Anwendungsfälle abdecken zu können, bietet FHIR eine Option zu Erweiterung des Standards.

Alle Use Cases werden durch die Standard-Bausteine Ressourcen, Referenzen und Profile abgebildet.

Ressource: Eine Ressource ist die kleinste atomare Einheit des Datenaustauschs. Die aktuell verfügbaren Ressourcen decken das gesamte Spektrum des Datenaustauschs im Gesundheitswesen ab (Beispiele: Patient, Auftrag, Medikation etc.). Jede Ressource besteht aus strukturierten und maschinenlesbaren Daten, einer menschenlesbaren textuellen Beschreibung des Inhalts sowie Erweiterungen (engl. extensions), welche über gängige Anwendungsfälle hinaus benötigte Daten enthalten.

Referenz: Ressourcen können mit Hilfe von Referenzen auf andere Ressourcen verweisen. Hierdurch können Datensätze für bestimmte Anwendungsfälle miteinander verknüpft werden.

Profil: Ein Profil ist die Zusammenstellung von Ressourcen und Referenzen, die für einen bestimmten Anwendungsfall benötigt wird. Hierbei unterliegt die Kombination von Ressourcen keinen Beschränkungen, und Profile werden durch HL7 International spezifiziert und können durch regionale HL7-Benutzergruppen an nationale Gegebenheiten oder Regularien angepasst werden.

Durch das agile Entwicklungsmodell kann sich FHIR schnell an aktuelle Anforderungen anpassen und neue Use Cases in den Standard aufnehmen. Aktuell liegt FHIR in der Version 4.0 vor und ist seit Ende 2018 ein normativer Standard.

2.1.3. DICOM E-Mail

Die Übertragung von Daten via E-Mail ist heute Stand der Technik und in zahlreichen Krankenhäusern und Arztpraxen etabliert. Sowohl die Infrastruktur mit E-Mail-Servern als auch die Sicherheit, was Firewall-Freischaltungen und ähnliches angeht, sind ein gelöstes Problem. Daher hat sich die Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft (@GIT) 2003 entschlossen, eine Standardempfehlung für

die Teleradiologie (TR) zu erarbeiten und ein Whitepaper 'Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat' zu entwickeln (Weisser et al., 2005; Mildnerberger et al., 2005).

Die Standardempfehlung basiert auf der Verwendung des *DICOM Supplement 54: DICOM MIME Type*. Das Supplement 54 beschreibt die Übertragung von DICOM-Daten als E-Mail-Anhang mit dem MIMEType 'application/dicom' in einer 'multipart/mixed' Nachricht (Listing 2.2). Aus diesem Supplement ist der RFC 3240 'Digital Imaging and Communications in Medicine (DICOM) - Application/dicom MIME Sub-type Registration' entstanden (Clunie and Cordonnier, 2002), welcher bei der Internet Assigned Numbers Authority (IANA) den neuen MIMEType registriert und damit im Bereich der E-Mail-Kommunikation etabliert wurde. Die Basis der Kommunikation war zu dieser Zeit bereits mit den RFCs 2045-2049 gelegt und kommt auch bei DICOM E-Mail unverändert zur Anwendung. Dies erlaubt zum Beispiel auch eine Fragmentierung von Nachrichten unter Zuhilfenahme des 'message/partial'-Konzepts, welches ein Zerteilen von großen E-Mails in kleine Teil-E-Mails ermöglicht, um so auch über einen das Transfervolumen begrenzenden Mailserver kommunizieren zu können.

Listing 2.2: Minimalbeispiel einer DICOM E-Mail (multipart/mixed)

```

1 Date: Thu, 8 Aug 2018 14:28:32 +0100 (GMT+01:00)
2 From: sender@somewhere.com
3 To: receiver@otherhost.com
4 Message-ID: <1.2.276.0.23.60.279807577.1565270912110.1_cm@nero>
5 Subject: CHILI/Mail DICOM E-Mail
6 Mime-Version: 1.0
7 Content-Description: CHILI/Mail DICOM E-Mail [2.73.0]
8 Content-Type: multipart/mixed; boundary="PART-BOUNDARY=_ch-xxxx-mp-mix_1565270912133"
9
10 This is the preamble area of a multipart mixed message.
11
12 If you are reading this text, you might want to
13 consider changing to a mail reader that understands
14 how to properly display MIME multipart messages.
15
16 --PART-BOUNDARY=_ch-xxxx-mp-mix_1565270912133
17 Content-Type: application/dicom; Name="123456789.dcm"
18 Content-Transfer-Encoding: base64
19
20 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
21 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
22 AAAAAAAAAAAAAAAAAAABESUNNAgAAAFVMBADOAAAAAgABAE9CAAACAAAAAEECAAIAVUkaADEuMi44
23 NDAuMTAwMDguNS4xLjQuMS4xLjEAAgADAFVJPAAxLjMuMTUuMi4xMTA3LjUuOC4yLjQ4NTI1Ny44
24 ...
25 --PART-BOUNDARY=_ch-xxxx-mp-mix_1565270912133--

```

Über die Verschlüsselung der Inhalte macht das Supplement 54 keine Vorgaben, schlägt aber die Verwendung von Secure / Multipurpose Internet Mail Extensions (S/MIME) vor, was in den USA auch häufig angewendet wird. Da die Etablierung einer zentralen Schlüsselverwaltung in einem Teleradiologienetzwerk, welches mehrere Krankenhäuser umspannt, organisatorisch schwierig ist, hat sich die @GIT für die Verwendung von PGP/GPG (RFC 4880) entschieden, was einen Schlüsselaustausch ad hoc und ohne zentrale Vergabestelle ermöglicht. Dies bringt wiederum das Problem der Verteilung der Schlüssel in einem Peer-to-Peer Netzwerk mit sich, ist aber dennoch einfacher zu etablieren als eine zentrale Schlüsselorganisation.

DICOM E-Mail-Netzwerke verwenden sowohl das Push- als auch das Pull-Modell der Teleradiologie (Kapitel 2.2.2). Daten werden auf dem Rechner beziehungsweise Server des Absenders verschlüsselt und dann mittels Simple Mail Transfer Protocol (SMTP) in einem spezifischen Postfach auf dem Mailserver abgelegt. Der Empfänger der Nachricht ruft die Daten dann entweder mittels Post Office Protocol (POP) oder Internet Message Access Protocol (IMAP) ab und entschlüsselt die für ihn bestimmten Daten (Abbildung

2.1). Weiterhin prüft der Empfänger idealerweise noch die Signatur des Absenders, um sicherzugehen, dass die Daten auch wirklich vom entsprechenden Absender kommen und damit von einer vertrauenswürdigen Quelle stammen.

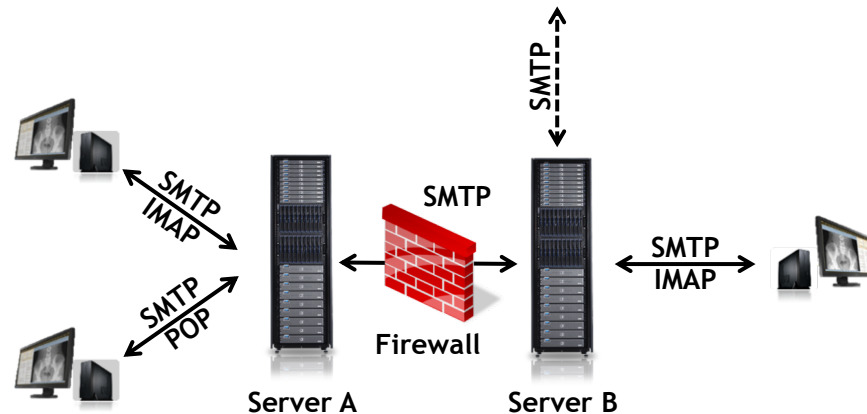


Abbildung 2.1.: Aufbau eines DICOM E-Mail-Netzwerks. Schematische Darstellung eines Netzwerks unter Verwendung der unterschiedlichen E-Mail-Protokolle.

Aufbau und Verschlüsselung von DICOM E-Mail

Wie oben beschrieben, beruht das im Whitepaper festgelegte Kryptographie-Verfahren zur Verschlüsselung und Signatur von DICOM E-Mails auf PGP/GPG. Die generierten Inhalte der E-Mail mit dem Mime-Type 'multipart/mixed' und 'application/dicom' werden so zusätzlich noch von einem 'multipart/encrypted' Container umschlossen (Abbildung 2.2). Dies ist keine Eigenheit des Whitepapers und entspricht dem Standard der E-Mail-Verschlüsselung mit PGP/GPG.

Versand von nicht-DICOM-Objekten

Eine zusätzliche Erweiterung des Whitepapers ist die Möglichkeit, auch nicht-DICOM-Objekte einfach per E-Mail zu übertragen. Hierbei erhält der entsprechende Mime-Part ein zusätzliches Header-Feld *X-Telemedicine-Studyid* (Abbildung 2.3). Diese StudyID entspricht der DICOM StudyInstanceUID und referenziert die zugehörige DICOM-Studie zu den nicht-DICOM-Daten.

From:	radiology_mainz@teleradiologie.de
To:	radiology_mannheim@teleradiology.de
Subject:	DICOM-email
MIME-Version:	1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted"	
Content-Type: application/pgp-encrypted	
Version: 1	
Content-Type: application/octet-stream	
Content-Type: multipart/mixed	
OpenPGP encrypted	Content-Type: application/dicom; name="1:23:456:7890:XXXXXXXX:01.dcm" [1:23:456:7890:XXXXXXXX:01.dcm]
	Content-Type: application/dicom; name="1:23:456:7890:XXXXXXXX:02.dcm" [1:23:456:7890:XXXXXXXX:02.dcm]
	Content-Type: application/dicom; name="1:23:456:7890:XXXXXXXX:03.dcm" [1:23:456:7890:XXXXXXXX:03.dcm]
	Content-Type: application/dicom; name="1:23:456:7890:XXXXXXXX:04.dcm" [1:23:456:7890:XXXXXXXX:04.dcm]
	Content-Type: application/dicom; name="1:23:456:7890:XXXXXXXX:XX.dcm" [1:23:456:7890:XXXXXXXX:XX.dcm]

Abbildung 2.2.: Aufbau einer DICOM E-Mail. Schematische Darstellung einer verschlüsselten DICOM E-Mail mit mehreren DICOM-Objekten in einer Nachricht. (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 20)

Auf diese Weise können beliebige Objekte, sofern sie einen Studienzusammenhang besitzen, per DICOM E-Mail übertragen werden. Dies eignet sich besonders für Standarddokumente wie Befunde im PDF oder Word-Format als auch für Bilder, die als JPEG oder PNG vorliegen.

Dies setzt allerdings voraus, dass die Gegenseite den Empfang, die Verarbeitung und die Anzeige dieser Dokumente unterstützt.

Empfangsbestätigungen

Weiterhin wurde im Rahmen der Standardisierung der Verschlüsselung zusätzlich noch das Benachrichtigungskonzept von E-Mail-Nachrichten erweitert. Der Standard Benachrichtigungsmechanismus Message Disposition Notification (MDN) nach RFC 8098 beziehungsweise RFC 3503 sieht lediglich eine Benachrichtigung des Empfängers auf Basis der kompletten E-Mail vor. Um dieses Problem zu lösen, wurde zusätzlich zur Standardbenachrichtigung, welche den Erhalt der gesamten E-Mail bestätigt, noch der Mail-Header X-Telemedicine-Disposition-Notification-To und -Key eingeführt, um Bestätigungen auf einzelne Teile von E-Mails anfordern zu können (Abbildung 2.4).

From:	radiology_mainz@teleradiologie.de
To:	radiology_mannheim@teleradiology.de
Subject:	DICOM-email
MIME-Version:	1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted"	
Content-Type: application/pgp-encrypted	
Version: 1	
Content-Type: application/octet-stream	
OpenPGP encrypted	Content-Type: multipart/mixed
	Content-Type: application/dicom; name="1.23.456.7890.XXXXXXXXXX.dcm" [1.23.456.7890.XXXXXXXXXX.dcm]
	Content-Type: text/plain; name="report.txt" X-TELEMEDICINE-STUDYID: 1.23.456.7890.XXXXXXXXXX [report.txt]
	Content-Type: image/jpeg; name="BrainReference.jpg" X-TELEMEDICINE-STUDYID: 7.13.645.0789.XXXXXXXXXX [BrainReference.jpg]
	Content-Type: application/pdf; name="TheBigBrainStudy2005.pdf" X-TELEMEDICINE-STUDYID: 7.13.645.0789.XXXXXXXXXX [TheBigBrainStudy2005.pdf]
...	

Abbildung 2.3.: DICOM E-Mail mit nicht-DICOM-Daten. Codierung von DICOM- und nicht-DICOM-Daten in einer DICOM E-Mail. (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 21)

Hierbei kann auch eine verschlüsselte und signierte Empfangsbestätigung unter Verwendung des KeyID-Headers versendet werden, so dass der gesamte DICOM E-Mail-Verkehr inklusive der Benachrichtigungen verschlüsselt erfolgen kann. Unter Verwendung dieses Mechanismus können so im Fehlerfall detaillierte und maschinenlesbare Fehlercodes pro E-Mail-Teil übermittelt werden, um zum Beispiel den Neuversand eines korrupten DICOM-Bildes anzustoßen oder dem Sender mitzuteilen, dass ein bestimmtes Objekt aus der E-Mail nicht verarbeitet werden konnte.

Da die Bestätigungsanforderung im potentiell verschlüsselten Teil der E-Mail enthalten ist, ist hier zwingend vorgesehen, dass immer auch eine Standard MDN angefordert und versendet wird, um dem Sender der E-Mail auch mitteilen zu können, wenn es Probleme mit der Entschlüsselung der E-Mail gab oder zum Beispiel der kryptographische Schlüssel abgelaufen ist und deshalb in Zukunft keine E-Mails von diesem Sender angenommen werden.

Message Sets

Der oben beschriebene Mechanismus der MDN erlaubt dem Versender der Daten, detailliert zu protokollieren, welche Objekte angekommen sind und wie lange der Versand



Abbildung 2.4.: Empfangsbestätigung bei DICOM E-Mail. Die dargestellte E-Mail enthält sowohl einen Disposition-Notification-To Header auf oberster Ebene als auch einen X-Telemedicine-Disposition-Notification-To beziehungsweise -Key Header auf Ebene jeden Mime-Parts. (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 30)

gedauert hat. Da die Kommunikation bei DICOM E-Mail über einen dedizierten E-Mail-Server erfolgt, kann der Empfänger der E-Mail aber nicht feststellen, ob eventuell Daten bei der Übermittlung verloren gegangen sind oder ob der Transfer abgeschlossen ist.

Aus diesem Grund führt das Whitepaper das Konzept der Message Sets ein, welches analog zum 'message/partial' Sub-Type aus RFC 2046 definiert ist. Ein Set von E-Mails kann über folgende Nachrichten-Header vom Absender als zusammengehörig markiert werden.

SETID - eine eindeutige ID für ein Set von zusammengehörigen E-Mails

SETPART - die Nummer der aktuellen E-Mail innerhalb eine Sets

SETTOTAL - die Anzahl der im Set enthaltenen E-Mails

Der Empfänger kann diese Header bei Empfang auswerten und kann so sicherstellen, dass er alle vom Absender versendeten E-Mails innerhalb eines Sets erhalten hat.

Weiterhin bietet das Message Set auch die Möglichkeit, Daten in einem Transfer als zusammengehörig zu kennzeichnen. Dies entspricht einer Association im Bereich der DICOM-Kommunikation, und so werden alle Daten einer Studie oder Serie meist zusammen in einem Set versendet (Abbildung 2.5).

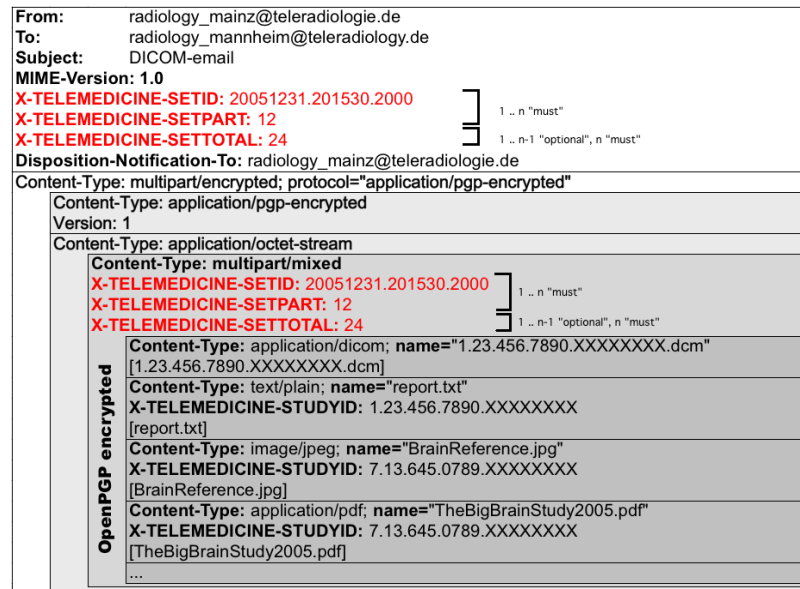


Abbildung 2.5.: DICOM E-Mail mit Message Sets. Implementierung einer Association mit DICOM E-Mail Message Sets. (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 23)

DICOM E-Mail in Deutschland

Als Beispiele für große auf das DICOM E-Mail-Whitepaper basierte Netzwerke in Deutschland sind das Teleradiologieprojekt Rhein-Neckar-Dreieck (<http://www.teleradiologie-rnd.de>, 15.01.2019) als auch der Westdeutsche Teleradiologieverbund (<https://www.medecon-telemedizin.de>, 15.01.2019) zu nennen.

2.1.4. Proprietäre Übertragung via HTTP und HTTPS

Neben der standardisierten Übertragung von Bild- und Befunddaten via HL7, DICOM oder DICOM E-Mail gibt es noch zahlreiche Varianten, um Daten proprietär über ein Netzwerk zu übertragen. Hierbei müssen Sender und Empfänger die Metadaten der Kom-

munikation auf anderem Wege aushandeln, bevor die eigentlichen Daten dann übermittelt werden können.

In diesem Bereich hat sich das Hypertext Transfer Protocol (HTTP) weitgehend durchgesetzt. Die Nutzlast kann so über Standard-Ports auch durch eine Firewall übertragen werden. Der verschlüsselte Transport via Hypertext Transfer Protocol Secure (HTTPS) ist somit einfach möglich. Zur weiteren Absicherung der Kommunikation können sowohl Server- als auch Client-Zertifikate eingesetzt werden.

Um zusätzlich zu den reinen Binärdaten auch Zusatzinformationen wie zum Beispiel Dateiname und -typ übertragen oder das aus dem DICOM-Standard etablierte Prinzip des sendenden und empfangenden Application Entity Title (AET) verwenden zu können, werden diese Informationen meist in den HTTP-Header-Daten mitgesendet und so von der Gegenseite ausgewertet. Diese Art des Datenaustauschs setzt allerdings voraus, dass beide Seiten mit den Daten umgehen können, da hier nicht wie bei der Übertragung mittels DICOM-Protokoll Transfersyntaxen ausgehandelt werden. Der Vorteil ist allerdings die Verwendung von Standard Web-Technologien, was den Einsatz von Web-Proxies, Load-Balancer oder einer Web Application Firewall (WAF) ermöglicht.

Durch diese Einschränkungen kommt diese Art der Übertragung zurzeit meist nur in homogenen Netzwerken unter dem Einsatz von proprietären Protokollen auf Basis von HTTP durch einzelne Hersteller zur Anwendung.

In den letzten Jahren hat sich der DICOM-Standard insbesondere durch Erweiterungen in *Part 18 - Web Services* auch dahingehend gewandelt, diese Vorteile immer mehr zu nutzen und die Übertragung via HTTP weiter zu standardisieren, so dass dieser auch im Bereich des HTTP-Transfers eine immer größere Rolle spielt (Koutelakis and Lymberopoulos, 2009; Lipton et al., 2012). Allerdings gibt der Standard nur Hilfestellung, was den Zugriff auf einzelne Ressourcen via HTTP angeht und beschreibt nicht den Aufbau von Netzwerken unter Zuhilfenahme dieser Technologie.

2.1.5. Patienten-CD

Eine weitere gängige und weit verbreitete Methode zum Austausch von Bilddaten sind die sogenannten Patienten-CDs, welche häufig zwischen niedergelassenen Ärzten beziehungsweise Radiologen und Krankenhäusern zum Einsatz kommen. Hierbei ist der Patient sowohl der Gegenstand der Daten als auch der Überbringer der CD, welche er statt der früher üblichen 'Röntgentüten' zwischen den Ärzten, also zwischen Sender und Empfänger, hin und her trägt.

Patienten-CDs sind in den meisten Fällen DICOM-CDs, welche nach dem DICOM-Standard erstellt wurden. Hierbei müssen die Daten als DICOM File Set auf einer streng nach ISO 9660 formatierten CD abgelegt werden. Die Dateinamen dürfen aus maximal acht Zeichen (nur Großbuchstaben und Ziffern) ohne Dateiendungen bestehen. Zusätzlich muss im Wurzelverzeichnis der CD eine Datei mit dem Namen DICOMDIR liegen, welche alle auf der CD vorhandenen Daten referenziert.

Trotz dieser einfachen und strikten Regel ist der Austausch von Daten via CD nicht immer unproblematisch (Walz, 2006). Die Vielzahl der unterschiedlichen Hersteller und Implementierungen hat eine sehr heterogene Implementierung von Patienten-CDs zu Tage gebracht. Ein Test von DICOM-CDs auf dem Röntgenkongress 2006 zeigte eine Abweichung von mehr als 70% von der vorgegebenen Struktur (Mildenberger et al., 2007). Aufgrund dieser Ergebnisse entwickelte die Deutsche Röntgengesellschaft (DRG) zusammen mit OFFIS (<http://dicom-cd.de>, 15.01.2019) einen Prozess zur Qualitätsverbesserung von DICOM-CDs. Folgende Schwerpunkte wurden dabei definiert:

- Genaue Spezifizierung von Anforderungen an die Hersteller der DICOM-CDs,
- einen Leitfaden für Anwender zum Umgang mit DICOM-CDs,
- die Entwicklung eines Testat-Prozesses zur Verifizierung von DICOM-CDs.

Dies brachte eine enorme Qualitätssteigerung der DICOM-CDs mit sich und führte dazu, dass Patienten-CDs bis heute eine einfache und auch kostengünstige Variante zur Übermittlung von Bilddaten durch den Patienten darstellen. Es gibt mittlerweile zahlreiche Anbieter von Brennrobotern und auch Lösungen für den automatischen Import

von Daten auf der Empfängerseite durch den Einsatz von Importrobotern. Eine Weiterentwicklung für steigende Datenmengen auf Basis von DVDs oder USB-Sticks deckt somit auch den Bedarf an größeren Medien ab.

Trotzdem bleibt der Import von Fremddaten in ein Krankenhaus problematisch. Die Bilder müssen meist manuell oder halbautomatisch mit der entsprechenden Patienten-ID gepatched werden, um diese korrekt einlesen zu können. Alternativ wird hier ein sogenanntes Schmutz- oder Shuttle-PACS vorangestellt, in das alle externen Aufnahmen eingelesen werden. Daten werden dann nur bei Bedarf in das Primärsystem des Krankenhauses übernommen.

Auf der anderen Seite eignen sich DICOM-CDs mit einem integrierten DICOM-Viewer gerade im Bereich der niedergelassenen Ärzte hervorragend, um einen kurzen Blick auf die Röntgenbilder eines Patienten zu werfen.

Aber gerade vor dem Hintergrund der Entstehung von webbasierten Portallösungen und den Möglichkeiten der XDS-basierten Vernetzung (Aryanto et al., 2013) erscheint die Patienten-CD eher als eine Brückentechnologie hin zur vollständigen elektronischen Kommunikation.

2.1.6. DICOM in the Cloud

Eine weitere Möglichkeit zur Übertragung von DICOM-Daten bietet die Cloud. Hierbei werden Daten in ein zentrales oder dezentrales Rechnernetz geladen und so dem Empfänger zugänglich gemacht (Armbrust et al., 2010). Dies hat den Vorteil, dass Daten zeitgleich von verschiedenen Empfängern betrachtet beziehungsweise heruntergeladen werden können. Da die Daten so frei über das Internet übertragen und auf fremden Systemen gespeichert werden, spielt hier die Verschlüsselung zum Schutz der personenbezogenen Daten eine sehr große Rolle. Hierbei sollte man sich immer bewusst sein, dass die Cloud nicht existiert und vielmehr mit folgenden Merksatz beschrieben werden muss:

”Es gibt keine Cloud, nur die Computer anderer Leute.” (Czeschik and Lindhorst, 2018)

Gerade im Bereich Cloud-Computing muss stark zwischen privaten und öffentlichen Clouds sowie den unterschiedlichen Servicemodellen und Betriebsarten unterschieden werden. Eine Cloud abstrahiert nicht einfach nur die Komplexität eines Rechnernetzwerks, sondern bringt auch zusätzliche Anforderungen an die Datensicherheit mit sich, da die Daten meist nicht mehr in abgesicherten Datenspeichern vorgehalten werden, sondern frei über das Internet zugänglich sind. Aber gerade durch das Nutzen von gemeinsamen Datenspeichern und Services wird Cloud-Computing auch im medizinischen Umfeld immer interessanter.

Bereits Anfang der 1990er Jahre kam die Idee auf, dass man Rechner in Netze verteilen sollte, um die Rechenlast zwischen vielen Computern aufteilen zu können. Diese Entwicklung wurde in Deutschland vor allem durch die Gesellschaft für Mathematik und Datenverarbeitung GmbH (GMD) vorangetrieben, welche 1995 mit BSCW (Basic Support for Cooperative Work) ein System zur Kollaboration von Benutzern in einem Online-System entwickelte, das seit der Fusion von GMD und der Fraunhofer-Gesellschaft zum Fraunhofer-Institut für Angewandte Informationstechnik (FIT) im Jahre 2001 auch kommerziell vertrieben wird. Die Kollaborationsplattform bietet zahlreiche Funktionen wie Aufgabenverwaltung, Terminplanung, Nachrichtendienste und Dateiablage, welche die Zusammenarbeit von Nutzern ermöglicht.

Das wohl bekannteste Soziale Netzwerk Facebook ist seit 2004 für Benutzer aus der ganzen Welt offen und bietet zahlreiche Kollaborations- und Interaktionsmöglichkeiten zwischen den mittlerweile mehr als 2,6 Milliarden Nutzern an (Roth and Wiese, 2018). Daten werden grundsätzlich zentral gespeichert und den Benutzern dann durch Freigabe zugänglich gemacht. Durch den raschen Anstieg der Datenmengen müssen auch besondere Konzepte der Datenhaltung entwickelt werden. Die Konzepte der Datenreduktion in Sozialen Netzwerken oder generell cloudbasierten Applikationen lassen sich so auch auf radiologische Bilddaten übertragen.

Datenkompression

Der erste Schritt zur Reduzierung der Datenmengen ist die Kompression der Daten. Hierbei unterscheidet man grundsätzlich zwischen verlustloser Kompression (engl. lossless compression) und verlustbehafteter Kompression (engl. lossy compression). Bei der verlustfreien Kompression wird der Informationsgehalt eines Datensatzes nicht verändert, die Daten aber dennoch komprimiert. Dies ist sowohl bei Bilddaten, zum Beispiel in Form der JPEG Lossless Kompression (Nivedha et al., 2017), als auch bei allen anderen Binärdaten, zum Beispiel durch den Einsatz der ZIP oder GZIP-Kompression, möglich.

Weiterhin können insbesondere Bilddaten auch verlustbehaftet komprimiert werden, so dass zwar der subjektive Bildeindruck erhalten bleibt, die Daten aber nicht ohne Verlust wieder in ihre ursprüngliche Form gebracht werden können. Diese Art der Kompression kann dazu beitragen, den immer größeren Datenmengen in der Radiologie entgegenzuwirken, ist aber insbesondere bei diagnostischen Bildern kritisch zu sehen. Aus diesem Grund wurde 2008 mit Mitgliedern der Arbeitsgemeinschaft Informationstechnologie (@GIT), der Arbeitsgemeinschaft Physik und Technik (APT) sowie der Deutschen Röntgengesellschaft (DRG) eine Konsensuskonferenz zur Kompression digitaler DICOM-Bilddaten in der Radiologie durchgeführt (Loose et al., 2008). Hierbei haben sich die teilnehmenden Radiologen sowie Vertreter aus Physik und Technik, Industrie und Behörden auf den möglichen Einsatz einer verlustbehafteten Kompression von DICOM-Bildern je nach Modalität und Körperregion zwischen 1:5 (CT Gehirn) und 1:15 (CR/DR Mammographie) geeinigt (Tabelle 2.1). Die erarbeiteten Ergebnisse wurden dann 2011 von der Strahlenschutzkommission (SSK) bestätigt und veröffentlicht (Strahlenschutzkommission, 2011). Sie sind heute gängige Praxis.

Deduplizierung

Die zentrale Speicherung bietet auch einen Ansatz für eine Deduplikation von Daten. Hierbei werden gleiche oder ähnliche Datensätze nicht mehrfach gespeichert, sondern nur deren Referenzen (He et al., 2010). Diese Technik findet im Kleinen bereits auf

Tabelle 2.1.: Kompressionsfaktoren für DICOM-Bilder nach 'Datenkompression bei Röntgenbildern - Empfehlung der Strahlenschutzkommission'. CT: Computertomographie, CR/DR: Digitale Radiographie (Speicherfolien/Festkörperdetektoren), MR: Magnetresonanztomographie, RF/XA: Fluoroskopie/Angiographie.

Bildgebung	Organ / Körperregion	Kompression
CT	Gehirn	1:5
CT	Abdomen	1:8
CT	Thoraxweichteile	1:8
CT	Lunge	1:8
CT	Skelett	1:8
CR/DR	Radiographie Lunge	1:10
CR/DR	Muskulo-Skelettsystem	1:10
CR/DR	Abdomen	1:10
CR/DR	Mammographie	1:15
MR	alle Anwendungen	1:7
RF/XA	Durchleuchtung/DSA/Kardangio	1:6

lokalen Festplatten von Computern statt und wird in diesem Fall durch das Dateisystem übernommen. Die beiden bekanntesten Vertreter sind hier das B-tree File System (BTRFS) (Winkler, 2015; Hilgert et al., 2018) und das Zettabyte File System (ZFS). Bei der Deduplizierung von Inhalten auf Festplatten erreicht ZFS mit ca. 16% eine ähnliche Platzersparnis wie eine GZIP-Kompression (Kluge, 2014).

Deduplizierung lässt sich aber nicht nur auf Ebene des Dateisystems durchführen. Durch die Speicherung von Daten in einer zentralen Instanz mit globalem Index können auch Daten, die über mehrere Server verteilt sind, auf ähnliche Weise dedupliziert werden. Weiterhin ist es durch die immer weiter verbreitete Nutzung von Virtualisierungs-umgebungen auch möglich, eine Deduplizierung auf virtuellen Maschinen anzuwenden, um so auch hier einen Effekt zu erzielen (Jin and Miller, 2009).

Verschlüsselung

Daten, die in öffentlichen oder halböffentlichen Rechnernetzen liegen und hier insbesondere Patientendaten, sind besonders schutzwürdig. Es müssen Maßnahmen ergriffen werden, diese Daten zu schützen. Hier kommen sowohl Verfahren der Transportverschlüsselung, also eine Verschlüsselung der Daten beim Transport zwischen Sender (Client) und

Empfänger (Server) zum Einsatz, als auch eine Verschlüsselung des Dateisystems oder eine Verschlüsselung der Daten an sich, so dass nur berechtigten Personen Zugriff auf einen Teil der Daten gewährt werden kann. Zu diesem Zweck kann auch eine Ende-zu-Ende-Verschlüsselung zum Einsatz kommen, bei der die Daten vor dem Versand oder Upload durch den Sender verschlüsselt und nur durch den Empfänger entschlüsselt werden können. So kann ein Zugriff durch unberechtigte Dritte wie zum Beispiel die Administratoren des Systems auch auf potentiell unsicheren Plattformen vermieden werden. Eine Verschlüsselung ist mittlerweile auch mit deduplizierten Daten möglich (Akhila et al., 2016), aber auch hier sind schon Angriffs-Szenarien bekannt (Haque, 2019).

Private und Öffentliche Cloud

Neben den Sozialen Netzwerken ist *Cloud-Computing* heute vor allem durch Amazon Web Services (AWS), die Google Cloud Platform (GCP) als auch die Microsoft Azure Cloud in der Industrie stark vertreten. Immer mehr Rechenleistung wird in die 'Cloud' verlagert.

Im September 2011 veröffentlichte das National Institute of Standards and Technology (NIST) eine Definition (Mell and Grance, 2011) über die unterschiedlichen Service- und Liefermodelle einer Cloud, welche heute weit verbreitet und gebräuchlich ist (Simmon and Bohn, 2012).

Servicemodelle

Cloud-Computing lässt sich grundsätzlich in drei verschiedene Servicemodelle einteilen.

SaaS Software as a Service

Der Provider einer SaaS-Cloud stellt eine Auswahl von Anwendungsprogrammen über das Netzwerk beziehungsweise Internet bereit, welche dann von den Nutzern der Cloud bei Bedarf abonniert werden können. Daher spricht man bei SaaS auch häufig von Software on Demand (Software bei Bedarf). Die Software wird hier nicht in Form eines Downloads angeboten, sondern bietet viel mehr einen Web-

oder API-Zugriff, um sie in die eigene Programmier- oder Anwendungsumgebung integrieren zu können.

PaaS Platform as a Service

Ein PaaS-Provider bietet den Nutzern einen Zugang zu Programmierung- und Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten, in denen sie ihrer eigene Anwendungen entwickeln und bereitstellen können. Die auf der Plattform entwickelten Anwendungen laufen auf der Infrastruktur des Providers und werden dann durch den Dienstanbieter bereitgestellt und unterhalten.

IaaS Infrastructure as a Service

Diese Betriebsart bietet dem Nutzer einen Zugang zu virtualisierten Hardware-Ressourcen wie Rechnern, Netzwerkkomponenten und Datenspeicher. Mit IaaS gestalten sich Nutzer ihre eigenen virtuellen Computer-Cluster und sind daher für die Auswahl, die Installation, den Betrieb und das Funktionieren ihrer Software selbst verantwortlich. IaaS bietet dem Nutzer also ein virtualisiertes Rechenzentrum, welches er dynamisch an seinen Bedarf anpassen kann.

Betriebsarten

Weiterhin lässt sich die Betriebsart von Cloud-Computing nach NIST in vier Gruppen einteilen.

Public Cloud, die öffentliche Rechnerwolke

bietet Zugang zu einer abstrahierten IT-Infrastruktur über das Internet. Public Cloud-Anbieter erlauben ihren Kunden IT-Infrastruktur zu mieten, wobei die Abrechnung meist auf einer flexiblen Basis anhand des tatsächlichen Nutzungsgrads beziehungsweise Verbrauchs oder der Rechenkapazität vorgenommen wird. Dadurch können Kunden die Rechner- und Datenzentrumsinfrastruktur flexibel und nach Bedarf nutzen, ohne in Hardware investieren zu müssen.

Private Cloud, die private Rechnerwolke

Eine Private Cloud stellt ähnlich einer Public Cloud-Umgebung abstrahierte IT-Infrastruktur für ihre Benutzer zur Verfügung. Die Private Cloud wird allerdings ausschließlich für eine einzige Organisation betrieben. Das Hosten und Verwalten der Cloud-Plattform kann intern durch ein firmeneigenes Rechenzentrum oder auch ausgelagert durch Dritte erfolgen.

Community Cloud, die gemeinschaftliche Rechnerwolke

bietet ähnlich die wie Public Cloud einen Zugang zu abstrahierten IT-Infrastrukturen, welcher jedoch für einen kleineren Nutzerkreis der die gleichen Interessen verfolgt, bestimmt ist. So können zum Beispiel Behörden, Forschungseinrichtungen oder -gemeinschaften eine zweckbezogene Cloud aufbauen und diese gemeinsam nutzen.

Hybrid Cloud, die hybride Rechnerwolke

Hybride Clouds bezeichnen die Nutzung von zwei oder mehr eigenständigen Cloud-Infrastrukturen über standardisierte Schnittstellen.

Zusätzlich lassen sich die oben genannten Servicemodelle und Betriebsarten miteinander kombinieren und erlauben Mischformen wie eine *Virtual Private Cloud*, welche grundsätzlich privat ist, aber auf einer öffentlichen Infrastruktur betrieben wird. Dies wäre zum Beispiel die Auslagerung von Diensten aus einem privaten Rechenzentrum in die Amazon-Cloud. Hier wären die Daten und Dienste (zumindest theoretisch) nur dem Auftraggeber beziehungsweise Kunden zugänglich, würden aber in einem Rechenzentrum des Cloud-Anbieters laufen. Je nach Vertrag mit einem Cloud-Anbieter kann rechtlich sichergestellt werden, dass Daten ausschließlich in Deutschland, Europa oder weltweit verteilt beziehungsweise gehostet werden.

Grundsätzlich ist Cloud-Computing nur die konsequente Weiterentwicklung, alle Daten nicht mehr selbst im eigenen Rechenzentrum zu hosten, sondern sowohl Daten als auch Dienste gezielt auszulagern und eine Kostenersparnis durch das Teilen von Ressourcen mit anderen Nutzern einer Cloud zu erreichen.

Als Beispiel für die Verwendung von Clouds im medizinischen Umfeld in Deutschland bieten die Firmen Telepaxx und Digithurst gemeinsam mit Health DataSpace (<https://healthdataspace.org>, 23.02.2019) eine Lösung zum Speichern von medizinischen Daten in der Cloud an. Diese SaaS-Komponente bietet Entwicklern ein API zum sicheren Speichern in der Cloud und Abrufen von Gesundheitsdaten aus der Cloud und löst so das Problem der Datenhaltung für Entwickler einer Gesundheits-App durch einen Cloud-Service.

Ein ähnliches Konzept verfolgt die amerikanische Firma Apple mit ihrem HealthKit (<https://developer.apple.com/healthkit/>, 23.02.2019). Das HealthKit bietet Entwicklern von iOS Apps für das iPhone die Möglichkeit, Gesundheitsdaten wie zum Beispiel die Herzfrequenz, die in Apps gemessen werden, über ein API in HealthKit zu speichern, ohne sich Gedanken über die Datensicherheit, Speicherung oder das Berechtigungskonzept machen zu müssen. Da die Daten in der Cloud (oder im Falle von Apple in der iCloud) gespeichert werden, stehen sie so allen berechtigten Nutzern und Geräten zur Verfügung.

2.1.7. Integrating the Healthcare Enterprise

Eine andere Herangehensweise, Daten und insbesondere Bilddaten krankenhausübergreifend zu speichern und zu kommunizieren, ist die Anwendung standardisierter Profile, wie sie durch die 1998 gegründete Integrating the Healthcare Enterprise (IHE) Initiative seit vielen Jahren entwickelt und weiter voran getrieben wurde.

Obwohl im Bereich der Kommunikation im Krankenhaus zahlreiche etablierte Standards wie zum Beispiel HL7, DICOM oder OASIS (Organization for the Advancement of Structured Information Standards) existieren, können nicht immer alle Workflows nur unter Zuhilfenahme dieser Standards komplett abgebildet werden. Es bestehen meist noch zu viele Freiheitsgrade, wodurch Geräte, Server beziehungsweise IT-Systeme trotz Implementierung dieser Standards nicht ohne Weiteres per Plug'n'Play integriert werden können.

IHE ist eine durch Anwender und Hersteller von Medizinprodukten gegründete Initiative, die sich zum Ziel gesetzt hat, den Datenaustausch zwischen IT-Systemen im Gesundheitswesen besser zu standardisieren beziehungsweise die bestehenden Standards besser zur Anwendung zu bringen. Hierbei steht vor allem die Interoperabilität zwischen den Systemen sowie der abzubildende Workflow und nicht so sehr die konkrete Implementierung der vernetzten Systeme im Vordergrund.

Der IHE-Prozess

Um die Interoperabilität zwischen den unterschiedlichen Systemen weiter voranzutreiben, identifiziert IHE Probleme und Workflows aus der Praxis und formuliert daraus Use Cases. Im weiteren Prozess (Abbildung 2.6) werden die dafür relevanten Standards identifiziert und technische Leitfäden, so genannte Technical Frameworks (TF), entwickelt. Der abzubildende Workflow wird dann in einem Profil festgeschrieben, welches Hersteller in ihrem Produkt umsetzen können, um den Workflow beziehungsweise das Profil als entsprechenden Akteur zu unterstützen. Die so entstandenen Profile können anschließend von den Herstellern auf den regelmäßig in Europa und Nord Amerika stattfindenden Connect-a-thons¹ getestet und verifiziert werden. Die Tiefe und der Umfang der Tests variieren je nach Profil zwischen einfachen Peer-to-Peer Tests bis hin zu aufwändigen Gruppentests mit mehr als vier Akteuren unterschiedlicher Hersteller sowie automatisierten Testumgebungen, die von der IHE zur Verfügung gestellt werden. Um sich überhaupt zur Teilnahme an einem solchen Testevent zu qualifizieren, müssen die Teilnehmer im Vorfeld diverse Pre-Tests gegen automatisierte Systeme bestehen, um dann vor Ort schon eine gewisse Grundkompatibilität zu gewährleisten. Grundsätzlich verstehen sich die etablierten Profile nicht als abgeschlossen, sondern werden kontinuierlich weiterentwickelt. Interoperabilitätsprobleme, die bei Connect-a-thons auftreten, fließen in den IHE-Prozess der Standardisierung zurück. Durch die erfolgreiche Implementierung und Teilnahme eines Herstellers an einem Connect-a-thon erhält dieser ein IHE Conformance Statement, welches den Test des Profils mit unterschiedlichen Herstellern als

¹"Connectathon - A five-day 'connectivity marathon' for testing the interoperability of health information systems."(<https://connectathon.ihe-europe.net>, 01.03.2019)

erfolgreich bescheinigt. Im Gegensatz zum DICOM Conformance Statement wird hier nicht die Implementierung eines bestimmten Teils des DICOM-Standards vom Hersteller selbst in Eigenverantwortung bescheinigt, sondern das Abbilden eines Workflows im Klinikumfeld, welches durch die erfolgreiche Teilnahme an einem Connect-a-thon und die unabhängige Überwachung durch die IHE bestätigt wird.

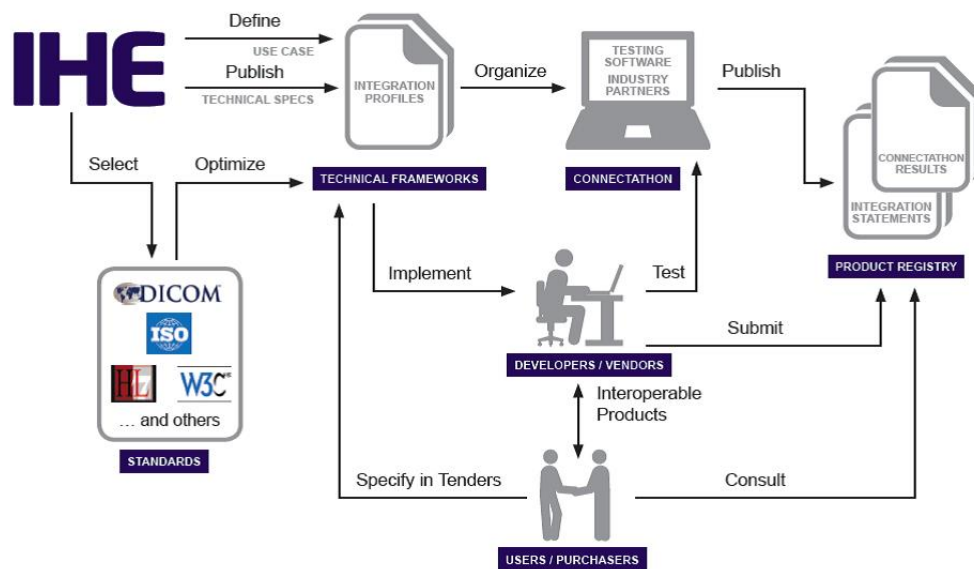


Abbildung 2.6.: Der IHE-Prozess. Von der Auswahl der zu verwendenden Standards bis zur Veröffentlichung des Conformance Statements durch die IHE. (Quelle: https://www.ihe.net/about_ihe/ihe_process, 01.03.2019).

IHE-Domäne: Ein Anwendungsbereich, für den ein IHE-Profil entwickelt wird. Zum Beispiel: Kardiologie (CARD), IT Infrastruktur (ITI) oder Radiologie (RAD).

Use Case: Ein spezifischer Anwendungsfall/Workflow, der durch ein IHE-Profil gelöst werden soll, zum Beispiel der Versand von radiologischen Befunden.

Integrationsprofil beschreibt die genaue Lösung des Problems mit dem Ziel, die Interoperabilität zwischen den Systemen unter Verwendung gängiger Standards herzustellen, zum Beispiel die radiologische Befundung mittels Reporting Workflow (RWF).

Aktor: Ein System innerhalb eines Profils, welchem verschiedene Rollen zugeordnet sind, zum Beispiel Reporting Workstation (RIS) oder Image Manager / Archive (PACS). Aktoren und Rollen können gruppiert werden, so dass ein System die Rolle von mehr als einem Aktor innerhalb eines Profils einnehmen kann, zum Beispiel die Gruppierung eines Image Managers (IM) mit einem Image Display (ID) als PACS mit integriertem DICOM-Viewer.

Transaktion: Die Kommunikation zwischen zwei Aktoren innerhalb eines Profils, die durch einen spezifischen Standard genau festgelegt ist, zum Beispiel der Versand eines radiologischen Befunds via HL7 in Version 2.5.1 als HL7 ORU^R01.

IHE und die Radiologie

Ursprünglich war die Kerndomäne von IHE die Radiologie, da auch die meisten Hersteller und Anwender in den Anfängen von IHE aus dem Bereich der Radiologie kamen. Eines der ersten umgesetzten Profile war Scheduled Workflow (SWF), welches den Behandlungsverlauf eines Patienten von der Aufnahme im Krankenhausinformationssystem (KIS) über die Terminanmeldung im Radiologieinformationssystem (RIS) und das Bildmanagement der Modalität bis hin zur Speicherung im Picture Archiving and Communication System (PACS) und Befundung an der Workstation des Radiologen beschreibt (Abbildung 2.7).

Im Falle von SWF identifiziert das Technical Framework genau die Rolle der einzelnen Aktoren sowie die zu verwendenden Standards, in diesem Falle ausschließlich HL7 und DICOM, die zur Übermittlung von Daten genutzt werden sollen. Das Profil stellt dadurch sicher, dass alle Nachrichten in der richtigen Reihenfolge durch die einzelnen Systeme verarbeitet werden und der Inhalt der Nachricht wohl definiert ist, indem die exakte Nachricht aus dem HL7-Standard mit einer definierten Version verwendet werden muss. Gleiches gilt auch für den Einsatz des DICOM-Standards zur Bildkommunikation und Prozesssteuerung der Modalitäten (medizinische bildgebende Geräte).

Die einzelnen Transaktionen zwischen den Aktoren sind in Abbildung 2.8 dargestellt. Hierbei sind die benötigten Aktoren (zum Beispiel Image Display oder Image Manager/Archive) inklusive ihrer Transaktionen (zum Beispiel Query Images [RAD-14], Retrieve Images [RAD-16]) aus dem Technical Framework genau festgelegt. Auch wenn hier

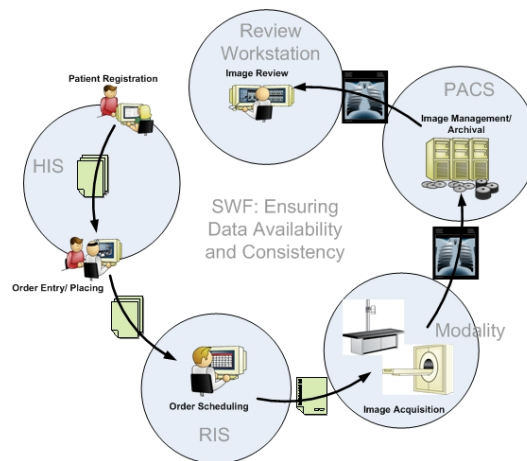


Abbildung 2.7.: Scheduled Workflow (SWF). Arbeitsablauf von der Patientenaufnahme bis zur Befundschreibung an der radiologischen Workstation. (Quelle: <https://wiki.ihe.net/index.php/File:Swf-v4.jpg>, 01.03.2019).

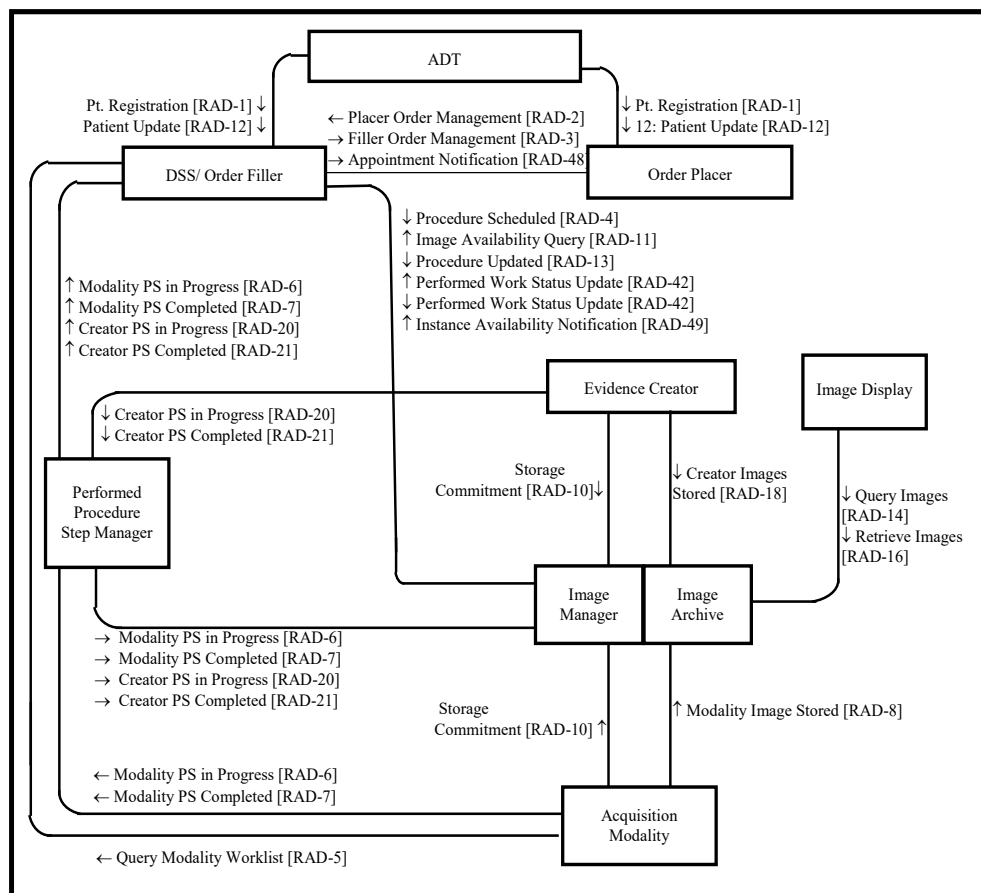


Abbildung 2.8.: Aktoren und Transaktionen (SWF). Übersicht über alle Aktoren und Transaktionen, die für das Profil 'Scheduled Workflow' benötigt werden. (Quelle: IHE RAD TF-1, Scheduled Workflow Diagram, 2019, S.46).

alle Aktoren einzeln mit ihren Transaktionen beschrieben sind, werden im späteren produktiven Einsatz im Krankenhaus meist mehrere Aktoren gruppiert. So beinhalten die meisten am Markt verfügbaren PAC-Systeme die Aktoren Image Manager (IM), Image Archive (IA) sowie Image Display (ID). Ein RIS beinhaltet den Aktor Order Filler (OF) zum Anlegen von Untersuchungen, kann aber in bestimmten Fällen auch ein Image Display zum Anzeigen von DICOM-Bildern bereitstellen. Aktoren können also nicht eins zu eins Herstellerprodukten zugeordnet werden, sondern bilden eher Funktionen eines Produkts ab.

2.1.8. IHE Cross-Enterprise Document Sharing

Um Gesundheitsdaten wie Befunde, Laborberichte, aber auch Bilddaten über die Grenzen eines Krankenhauses hinweg zugänglich zu machen, wurde das IHE-Profil Cross-Enterprise Document Sharing (XDS) beziehungsweise Cross-Enterprise Document Sharing for Imaging (XDS-I) entwickelt. Hierbei wurde das Konzept einer XDS Affinity Domain eingeführt.

Affinity Domain: Eine Affinity Domain beschreibt eine Gruppe oder einen Zusammenschluss von unterschiedlichen Systemen in einem Netzwerk, die eine gemeinsame Infrastruktur unterhalten und die gleichen Regeln und Policies der Kommunikation verwenden.

Innerhalb einer Affinity Domain existiert genau eine *Document Registry* (Abbildung 2.9). Jeder Anbieter beziehungsweise jede Quelle von Dokumenten kann in seiner Rolle als *Document Source* Dokumente in einem beliebigen *Document Repository* ablegen und die Daten in der zentralen *Document Registry* registrieren. Sobald die Daten in der *Document Registry* bekannt sind, können diese durch *Document Consumer* abgefragt werden. Erhält ein *Document Consumer* Zugriff auf das entsprechende *Document Repository*, kann er die Daten von dort abrufen.

In den Grenzen einer Affinity Domain existiert auch immer eine *Patient Identity Source*, ein so genannter Master Patient Index (MPI), der jedem Patienten aus einer lokalen

Klinik eine globale Patienten-ID zuordnet, so dass Patienten innerhalb einer Affinity Domain über die Grenzen eines lokalen Krankenhauses hinweg eindeutig identifiziert werden können.

Während für die Übertragung von Bild- und Befunddaten im Bereich SWF (Kapitel 2.1.7) noch ausschließlich HL7 und DICOM zum Einsatz kommt, findet die Kommunikation der Daten im Profil XDS mittels Transaktionen aus der IHE-Domäne IT Infrastruktur statt. Hier werden Dokumente mittels WeServices beziehungsweise HTTP und HTTPS transportiert, und der Inhalt als XML beziehungsweise SOAP kodiert. Dies ermöglicht die Einbeziehung aktueller Kommunikationsstandards und die Einbindung der Prozesse in die Krankenhausinfrastruktur unter Verwendung bekannter Sicherheitskonzepte wie einen Web Proxy oder eine Web Application Firewall (WAF).

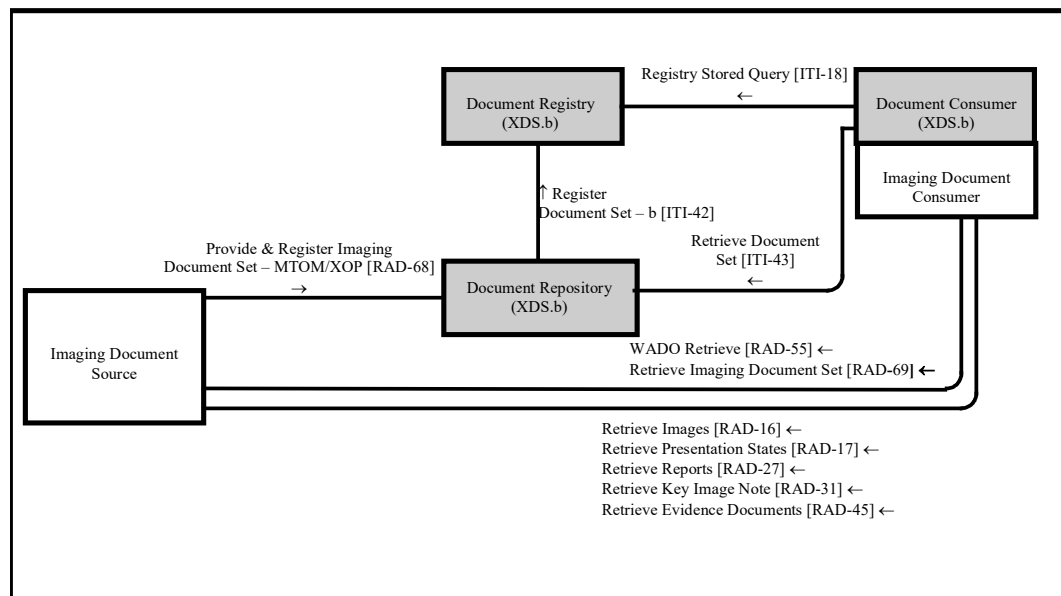


Abbildung 2.9.: Akteure und Transaktionen (XDS-I). Übersicht über alle Akteure und Transaktionen, die für den Bilddatenaustausch via XDS-I benötigt werden. (Quelle: IHE RAD TF-1, Cross-Enterprise Document Sharing for Imaging Diagram, 2019, S. 194).

Eine bildspezifische Erweiterung des XDS-Konzepts ist Cross-Enterprise Document Sharing for Imaging (XDS-I). Dokumente werden auch hier innerhalb einer Affinity Domain über entsprechende Repositories den Konsumenten bereitgestellt. Insbesondere DICOM-Bilder werden aber gesondert behandelt. Da es sich bei DICOM-Bildern um ein spezielles Bildformat handelt, welches einen erhöhten Platzbedarf erfordert und zu dessen

Betrachtung immer ein Spezialesystem nötig ist, sieht XDS-I vor, die Bilder grundsätzlich im Primärsystem zu belassen und nur Referenzen auf Bilddaten in einem Repository abzulegen. Möchte ein DICOM-fähiger *Imaging Document Consumer* die Bilder zur Anzeige bringen, dann ruft er zuerst die entsprechende Key Object Selection (KOS) aus dem Repository ab, welche die Quelle der registrierten Bilder enthält, um diese anschließend beim Primärsystem (meist ein auf die Ablage von Bilddaten spezialisiertes PACS) abzurufen. Durch dieses Konzept werden DICOM-Bilder in den Standard XDS-Workflow aufgenommen und unterliegen den gleichen Regeln und Beschränkungen wie alle anderen Objekte innerhalb der Affinity Domain, ohne dass die Datenmengen durch eine redundante Datenhaltung im Netzwerk überproportional anwachsen.

Value Sets für XDS

Werden IHE-Profile, insbesondere XDS/XDS-I, zum einrichtungsübergreifenden Austausch medizinischer Dokumente eingesetzt, so muss zwischen den einzelnen Einrichtungen, die innerhalb einer Affinity Domain kommunizieren wollen, ein einheitliches Verständnis über die Metadaten der ausgetauschten Dokumente existieren. Da eine Affinity Domain nicht genauer beschrieben ist und innerhalb eines Kontextes (wie zum Beispiel Trauma- oder Schlaganfall-Netzwerk), eines Bundeslandes, eines Landes oder sogar länderübergreifend existieren kann, werden die spezifischen Ausprägungen von Metadaten in einer Affinity Domain nicht durch das IHE-Profil festgelegt.

Um innerhalb einer Affinity Domain mit Dokumenten umgehen zu können, müssen zum einfachen Wiederfinden, zur Anzeige sowie Auswertung und Archivierung bestimmte Metadaten für Dokumente existieren, deren Werte und Ausprägungen durch domain-spezifische Codes beziehungsweise Value Sets codiert sind. Diese Codes umfassen Metadaten wie zum Beispiel Fachrichtung, Einrichtungsart und Dokumententyp zur einheitlichen Beschreibung der medizinischen Dokumente. Hierunter fallen vor allem:

Dokumentenklasse: `DocumentEntry.classCode` zur Beschreibung des Inhalts. Beispiel: Befunde, Bilddaten, Dokumentation, Medikation.

Dokumententyp: `DocumentEntry.typeCode` zur detaillierteren Beschreibung des Dokuments. Beispiel: Arztbrief, Pathologiebefund, Radiologiebefund, Computertomographie.

Einrichtungsart: `DocumentEntry.healthcareFacilityTypeCode` zur Identifizierung der erstellenden Institution. Beispiel: Krankenhaus, MVZ, Praxis.

Fachrichtung: `DocumentEntry.practiceSettingCode` zur Identifizierung der erstellenden Abteilung. Beispiel: Chirurgie, Radiologie, Orthopädie.

Dokumentenformat: `DocumentEntry.formatCode` zur leichteren Dokumentenverarbeitung. Beispiel: Word, PDF, DICOM.

Zusätzlich existieren noch eine Vielzahl von weiteren Metadaten wie beispielsweise der *AvailabilityStatusCode* oder *ConfidentialityCode*, die bei Bedarf weiteren Aufschluss über die Dokumente geben können. Einfache Metadaten wie Erzeuger oder Erstellungsdatum, die kein Mapping benötigen, werden nicht mit Value Sets, sondern direkt codiert.

Um diese Daten einfacher zwischen den Standorten austauschen zu können, werden nicht die textuellen Repräsentationen verwendet, sondern deren Codes. Somit ist jeder Wert individuell codiert und besitzt sowohl einen Code als auch ein `codingScheme` sowie einen anzeigbaren Namen (Listing 2.3).

Listing 2.3: IHE Value Sets - Beispiel für unterschiedliche Codes

```

1 <Codes>
2   <Code code="C_Bild" codingScheme="1.2.276.0.76.4.177.1.0.30.4" codingSchemeName=
3     "AD_ClassCode" display="Bilddaten"/>
4   <Code code="T_BildCT" codingScheme="1.2.276.0.76.4.15.1.0.30.5" codingSchemeName=
5     "AD_TypeCode" display="Computertomographie"/>
6   <Code code="EV_Rad" codingScheme="1.2.276.0.76.4.15.1.0.30.3" codingSchemeName=
7     "AD_EventCodeList" display="Radiologie"/>
8   <Code code="CC_N" codingScheme="2.16.840.1.113883.5.25" codingSchemeName=
9     "AD_ConfidentialityCode" display="normal"/>
10  ...
11 </Codes>

```

Durch diese Art der Codierung ist es einfach, ein gemeinsames Codesystem für eine Affinity Domain einzuführen, ohne jedoch die (sprachlichen) Individualitäten der einzelnen Teilnehmer zu ignorieren. So spielt es keine Rolle, ob der `ClassCode` 'C_Bild' als

'Bilddaten' oder 'Images' angezeigt wird, solange sich alle Teilnehmer auf den gemeinsamen Code 'C_Bild' geeinigt haben. Gleiches gilt auch für alle anderen verwendeten Codes wie zum Beispiel den TypeCode, EventCode oder ConfidentialityCode.

IHE-D Cookbook

Um die Vernetzung und einrichtungübergreifende Kommunikation (auch als intersektorale Kommunikation oder integrierte Versorgung bekannt) vor allem in Deutschland weiter voranzutreiben und zu standardisieren, wurde 2012 von IHE Deutschland eine Initiative gestartet, ein Cookbook für den deutschen Gesundheitsmarkt zu erstellen. Das Cookbook beschreibt anhand von den drei Use Cases beziehungsweise Anwendungsszenarien Mamma-Diagnostik, Kolorektales Karzinom und Akutversorgung Schwerverletzter (Polytrauma), wie eine Akten- und Vernetzungsstruktur in Deutschland mit der abschließlichen Verwendung von IHE-Profilen implementiert werden kann. Das Cookbook liegt aktuell in der Version 1.0 vor und verwendet hauptsächlich Profile aus dem Bereich XDS/XDS-I sowie die erweiterten Profile, die zum Betrieb einer XDS-Infrastruktur notwendig sind:

- XDS - Cross-Enterprise Document Sharing: Austausch von Dokumenten
- XDS-I - Cross-Enterprise Document Sharing for Imaging: Austausch von Bild-dokumenten
- PIX - Patient Identifier Cross-referencing: Einrichtungsübergreifende Verwaltung von Patienten-IDs mittels Master Patient Index (MPI)
- PDQ - Patient Demographics Query: Abfrage von Patientenstammdaten via HL7
- HPD - Healthcare Provider Directory: Verzeichnis von Netzwerkteilnehmern mittels LDAP
- CT - Consistent Time: Protokoll zur Zeitsynchronisation via NTP
- ATNA - Audit Trail and Node Authentication: Zur Absicherung der Kommunikation sowie zur Zugriffsprotokollierung

- XUA - Cross-Enterprise User Assertion: Einrichtungsübergreifender Login und Single-Sign-On via SAML
- BPPC - Basic Patient Privacy Consents: Rechte- und Zugriffsmanagement für den Zugriff auf Dokumente via XACML

Weiterhin wurden im Rahmen des Cookbooks auch die Value Sets für den Austausch von Dokumenten über eine XDS-basierte Vernetzung erarbeitet und festgelegt. Sie existieren unter dem Namen 'Value Sets für Aktenprojekte im deutschen Gesundheitswesen' seit 2018 in Version 2.0. Die aktualisierte Version ermöglicht die bessere Zuordnung von Dokumenten zu deren Autor durch die Festlegung von *DocumentEntry.authorRole* und *DocumentEntry.authorSpecialty*. Weiterhin wurden *DocumentEntry.confidentialityCodes* eingeführt, welche es erlauben, Dokumente in entsprechende Vertraulichkeitsstufen (von 'normal' bis 'gesperrt') einzuteilen.

Austausch zwischen Affinity Domains

Um den Austausch von Daten über die Grenzen von Affinity Domains hinweg zu realisieren, existiert das Konzept des Cross-Community Access (XCA). Hierbei wird zwischen der *Initiating Community* und der *Responding Community* durch Gateways vermittelt (Abbildung 2.10). Dabei kann ein *Document Consumer* transparent ein *Initiating Gateway* ansprechen, ohne Kenntnisse über die Infrastruktur und geltenden Regeln (in Form von Value Sets und Format Codes) der anderen Affinity Domain besitzen zu müssen. Die Kommunikation zwischen den Affinity Domains übernehmen jeweils die entsprechenden Gateways, welche die Grenzen der Affinity Domain nach außen öffnen und im umgekehrten Fall aufgrund eines hinterlegten Berechtigungs- beziehungsweise Sicherheitskonzepts nach außen absichern.

Auch wenn dadurch scheinbar eine einfache Vernetzung zwischen den unterschiedlichsten Akteuren gegeben ist, so ist diese jedoch nur auf einer abstrakten Ebene ad hoc möglich. Um eine reibungslose Kommunikation zu gewährleisten, müssen natürlich trotzdem alle Akteure physikalisch miteinander verbunden sein, und Netzwerk, Routing sowie Si-

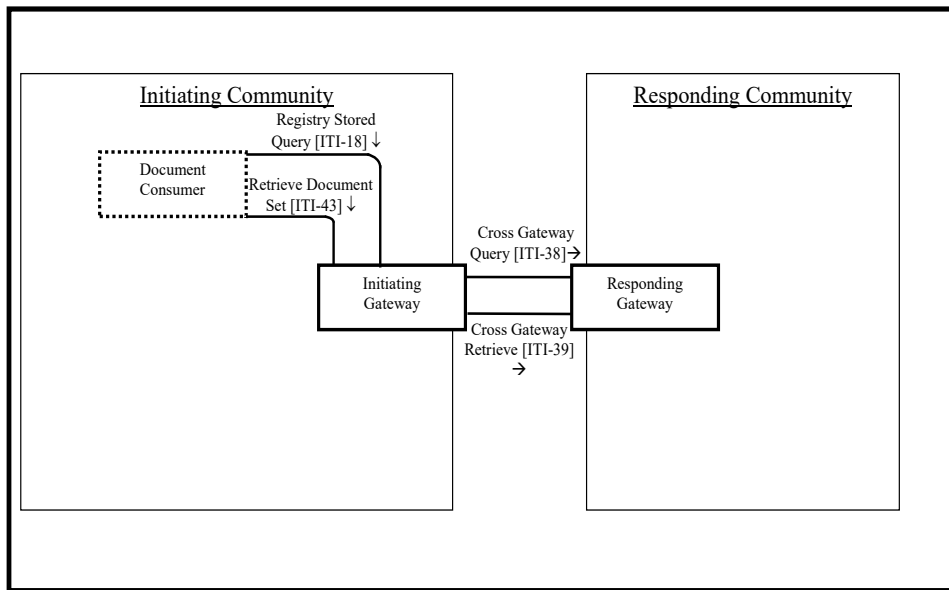


Abbildung 2.10.: Cross-Community Access (XCA). Austausch von Daten zwischen verschiedenen Affinity Domains. (Quelle: IHE ITI TF-1, XCA Actor Diagram, 2019, S. 184).

cherheit durch VPNs oder Zertifikate zwischen den teilnehmenden Partnern abgestimmt werden.

2.2. Modelle der Teleradiologie

Um Dokumente oder Bilddaten zwischen unterschiedlichen Standorten zu übertragen, gibt es zahlreiche Möglichkeiten. Hierbei spielt zum einen die Topologie des Netzwerks und zum anderen die Richtung des Datenflusses eine wichtige Rolle. Die unterschiedlichen Modelle weisen sowohl Vor- als auch Nachteile auf und müssen immer dem Einsatz entsprechend gewählt werden.

2.2.1. Netzwerktopologie

Informationsnetzwerke lassen sich grundsätzlich in unterschiedliche Kategorien einteilen (Traeger and Volk, 2001), wobei die Punkt-zu-Punkt-Verbindung (engl. Point-to-Point) und die sternförmige Verbindung die in der Teleradiologie am häufigsten vorkommenden sind und alle weiteren sich davon ableiten lassen (Abbildung 2.11).

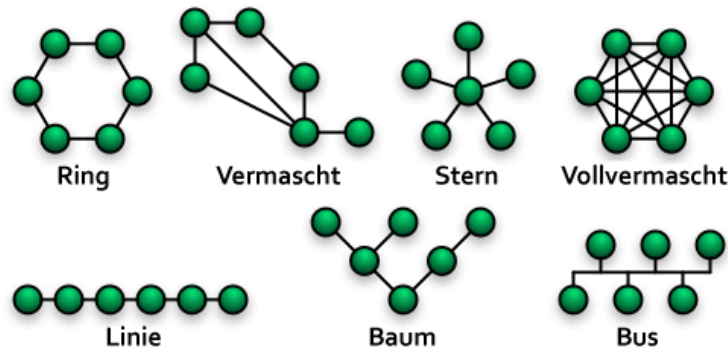


Abbildung 2.11.: Netzwerktopologien. Schematische Veranschaulichung der grundlegenden Arten von Netzwerktopologien. (Quelle: <https://commons.wikimedia.org/wiki/File:NetzwerkTopologien.png>, 01.03.2019).

Punkt-zu-Punkt-Verbindung

Die einfachste Art, zwei Kommunikationsteilnehmer miteinander zu vernetzen, ist die Punkt-zu-Punkt-Verbindung. Bei dieser Art der Verbindung findet die Datenübertragung direkt zwischen den beiden Teilnehmern statt. Hierbei kann sowohl die physikalische Topologie, eventuell durch ein Virtual Private Network (VPN), Transport Layer Security (TLS) oder eine Firewall geschützt, als auch der Datenfluss gemeint sein, obwohl die physikalische Verbindung an sich nicht auf direktem Weg erfolgt oder zur Ausfallsicherheit mehr als eine Route zwischen zwei Teilnehmern existiert. Im Bereich der Radiologie kommt hier oft das herstellerunabhängige DICOM-Protokoll zum Einsatz.

Ein großer Vorteil der direkten Punkt-zu-Punkt-Verbindung ist der einfache initiale Aufwand, um zwei Partner miteinander zu verbinden. Dies ist zumindest auf Ebene der DICOM-Kommunikation gegeben. Wesentlich aufwändiger ist die Absicherung der Verbindung mittels VPN oder anderer geeigneter Techniken. Hier kommt seit der Veröffentlichung des RFC 7525 'Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)' im Mai 2015 (Sheffer et al., 2015), welcher auch als Best Current Practice (BCP) 195 bekannt ist, immer mehr zertifikatsbasierte Kommunikation zum Einsatz. Hierfür existiert mit dem DICOM Supplement 204 - *TLS Security Profile* als auch mit dem Change Proposal des IHE-Profiles ATNA (CP-ITI-1145) ein Sicherheits-Profil (IHE Europe, 2018), welches zum ersten

Mal auf dem IHE Connect-a-thon 2019 in Rennes (Frankreich) zwischen verschiedenen Herstellern erfolgreich getestet wurde.

Der Nachteil eines auf Punkt-zu-Punkt-Verbindungen basierenden Netzes ist die schlechte Erweiterbarkeit. Kommt ein weiterer Teilnehmer hinzu, so muss dieser an die beiden existierenden Teilnehmer angeschlossen werden. Kommen weitere Partner hinzu, so ist dieser Schritt für jeden Partner zu wiederholen und stellt einen enormen administrativen Aufwand da. Hierbei wird das Netzwerk dann von einer einfachen Punkt-zu-Punkt-Topologie in ein vollvermaschtes bzw. teilvermaschtes Netzwerk (engl. Mesh) transformiert (Abbildung 2.12).

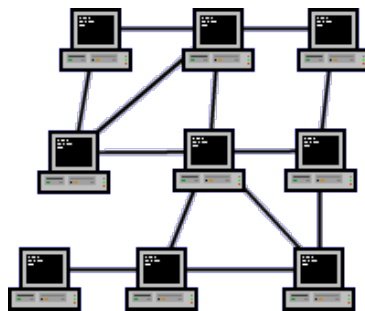


Abbildung 2.12.: Mesh Netzwerk. Übergang von Punkt-zu-Punkt-Netzwerken hin zu einem Mesh. (Quelle: https://commons.wikimedia.org/wiki/File:Netzwerktopologie_vermascht.png, 01.03.2019).

Dabei steigt die Anzahl der Verbindungen überproportional, da jeder neue Partner mit allen bereits bestehenden Partnern verbunden werden muss (nach Gleichung 2.1).

$$\binom{n}{2} = \sum_{i=1}^{n-1} i = \frac{(n-1) \cdot n}{2} = \frac{1}{2}(n^2 - n) \quad (2.1)$$

Hat ein Netzwerk fünf Partner, so existieren bereits zehn Verbindungen. Kommt ein weiterer Partner hinzu, so steigt die Anzahl der Verbindungen bereits auf 15.

Sternförmige Verbindung

Die verbreitetste Art der Verbindung bei vielen teilnehmenden Partnern ist die sternförmige Verbindung. Hier wird der Netzwerkverkehr durch einen (oder mehrere) zentralen

Server in der Mitte des Teleradiologienetzwerks gesteuert. Alle teilnehmenden Partner können über diesen Server miteinander kommunizieren und Daten austauschen. Hierbei findet dann keine direkte Kommunikation zwischen den Partnern statt, die Datenübertragung wird immer über den Server realisiert. Beispiele sind hier Protokolle wie E-Mail, HTTP oder auch DICOM.

Der zentrale Knoten empfängt die Daten der Teilnehmer, und die eigentlichen Empfänger der Daten können sich die für sie bestimmten Daten dann aktiv vom Server abholen (Abbildung 2.13). Auf diese Weise sind zum Beispiel DICOM E-Mail-Netzwerke realisiert. Eine andere Möglichkeit ist der Einsatz von Autorouting auf dem zentralen Server, so dass die Daten an die entsprechenden Partner weitergeleitet werden. Dies kann zum Beispiel bei einer regulären DICOM-Kommunikation eingesetzt werden. Ein entsprechender Server kann auch Partner mit unterschiedlicher Protokollunterstützung anbinden, indem er eine Konvertierung der Datenformate zum Beispiel von DICOM E-Mail zu DICOM oder HTTP durchführt, ohne dass die einzelnen Teilnehmer dafür Sorge tragen müssen.

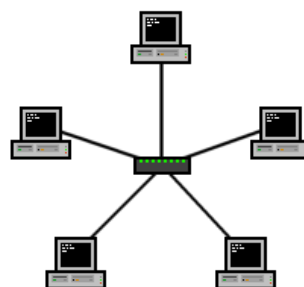


Abbildung 2.13.: Sternförmiges Netzwerk. Zentraler Server mit angeschlossenen Clients. (Quelle: https://commons.wikimedia.org/wiki/File:Netzwerktopologie_Stern.png, 01.03.2019).

Ein weiterer Vorteil von sternförmigen Netzwerken ist der einfache Anschluss neuer Partner an das Netzwerk. Neue Kommunikationspartner benötigen nur eine Kommunikationsverbindung zum Server, aber nicht zu allen anderen Partnern. Dadurch gestaltet sich die Administration eines solchen Netzwerkes zumindest auf der Transportebene einfacher, da Firewallfreischaltungen und Datenschutzüberlegungen nur einmal für den Server gemacht werden müssen und nicht mit jedem Partner einzeln. Außerdem kann der

Datenverkehr durch den Server einfacher protokolliert und Regeln einfacher durchgesetzt werden. Aber auch wenn das Netzwerk durch die sternförmige Architektur wesentlich vereinfacht wird, muss die Adressierung der einzelnen Partner immer noch auf jedem angeschlossenen Client separat konfiguriert werden.

Bei dieser Art der Topologie ist es zwingend notwendig, den zentralen Server ausreichend zu dimensionieren, da die Last auf dem Server proportional mit der Anzahl der Teilnehmer steigt. Weiterhin muss hier über ein Ausfallkonzept nachgedacht werden, da die zentrale Komponente einen Single Point of Failure (SPOF) darstellt. DICOM E-Mail-Netzwerke sind nach diesem Schema realisiert und leiten ihren Datenverkehr über mehrere dedizierte Mailserver, so dass immer eine alternative Route zwischen den Teilnehmern des Netzwerks besteht.

2.2.2. Datenfluss

Neben der Topologie des Netzwerks lässt sich ein Teleradiologiesystem auch nach dem Datenfluss einteilen. Dabei können die unten beschriebenen Modelle *Push* und *Pull* auch in Kombination auftreten.

Push-Modell

Das Push-Modell der Teleradiologie (Abbildung 2.14) ist die klassische Form der Verbindung von zwei Partnern, welche besonders bei Punkt-zu-Punkt-Verbindungen zum Einsatz kommt.

Hierbei besteht meist eine direkte Verbindung zwischen beiden Partnern. Daten werden aktiv vom Sender zum Empfänger geschickt. Dies hat den Vorteil, dass Daten direkt und ohne Wartezeit oder Verzögerung beim Empfänger ankommen. Nachteilig ist jedoch die durch das Modell vorausgesetzte ständige Erreichbarkeit des Empfängers. Da hier keine Zwischenspeicherung gegeben ist, muss bei einem Verbindungsabbruch zwischen Absender und Empfänger der Sender den Versand erneut anstoßen. Auch eine Änderung des Empfängers muss immer dem Sender bekannt gegeben werden und bedingt neben

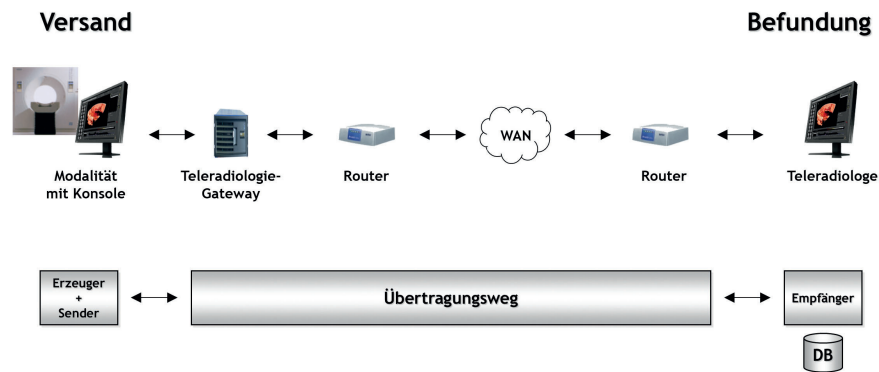


Abbildung 2.14.: Push-Modell der Teleradiologie. Die Bilder werden vom Sender bis zum Empfänger gesendet und dort gespeichert. (Quelle: E-Health-Ökonomie, 2017, S. 685).

der Rekonfiguration des Sender auch eine Änderungen in der Firewall, was meist mit einem hohen administrativen Aufwand einher geht.

Pull-Modell

Im Gegensatz zur Push-Variante besteht beim Pull-Modell meist keine direkte Verbindung zwischen Sender und Empfänger (Abbildung 2.15). Der Sender legt seine Daten an eine zentrale Stelle, und der Empfänger ruft diese von dort ab. Dadurch müssen sowohl Sender als auch Empfänger nur eine Verbindung zum Server aufbauen und nicht gegenseitig verbunden sein.

Dies hat den Vorteil, dass jeder Partner nur die Verbindungen zum Server konfigurieren muss. Da keine Verbindungen vom Server in Richtung der Teilnehmer gehen, ist hier meist auch keine besondere Firewallfreischaltung nötig. Dies vereinfacht die Administration erheblich, da auf dem Server nur 'Postfächer' konfiguriert werden müssen, die zum Austausch der Daten verwendet werden. Baut man das Konzept weiter aus, dann ist auch ein Mehrfachversand an unterschiedliche Teilnehmer ressourcenschonend möglich, indem die Daten nur einmal vom Sender zum Server übertragen werden, dann aber in mehreren Postfächern für die verschiedenen Empfänger bereitgestellt werden. Nach diesem Prinzip funktioniert zum Beispiel DICOM E-Mail, wobei es auch andere Netzwerke nach dem Pull-Konzept aber mit anderem Protokoll gibt. Hier wäre zum Beispiel das TKmed-Netzwerk (<https://tkmed.org>, 01.03.2019) mit dem Transport über

HTTP beziehungsweise HTTPS zu nennen (Staemmler et al., 2012; Staemmler et al., 2014; Reichardt et al., 2016).

Ein weiterer Vorteil ist die Zwischenspeicherung der Daten auf dem Server. So muss der Sender nur für eine stabile Verbindung zwischen sich und dem Server sorgen. Sollte beim Abrufen durch den Empfänger ein Fehler passieren, so kann dieser die Daten in einem weiteren Versuch selbstständig erneut abrufen. Auch kann der Empfänger seinen Standort wechseln, ohne dass der Sender etwas an seiner Konfiguration ändern muss. Die Daten werden weiterhin zur Zentrale übermittelt, und der Empfänger kann sie zeitsouverän abholen, sobald er dazu bereit ist beziehungsweise an das Netzwerk angeschlossen ist.

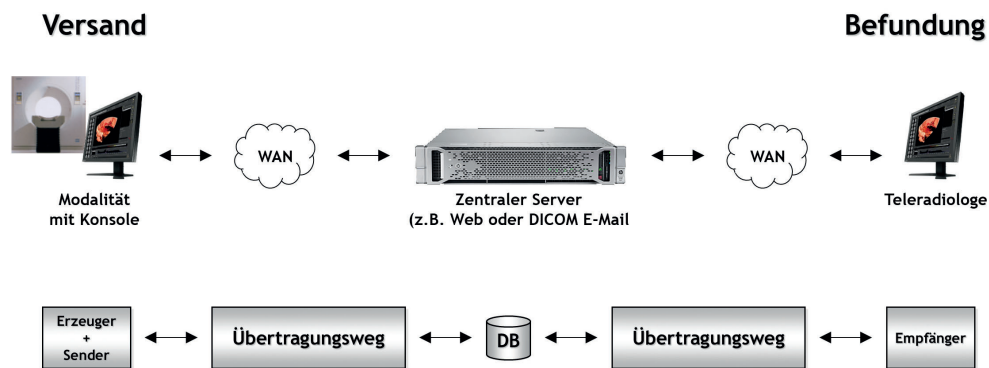


Abbildung 2.15.: Pull-Modell der Teleradiologie. Die Bilder werden auf einem Server zur Abholung bereitgestellt und zur Befundung vom Teleradiologen geholt. (Quelle: E-Health-Ökonomie, 2017, S. 685).

Ein Nachteil solcher Verbindungen ist allerdings die Zeitverzögerung zwischen Sender und Empfänger. Da die Daten bei diesem Verfahren nur durch aktives Abfragen (engl. polling) auf Seiten des Empfängers vom Server geholt werden können, ist die Pull-Methode immer langsamer als die Push-Methode. Die Verzögerung kann durch Verringerung des Abfrageintervalls nur in bestimmten Grenzen verkleinert werden. Weiterhin besteht die Möglichkeit, den Empfänger der Daten aktiv zum Pollen aufzufordern oder dem Empfänger zu erlauben, aktiv auf Daten zu warten, wie es zum Beispiel auch schon die Erweiterung des E-Mail-Protokolls IMAP um die Variante IDLE mit RFC 2177 vorsieht (Leiba, 1997).

2.3. Qualitätssicherung

Die Qualitätssicherung spielt in allen Bereichen der medizinischen Software eine große Rolle. Besonders wichtig wird sie jedoch im Bereich der Teleradiologie, wo nicht nur die korrekte Darstellung der Bilder sowie die richtige Kalibrierung der verwendeten Befundungsmonitore sichergestellt sein muss, sondern auch die Übertragungszeit der Bilder innerhalb eines festgelegten Rahmens liegen muss.

2.3.1. Qualitätssicherung in der Softwareentwicklung

Software, die im medizinischen Umfeld eingesetzt wird, fällt in Deutschland unter das Medizinproduktegesetz (MPG), welches die nationale Umsetzung der europäischen Richtlinien 93/42/EWG für Medizinprodukte (Medical Device Directive - MDD), 90/385/EWG für aktive implantierbare medizinische Geräte (Active Implantable Medical Device - AIMD) sowie 98/79/EG für In-vitro-Diagnostik (Invitro Diagnostik Directive - IVDD) darstellt. Die Active Implantable Medical Device (AIMD) und Medical Device Directive (MDD) wurden am 05. April 2017 in die Verordnung über Medizinprodukte (EU) 2017/745 überführt (Europäische Union, 2017), die auch als Medical Device Regulation (MDR) bekannt ist und drei Jahre nach Veröffentlichung, also am 26. Mai 2020, in Kraft getreten ist (Abbildung 2.16). Für Hersteller von Softwareprodukten im medizinischen Bereich ergeben sich dadurch zahlreiche Änderungen, aber die grundlegende Festlegung von Software als Medizinprodukt sowie die Einteilung der Software in Risikoklassen bleiben erhalten.

Risikoklassen von Medizinprodukten

Bei Software im Bereich von Medizinprodukten unterscheidet man grundsätzlich zwischen drei Fällen:

Embedded Software: Software kann Teil eines Medizinproduktes sein, wenn sie zum Beispiel als eingebettete Software in einem Medizingerät läuft (zum Beispiel Steuersoftware einer Spritzenpumpe).

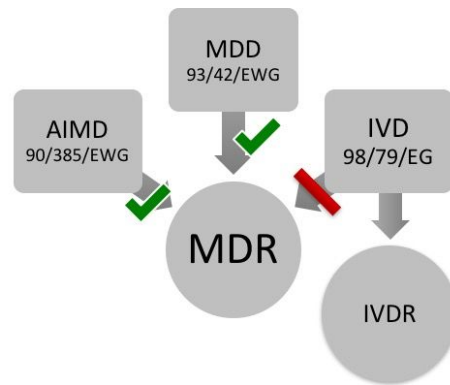


Abbildung 2.16.: Medical Device Regulation. Überführung der MDD und AIMD in die MDR unter Beibehaltung der IVD. (Quelle: <https://www.johner-institut.de/blog/regulatory-affairs/medical-device-regulation-mdr-medizinprodukteverordnung>, 30.05.2019).

Standalone Software: Software, die als eigenständiges Medizinprodukt läuft (zum Beispiel Radiologische Workstation).

Zubehör: Software, die ein Zubehör zu einem Medizinprodukt ist (zum Beispiel Kalibrierungssoftware für Monitore).

Ob eine Software ein Medizinprodukt ist, hängt von der Zweckbestimmung des Herstellers und nicht primär von der eigentlichen Funktion der Software ab. Eine Software ist genau dann ein Medizinprodukt, wenn die Zweckbestimmung der Definition des Begriffs 'Medizinprodukt' gemäß §3 MPG entspricht, oder einfacher nach Johner (Johner, 2019):

”Software ist ein Medizinprodukt, wenn der Hersteller sie zur Diagnose, Therapie oder Überwachung von Krankheiten und Verletzungen vorgesehen hat.”

Die Festlegung der Zweckbestimmung ist allerdings nicht immer einfach. So kann die Zweckbestimmung eines Krankenhausinformationssystems (KIS) darin bestehen, ein reines Dokumentations- und Abrechnungssystem darzustellen. Das KIS wäre in diesem Falle also kein Medizinprodukt. Andererseits kann der Zweck des KIS auch sein, den Anwender bei der Diagnose, Behandlung und Überwachung des Patienten zu unterstützen und zum Beispiel aufgrund von eingegebenen Werten Therapieempfehlungen

anzuzeigen, so wäre es als Medizinprodukt zu verstehen. Ähnlich schwierig verhält es sich mit anderen Systemen, die primär zur Dokumentation eingesetzt werden (RIS, Laborinformationssystem (LIS) etc.), aber Zusatzfunktionen bieten, die den Benutzer bei der Diagnose unterstützen. In diesem Falle wäre es auch denkbar, nur einzelne Module eines Softwareprodukts als Medizinprodukt zu spezifizieren. Ein PACS oder eine radiologische Workstation sind aufgrund ihres Zwecks immer als Medizinprodukt anzusehen.

Ist eine Software ein Medizinprodukt, dann muss sie je nach Risiko in eine der vier Risikoklassen (nach MDD 93/42/EWG) eingeteilt werden.

- I** Geringes Risiko: Medical Apps, Lesebrillen, Rollstühle, Mullbinden, Fieberthermometer u.a.
- IIa** Mittleres Risiko: Zahnfüllungen, Röntgenfilme, Hörgeräte, Ultraschallgeräte u.a.
- IIb** Hohes Risiko: Intraokularlinsen, Kondome, Röntgengeräte, Infusionspumpen u.a.
- III** Sehr hohes Risiko: Hüft- und Kniegelenkimplantate, Herzkatheter, Brustimplantate u.a.

Die neue MDR legt mit der *Regel 11* (MDR S. 144) die Risikoklassen für medizinische Software nun strikter fest als zuvor.

”Software, die dazu bestimmt ist, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:

- Den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder
- eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse IIb zugeordnet.

Software, die für die Kontrolle von physiologischen Prozessen bestimmt ist, gehört zur Klasse IIa, es sei denn, sie ist für die Kontrolle von vitalen physiologischen Parametern bestimmt, wobei die Art der Änderung dieser Parameter zu einer unmittelbaren Gefahr für den Patienten führen könnte; in diesem Fall wird sie der Klasse IIb zugeordnet.

Sämtliche andere Software wird der Klasse I zugeordnet.”

Da fast jede Software, die zur Diagnose, Überwachung, Vorhersage oder Behandlung dient, auch Informationen zur Entscheidungsfindung bereitstellt, ist diese nach Regel 11 nun als mindestens IIa oder höher einzustufen. Schon eine App zur Verwaltung von Blutzuckerwerten mit einer Warnfunktion bei Über- oder Unterschreiten eines Schwellwerts ist damit der Klasse IIa oder sogar IIb zuzuordnen. Somit sind fast alle Medical Apps, welche nach der MDD noch in Risikoklasse I fallen, nun mindestens IIa. Nach Inkrafttreten der MDR gibt es damit kaum noch Software, die in Klasse I fällt.

Qualitätsmanagement von Medizinprodukten

Medizinprodukte müssen in Europa eine Konformitätsbewertung nachweisen. Im Rahmen des Konformitätsbewertungsverfahrens stellen Hersteller selbst die Konformität ihres Produkts mit den grundlegenden Anforderungen und europäischen Richtlinien fest. Hierzu zählt auch die MDR. In vielen Fällen ist hier die vollständige Zertifizierung eines Qualitätsmanagementsystems QMS nach der Norm EN ISO 13485 Voraussetzung.

Die Norm EN ISO 13485 *‘Medizinprodukte: Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke’* befasst sich mit den Anforderungen, die Hersteller und Anbieter von Medizinprodukten bei der Entwicklung, Umsetzung und Aufrechterhaltung von QM-Systemen erfüllen müssen. Sie enthält Anforderungen an das QMS, Kundenanforderungen, aber auch die regulatorischen Anforderungen der Europäischen Union. So werden auch Forderungen zum Design, zu der Herstellung und der Inverkehrbringung von Medizinprodukten detailliert gestellt. In großen Teilen ist sie mit der Norm EN ISO 9001 identisch, setzt aber besonderen Wert auf die Produktsicherheit und Wirksamkeit und stellt spezifische Anforderungen für Medizinprodukte. Es soll die Erfüllung

der Anforderungen an das Produkt durch die Wirksamkeit der eingeführten Prozesse sichergestellt werden.

2.3.2. Monitor-Konstanzprüfung

Um die korrekte Darstellung von radiologischen Bilder auf einem Monitor in Befundqualität zu gewährleisten, ist es zwingend nötig, die Norm DIN 6868 *'Sicherung der Bildqualität in röntgendiagnostischen Betrieben'* und hier insbesondere den Teil 157 *'Abnahme- und Konstanzprüfung nach RöV an Bildwiedergabesystemen in ihrer Umgebung'* zu erfüllen.

Die DIN 6868-157 umfasst hier die gesamte Bilddarstellungskette (einschließlich Hardware, Software und Bildwiedergabegerät) und setzt eine Prüfung voraus. Eine initiale Abnahmeprüfung mit standardisierten Testbildern ist durch eine halbjährliche Konstanzprüfung in Bezug auf Homogenität der Leuchtdichte sowie Farbeindruck und Gleichmäßigkeit zu bestätigen. Die Gesamtbildqualität ist dabei arbeitstäglich zu überprüfen.

Als neues Konzept der Norm gegenüber ihrem Vorgänger DIN 6868-57 wurden Raumklassen eingeführt, die die Beleuchtungsstärke des Umgebungslichts und den Tätigkeitsbereich (Untersuchungsarten) in den Anforderungen berücksichtigen.

Eine weitere wichtige Änderung ist die Einführung einer Mindestpixelgröße statt der Forderung nach einer Mindestbildschirmgröße (Madsack et al., 2014). Diese beträgt nach der Norm 140 μm . Dadurch ist es mit entsprechender Kalibrierungssoftware und der Verwendung von Pixel-Binning, also dem Zusammenfassen von mehreren Pixeln zu einem, auch möglich, einen Tablet Computer wie zum Beispiel ein iPad zur radiologischen Befundung einzusetzen.

2.3.3. Teleradiologie nach Röntgenverordnung

In der Medizin bezeichnet man den Vorgang der Übertragung von radiologischem Bildmaterial über eine Telekommunikationseinrichtung an einen entfernten Ort als Teleradiologie. Da bei der Teleradiologie immer die Bilder an sich übertragen werden, darf

dies nicht mit der Übertragung des Bildschirminhalts über Programme wie Skype und TeamViewer oder anderen Bildschirmübertragungslösungen gleichgesetzt werden.

Eine besondere Form der Teleradiologie ist die *Teleradiologie nach RöV*. Diese wird in § 3 Abs. 4 Röntgenverordnung (RöV) genau beschrieben. Die Definition greift auch die Norm DIN 6868 Teil 159 *Abnahme- und Konstanzprüfung in der Teleradiologie* auf und definiert (DIN, 2017):

”Untersuchung eines Menschen mit RÖNTGENSTRAHLUNG unter der Verantwortung eines TELERADIOLOGEN, der sich nicht am Ort der technischen Durchführung befindet und der mithilfe elektronischer Datenübertragung und Telekommunikation, insbesondere zur rechtfertigenden Indikation und Befundung, unmittelbar mit den Personen am Ort der technischen Durchführung in Verbindung steht.”

Die Teleradiologie nach RöV erlaubt es dadurch auch kleinen Krankenhäusern, eine Radiologie in der Nacht und am Wochenende zu betreiben, ohne dass der Arzt am Ort der Aufnahme sein muss, sowie Befundung zum Beispiel in einem benachbarten Krankenhaus durchzuführen. Durch diese Möglichkeit etablieren sich auch in Deutschland Befundernetzwerke, die die nächtliche Befundung von Kliniken kommerziell übernehmen.

Die Teleradiologie nach RöV stellt allerdings hohe Anforderungen an die Qualität und Geschwindigkeit des Dienstes. So muss bei Genehmigung der Teleradiologiestrecke eine Abnahmeprüfung durchgeführt werden, welche sowohl die Übertragungszeit als auch die Bildwiedergabequalität sowie die Stabilität des Teleradiologiesystems für die jeweils beantragte Untersuchungsart überprüft. Grundsätzlich müssen alle Daten innerhalb von 15 Minuten übertragen werden und auf der Gegenseite zur Anzeige gebracht werden können. Die Abnahmeprüfung ist immer wieder durch eine wiederkehrende monatliche Konstanzprüfung sowie eine arbeitstägliche Funktionsprüfung zu bestätigen. Bei wesentlichen Änderungen an der Teleradiologiestrecke wie einen Wechsel des Telekommunikationsbetreibers oder auch Hardware- oder Softwaretausch ist die Abnahme erneut durchzuführen, wobei die Norm hier auch eine Teilabnahme zulässt.

2.4. Zugriff auf Daten für Ärzte und Patienten

Mit der Teleradiologie wird insbesondere eine Vernetzung von Ärzten ermöglicht, die eine zweite Meinung anfragen oder im Rahmen der Teleradiologie nach RÖV eine telerradiologische Befundung durchführen, ohne am Ort der Bildaufnahme zu sein. Im Rahmen des Patient Empowerment wird es aber auch immer wichtiger, Daten den Patienten zur Verfügung zu stellen oder diese von den Patienten zu erhalten und sie so am Behandlungsprozess teilhaben zu lassen.

2.4.1. Zuweiserportale

Wird ein Patient von einem niedergelassenen Arzt zur Behandlung in ein Krankenhaus überwiesen, so kann der Behandlungsprozess dadurch beschleunigt und verbessert werden, dass alle relevanten Daten zur Weiterbehandlung dem Krankenhaus im Vorfeld übermittelt werden. Das geschah früher auf rein analogem Weg, indem einem Patienten der Arztbrief zum eigenhändigen Überbringen von seinem Arzt zusammen mit dem 'Überweisungsschein' mitgegeben wurde. Zusätzlich konnten radiologische Aufnahmen mit Hilfe der 'Röntgentüte' übergeben werden. Dies war meist ein brauner Umschlag, in dem alle verfügbaren Bildaufnahmen des Patienten gesammelt waren.

Heute stehen im Rahmen der Digitalisierung modernere Verfahren zur Verfügung. So kann der niedergelassene Arzt mit dem Krankenhaus über ein Zuweiserportal kommunizieren. Hier können Daten des Patienten wie Vorbefunde, Laborwerte und ähnliches im Vorfeld übermittelt werden. Die Übertragung von DICOM-Daten stellt hierbei meist noch eine größere Hürde dar, da hierfür auf Seiten des Zuweisers ein spezieller DICOM-Viewer beziehungsweise DICOM-Uploader benötigt wird.

2.4.2. Patientenportale

Ähnlich wie die Zuweiser können auch Patienten den Behandlungsprozess entscheidend verbessern, indem sie im Vorfeld des Krankenhausbesuchs bereits alle ihnen vorliegenden Daten der Klinik zugänglich machen. Da die Patienten unter Umständen Dokumente von

mehr als einem Arzt zusammengetragen haben, ist ein Patientenportal eine geeignete Möglichkeit, die Daten gebündelt der Klinik im Vorfeld zukommen zu lassen.

Ein Beispiel für eine solche Lösung ist das Patientenportal des International Office des Universitätsklinikums Heidelberg (<https://www.heidelberg-university-hospital.com/treatment-inquiry-appointment>, 14.01.2019). Hier können Patienten aus dem Ausland eine Terminanfrage stellen und außerdem wichtige Befunde in das Portal stellen. Eingänge in das Portal, welche sowohl Fragebogenelemente und hochgeladene Dokumente umfassen, werden durch das Team des International Office auf Vollständigkeit geprüft und bei Bedarf übersetzt. So entsteht eine vollständige elektronische Akte, die Arztbriefe, Laborbefunde, aber auch radiologische Bilder im DICOM-Format umfasst.

Aufgrund der gesammelten Daten kann der Fall im Vorfeld bearbeitet und gegebenenfalls eine Behandlungsempfehlung ausgesprochen werden. Bei Rückfragen zu Dokumenten ist der Patient jederzeit erreichbar, da ein funktionierender Rückkanal über das Portal durch die einfache Registrierung des Patienten aufgebaut wurde. Der Patient oder ein von ihm Beauftragter gibt bei der Registrierung seine Kontaktdaten mit Adresse und Telefonnummer sowie zwingend eine E-Mail-Adresse an. Über die intern generierte Anfragenummer und die hinterlegte E-Mail-Adresse können Daten und Patient leicht zugeordnet werden. Bei ausländischen Patienten wird die Registrierung außerdem meist nicht persönlich, sondern über eine Botschaft oder Vertretung vorgenommen, welche bereits bekannt ist. Da dieses Portal ausschließlich in Richtung der Klinik genutzt wird und über diesen Weg keine Daten an den Patienten zurückgeleitet werden, ist eine einfache Registrierung in diesem Falle ausreichend. Wird der Patient dann zur Behandlung aufgenommen, können alle Daten per Knopfdruck problemlos in die Primärsysteme des Krankenhauses übernommen und zur weiteren Behandlung verwendet werden. Das Portal ersetzt also das Zusenden von behandlungsrelevanten Papierdaten und DICOM-CDs per Post.

Patientenportale lassen sich grundsätzlich auch für eine Zwei-Wege-Kommunikation einsetzen. In diesem Fall kann ein Patient vor Besuch einer Klinik selbst seine Daten

einstellen, und die Klinik kann während oder nach dem Klinikaufenthalt Bilder, Laborbefunde und Arztbriefe an den Patienten übermitteln beziehungsweise ihm diese über das Portal zur Verfügung stellen. Wird ein Portal auf diese Weise genutzt, so ist es wichtig, den Patienten eindeutig zu identifizieren, um sicherzustellen, dass Daten immer nur für den richtigen Patienten freigegeben werden. Hierzu kann bei der Registrierung durch den Patienten ein Double Opt-in-Verfahren mit Bestätigungs-E-Mail verwendet werden. In diesem Fall ist sichergestellt, dass die E-Mail-Adresse, die bei der Registrierung verwendet wurde, auch wirklich im Besitz des Patienten ist und so nicht fälschlicherweise Daten an jemand anderen gesendet werden. Dies stellt aber immer noch nicht sicher, dass es sich dabei wirklich um die richtige Person handelt, und so müssen weitere Verfahren zur Identitätsprüfung zum Einsatz kommen. Bis Patienten sich über eine Gesundheitskarte oder den elektronischen Personalausweis identifizieren können, ist die einfachste Art des Identitätsnachweises immer noch die persönliche Registrierung während des Krankenhausaufenthaltes.

2.4.3. Patientenakten

Für die einrichtungsübergreifende Kommunikation von Patientendaten mittels Aktensystemen gibt es in Deutschland drei wesentliche Architekturkonzepte, die sich in ihrer Organisationsart und Verwaltung grundsätzlich unterscheiden.

Elektronische Fallakte (EFA)

Der Elektronischen Fallakte (engl. Electronic Case Record, ECR) liegt das Konzept eines Behandlungsfalls zugrunde. Sie dient der zweckgebundenen Sammlung beziehungsweise Zusammenführung von Behandlungsdaten über einen längeren Zeitraum und wird einrichtungsübergreifend geführt. In ihr werden alle Daten zu einem aktuellen Behandlungsfall gesammelt und zwischen den verschiedenen berechtigten Benutzern kommuniziert. Die EFA ist arztgeführt, und der Patient gibt meist lediglich die Einwilligung zur Anlage einer solchen Akte über seinen Behandlungsfall, bekommt aber im Normalfall keinen Einblick oder Zugriff auf die gespeicherten Daten. Dies ist am ehesten mit

der papierbasierten Akte zu vergleichen, in der im Laufe eines Krankenhausaufenthalts alle anfallenden Untersuchungen dokumentiert werden. Ist der Behandlungsfall abgeschlossen, so wird auch die Fallakte geschlossen. Es besteht zwar noch länger Zugriff auf die Akte, aber weitere Daten werden nicht mehr hinzugefügt. Entsteht ein zweiter Behandlungsfall für denselben Patienten, so wird hierfür eine weitere Akte angelegt.

Elektronische Patientenakte (EPA) der Leistungserbringer

Im Gegensatz zur EFA werden in der elektronischen einrichtungsübergreifenden Patientenakte (engl. Electronic Health/Patient Record, EHR) alle Gesundheitsinformationen zu einem Patienten in zeitlich linearer (longitudinal) Form erfasst und eingestellt. Sie bildet damit ein holistisches Bild des Patienten, welches einrichtungsübergreifend allen berechtigten Benutzern verfügbar ist. Auch bei diesem Modell handelt es sich um eine arztgeführte Akte, welche nach einmaliger Zustimmung des Patienten erstellt wird. In dieser Art der Akte ist es unter Umständen möglich, dass für den Patienten einzelne Dokumente oder Informationen wie zum Beispiel Laborbefunde oder Entlassberichte freigegeben werden. Welche Dokumente das sind, wird durch den Arzt beziehungsweise Betreiber der Akte entschieden. Die Elektronische Patientenakte kann sowohl einrichtungsübergreifend als auch rein institutional innerhalb eines Krankenhauses oder Krankenhauskonzerns geführt werden.

Persönliche Elektronische Patientenakte (PEPA)

Die PEPA (engl. Personal Electronic Health/Patient Record, PEHR), oft auch Persönliche einrichtungsübergreifende Patientenakte genannt, unterscheidet sich von den beiden anderen Aktenarten dahingehend, dass sie vollständig vom Patienten geführt wird. In der PEPA werden, wie auch in der EPA, alle Gesundheitsdaten zu einem Patienten zusammengetragen. Die Zugriffsberechtigungen werden bei dieser Art der Akte aber nicht durch einen Arzt, sondern durch den Patienten selbst vergeben. Hierbei kann der Eigentümer der Akte, also der Patient, feingranular entscheiden, wer auf welche Dokumente Zugriff erhält. Die Freigabe kann dabei für einzelne Dokumente oder Dokumententypen

an Personen, Abteilungen oder Einrichtungen vergeben werden. Die Patienten haben Zugriff auf alle Daten in ihrer persönlichen Akte und können dieser auch selbst Dokumente hinzufügen. Dadurch ist dies die umfassendste Form der elektronischen Patientenakte, welche dem Patienten die volle Hoheit und Kontrolle über seine Gesundheitsdaten gibt. Eine Akte unter vollständiger Hoheit des Patienten birgt aber auch Gefahren für den Arzt, da dieser sich nicht sicher sein kann, ob der Patient ihm alle behandlungsrelevanten Daten zur Verfügung gestellt hat.

Die Akte nach § 291a

Nach Paragraf 291a SGB V (Fünftes Buch Sozialgesetzbuch) heißt es:

”Die Krankenkassen sind verpflichtet, ihren Versicherten spätestens ab dem 1. Januar 2021 eine von der Gesellschaft für Telematik nach § 291b Absatz 1a Satz 1 zugelassene elektronische Patientenakte zur Verfügung zu stellen.”

Eine solche Akte nach § 291a kann nicht eindeutig einem der drei oben skizzierten Aktenkonzepte zugeordnet werden:

- EFA - Einrichtungsübergreifende medizinische Fallakte (arztgeführt)
- EPA - Einrichtungsübergreifende elektronische Patientenakte (arztgeführt)
- PEPA - Persönliche einrichtungsübergreifende elektronische Patientenakte (patientengeführt)

Je nach Sichtweise auf die 'Akte 291a' steht diese in der Hoheit des Bürgers beziehungsweise Patienten und kommt damit dem Konzept der PEPA nahe. Andererseits könnte die Akte prinzipiell auch als EPA unter der Hoheit der Leistungserbringer ausgestaltet werden und dem Patienten lediglich erweiterte Zugriffsmöglichkeiten auf seine Daten bieten (Hellmuth et al., 2014).

Nach dem aktuellen Entwurf des Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG - Patientendaten-Schutz-Gesetz) ist eine 'Akte 291a' unter der Verwaltung der Leistungserbringer jedoch ausgeschlossen, der Patient

beziehungsweise der Versicherte hat die alleinige Verfügungsgewalt über seine Daten (Bundesministerium für Gesundheit, 2020). Die §§ 336 und 337 regeln die Zugriffsrechte der Versicherten sowie die Rechte der Versicherten auf Verarbeitung ihrer Daten und stärken somit die Rechte der Patienten. § 352 geht auf die Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer und andere zugriffsberechtigte Personen genauer ein und nennt Personen- und Berufsgruppen, die mit Einwilligung durch den Versicherten Zugriff auf dessen Daten erhalten können.

Da der Patient nicht alle Informationen für eine umfassende Akte besitzt oder bereitstellen möchte, werden die Leistungserbringer neben der Akte unter Hoheit des Patienten auch eine eigene Akte zur vollständigen Kommunikation der behandlungsrelevanten Daten führen müssen. Diese wird über geeignete Schnittstellen an die 'Akte 291a' angebunden werden, Leistungserbringer können Daten, für die sie durch den Versicherten berechtigt wurden, in ihre eigenen Systeme überführen.

So gesehen kann es nicht die eine Akte geben, die alle Bedürfnisse erfüllt.

2.4.4. Vendor Neutral Archive

Bei der Vielzahl an unterschiedlichen Datenhaltungs-, Archivierungs-, Aktensystemen und Bilddatenspeichern, die in einem Krankenhaus zum Einsatz kommen, bietet das Vendor Neutral Archive (VNA) eine Möglichkeit zur Archivierung aller im Krankenhaus anfallenden Daten (Clunie et al., 2016). Das VNA stellt hierbei eine architekturunabhängige Schnittstelle zwischen den unterschiedlichen Subsystemen und Archivsystemen beziehungsweise PACS-Archiven zur Verfügung (Sanjeev and Agarwal, 2012). Die Abgrenzung zu einem PACS ist hierbei fließend, da die eigentliche Archivierung der Bilddaten auch bei Einsatz eines VNA meist durch ein PACS übernommen wird. Das VNA ist viel mehr als ein Enterprise Archiv zu sehen, welches eine Vielzahl an unterschiedlichen Datentypen speichern kann. Daher ist ein VNA eher ein Konzept als eine konkrete Implementierung und kann auch als XDS Document Repository oder Imaging Document Repository verstanden werden.

In Verbindung mit einer Patientenakte wie zum Beispiel einer EFA können wesentliche Mehrwerte durch den Einsatz eines digitalen Multimediarhives für den Patienten entstehen. Nach Abschluss eines Behandlungsfalls können alle Daten physikalisch am Ort der Entstehung, also dem Krankenhaus oder der Arztpraxis verbleiben und werden in der übergreifenden, digitalen Fallakte oder EPA lediglich referenziert (Schmücker, 2013). Die Fallakte beziehungsweise Patientenakte bildet somit einen Index über alle relevanten Dokumente und Bilder und kann bei Bedarf diese aus den jeweiligen Primärsystemen holen. Auch hier sind die Übergänge zu einem XDS Document Repository fließend.

3. Material und Methoden / Konzeption und Realisierung

Konzeption und Realisierung von Technologien und Werkzeugen für die qualitätsgesicherte intersektorale Vernetzung

Zu Beginn dieses Kapitels werden die im Rahmen dieser Arbeit durch den Autor neu entwickelten und implementierten Techniken zum qualitätsgesicherten Austausch von Bilddaten zwischen den unterschiedlichen Akteuren in Teleradiologienetzwerken ausführlich beschrieben. Anschließend wird auf die Neuerungen in der intersektoralen Vernetzung eingegangen und die Möglichkeit der Patienten zur Partizipation am Behandlungsprozess durch den Einsatz von workfloworientierten Patientenportalen dargestellt. Zum Schluss werden die entwickelten Erweiterungen zur Qualitätssicherung und Performancemessung von Teleradiologiesystemen besprochen.

Die hier vorgeschlagenen und umgesetzten Lösungen bilden die Basis zur Unterstützung von Prozessen der intersektoralen Vernetzung mit medizinischen Bildern und bieten eine Weiterentwicklung und Standardisierung von Teleradiologiekomponenten unter Berücksichtigung der Qualitätssicherung.

3.1. DICOM E-Mail und Qualitätssicherung

Durch die weite Verbreitung der E-Mail-basierten Teleradiologie in Deutschland und dem damit verbundenen administrativen Aufwand zur Inbetriebnahme sowie zur konstanten Überwachung des Netzwerks müssen Methoden entwickelt werden, die diese Aufgaben halb- oder vollautomatisch unterstützen.

3.1.1. DICOM E-Mail Service Parts

Die Kommunikation mittels DICOM E-Mail stellt eine einfache Möglichkeit zum Ad-hoc-Austausch von Daten via Teleradiologie dar, allerdings ist die Administration eines DICOM E-Mail Netzwerks relativ aufwändig, da durch den Einsatz dedizierter E-Mail Server die Kommunikation zwar sternförmig verläuft, angeschlossene Partner die Schlüssel- und Adressverwaltung aber dennoch Peer-to-Peer vornehmen müssen.

Aus diesem Grund wurde das Whitepaper 'Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat' in Zusammenarbeit mit der Arbeitsgruppe @GIT durch den Autor in zwei Schritten um administrative Funktionen wie die Schlüssel- und Adressverwaltung sowie eine Möglichkeit zur Konstanzprüfung eines DICOM E-Mail Netzwerks erweitert. Diese Neuerungen werden durch die Einführung sogenannter DICOM E-Mail Service Parts in das Whitepaper aufgenommen.

Unterstützte Workflows

Um den administrativen Aufwand zu verringern und die Kommunikation in einem DICOM E-Mail Netzwerk einfacher zu überwachen, werden folgende Workflows unterstützt:

- Sicherer Austausch und Management von PGP/GPG-Schlüsseldaten
- Austausch von Adressdaten beziehungsweise E-Mail Adressen von DICOM E-Mail-Partnern
- Austausch von Kontaktdaten (zum Beispiel Postadresse, Telefonnummer etc.)

- Übermittlung von Daten, die zur Konstanz und Funktionsprüfung nach DIN 6868-159 nötig sind
- Erweiterung der Statusnachrichten (MDN) für einfache und spezifische Rückmeldungen
- Abfrage von Verbindungsdaten mittels DICOM E-Mail Query

Anforderungen an Service Part E-Mails

Die Erfahrungen mit den verschiedenen Umsetzungen der Standardempfehlung des Whitepapers durch unterschiedliche Hersteller hat in der Vergangenheit gezeigt, dass die Einstiegshürde aufgrund der Minimalempfehlung zwar sehr niedrig ist, durch die vielen sinnvollen, aber optionalen Funktionen in der Regel nur der minimale Standard implementiert wurde. Dies hatte zur Folge, dass in einem Netzwerk meist nur die Minimalfunktion des Whitepapers genutzt werden konnte. Aus diesen Erfahrungen heraus wurden für alle neu entwickelten Service Part E-Mails und Erweiterungen folgende Grundannahmen getroffen und nur wenige Funktionen als optional deklariert:

- Alle E-Mails müssen zwingend verschlüsselt und signiert versendet werden (nach RFC 3135 u. 1847).
- Alle Teilnehmer im Netzwerk sind angehalten, eine Whitelist von PGP/GPG-Schlüsseln zu führen, um ungewünschte Service Part E-Mails direkt ohne Bearbeitung ablehnen zu können.
- Alle Inhalte werden grundsätzlich als XML-Struktur mit dem Mime-Type text/xml übermittelt.
- Das Encoding aller Inhalte wird auf UTF-8 festgelegt.
- Alle Service Part E-Mails sind mit dem Mime-Type multipart/mixed zu versenden.
- Eine Service Part E-Mail kann 1-N Service Parts beinhalten.

- Alle Zeitstempel werden nach ISO 8691 im Format YYYY-MM-DDThh:mm:ssZ als UTC Zeit codiert.
- Alle IDs sind als UUIDs nach RFC 4122 zu codieren.
- Service Part E-Mails müssen die aktuell unterstützte Version im Message Header enthalten (aktuell 1.7.0).
- Empfangsbestätigungen auf Service Part E-Mails müssen selbst auch in der Form einer Service Part E-Mail versendet werden.

Der Standardaufbau eines Service Part ist in Listing 3.1 dargestellt. Jeder Service Part wird durch ein 'name', 'action' und 'timestamp' Attribut genau definiert. Hierbei werden per Definition alle Elemente strikt in CamelCase-Schreibweise und alle Attribute in vollständiger Kleinschreibung codiert. Alle verfügbaren Service Parts sind in der Tabelle 3.1 aufgeführt.

Listing 3.1: XML-Struktur eines Service Part

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="" action="" timestamp="YYYY-MM-DDThh:mm:ssZ">
3 ...
4 </ServicePart>
```

Jede Service Part E-Mail muss in ihrem unverschlüsselten Header mit dem X-Tag X-Telemedicine-Servicepart und der entsprechenden Aktion markiert werden. Sollte eine E-Mail mehr als einen Service Part enthalten, so wird diese mit dem X-Tag X-Telemedicine-Servicepart:MULTIPART versehen. Dies erlaubt eine performante Filterung von Service Parts, ohne die E-Mail entschlüsseln zu müssen. Diese Filterung ist notwendig, sollte nur ein Teil des Standards unterstützt oder nur eine bestimmte Art von Service Part verarbeitet werden. Der Anhang A.1 zeigt eine Service Part E-Mail für ein Update eines PGP/GPG-Schlüssels mittels der Aktion KEYUPDATE.

Tabelle 3.1.: Definierte Service Parts mit Name und Aktion. [Opt.; Optionality: (R)equired, (O)ptional] (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 40)

Service Part Name	Aktion	Opt.	Beschreibung
ADDRESSUPDATE	SET	R	Adressdatenverwaltung für DICOM E-Mail-Partner
	GET	R	
	REMOVE	R	
	CLEAN	R	
KEYUPDATE	SET	R	Schlüsselverwaltung für DICOM E-Mail-Partner
	GET	R	
	REMOVE	R	
	CLEAN	R	
CONTACTUPDATE	SET	R	Kontaktdatenverwaltung für Kommunikationspartner
	GET	R	
	REMOVE	R	
	CLEAN	R	
CONNECTIONUPDATE	GET	O	Kombination aus Adress-, Schlüssel- und Kontaktabfrage
DISPOSITIONNOTIFICATION	-	R	Bestätigungsnachrichten
TESTTRANSFER PROTOCOL	-	R	Konstanzprüfung
	-	R	
QUERY	FIND	O	Adressbuchabfrage
	RESULT	O	

3.1.2. Verwaltung von DICOM E-Mail Adresdaten

Durch die Aktion ADDRESSUPDATE ist es möglich, die Adresdaten eines Kommunikationspartners, insbesondere die zu verwendende E-Mail Adresse und den Mailserver, abzufragen, zu erstellen, zu ändern oder zu löschen. Hierbei wird wie in Listing 3.2 dargestellt, ein kompletter Adresdatensatz bei einem Partner angelegt.

Listing 3.2: Service Part zum Erstellen/Ändern von Adresdaten

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="ADDRESSUPDATE" action="SET" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Connection>
4     <ID />
5     <DisplayConnectionName />
6     <Mailserver />
7     <Port />
8     <EmailAddress />
9     <GPGKeyID />
10  </Connection>
11 </ServicePart>

```

Ein Adressdatensatz umfasst eine eindeutige Connection-ID, die als Referenz für alle weiteren Änderungen an diesem Datensatz verwendet wird. Connection-IDs sind UUIDs nach RFC 4122 und beschreiben einen Datensatz damit eindeutig im gesamten Netzwerk. Weitere verpflichtende Felder sind der DisplayConnectionName zur Anzeige beim Benutzer sowie die für die Übertragung von Daten zwingend notwendige E-Mail Adresse als auch die ID des zu verwendenden PGP/GPG-Schlüssels. Optional kann noch der zu verwendende Mailserver sowie dessen Port angegeben werden.

Um einen neuen Adressdatensatz bei einem Partner anzulegen, wird die Aktion SET verwendet. Später kann dann für ein Update der so angelegten Adresse die gleiche Nachricht genutzt werden, wobei hier die Connection-ID zur Identifizierung der Verbindung verwendet wird.

Analog zum Anlegen von Adressdaten können diese auch mittels einer Service Part E-Mail gelöscht werden. Hierbei gibt es die Möglichkeit, mit der Aktion REMOVE genau einen Datensatz unter Angabe einer bestimmten Connection-ID zu löschen (Listing 3.3) oder mit der Aktion CLEAN alle Daten außer einer mittels KeepConnectionID explizit angegebenen Liste von Adressen zu entfernen (Listing 3.4).

Listing 3.3: Service Part zum Löschen von Adressdaten

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="ADDRESSUPDATE" action="REMOVE" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Connection>
4     <ID />
5   </Connection>
6 </ServicePart>
```

Listing 3.4: Service Part zum Bereinigen des Adressbuchs

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="ADDRESSUPDATE" action="CLEAN" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Connection>
4     <KeepConnectionID />
5   </Connection>
6 </ServicePart>
```

Neben dem Anlegen, Ändern und Löschen von Adressdaten ist es weiterhin möglich, unter Verwendung der GET-Nachricht die gespeicherten Adressdaten für eine spezifische Connection-ID von der Gegenseite anzufordern (Listing 3.5).

Listing 3.5: Service Part zum Abfragen von Adresdaten

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="ADDRESSUPDATE" action="GET" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Connection>
4     <ID />
5   </Connection>
6 </ServicePart>

```

3.1.3. Verwaltung von DICOM E-Mail Schlüsseldaten

Die im vorherigen Abschnitt beschriebene Adresdatenverwaltung dient ausschließlich zum Anlegen und Ändern von Kommunikationsdaten wie E-Mail Adresse, Mailserver und ähnlichem. Die Verwaltung der PGP/GPG-Schlüsseldaten wird durch einen eigenen Service Part gesteuert und ist von den Kommunikationsdaten getrennt. Um Schlüsseldaten in einem DICOM E-Mail Netzwerk auszutauschen, genügt ein Service Part KEYUPDATE SET, der den aktuell gültigen öffentlichen Schlüssel enthält (Listing 3.6).

Listing 3.6: Service Part zum Anlegen eines PGP/GPG-Schlüssels

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="KEYUPDATE" action="SET" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <PublicKeyASCIIData />
4 </ServicePart>

```

Da der verwendete PGP/GPG-Schlüssel bereits die entsprechenden Meta-Daten in sich codiert hat, genügt hier, wie in Listing 3.7 dargestellt, der Versand des BASE64 codierten PGP/GPG-Schlüssels als PublicKeyASCIIData. Es werden keine weiteren IDs zur Identifizierung benötigt.

Listing 3.7: Beispiel eines PGP/GPG-Schlüsselupdates

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="KEYUPDATE" action="SET" timestamp="2019-01-02T08:42:23Z">
3   <PublicKeyASCIIData>
4     -----BEGIN PGP PUBLIC KEY BLOCK-----
5
6     0Wh7seClfszkKVpnfiVY+thZmFw2r/odGXPLl88dXK7mzF8bFv1DmtrMG2mjzyk7MXX3eEZ
7     kRD+Uj5B/DKuLbOIMwphEvu8+RGmEMPiB+wDMrrZdZwMzeb6JDS69Rs2sGKSdr4bOU3STPc
8     geokWVS1A0qUOoljykuWBrZPLuU21D3MJZVZeMeXW5GoOXkwMMfkUJzZ2Jq2QljT1hnV/IJ
9     inNPLSb9GCCDD2xqKJMj5pSS0+gGg75UCtUPr6RXtSpkB+DHW4lsN6C9eaZvnAmoqY4eSJVA
10    ncNDKevCqb0LQfuFf2Mtv8VHhnrWr1ljN7uF7TmrtpsD7apEjwe12C5BQlwQcUAJ3DVHYa4e
11    -----END PGP PUBLIC KEY BLOCK-----
12  </PublicKeyASCIIData>
13 </ServicePart>

```

Die Aktionen zum Abfragen und Löschen eines Schlüssels, also GET, REMOVE und CLEAN, sind analog zu den Service Parts für ein Adress-Update definiert.

3.1.4. Verwaltung von Kontaktdaten

Um neben den für die technische Kommunikation benötigten Adress- und Schlüsseldaten auch Kontaktdaten von realen Personen und Organisationseinheiten austauschen und verwalten zu können, wurde die Option des CONTACTUPDATE entwickelt. Das CONTACTUPDATE weist mit den Aktionen SET, GET, REMOVE und CLEAN die gleichen Funktionen wie auch ADDRESS- und KEYUPDATE auf.

Jeder übermittelte Service Part ist durch eine eindeutige ContactID identifizierbar und kann durch die ConnectionID einem ADDRESSUPDATE zugeordnet werden. Neben den Basisdaten des Kontakts wie Name, Geschlecht, Fachrichtung etc. können beliebig viele Kontaktinformationen in Form von Telefon-, Fax- oder Pagenummer sowie Adressinformationen wie Straße, Hausnummer und Stadt angegeben werden (Listing 3.8).

Listing 3.8: Beispiel eines einfachen Kontakt-Updates

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="CONTACTUPDATE" action="SET" timestamp="2018-09-02T11:41:42Z">
3   <ContactID>44849e25-1fae-46f6-8edf-7ae3b5d0938d</ContactID>
4   <Title>Dr.</Title>
5   <GivenName>Peter</GivenName>
6   <Name>Mayer</Name>
7   <Sex>M</Sex>
8   <Unit>PERSON</Unit>
9   <ContactInformation order="1">
10    <RealLifeEMailAddress>peter.mayer@krankenhaus.de</RealLifeEMailAddress>
11    <Phone>+49 0815 4711</Phone>
12    <Website>rad.krankenhaus.de</Website>
13  </ContactInformation>
14  <ContactInformation order="2">
15    <RealLifeEMailAddress>p.mayer@hoster.de</RealLifeEMailAddress>
16  </ContactInformation>
17  <RelatedID>a709fe4b-62e6-4b6c-924a-8d3ccacf7ec2</RelatedID>
18  <ContainerID>dd5cc591-e2c7-405f-b025-afecf194ead9</ContainerID>
19 </ServicePart>

```

Außer der ContactID, der Organisationseinheit, dem Namen und dem Geschlecht sind alle weiteren Angaben optional (Tabelle 3.2). Neben den eigentlichen Kontaktdaten des Service Parts ist es möglich, jeden Eintrag über die RelatedID einem anderen Kontakt

Tabelle 3.2.: Elemente und Attribute für eine ContactUpdate-Nachricht. [Opt.; Optionality: (R)equired, (O)ptional - Mul.; Multiplicity] (Quelle: DICOM E-Mail Standardempfehlung 1.7, S. 47)

Name	Mul.	Opt.	Beschreibung
ContactID	1	R	Eindeutige ID des Service Parts
ConnectionID	1-N	O	Referenz auf ADDRESSUPDATE
Role	1-N	O	Rollen: MED, TEC, ADMIN, DOC
Unit	1	R	Einheiten: PERS, DEP, HOSP, ORG
Speciality	1-N	O	Fachrichtung (zum Beispiel Radiologie)
Title	1	O	Akademischer Grad (zum Beispiel Dr., Prof.)
Sex	1	R	Geschlecht: M, F, O
Name	1	R	Familienname
GivenName	1	O	Rufname
Comment	1	O	Feld für Kommentare
ContactInformation	1-N	O	Kontaktdaten
../RealLifeEMailAddress	1	O	Persönliche E-Mail Adresse
../Fax	1	O	
../Mobile	1	O	
../Phone	1	O	
../Pager	1	O	
../Website	1	O	
../Comment	1	O	
Address	1-N	O	Adressdaten
../Street_1	1	O	
../Street_1	1	O	
../City	1	O	
../ZipCode	1	O	
../State	1	O	
../Country	1	O	
../Comment	1	O	
RelatedID	1-N	O	ID eines referenzierten Datensatzes
ContainerID	1	O	ID des übergeordneten Datensatzes
Custom	1-N	O	Zusätzliche Daten

zuzuordnen und über die ContainerID eine Zuordnung zu einer übergeordneten Einheit herzustellen. Ein vollständiges Beispiel-Listing befindet sich in Anhang A.2.

Grundsätzlich bietet das IHE Healthcare Provider Directory (HPD) eine ähnliche Struktur und Funktionen für das Speichern und Abfragen von Adressdaten. Der Hauptaspekt bei der Entwicklung des CONTACTUPDATES liegt allerdings auf der strukturierten Übermittlung der Daten via DICOM E-Mail und der Zuordnung der Kontaktdaten zu den für DICOM E-Mail benötigten technischen Kommunikationsdaten wie

E-Mail-Adresse und PGP/GPG-Schlüssel. Alle durch das CONTACTUPDATE ausgetauschten Daten lassen sich auch mit einem HPD als Backend speichern und über die HPD Standard Schnittstellen abfragen, so dass einem parallelen Betrieb hier nichts im Wege steht.

3.1.5. Verbindungsupdate

Unter Verwendung der Connection-ID kann auch ein kompletter Datensatz aller dieser ID zugehörigen Kommunikationsdaten abgefragt werden (Listing 3.9). Der Service Part CONNECTIONUPDATE ist also eine Kombination aus ADDRESS-, KEY- und CONTACTUPDATE. Bei dieser Abfrage wird ausschließlich die Option GET unterstützt. Weiterhin müssen die IDs dem Anfragenden bekannt sein, so dass hier nur ein Abfragen bekannter Verbindungsdaten realisiert wird, um eventuelle Konfigurationsänderungen zum Beispiel mit einem zentralen Server abzugleichen. Da hier keine neuen Verbindungsdaten angelegt werden können, ist das CONNECTIONUPDATE daher als Synchronisationsmechanismus zu verstehen und muss nur optional unterstützt werden.

Listing 3.9: Service Part zum Abfragen von Verbindungsdaten

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="CONNECTIONUPDATE" action="GET" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Connection>
4     <ID />
5   </Connection>
6   <GPGKeyID />
7   <ContactID />
8 </ServicePart>
```

3.1.6. Empfangsbestätigung

Das Grundkonzept von Service Part E-Mails sieht vor, mehr als einen Service Part pro E-Mail zu übermitteln. Dadurch wird unter anderem ermöglicht, das komplette Adressbuch in einer einzigen E-Mail zu aktualisieren. Dieses Konzept der Mehrfachanforderung muss sich daher auch in der Empfangsbestätigung der Service Parts widerspiegeln. Mit den erweiterten Benachrichtigungsmechanismus von DICOM E-Mail (Abschnitt 2.1.3) ist es zwar möglich, Bestätigungen für einzelne Teile von E-Mails anzufordern, was auch für

Service Parts gilt, allerdings löst dies pro Service Part eine eigene Bestätigungs-E-Mail aus, was beim Update eines kompletten Adressbuchs unter Umständen zu einer Flut von E-Mails im Netzwerk führen kann.

Um dies zu umgehen, wurde der Service Part DISPOSITIONNOTIFICATION eingeführt, welcher es erlaubt, innerhalb einer Bestätigungs-E-Mail mehr als einen Status für unterschiedliche E-Mail Teile zum Absender der Service Part E-Mail zu übermitteln (Listing 3.10). Jeder Service Part kann so exakt durch die MessageID der E-Mail sowie durch die ContentID einem bestimmten Teil einer E-Mail zugeordnet werden.

Listing 3.10: Empfangsbestätigung mit der Verwendung von Service Part E-Mails

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="DISPOSITIONNOTIFICATION" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <MessageID />
4   <Notification>
5     <ContentID />
6     <DispositionField />
7     <Response>
8       <ErrorCode />
9       <Comment />
10    </Response>
11  </Notification>
12 </ServicePart>

```

Die einzelnen Felder beziehungsweise Inhalte der Empfangsbestätigung unterscheiden sich in diesem Anwendungsfall nicht von denen der Standardbenachrichtigung, wobei hier noch das zusätzliche Feld 'Comment' hinzugefügt wurde, um zu erlauben, weitere Nachrichten, die nicht in Fehler-Codes ausgedrückt werden können, zu übermitteln.

Tabelle 3.3.: RFC 3798 konforme Statusnachrichten für Service Part E-Mails. Bestätigungen im Erfolgs- und Fehlerfall mit Fehlercode.

Element	Wert	Bedeutung
DispositionField	displayed	erfolgreich
	displayed/warning	teilweise erfolgreich, leichter Fehler ohne Einfluss auf die Übertragung (z.B. PGP/GPG-Schlüssel läuft bald ab)
	deleted/error	fehlerhafte Übertragung
	deleted	fehlerhafte Übertragung
Error	Fehlercode	definierter Fehlercode
Comment	Fehlerbeschreibung	textuelle Beschreibung des Fehlers

3.1.7. Konstanzprüfung

Mit den im obigen Abschnitt beschriebenen Nachrichten stehen somit alle Möglichkeiten zur Administration eines DICOM E-Mail Netzwerks zur Verfügung. Neben der Verwaltung von Postfächern und PGP/GPG-Schlüsseln spielt die Konstanzprüfung (nach DIN 6868-159) in einem solchen Netzwerk eine große Rolle. Die Verbindungen zwischen den einzelnen Partnern müssen regelmäßig monatlich auf Konstanz und täglich auf Funktion geprüft werden. Aus diesem Grund wurde der Service Part TESTTRANSFER mit der Aktion QOSCHECK (Quality of Service) eingeführt.

Dieser Service Part ermöglicht es einem Teilnehmer im Netzwerk, einen Transfer mit einem definierten Datensatz zwischen zwei beliebigen Knoten anzustoßen und im Anschluss ein Protokoll über die durchgeführte Übertragung zu erhalten. Die Testtransfer-Nachricht kann dazu verwendet werden, den Empfänger anzuweisen, einen DICOM E-Mail Testdatensatz ad hoc an den Sender der Testtransfer-Nachricht zu senden. Außerdem kann ein Administrator im Teleradiologienetzwerk über diesen Mechanismus die regelmäßige Konstanzprüfung im Netzwerk durchführen und die Protokolle alle Übertragungen erhalten.

Als Trigger für eine Konstanzprüfung wird die in Listing 3.11 dargestellte XML-Struktur verwendet, welche dann in einer Service Part E-Mail übertragen wird. Der Anforderer der Konstanzprüfung definiert mit den beiden Knoten 'TestDataReceiver' und 'ProtocolReceiver', zwischen welchen Knoten die Konstanzprüfung stattfinden soll und wer im Anschluss das Protokoll der durchgeführten Prüfung erhalten soll.

Listing 3.11: Service Part TESTTRANSFER für die Konstanzprüfung nach DIN 6868-159

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="TESTTRANSFER" action="QOSCHECK" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <TestDataReceiver>
4     <EmailAddress />
5     <GPGKeyID />
6   </TestDataReceiver>
7   <ProtocolReceiver>
8     <EmailAddress />
9     <GPGKeyID />
10  </ProtocolReceiver>
11  <TestDataSetID />
12  <ErrorTimeOut />
13 </ServicePart>
```


Mit der 'TestDataSetID' kann der Administrator den zu verwendenden Testdatensatz angeben. Hierbei sind nur zwei Datensätze durch das Whitepaper fest definiert, und die Organisation weiterer Testdatensätze obliegt dem Betreiber des Netzwerks. Der Datensatz mit der ID TESTDATASET_1 beinhaltet einen möglichst kleinen Datensatz zur arbeitstäglichen Funktionsprüfung nach DIN 6868-159 und mit der ID TESTDATASET_2 den größtmöglichen Datensatz, für den die Teleradiologiestrecke abgenommen wurde. Dieser Datensatz kann dann zur monatlichen Konstanzprüfung nach DIN 6868-159 verwendet werden. Weitere Datensätze wie zum Beispiel TESTDATASET_CT_HEAD oder TESTDATASET_CR_THORAX können frei definiert werden. Durch Angabe des 'Error-TimeOut' kann dem Empfänger der Testtransfer-Nachricht ein konfigurierbarer Timeout in Sekunden mitgegeben werden, ab welchem Zeitpunkt das Protokoll erstellt werden soll, auch wenn der Transfer noch nicht vollständig beendet ist. Da ein Transfer nach DIN 6868-159 nach maximal 15 Minuten abgeschlossen sein sollte, empfiehlt sich hier ein Timeout von nicht länger als 900 Sekunden, um so auch zeitnah eine Aussage über die Funktionsfähigkeit des Netzwerks treffen zu können.

Nach Beendigung des Testtransfers erstellt der Sender der Testdaten ein Protokoll und sendet dieses als Service Part PROTOCOL an den angegebenen Protokollempfänger (Abbildung 3.1). Der Empfänger des Protokolls und der Administrator können je nach Konfiguration auch identisch sein. Das Protokoll (Listing 3.12) enthält eine detaillierte Auflistung über alle übertragenen beziehungsweise fehlgeschlagenen Objekte inklusive Größe und Übertragungsdauer sowie im Fehlerfall den DICOM E-Mail Error-Code je fehlgeschlagener E-Mail.

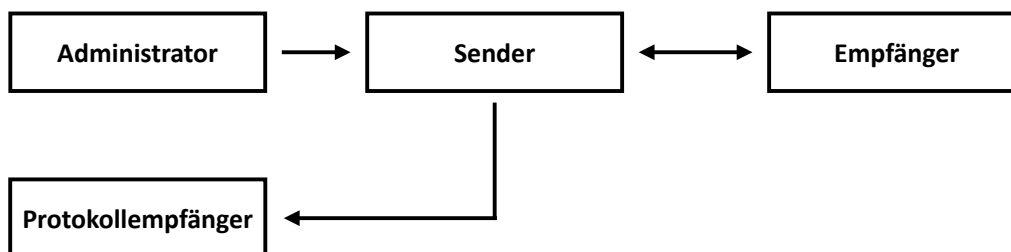


Abbildung 3.1.: Ablauf der Konstanzprüfung mit DICOM E-Mail Service Parts.

Listing 3.12: Service Part PROTOCOL für die Konstanzprüfung nach DIN 6868-159

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="PROTOCOL" action="" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <TransmissionStatus /> <!-- Status: COMPLETED, ABORTED -->
4   <TestDataSetID /> <!-- ID des Testdatensatz -->
5
6   <ObjectsSent>
7     <Count /> <!-- Anzahl versendete Objekte -->
8   </ObjectsSent>
9   <ObjectsReceivedConfirmed>
10    <Count /> <!-- Anzahl bestätigter Objekte -->
11    <Time /> <!-- Übertragungszeit in Sekunden -->
12    <MailSize /> <!-- Größe aller übertragener E-Mails -->
13    <ObjectSize /> <!-- Größe aller übertragener Objekte -->
14  </ObjectsReceivedConfirmed>
15
16  <DataSender> <!-- DICOM E-Mail Adresse des Absenders -->
17    <EmailAddress />
18  </DataSender>
19  <DataRecipient> <!-- DICOM E-Mail Adressee des Empfängers -->
20    <EmailAddress />
21  </DataRecipient>
22  <ProtocolRecipient> <!-- E-Mail Adresse des Protokoll-Empfängers -->
23    <EmailAddress />
24  </ProtocolRecipient>
25
26  <ErrorTimeOut /> <!-- Fehler Timeout, falls angegeben -->
27
28  <DatagramMail EMailMessageID=""> <!-- Fehlerbeschreibung pro DICOM E-Mail (0-N Mal)-->
29    <ErrorID />
30    <EMailContentID />
31    <StartDateTime />
32    <NotifyDateTime />
33    <MailSize />
34    <ObjectSize />
35  </DatagramMail>
36 </ServicePart>

```

Aus diesem maschinenlesbaren Protokoll kann anschließend eine Anzeige für den Nutzer zur Überwachung des Netzwerks oder ein Protokoll zur Vorlage bei der Ärztlichen Stelle generiert werden.

3.1.8. Abfrage des Adressverzeichnisses

Mit den oben eingeführten ServiceParts ADDRESS-, KEY- und CONTACTUDPATE und deren Aktion GET ist es zwar möglich, Informationen über eine Verbindung bei der Gegenseite abzufragen, allerdings funktioniert dies nur, wenn die Connection-ID der Verbindung dem Anfragenden bekannt ist.

Um auch Daten mit bislang unbekannter Connection-IDs abzufragen, wurde im Rahmen des Whitepapers der optionale Service Part QUERY mit den beiden Aktionen FIND und RESULT implementiert.

Die Anfrage der Gegenseite (Listing 3.13) wurde an das Konzept von DICOM C-FIND angelehnt. Im Knoten 'Search' werden alle Abfrage-Parameter über das Filter-Element definiert. Diese Parameter in Form von DataTags können einen Modifier wie AND, OR und NOT besitzen und damit beliebige Abfragen auf das Repository abbilden.

Listing 3.13: Service Part QUERY/FIND zur Abfrage eines Adressverzeichnisses

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="QUERY" action="FIND" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <Search maxCount=[int] >
4     <Filter>
5       <DataTag modifier="[mod]">[value]</DataTag> <!-- Modifier: AND, OR, NOT -->
6     </Filter>
7   </Search>
8   <ResultSet filtered="[boolean]"> <!-- true, false -->
9     <ContactID />
10    <ConnectionID expand="[boolean]"> <!-- true, false -->
11    <Address>
12      <AddressDataTag 1 />
13      <AddressDataTag 2/>
14      ...
15    </Address>
16  </ResultSet>
17 </ServicePart>

```

Im Element 'ResultSet' werden die gewünschten Informationen angegeben, so dass die Gegenseite nicht die kompletten Informationen zu einem Versandpartner, sondern nur ein ausgewähltes Subset wie zum Beispiel die DICOM E-Mail Adresse übertragen muss. Sollen hingegen alle verfügbaren Informationen zu einer Verbindung übertragen werden, dann kann auch ein ResultSet mit dem Attribute 'filtered=false' angefordert werden, welches dann keinerlei Filterung anwendet.

Als Antwort auf eine solche Service Part QUERY sendet die Gegenseite ein RESULT mit den gewünschten Informationen (Listing 3.14).

Listing 3.14: Service Part QUERY/RESULT als Antwort auf eine Adressanfrage

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="QUERY" action="RESULT" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <ResultSet>
4     <Result> <!-- Enthält das Ergebnis genau einer QUERY -->
5       <DataTag 1 /> <!-- Ausgefülltes Such-Tag aus der Anfrage -->
6       <DataTag 2 />
7       ...
8     </Result>
9   </ResultSet>
10 </ServicePart>

```

Auch hier bietet es sich an, ein Whitelisting für erlaubte Kommunikationspartner zu pflegen, um unerwünschte Anfragen herausfiltern zu können. Ein komplettes Beispiel für eine Anfrage und ein Ergebnis befindet sich in den Anhängen A.3 und A.4.

3.2. Multiknotenstatistik

Seit 2009 existiert eine Norm zur Qualitätssicherung in der Teleradiologie (DIN 6868-159), die bei der Konstanz- und Abnahmeprüfung von Teleradiologiesystemen zur Anwendung kommt (Abschnitt 2.3.3). Diese Norm schreibt unter anderem vor, dass die Zeit vom Versand bis zum Empfang auf der Gegenseite gemessen werden muss. Bei einem direkten Datentransfer zwischen Sender und Empfänger ist eine automatisierte Messung der Übertragungszeit leicht möglich. Hierfür stellt der DICOM-Standard geeignete Methoden wie zum Beispiel Storage Commitment für DICOM C-Store oder die in Abschnitt 2.1.3 und 3.1.6 beschriebenen Empfangsbestätigungen für DICOM E-Mail zur Verfügung. Diese lassen sich bei einem Versand über mehrere Knotenpunkte (Abbildung 3.2) jedoch nur bedingt anwenden.

Weiterhin ist oft nicht sichergestellt, dass alle beteiligten Systeme zeitsynchron arbeiten. Besonders bei virtualisierten Systemen ist dies nicht immer problemlos möglich (Chauhan et al., 2011). Dadurch weiß der Sender, wann er die Daten abgesendet hat, und der Empfänger kennt den Zeitpunkt des Erhalts der Daten, aber beide Zeiten sind nicht ohne weiteres miteinander vergleichbar.

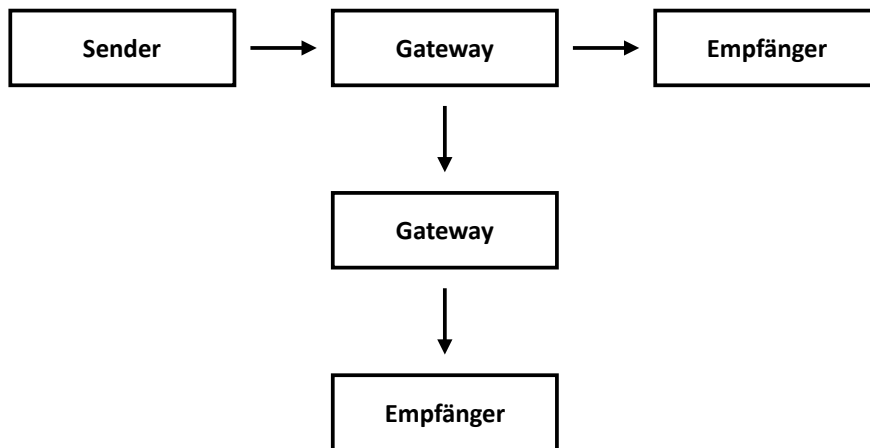


Abbildung 3.2.: Beispiel eines heterogenen Teleradiologienetzwerks. Vereinfachte Darstellung einer Teleradiologiestrecke mit mehr als einem Knoten.

Aus diesem Grund wurde durch den Autor mit der Methode der Multiknotenstatistik ein Verfahren konzipiert und umgesetzt, welches es erlaubt den Datenversand über beliebige und nicht zeitsynchrone Knoten zu protokollieren.

3.2.1. Datentransfer

Gerade in heterogenen Netzwerken, die mehr als eine Organisation umspannen und somit auch sicherheits- und netzwerktechnisch besonderen Regeln unterliegen, ist es meist nicht möglich, eine Kommunikation sowohl in Hin- als auch Rückrichtung aufzubauen. Aus diesem Grund setzt das Protokoll zur Multiknotenstatistik nur einen Verbindungskanal vom Sender zum Empfänger, aber keinen expliziten Rückkanal voraus (Abbildung 3.3).

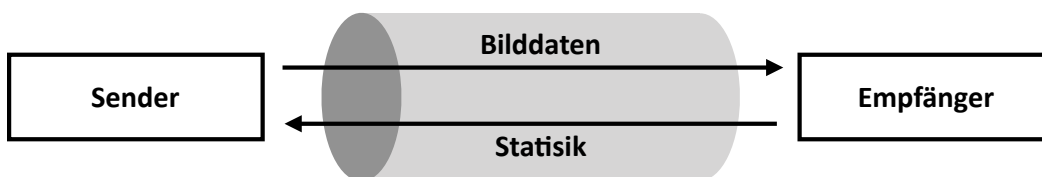


Abbildung 3.3.: Austausch von statistischen Daten. Übertragung von Bilddaten und Rückübermittlung von Statistikdaten unter Verwendung des gleichen Kommunikationskanals.

Da von einem bestehenden Netzwerk ausgegangen werden muss, stützt sich die Multiknotenstatistik hierbei auf folgende Punkte:

- Jeder Knoten in der Versandkette kennt nur seinen direkten Nachfolger.

- Die Kommunikation wird immer nur durch den Sender initiiert.
- Vor jedem Bildtransfer wird zusätzlich eine Statistiknachricht (inklusive der aktuellen Systemzeit) versandt.
- Nach Beendigung des Transfers zwischen zwei Knoten werden die statistischen Daten beim Empfänger aktiv abgefragt.

Alle Nachrichten, die im Rahmen der Transferstatistik zwischen den Knoten in einem Netzwerk ausgetauscht werden, sind in einem XML-Format codiert und weisen den gleichen Grundaufbau vor. Jede Nachricht besteht aus einem HEAD, der die Informationen des Absenders der Nachricht, also Hardware- beziehungsweise MAC-Adresse (Media Access Control), Hostname und -adresse sowie den Typ der Nachricht enthält (Listing 3.15). Die eigentliche Payload der Nachricht wird im BODY Teil transportiert, welcher durch den Typ der Nachricht näher bestimmt ist. Zur eindeutigen Identifizierung von Nachrichten und Knoten innerhalb einer Versandstrecke wird die MAC-Adresse des jeweiligen Senders beziehungsweise Empfängers herangezogen, da diese sich im Gegensatz zu Hostname und IP-Adresse für einen Knoten selten ändern. Eine Änderung oder Manipulation ist zwar grundsätzlich möglich (Lee et al., 2016), kommt aber meist nur im Bereich von drahtlosen 802.11 W-Lan Netzwerken (Tao et al., 2008) als Angriffsvektor für Man-in-the-Middle Attacken zum Einsatz, welche in Teleradiologienetzwerken generell durch geeignete Sicherheitsmaßnahmen verhindert werden müssen. Daten wie Hostname und -adresse werden lediglich zur einfacheren Identifizierung eines Knotens durch den Benutzer mit übermittelt.

Listing 3.15: XML-Struktur einer Transferstatistiknachricht

```
1 <statisticmessage version="1.71.0">
2   <head>
3     <macid>DE:AD:BE:EF:23:42</macid>
4     <hostname>sender</hostname>
5     <hostaddress>192.168.1.28</hostaddress>
6     <type>TRANSFER</type>
7   </head>
8   <body>
9     ...
10  </body>
11 </statisticmessage>
```

Nachrichten

Die nach dem obigen Schema erzeugten Statistikenachrichten können einen der folgenden Typen aufweisen:

TRANSFER: TransfERNachricht, welche die Daten eines kompletten Transfers inklusive aller Knoten beinhaltet. Diese wird sowohl zur Initiierung eines Transfers als auch als Antwort auf eine DATAREQUEST-Nachricht versendet.

DATAREQUEST: Nachricht, um die Daten eines Transfers bei der Gegenseite anzufordern.

NODATA: Antwortnachricht, die besagt, dass keine neuen Daten bei der Gegenseite vorhanden sind.

ERROR: Antwortnachricht, die bei einem Fehlerzustand versendet wird.

SYN: Nachricht zum Test der Transferstrecke.

ACK: Antwortnachricht auf eine SYN-Nachricht.

Erzeugung von Transfer-IDs

Vor einer Datenübertragung generiert der Absender eine eindeutige Transfer-ID, welche zusammen mit der aktuellen Systemzeit sowie den Kenndaten des Absenders (MAC- und IP-Adresse) in einer TRANSFER Statistikenachricht im XML-Format (Listing 3.16) auf einem zweiten Kommunikationskanal zum Empfänger der Bilddaten transportiert wird. Dies ist nötig, um den anschließend folgenden Transfer im Netzwerk identifizieren und um die Uhrzeit zwischen den Systemen abgleichen zu können. Als zweiter Kanal wird ein HTTP Request verwendet, welcher an den Statistikendpunkt auf der Gegenseite gesendet wird. Die Verwendung von HTTP als Standardprotokoll erlaubt eine einfache und sichere Anbindung von Statistiknoten, da dieses Protokoll auch im Klinikumfeld gebräuchlich ist und hier meist schon diverse Sicherheitsmaßnahmen zur Filterung des Datenverkehrs auf Basis von HTTP beziehungsweise HTTPS etabliert sind.

Listing 3.16: Beispiel einer Statistiknachricht

```

1 <statisticmessage version="1.71.0">
2   <head>
3     <type>TRANSFER</type>
4     ...
5   </head>
6   <body>
7     <transfer>
8       <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
9       <type>CSTORE</type>
10      <sender>
11        <macid>DE:AD:BE:EF:23:42</macid>
12        <time>1550927907000</time>
13      ...
14    </sender>
15  </transfer>
16 </body>
17 </statisticmessage>

```

Der Empfänger der Nachricht speichert daraufhin die übermittelte Transfer-ID in seiner Datenbank und berechnet mit der Zeit des Absenders und seiner eigenen Systemzeit den Offset zwischen sich und dem Absender. Sobald der Empfänger der Statistiknachricht den Empfang erfolgreich quittiert hat, sendet der Absender nun die Daten unter Verwendung der zuvor generierten Transfer-ID. Sollte der Empfänger nicht in einer vorgegebenen Zeit, also nach Ablauf eines Timeouts, oder mit einem Fehlercode antworten (Listing 3.17), so werden die Daten dennoch versendet, und die weitere Datenverarbeitung verläuft wie zwischen zwei Partnern ohne Verwendung der Multiknotenstatistik.

Listing 3.17: Beispiel einer Fehlernachricht

```

1 <statisticmessage version="1.71.0">
2   <head>
3     <macid>AB:CD:EF:12:34:56</macid>
4     <hostname>receiver</hostname>
5     <hostaddress>192.168.161.23</hostaddress>
6     <type>ERROR</type>
7   </head>
8   <body>
9     <error>Database not available</error>
10  </body>
11 </statisticmessage>

```


Datenübertragung

Je nach verwendetem Transportweg der Bilddaten kann diese Transfer-ID auf unterschiedliche Weise zusammen mit den Daten übertragen werden. Im Fall eines einfachen HTTP-Transfers wird die ID in einem HTTP-Header-Parameter (stat_transferid beziehungsweise stat_subid) zusammen mit jedem Objekt übertragen. Im Fall eines DICOM Versands via DICOM C-Store wird die ID beim Aufbau der Association in privaten Tags einer DIMSE Message (Transfer-ID (0003,1010) beziehungsweise Sub-ID (0003,1020)) übermittelt. Bei DICOM E-Mail Verbindungen kann hierfür ein X-Header-Tag (RFC 822 - 4.7.4. EXTENSION-FIELD) verwendet werden (Crocker, 1982).

Erhält nun der Empfänger die Bilddaten, so ist jedes einzelne Objekt eindeutig mit der zuvor generierten Transfer-ID markiert und kann hierdurch dem Transfer zugeordnet werden. Der Empfänger hat dadurch die Möglichkeit, den Transfer zusammenzuhalten und die Dauer des Empfangs aufgrund des zuvor berechneten Offsets genau zu bestimmen.

Werden die Daten nun innerhalb dieses Transfers noch zu einem weiteren Knoten versendet, so wechselt die Rolle der Empfänger nun zum Sender. Dieser generiert eine neue Transfer-ID und sendet wiederum selbst eine Statistiknachricht mit dem vollständigen Inhalt der bisherigen Versand-Statistik zum nächsten Knoten. Hierbei wird die ursprüngliche Transfer-ID nicht ersetzt, sondern weiterhin beibehalten, die neue ID wird als Sub-ID an den Transfer angehängt (Listing 3.18).

Listing 3.18: Beispiel einer TransfERNachricht

```

1 <statisticmessage version="1.71.0">
2   <head>
3     ...
4   </head>
5   <body>
6     <transfer>
7       <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
8       <subid>f5a7a7b1-dd13-429f-8763-a0d894986ed3</subid>
9       ...
10    </transfer>
11  </body>
12 </statisticmessage>

```

Jeder weitere Knoten in der Versandkette kennt dadurch die bisherige Versandstrecke und kann die Statistik mit seinen eigenen Daten weiter anreichern. Auf diese Weise ist es auch möglich, die interne Verarbeitung von Daten wie zum Beispiel eine Kompression oder Dekompression auf dem Knoten durch einen eigenen Eintrag darzustellen und in die Gesamtstatistik einfließen zu lassen. Die Fortschreibung der statistischen Daten endet mit dem ersten Knoten in der Versandkette, der die Multiknotenstatistik nicht unterstützt. In diesem Fall wird der Transfer dann ohne eine Bestimmung des Offsets beim Empfänger berechnet und nur die Übertragungszeit auf Seiten des Senders gemessen.

3.2.2. Anforderung der Statistik

Ist der Versand auf einem Knoten abgeschlossen, beginnt dieser Knoten aktiv beim Empfänger nachzufragen, ob die Verarbeitung auf der Gegenseite beendet ist (Abbildung 3.4).

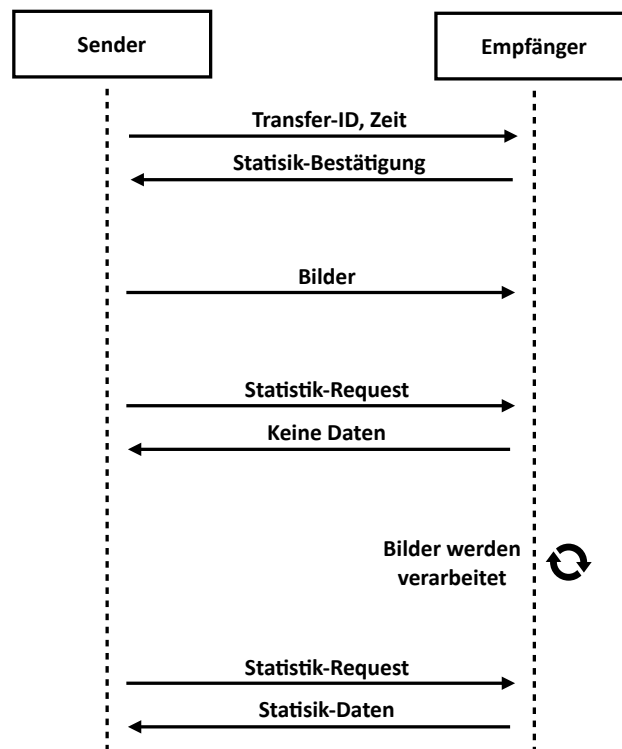


Abbildung 3.4.: Ablauf der Datenübertragung bei der Multiknotenstatistik zwischen zwei Knoten.

Diese Anfrage zur Übermittlung der statistischen Daten verwendet den gleichen Nachrichtenkanal über HTTP, der zur initialen Übermittlung der Statistknachricht verwendet wurde. Um nur die für den Sender relevanten Daten von der Gegenstelle abzufragen, werden hierbei die vom Sender initial generierten Transfer-IDs als Anfrageliste in der DATAREQUEST-Nachricht übermittelt (Listing 3.19).

Listing 3.19: Beispiel einer Anfragenachricht der Multiknotenstatistik

```

1 <statisticmessage version="1.71.0">
2   <head>
3     <macid>DE:AD:BE:EF:23:42</macid>
4     <type>DATAREQUEST</type>
5     ...
6   </head>
7   <body>
8     <transfers>
9       <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
10      <transferid>8a817850-59d0-4dd4-b28a-43ba27a61c1c</transferid>
11      ...
12    </transfers>
13  </body>
14 </statisticmessage>

```

Der Empfänger der Nachricht sendet dann alle ihm bekannten statistischen Daten zu den angefragten Transfers sowie eventuell zusätzliche Sub-Transfers zu weiteren Knoten. Die Anfrage des Senders wird auch dann beantwortet, wenn noch nicht alle Daten der nachfolgenden Transfers vorliegen. In diesem Fall wird der Transfer als offen zurückgemeldet, und der Sender hat die Möglichkeit, den Request erneut zu senden, bis alle Daten vorliegen oder ein Timeout abgelaufen ist.

Listing 3.20 zeigt die Rückantwort einer DATAREQUEST-Nachricht. Hier wurden 144 Objekte zwischen dem Sender und dem Empfänger übermittelt, von denen eins beim Empfänger nicht erfolgreich verarbeitet werden konnte. Mit Verarbeitung ist hier explizit die Verarbeitung und nicht der Empfang gemeint, da die Rückmeldung über den Empfang ja bereits durch den erfolgreichen Auf- und Abbau einer DICOM-Verbindung protokolliert wird. Weiterhin sieht man in der Antwort, dass der Empfänger einen zeitlichen Offset von 85281 ms angegeben hat.

- Versand erstes Bild: 23.02.2019 14:18:27 (1550927907000 ms seit 01.01.1970)
- Empfang letztes Bild: 23.02.2019 14:22:42 (1550928162000 ms seit 01.01.1970)

Daraus ergibt sich eine Bruttoversanddauer von 255000 ms beziehungsweise 4:15 Minuten. Unter Berücksichtigung des Offsets muss die Übertragungszeit um 85281 Millisekunden auf Netto 169719 Millisekunden beziehungsweise ca. 2:50 Minuten korrigiert werden, was dann der wirklichen Übertragungs- und Verarbeitungsdauer entspricht.

Listing 3.20: Beispiel einer Antwortnachricht der Multiknotenstatistik

```

1 <statisticmessage version="1.71.0">
2   <head>
3     ...
4     <type>DATA</type>
5   </head>
6   <body>
7     <transfer>
8       <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
9       <type>CSTORE</type>
10      <sender>
11        <macid>DE:AD:BE:EF:23:42</macid>
12        <time>1550927907000</time>
13        ...
14      </sender>
15      <receiver>
16        <macid>AB:CD:EF:12:34:56</macid>
17        <time>1550928162000</time>
18        <offset>85281</offset>
19        <objects>144</objects>
20        <failed>1</failed>
21        <size>72837</size>
22        ...
23      </receiver>
24    </transfer>
25  </body>
26 </statisticmessage>

```

Da dieses Protokoll allen am Transfer beteiligten Knoten vorliegt, werden dadurch sowohl Sender als auch Empfänger in die Lage versetzt, den Transfer inklusive aller Zwischenschritte komplett nachzuvollziehen. Ein vollständiges Beispiel für eine Transferstatistik über mehrere Knoten befindet sich im Anhang (A.5, A.6).

3.3. IHE XDM und DICOM E-Mail

In der Teleradiologie in Deutschland existiert mit DICOM E-Mail und der beschriebenen Erweiterung zur Qualitätssicherung und Administration mittels DICOM E-Mail Service Parts (Abschnitt 3.1.1) ein etablierter technischer Standard für die Vernetzung medizinischer Einrichtungen. Auf der anderen Seite entstehen immer mehr Netzwerke, die sich

mittels XDS und anderen weltweit verfügbaren IHE-Profilen vernetzen wollen. Beides hat seine Berechtigung sowie seine Vor- und Nachteile. Jedoch ist es aktuell schwer, diese beiden Arten der Vernetzung zusammen zu bringen.

DICOM E-Mail ist für eine schnelle Vernetzung mehr als geeignet und baut auf eine robuste und sichere Infrastruktur auf, lässt sich allerdings schwer in eine bestehende XDS-Infrastruktur integrieren. XDS beziehungsweise XDS-I hingegen benötigen eine komplexe Infrastruktur mit Affinity Domain und den dazugehörigen Codes und Value Sets, was eine Ad-hoc-Kommunikation nur schwer möglich macht. Weiterhin fehlt XDS die mit DICOM E-Mail bereits etablierte Möglichkeit zur Qualitätskontrolle, welche für die Teleradiologie nach RöV zwingend notwendig ist.

Aus diesem Grund wurde in Zusammenarbeit mit IHE Deutschland und einer Arbeitsgemeinschaft der Deutschen Röntgengesellschaft (@GIT) ein neues IHE-Profil entwickelt, das einen einfachen Einstieg in die Teleradiologie mittels XDS ermöglicht.

Dieses Profil und die beschriebenen Erweiterungen wurden 2016 durch das Konsortium als Draft in das IHE Radiology Planning Committee eingereicht und stellen eine Erweiterung des IHE Radiology Technical Framework Volume 1 und 2 dar. Trotz der Bemühungen der Arbeitsgruppe wurde der Entwurf leider nicht in den Prozess zur Aufnahme in das Technical Framework angenommen (Kapitel 4.4).

3.3.1. Quality Controlled Image Transfer

Quality Controlled Image Transfer (QCIT) baut auf das bereits vorhandene IHE-Profil Cross-Enterprise Document Media Interchange (XDM) auf und erweitert dieses um die beiden neuen Akteure *Transmission Set Creator* sowie *Transmission Set Receiver* mit der Transaktion *Distribute Transmission Set via e-mail* (Abbildung 3.5).

Um die Verfügbarkeit von Partnern zu überwachen und eine Basis für die teleradiologische Konstanzprüfung zu schaffen, wurde das Profil gegenüber XDM um einen Mechanismus zur einfachen sowie detaillierten Empfangsbestätigung erweitert. Verschlüsselung und Signatur soll durch das standardisierte S/MIME Verfahren gewährleistet werden,

wodurch Patientendaten geschützt und die Authentizität des Senders sichergestellt werden können.

Gegenüber XDM erlaubt QCIT das Aufteilen von Übertragungen auf mehrere E-Mails analog zu den bekannten Mechanismen aus DICOM E-Mail. Durch den Einsatz von X-HEADER E-Mail Tags können einzelne E-Mails einem Transfer eindeutig zugeordnet werden. Ähnlich wie auch in DICOM E-Mail können Empfangsbestätigungen sowohl pro E-Mail als auch pro Dokument verwendet werden.

Da QCIT auf XDM aufbaut, ist es grundsätzlich offen gegenüber dem Format der übertragenen Dokumente und eignet sich somit sowohl zur Übertragung von DICOM- als auch nicht-DICOM-Objekten. Metadaten von nicht-DICOM-Objekten müssen nicht wie bei DICOM E-Mail über das X-HEADER Tag X-TELEMEDICINE-STUDYID einer DICOM-Studie zugewiesen werden, sondern können unter Verwendung der standardisierten XDS-Metadaten leicht einem Patienten zugeordnet werden.

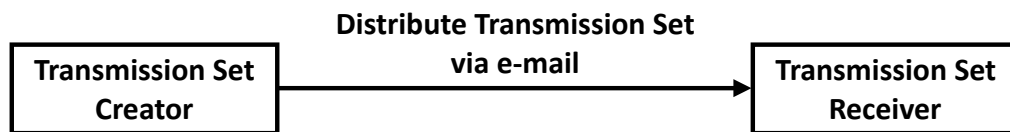


Abbildung 3.5.: QCIT Akteur Diagramm mit Transaktion.

Transmission Set Creator erstellt Transmission Sets und sendet diese verschlüsselt und mit einer elektronischen Signatur versehen via E-Mail an den Empfänger. Die übermittelten Daten können zum Beispiel aus einem RIS, KIS, PACS oder einer Patientenakte stammen.

Transmission Set Receiver empfängt Transmission Sets, validiert deren Signatur und extrahiert und verarbeitet die verschlüsselten Daten. Die empfangenen Daten werden dann an die entsprechenden Systeme wie RIS, KIS, PACS oder einer Patientenakte zur weiteren Verarbeitung übergeben.

Transmission Set beinhaltet ein oder mehrere XDS Submission Sets unter der Verwendung der XDM-Verzeichnisstruktur. Weiterhin beschreibt ein Transmission Set eine Serie von zusammengehörigen E-Mails wie zum Beispiel eine DICOM-Studie.

QCIT Actor Options

Tabelle 3.4.: QCIT - Actors and Options. Note*: The ZIP over Email Option, the ZIP over Email Response Option, and the ZIP over Email QC Request Option are required for both Transmission Set Creator and Transmission Set Receiver. (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 9)

Actor	Option Name	Optionality	Reference
Transmission Set Creator	ZIP over Email*	R	RAD TF-2: X.2.1
	ZIP over Email Resp.*	R	RAD TF-2: X.2.2
	ZIP over Email Enhanced Resp.	O	RAD TF-2: X.2.3
	ZIP over Email QC Req.*	R	RAD TF-2: X.2.4
Transmission Set Receiver	ZIP over Email*	R	RAD TF-2: X.2.1
	ZIP over Email Resp.*	R	RAD TF-2: X.2.2
	ZIP over Email Enhanced Resp.	O	RAD TF-2: X.2.3
	ZIP over Email QC Req.*	R	RAD TF-2: X.2.4

ZIP over Email

Alle zu übermittelnden Daten werden grundsätzlich als ZIP komprimiert versendet. Ein ZIP-Container enthält ein oder mehrere XDS Submission Sets unter Verwendung der XDM-Verzeichnisstruktur. Der verschlüsselte und signierte Container wird als Anhang an eine E-Mail versendet und kann den gleichen Message Partial Mechanismus wie auch DICOM E-Mail verwenden. Als Verschlüsselung kommt bei QCIT anstelle von PGP/GPG das in XDM bereits gebräuchliche S/MIME Verfahren zur Anwendung.

ZIP over Email Response

Diese Option ist für beide Aktoren verpflichtend zu implementieren. Der Transmission Set Receiver sendet eine MDN-basierte Antwort an den Transmission Set Creator, um

den Status der Verarbeitung jeder einzelnen E-Mail zu übermitteln. Dies geschieht analog zu DICOM E-Mail Empfangsbestätigungen (Abschnitt 2.1.3).

ZIP over Email Enhanced Response

Die Enhanced Response ist für beide Akteure optional. Eine Implementierung dieser Option ermöglicht dem Transmission Set Receiver, Benachrichtigungen zu übermitteln, die um zusätzliche Informationen mit entsprechenden Error-Codes erweitert wurden. Analog zu den erweiterten DICOM E-Mail Empfangsbestätigungen (Abschnitt 2.1.3) können diese Benachrichtigungen nicht nur pro empfangener E-Mail, sondern pro XDS Submission Set beziehungsweise Dokument verwendet werden.

ZIP over Email QC Request

Die Option Quality Control Request erlaubt dem Transmission Set Creator, eine Konstanzprüfung mit definierten Daten bei der Gegenseite anzustoßen.

Um diese Option zu unterstützen und einen QC Request verarbeiten zu können, ist es notwendig, dass jeder Transmission Set Receiver mit einem Transmission Set Creator gruppiert ist. Der Creator sendet eine QC Request an den Receiver, welcher hierauf die Rolle eines Creators annimmt und die im QC Request angeforderten Daten dann an einen weiteren Receiver versendet. Bei Abschluss des Testtransfers sendet dieser dann ein detailliertes Protokoll über den Status der Übertragung (Anzahl der Objekte, Übertragungszeit und Fehlercodes) an einen definierten Empfänger.

3.3.2. Übertragung von DICOM- und nicht-DICOM-Daten mittels QCIT

Werden Daten via QCIT übertragen, so erstellt der Transmission Set Creator als erstes eine XDM-konforme Verzeichnisstruktur (Abbildung 3.6) inklusive einer METADATA.XML pro Submission Set, welche die Metadaten der zu übertragenden Dateien sowie einen Hash zur Integritätsprüfung enthält. Grundsätzlich unterscheidet sich die Ordnerstruktur nicht von der einer DICOM Patienten-CD (nach dem IHE-Profil Portable Data

for Imaging (PDI)) und kann bei Bedarf neben den zu übertragenden Daten auch ein DICOMDIR (als Verzeichnisindex) oder weitere für das QCIT-Profil nicht relevante Dokumente enthalten.

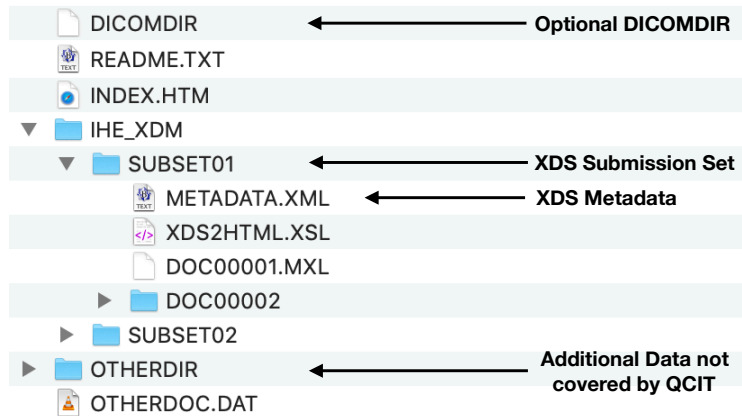


Abbildung 3.6.: Beispielhafter Aufbau einer XDM-Verzeichnisstruktur

Nach Erstellung dieser Verzeichnisstruktur erzeugt der Transmission Set Creator im Unterschied zu XDM beliebig viele ZIP-Container für die einzelnen Einträge. Die Aufteilung der Dokumente auf die einzelnen Container ist dem Sender überlassen. Im Anschluss wird jeder einzelne ZIP-Container per E-Mail übertragen. Um die einzelnen Container einem Transmission Set zuzuordnen, so dass sie auf Seiten des Empfängers wieder zu dem initialen Verzeichnisbaum zusammengesetzt werden können, werden die einzelnen E-Mails analog zu den X-HEADER Tags in DICOM E-Mail mit entsprechenden Tags markiert.

X-IHE-QCIT-SETID: Eine eindeutige ID für ein Set von zusammengehörigen E-Mails.

X-IHE-QCIT-SETPART: Die Nummer der aktuellen E-Mail innerhalb eines Sets.

X-IHE-QCIT-SETTOTAL: Die Anzahl der im Set enthaltenen E-Mails.

Diese drei X-Tags ordnen E-Mails eindeutig einem Transmission Set zu und erlauben es dem Empfänger, die Vollständigkeit der Übertragung zu überprüfen. Die Tags folgen den folgenden Regeln:

1. X-Tags werden ausschließlich außerhalb der S/MIME Container verwendet, um auch bei Problemen mit der Ver-/Entschlüsselung noch Informationen über den Transfer transportieren zu können.
2. SETID und SETPART müssen in jeder E-Mail vorhanden sein.
3. SETTOTAL muss mindestens in der letzten E-Mail des Transmission Sets vorhanden sein und ist für alle anderen E-Mails des Sets optional. Dies erlaubt dem Transmission Set Creator bereits den Versand der ersten E-Mail, ohne dass er zu diesem Zeitpunkt schon weiß, auf wie viele E-Mails er das Transmission Set aufteilen wird.

Die so erzeugten Daten werden per E-Mail übertragen (Abbildung 3.7) und bei Erhalt durch den Transmission Set Receiver entschlüsselt, entpackt und wieder zu einem XDM-Verzeichnisbaum zusammengesetzt. Anhand der enthaltenen METADATA.XML kann der Empfänger die Integrität der empfangenen Daten prüfen und nicht-DICOM-Daten entsprechend zuordnen. Sind alle Daten empfangen, kann der komplette Verzeichnisbaum zur weiteren Verarbeitung an Subsysteme wie RIS, KIS oder PACS übergeben werden.

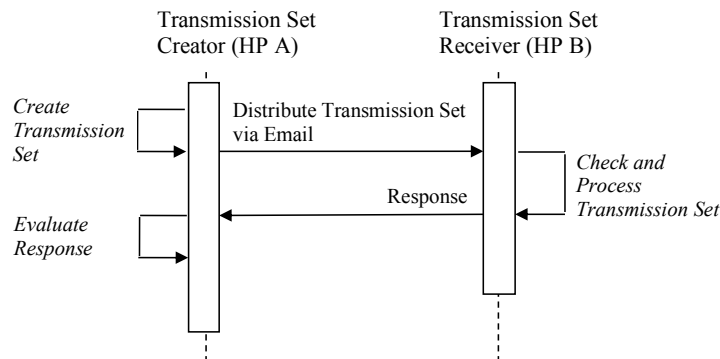


Abbildung 3.7.: Datenübertragung mittels QCIT (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 13)

Weiterhin wird für die angeforderte Empfangsbestätigung pro E-Mail eine MDN-Nachricht an den Creator gesendet. Hierbei werden, um standardkonforme Nachrichten zu erzeugen, ausschließlich die beiden Stati Success und Error verwendet.

Success: Dem MDN-Feld 'disposition-type' wird der Wert 'displayed' zugewiesen.

Error: Dem MDN-Feld 'disposition-type' wird der Wert 'deleted' zugewiesen, und es wird der MDN 'disposition-modifier' entsprechend dem Fehler mit einem definierten Code gefüllt.

Im Fehlerfall werden folgende standardisierten Codes verwendet:

- 'signature-verification-error' - Fehler bei der Verifizierung der Signatur
- 'decryption-error' - Fehler bei der Entschlüsselung
- 'mail-syntax-error' - Fehlerhafte Formatierung der E-Mail
- 'mail-attachment-error' - Fehler beim Extrahieren des E-Mail Anhangs
- 'application-processing-error' - Genereller Fehler bei der Verarbeitung

Durch die Verwendung der Transmission Set X-Tags sowie die Anforderung von Bestätigungs-E-Mails können sowohl Sender als auch Empfänger die Vollständigkeit eines Transfers überprüfen.

3.3.3. Erweiterte Empfangsbestätigung mittels QCIT

Da die oben beschriebenen Basis-Empfangsbestätigungen nur pro E-Mail, nicht aber pro XDS Submission Set beziehungsweise Dokument verwendet werden können, wurde hier analog zu den erweiterten Empfangsbestätigungen bei DICOM E-Mail auch ein Enhanced Response eingeführt. Die Anforderung einer Benachrichtigung auf Seiten des Creators unterscheidet sich nicht von der Basis-Empfangsbestätigung, jedoch können hier bei der Beantwortung der Nachricht Daten über die einzelnen Dokumente im XML-Format übermittelt werden.

Sollte der Transmission Set Receiver diese erweiterte Bestätigung unterstützen, so sendet er ein XML-Dokument (Listing 3.21) mit entsprechendem Aufbau nach Tabelle 3.5 als MIME-Anhang in einer Standard-MDN-Bestätigungs-E-Mail. Sollte der Empfänger die Option nicht unterstützen, so verwirft er den Anhang der MDN und wertet nur den Standardinhalt der Nachricht aus.

Tabelle 3.5.: Elemente und Attribute für eine QCIT Enhanced Response-Nachricht. [Opt.; Optionality: (R)required, (O)ptional - Mul.; Multiplicity] (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 22)

Name	Mul.	Opt.	Description
notification	1	R	
../Entry	1-N	R	
../..../submissionSet	1	R	
../..../..../entryUUID	1	R	The UUID of the submission set
../..../..../errorCode	1	R	The error code for the submission set
../..../..../resend	0-1	R	Indicates a request for resending the submission set
../..../..../document	1-N	R	
../..../..../entryUUID	1	R	The UUID of the document
../..../..../errorCode	1	R	The error code for the document
../..../..../resend	0-1	R	Indicates a request for resending the document
notification/signature	0-1	O	Signature over all notificationDataEntry elements

Listing 3.21: Beispiel einer erweiterten Bestätigung mit QCIT

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <notification version="1.0">
3   <notificationDataEntry>
4     <submissionSet>
5       <entryUUID>1.2.3.4.5.6.7.8.9</entryUUID>
6       <errorCode>mime-type-not-supported</errorCode>
7       <resend>no</resend>
8     <document>
9       <entryUUID>2.3.4.5.6.7.8.9.0</entryUUID>
10      <errorCode>sop-class-not-supported</errorCode>
11      <resend>no</resend>
12    </document>
13    <document>
14      <entryUUID>3.4.5.6.7.8.9.0.1</entryUUID>
15      <errorCode>sop-class-not-supported</errorCode>
16      <resend>no</resend>
17    </document>
18    ...
19  </submissionSet>
20 </notificationDataEntry>
21 <notificationDataEntry>
22   ...
23 </notificationDataEntry>
24 </notification>

```

Der Nachrichtenfluss sowie die Auswertung der Bestätigungs-E-Mails sind in Abbildung 3.8 dargestellt. Dies hat gegenüber den unterschiedlichen Bestätigungsmechanismen aus DICOM E-Mail den Vorteil, dass hier nur eine Art von Bestätigung versendet

wird und die beiden Teilnehmer je nach Implementierungsstand diese Bestätigungs-E-Mails mit mehr Daten anreichern beziehungsweise diese umfangreich auswerten können. Unterstützen beide Teilnehmer das Profil inklusive der erweiterten Bestätigung, so können sowohl auf Seiten des Empfängers als auch auf Seiten des Senders die Vollständigkeit der Übertragung gewährleistet und Unregelmäßigkeiten schnell erkannt werden.

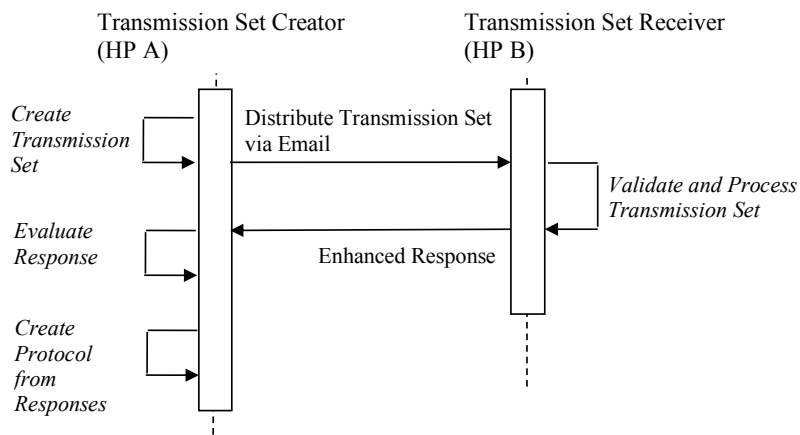


Abbildung 3.8.: Erweiterte Empfangsbestätigung mittels QCIT (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 14).

3.3.4. Teleradiologische Konstanzprüfung mittels QCIT

Die Implementierung der Option 'Zip over Email QC Request' ermöglicht es dem Sender des Requests, eine Konstanzprüfung zwischen zwei Teilnehmern anzustoßen und im Anschluss ein Protokoll über den Versand zu erhalten (Abbildung 3.9).

Wie in Tabelle 3.6 dargestellt, spezifiziert der Anforderer, zwischen welchen Partnern eine Konstanzprüfung durchgeführt werden soll. In seiner Anforderung (Listing 3.22) hat er weiterhin die Möglichkeit, einen bestimmten Testdatensatz anzugeben. Sollte dieser Datensatz nicht verfügbar sein, oder die Angabe in der Anforderung fehlen, so wird ein definierter Standarddatensatz für die Übertragung verwendet. Weiterhin hat der Anforderer unter Verwendung des Elements 'errorTimeout' die Möglichkeit, einen Timeout anzugeben, zu welcher Zeit er in jedem Fall ein Protokoll über den Transfer erhalten möchte, selbst wenn noch nicht alle Bilder übertragen wurden. Dies kann auf

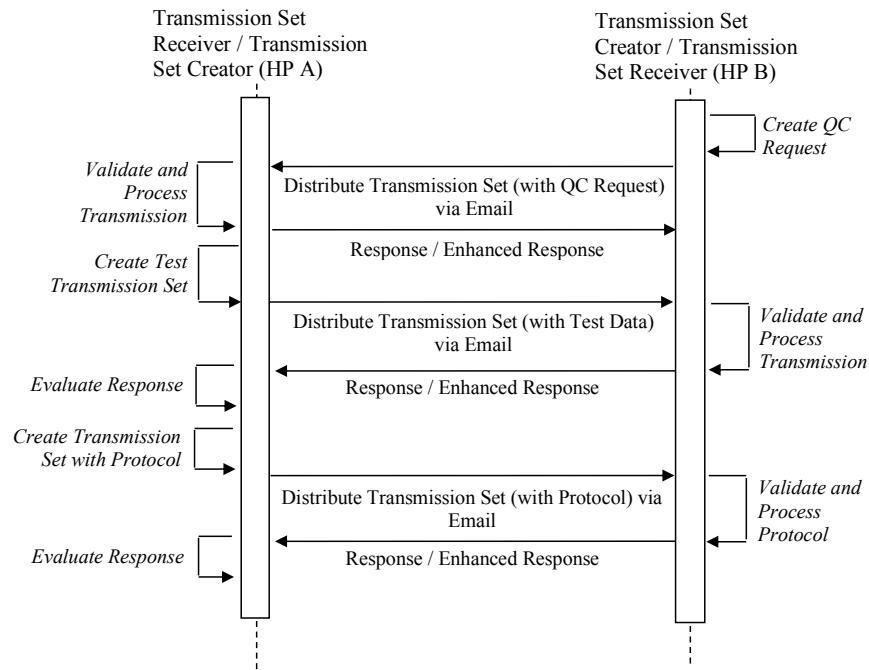


Abbildung 3.9.: Konstanzprüfung mittels QCIT (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 15).

der einen Seite nötig sein, falls die Übertragung sehr lange dauert, oder auf der anderen Seite, falls während der Übertragung Teile der Bilder verloren gehen.

Listing 3.22: Beispiel einer QC Anforderung mit QCIT

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <qcCheck version="1.0">
3   <dataReceiver>
4     <emailAddress>datarecevier@mail.test</emailAddress>
5   </dataReceiver>
6   <protocolReceiver>
7     <emailAddress>protocollrecevier@mail.test</emailAddress>
8   </protocolReceiver>
9   <dataSetUID>23.42.1.2.3.4.5.6</dataSetUID>
10  <errorTimeOut>900</errorTimeOut>
11 </qcCheck>
    
```

Nach Abschluss des Testtransfers erhält der angegebene Protokollempfänger ein detailliertes maschinenlesbares Protokoll der Übertragung im XML-Format. Dieses Protokoll kann sowohl dem Anwender angezeigt als auch automatisch ausgewertet werden, um so regelmäßige Prüfungen der Übertragungszeiten durchführen und dokumentieren zu können. Der Inhalt beziehungsweise die möglichen Ausprägungen des Protokolls sind in Tabelle 3.7 dargestellt.

Tabelle 3.6.: Elemente und Attribute für eine QCIT QC Request-Nachricht. [Opt.; Optionality: (R)required, (O)ptional - Mul.; Multiplicity] (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 24)

Name	Mul.	Opt.	Description
qcCheck	1	R	
qcCheck/dataReceiver	1	R	Receiver of the Transmission Set
qcCheck/dataReceiver/emailAddress	1	R	Email address
qcCheck/protocolReceiver	0-1	O	Receiver of the protocol
qcCheck/protocolReceiver/emailAddress	1	R	Email address
qcCheck/dataSetUID	0-1	O	Unique ID of the test data set
qcCheck/errorTimeOut	0-1	O	Timeout in [s] for sending the protocol, regardless of the test transfer status

Tabelle 3.7.: Elemente und Attribute für eine QCIT QC Protocol-Nachricht. [Opt.; Optionality: (R)required, (O)ptional - Mul.; Multiplicity] (Quelle: IHE Draft for Quality-Controlled Image Transfer (QCIT), S. 25)

Name	Mul.	Opt.	Description
qcProtocol	1	R	
../transmissionStatus	1	R	Status, COMPLETED if send and received mail count match, else ABORTED
../requestMessageID	1	R	Message ID of the QC Request mail
../transmissionSetMailsSentCount	1	R	Total mail count of the Transmission Set
../transmissionSetMailsRecConfirmed/mailSize	1	R	Total size of all confirmed mails in bytes
../transmissionSetMailsRecConfirmed/objectSize	1	R	Total size of all confirmed objects in bytes
../dataSender	1	R	
.././emailAddress	1	R	Email address
../dataRecipient	1	R	
.././emailAddress	1	R	Email address
../protocolRecipient	1	R	
.././emailAddress	1	R	Email address
../errorTimeOut	0-1	O	Timeout as specified in the request mail
../transmissionSetMail	1-N	R	
.././eMailMessageID	1	R	Message ID of the Transmission Set mail
.././errorCode	0-1	O	
.././submissionSet	1-N	R	
.././submissionSet/entryUUID	1	R	EntryUUID as defined in Metadata.XML
.././submissionSet/errorCode	0-1	O	
.././submissionSet/document	1-N	R	
.././submissionSet/./entryUUID	1-N	R	EntryUUID as defined in Metadata.XML
.././submissionSet/./errorCode	0-1	O	
.././startDateTime	1	R	Data transmission start date and time
.././notifyDateTime	1	R	Notification email receiving date and time
.././mailSize	1	R	Total size of all transmitted mails in bytes
.././objectSize	1	R	Total size of all transmitted objects in bytes

Hierbei ist es wichtig, zwischen der Anzahl und Größe der einzelnen E-Mails sowie der Anzahl und Größe eines einzelnen Objekts in einem Transmission Set zu unterscheiden.

Da jedes einzelne Objekt eindeutig einer E-Mail zugeordnet werden kann, ist es so auch möglich, Aussagen über die Qualität der Teleradiologiestrecke zu treffen.

3.4. Intersektorale Vernetzung mit IHE XDS

In Deutschland gibt es eine Reihe von Teleradiologienetzwerken, die auch heute schon genutzt werden, um gezielt Bilder und Dokumente auszutauschen. Im Rahmen dieser Vernetzung können Szenarien wie zum Beispiel Konsile oder die Verlegung eines Patienten zwischen zwei Krankenhäusern gut abgebildet werden. In der Vergangenheit beruhte die Kommunikation dieser Netzwerke fast ausschließlich auf DICOM E-Mail, anderen proprietären Lösungen oder zum Beispiel dem Einsatz von VPN und der direkten Vernetzung via DICOM Q/R und DICOM C-Store.

Obwohl es in solchen Netzwerken generell möglich ist, gemeinsam mit medizinischen Daten zu arbeiten, gewinnt die Vernetzung mittels IHE Cross-Enterprise Document Sharing (XDS) immer mehr an Bedeutung, um dadurch standardisierte Vernetzungslösungen zu schaffen. Mit dem Konzept einer XDS Affinity Domain mit einem zentralen Document Registry sowie bekannten und autorisierten Document Source und Document Consumer ist es möglich, Daten für zukünftige Akteure verfügbar zu machen, auch wenn sie aktuell noch nicht Teil des Netzwerks sind. Document Repositories fungieren hier als Datenspeicher und sammeln Daten für den späteren Zugriff berechtigter Akteure (Abbildung 3.10). Existieren mehrerer XDS Affinity Domains, so gibt es in jeder Affinity Domain eine eigene Document Registry. Der Austausch von Daten über die Grenzen der Affinity Domain hinweg kann dann mittels IHE XCA ermöglicht werden (Kapitel 2.1.8).

Die Verwendung von Cross-enterprise Document Sharing for Imaging (XDS-I) hilft den Datentransfer in solchen Netzwerken zu reduzieren, indem DICOM-Bilder an ihrer Quelle, dem primären PACS des Krankenhauses, verbleiben. Im Document Repository werden in diesem Fall lediglich die Referenzen auf die Originaldaten gespeichert, welche dann im Bedarfsfall direkt zwischen Document Consumer und Document Source ausgetauscht werden. Hierdurch behält das Primärsystem maximale Kontrolle über die DICOM-Daten, diese werden nur im Bedarfsfall zwischen den autorisierten Partnern

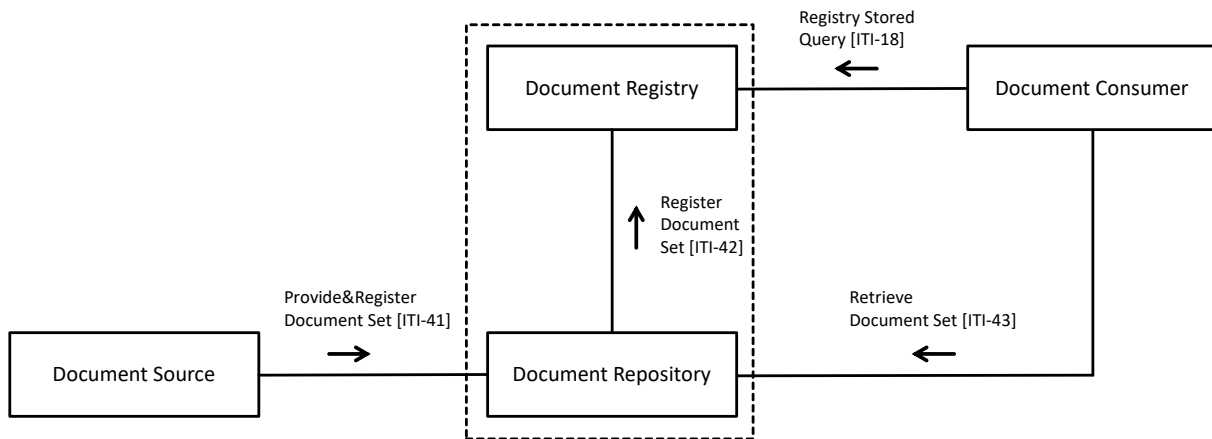


Abbildung 3.10.: Vereinfachter XDS-Workflow mit Aktoren und Transaktionen. Hierbei können Registry und Repository auch gruppiert werden und so die Funktionen einer Patientenakte abdecken. (Der vollständige XDS-Workflow ist unter https://wiki.ihe.net/index.php/Cross-Enterprise_Document_Sharing#Systems_Affected abgebildet, 05.08.2018).

übertragen. Dies bringt allerdings auch den Nachteil, dass bei tatsächlichem Zugriff große Datenmengen ad hoc übertragen werden müssen, um sie beim Document Consumer zur Anzeige bringen zu können (Abbildung 3.11).

Hierbei gibt es zwei grundlegende Probleme. Zum einen ist die Kompatibilität zu XDS beziehungsweise XDS-I in Deutschland aktuell noch sehr gering und es können nicht alle Geräte oder Systeme in einem Teleradiologienetzwerk durch reine XDS basierte Kommunikation angeschlossen werden. Zum anderen wird zwar Speicherplatz gespart, da Bilddaten nur in den Primärsystemen vorgehalten werden. Dadurch ergibt sich allerdings eine Verzögerung der Auslieferung dieser Daten beim Ad-hoc-Zugriff, da diese dann erst durch den Document Consumer von der Document Source abgerufen (engl. retrieved) werden müssen.

Aus diesen Gründen wurden im Rahmen dieser Arbeit mehrere Methoden zur flexiblen und performanten Anbindung von Primärsysteme ohne IHE-Funktionalität durch den Autor konzipiert und entwickelt.

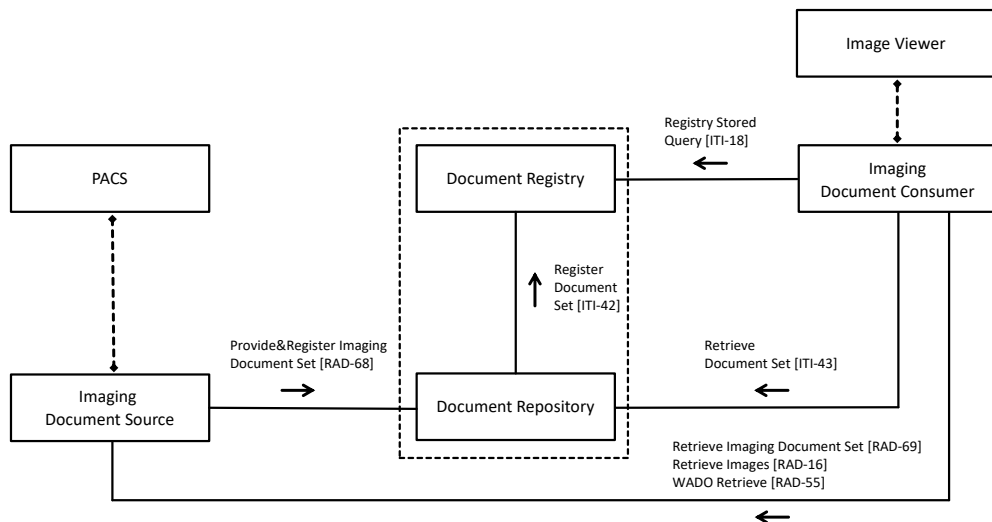


Abbildung 3.11.: Vereinfachter XDS-I Workflow für Bilddaten mit Aktoren und Transaktionen. Der vollständige XDS-I Workflow ist unter https://wiki.ihe.net/index.php/Cross-enterprise_Document_Sharing_for_Imaging#Systems_Affected abgebildet, 05.08.2018)

3.4.1. XDS-Adapter für Systeme ohne IHE-Unterstützung

Wie oben beschrieben, werden DICOM-Daten im XDS-Umfeld grundsätzlich anders als die sonstigen Dokumente behandelt. Aufgrund der Größe von DICOM-Bildern und der Tatsache, dass sie selten mit Standard-Bildbetrachtern geöffnet und angezeigt werden können, macht es keinen Sinn, diese mehrfach, also im PACS und im Document Repository, zu speichern. Daher generiert die Imaging Document Source, welche mit der primären Bildquelle (PACS, Modalität etc.) verknüpft ist, eine Referenz zu den Bildern und stellt nur diese Key Object Selection (KOS) dem Repository mittels einer Provide & Register Imaging Document Set Transaktion (RAD-68) zur Verfügung. Dieses KOS-Objekt wird nach Erhalt, wie in Abbildung 3.11 vereinfacht dargestellt, selbstständig vom Document Repository im Document Registry registriert (ITI-42). Ein KOS ist hierbei ein spezielles und kleines DICOM-Objekt ohne Pixeldaten beziehungsweise Bilddaten, welches nur Referenzen auf Bilder und ihre Quellen beinhaltet.

Sobald der Imaging Document Consumer im Document Registry nach den Bildern eines Patienten sucht (ITI-18), erhält er den Speicherort des KOS-Objekts, welches er dann aus dem zugehörigen Repository, falls er dazu berechtigt ist, abrufen kann (ITI-

43). Die Berechtigungsprüfung kann beispielsweise mit Hilfe des IHE Profiles Basic Patient Privacy Consents (BPPC) umgesetzt werden, welches aber nicht zwingend Teil des Workflows sein muss. Mit den im KOS enthaltenen Informationen ist es dem Consumer nun möglich, die DICOM-Daten aus der originären Quelle abzurufen und zur Anzeige zu bringen. Hierfür wird ein spezieller DICOM-Viewer benötigt, welcher meist Teil eines Imaging Document Consumer ist. Unter Verwendung dieses Workflows ist es nötig, dass Imaging Document Consumer und Imaging Document Source für den Transfer der Daten zum Beispiel via DICOM Query/Retrieve Protokoll (RAD-16) oder über das einfachere Web Access to DICOM Persistent Objects (WADO) direkt miteinander kommunizieren.

Da nicht alle PACS eine IHE konforme Schnittstelle besitzen, war es erforderlich, diese nachträglich durch das Implementieren eines IHE-Adapters zu ergänzen. Der neue XDS Imaging Document Source Adapter (Abbildung 3.12) erweitert die Schnittstellen des Primärsystems um die IHE Transaktion Provide and Register (RAD-68).

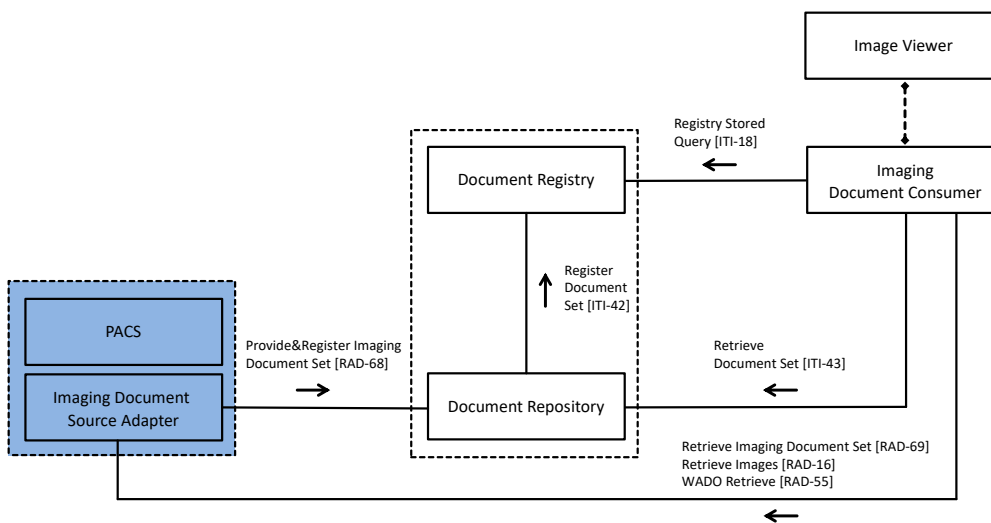


Abbildung 3.12.: PACS mit Adapter für XDS Imaging Document Source.

Der Imaging Document Source Adapter kommuniziert mit dem PACS über standardisierte DICOM-Schnittstellen wie DICOM C-Store oder DICOM Q/R und ermöglicht so dem Primärsystem die IHE XDS spezifische Kommunikation via Webservice. Als Trigger für die Kommunikation gibt es verschiedene Möglichkeiten.

DICOM basiert: Das Primärsystem sendet aktive Daten via DICOM C-Store zum Adapter. Dieser generiert aus allen Daten, die zum Beispiel in einer DICOM Association übermittelt werden, ein neues KOS-Objekt, welches im Anschluss in einem XDS SubmissionSet an das Document Repository übertragen wird. Als Quelle der Daten für den späteren DICOM Retrieve wird der RetrieveAETitle (0008,0054) des KOS-Objekts auf den AET des Primärsystems gesetzt, so dass die Daten im Bedarfsfall direkt aus dem PACS abgerufen werden können (Listing 3.23).

Listing 3.23: Auszug eines DICOM-Dumps für RetrieveAETitel und RetrieveLocationUID eines KOS-Objekts

```

1 (0008,0054) AE [SOURCE_PACS] # 10, 1 RetrieveAETitle
2 (0040,E011) UI [1.2.3.45.1.1.34.3.1] # 19, 1 RetrieveLocationUID
3 ...

```

Auf die gleiche Weise kann auch die XDS spezifische RetrieveLocationUID (0040,E011) für das Primärsystem ermittelt werden.

HL7 basiert: Ähnlich wie der direkte DICOM-Versand kann die Registrierung über den IHE-Adapter auch via HL7 angestoßen werden. Als Basis kann hier zum Beispiel eine HL7-Befundnachricht dienen. Sobald ein radiologischer Befund abgeschlossen ist, erhält der IHE-Adapter diesen als HL7-Nachricht und ruft darauf hin die entsprechenden Bilddaten aus dem primären PACS ab. Der Versand der HL7-Nachricht kann hierbei direkt durch das primäre PACS, aber auch zum Beispiel durch ein RIS oder über einen Kommunikationsserver angestoßen werden. Sobald die Bilder zur entsprechenden DICOM-Studie vollständig abgerufen werden konnten, generiert der IHE-Adapter wiederum das KOS-Objekt und sendet es in das angeschlossene Repository.

Neben den HL7-Befundnachrichten wie zum Beispiel ORU^R01, MDM^T01 oder MDM^T02 eignen sich auch Auftragsnachrichten wie ORM^O01 als Trigger, da sie direkt die Bilddaten betreffen und bereits die für eine XDS-Registrierung benötigten Metadaten enthalten. Grundsätzlich können aber auch andere HL7-Nachrichten als Trigger herangezogen werden.

Manuell durch den Benutzer: Weiterhin kann die Generierung des KOS-Objekts und dessen Versand auch manuell über den Adapter angestoßen werden. Hierbei werden die Daten dann vorher dem Adapter übergeben, und der Benutzer wählt händisch die entsprechenden Daten, aus denen ein KOS-Objekt erstellt werden soll, welches dann in einem XDS SubmissionSet an das Repository übertragen wird. So hat der Benutzer eine feingranulare Kontrolle, welche Daten per XDS registriert werden sollen.

Dies lässt sich nicht nur direkt im Versand-Plugin des IHE-Adapters auswählen, sondern kann alternativ auch über das Primärsystem erfolgen, indem nur ausgewählte Daten einer DICOM-Studie via DICOM C-Store an den Adapter übergeben werden.

Über das Dateisystem: Sollte das Primärsystem über keine DICOM-Schnittstelle verfügen und weder DICOM C-Store noch DICOM Q/R unterstützen, so können die Daten auch über ein Importverzeichnis auf einem Netzwerk-Share übergeben werden. Bei dieser Art der Registrierung legt das System alle relevanten DICOM-Daten in einen Ordner, welcher durch den IHE-Adapter regelmäßig abgefragt wird. In diesem Fall wird die Signalisierung des Abschlusses eines Transfers asynchron über ein Datei-Semaphor realisiert, so dass der Transfer als abgeschlossen gilt, sobald eine '.complete'-Datei im Ordner existiert. Zusätzlich kann ein Transfer als beendet markiert werden, sobald sich in einem definierten Zeitraum keine Änderungen an den Dateien mehr feststellen lassen. In beiden Fällen wird anschließend analog zu den obigen Varianten auch ein KOS-Objekt erzeugt und an das Repository übergeben. Da die Daten aber in diesem Fall später nicht per DICOM Q/R vom Primärsystem abgerufen werden können, muss hier für den späteren Retrieve eine alternative Methode verwendet werden.

3.4.2. Mapping von Metadaten zu XDS Value Sets

Werden Daten per XDS registriert, so müssen diese mit den entsprechenden Metadaten versehen werden, um die Dokumente bei der XDS Registry richtig anzulegen und eine spätere Suche und Filterung ermöglichen zu können. Hierbei sind die zu verwendenden

Metadaten innerhalb einer XDS Affinity Domain festgelegt und werden durch sogenannte Value Sets beziehungsweise Codes repräsentiert. Ein Value Set besteht im Normalfall aus:

Code: Der innerhalb einer Affinity Domain definierte und zu benutzende Code.

CodingScheme: Klassifizierung zusammenhängender Codes innerhalb einer Affinity Domain, meist durch eine OID repräsentiert.

DisplayName: Textuelle Beschreibung beziehungsweise der Anzeigename für den Benutzer (unter Umständen lokalisiert).

Der XDS Document.TypeCode (Listing 3.24) beschreibt zum Beispiel, um welche Art von Dokument es sich handelt.

Listing 3.24: Auszug aus der codes.xml für XDS Document.TypeCode

```

1 <CodeType name="Set_TypeCode" classScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983">
2   <Code code="T_BildRöntgen" codingScheme="1.2.276.0.76.4.177.1.0.30.5" display="Röntgen"/>
3   <Code code="T_BildAngio" codingScheme="1.2.276.0.76.4.177.1.0.30.5" display="Röntgen-Angiographie"/>
4   <Code code="T_BildCT" codingScheme="1.2.276.0.76.4.177.1.0.30.5" display="Computertomographie"/>
5   <Code code="T_BildMRT" codingScheme="1.2.276.0.76.4.177.1.0.30.5" display="Magnetresonanztomographie"/>
6   <Code code="T_BildMammo" codingScheme="1.2.276.0.76.4.177.1.0.30.5" display="Mammographie"/>
7   ...
8 </CodeType>

```

Value Sets und Codes sind ein übergeordnetes Konzept in IHE XDS, und ihre spezifische Ausprägung findet dadurch keine eindeutige Entsprechung im DICOM- oder HL7-Standard. Um bei einer Registrierung von PACS-Daten über den XDS-Adapter diese Codes automatisch anwenden zu können, müssen daher entsprechende Standardparameter gefunden oder ein Mapping implementiert werden.

Das IHE Document Sharing Metadata Handbook (ITI Technical Committee, 2018) gibt gute Hinweise zum Mapping auf IHE XDS Metadaten. Auch das IHE Technical File Radiology (ITI Technical Committee, 2019) beschreibt das Mapping von DocumentEntry Metadaten ausführlich. Jedoch sind nicht immer alle Informationen in der gewünschten Form verfügbar, da Modalitäten und Worklistprovider diese meist nicht einheitlich zur Verfügung stellen. Aus diesem Grund ist die Implementierung eines flexiblen Mappings unumgänglich.

Direktes Mapping zu DICOM Tags: Für spezielle Codes ist es möglich, diese auf eine Entsprechung des DICOM-Standards zu mappen. Diese Variante bietet sich zum Beispiel für den 'DocumentEntry.typeCode', der die Art des Dokuments in XDS genauer spezifiziert, an. Die Art der Aufnahme wird in DICOM durch das Feld Modality beschrieben. Hier entspricht die Modalität *CT* dann dem TypeCode *Computertomographie* und *MR* dem TypeCode *Magnetresonanztomographie*, welche im Listing 3.25 als Code 'T_BildCT' und 'T_BildMRT' auf den TypeCode aus Listing 3.24 abgebildet werden können.

Listing 3.25: Auszug aus der mappings.xml für Mapping von DICOM Modality nach XDS Document.TypeCode

```

1 < mappings >
2   < typeCode mappingType="code" classScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983" >
3     < mapping key="CR" code="T_BildRöntgen" />
4     < mapping key="DX" code="T_BildRöntgen" />
5     < mapping key="MG" code="T_BildMammo" />
6     < mapping key="MR" code="T_BildMRT" />
7     < mapping key="CT" code="T_BildCT" />
8     ...
9     < mapping key="" code="T_BildSonstige" />
10  < /typeCode >
11  ...
12 < / mappings >

```

AET basiertes Mapping: Codes wie der 'DocumentEntry.healthcareFacilityTypeCode', der die erstellende Institution, also zum Beispiel das Krankenhaus, das MVZ oder die Praxis, beschreibt, können durch ein AET basiertes Mapping abgebildet werden, da Daten aus unterschiedlichen Institutionen meist auch in den Primärsystemen bereits in unterschiedlichen Datenquellen gespeichert und auf unterschiedlichen Wegen kommuniziert werden.

Mapping über HL7-Felder: Findet zusätzlich zur reinen DICOM-Kommunikation zwischen XDS-Adapter und Primärsystem noch eine HL7-Kommunikation zum Beispiel aufgrund der Befundberichte statt, dann können auch beliebige Felder aus der HL7-Nachricht für ein Mapping herangezogen werden. Auf diese Weise kann dann unter anderem die Fachrichtung der erstellenden Institution (Chirurgie, Radiologie, Orthopädie

etc.) für den 'DocumentEntry.practiceSettingCode' auf die ausstellende Organisationseinheit des HL7-Befunds abgebildet werden.

Standardwerte: Für Codes wie zum Beispiel den 'DocumentEntry.classCode', der die Klasse beziehungsweise den Inhalt eines Dokuments festlegt, kann im Fall von DICOM-Bildern meist ein Standard angewendet werden, da es sich hier im Normalfall um reine Bilddaten handelt. Ähnliches gilt auch für den 'DocumentEntry.formatCode', der in diesem Szenario fast immer fest auf DICOM konfiguriert werden kann.

Sollten Codes nicht vollständig über ein automatisches Mapping abgebildet werden können, so bietet der XDS-Adapter auch die Möglichkeit, spezielle Mappings von Hand vorzunehmen zu können. Dies kann zum Beispiel für das Setzen des 'confidentialityCode' genutzt werden, sofern dieser nicht auch in einem HL7-Feld im Vorfeld übermittelt wurde.

3.4.3. Imaging Cache als Proxy für beschleunigtes Bildladen

Kommt der XDS-Adapter in einem Vernetzungsszenario zum Einsatz, so übernimmt dieser im ersten Schritt nur die XDS-Kommunikation mit dem Repository und erlaubt einem PACS ohne XDS-Funktionalität, auf diese Weise KOS-Objekte zu erstellen und sie in der Affinity Domain zu registrieren. Möchte ein XDS Consumer nun Zugriff auf die im PACS gespeicherten DICOM-Daten erhalten, so muss er die Daten direkt aus dem PACS abrufen.

Um diese Einschränkung zu eliminieren, können im XDS-Adapter auch Imaging Document Source und Imaging Document Consumer in einem Imaging Cache kombiniert werden (Abbildung 3.13). Der Imaging Cache hat einen dedizierten Speicher für DICOM-Bilder und übernimmt nach außen die Kommunikation mit dem XDS-Netzwerk. Die Größe des Caches kann an die aktuellen Gegebenheiten und Vorhaltezeiten für DICOM-Bilder angepasst werden.

Die registrierten DICOM-Studien verbleiben danach für einen schnellen Zugriff im Cache-Server. Die Invalidierung des Caches geschieht aufgrund des Studiendatums und

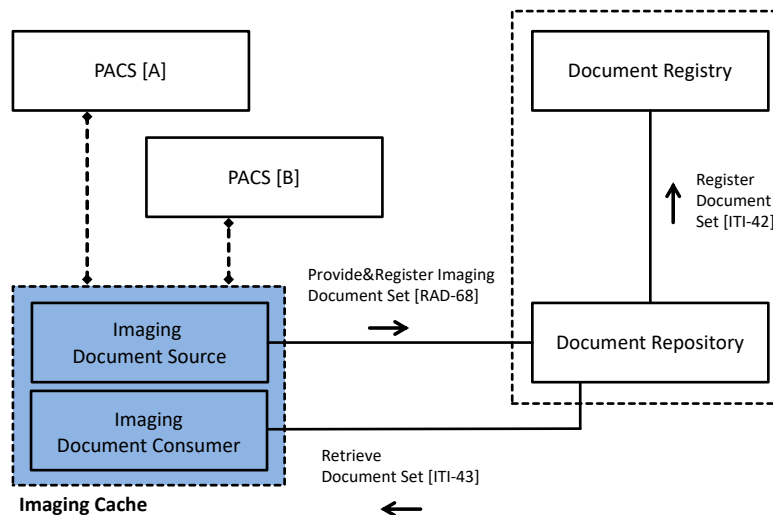


Abbildung 3.13.: XDS Imaging Cache zur Speichererweiterung und Performanceoptimierung der Document Source

der letzten Zugriffszeit auf die Bilddaten. Hierdurch wird gewährleistet, dass aktuelle und häufig angefragte Studien für den schnellen Zugriff im Cache verbleiben. Hierbei ist es zusätzlich möglich, den Imaging Cache als Proxy zu verwenden und mehr als ein Primärsystem an den XDS-Adapter anzuschließen.

Sobald eine DICOM-Studie eines Patienten angefragt wird, wird der reguläre XDS-Workflow durch einen Request auf den Imaging Cache Server ersetzt, welcher dann einen webbasierten DICOM-Viewer mit den angeforderten Bildern in Befundqualität ausliefert. Dies wird erreicht, indem der Cache aufgrund der übergebenen XDS Document ID das angeforderte KOS-Objekt aus dem Document Repository abrufen und die darin referenzierten Bilder dem Nutzer direkt aus dem Cache angezeigt. Sollten die Bilder in der Zwischenzeit aus dem Cache verdrängt worden sein, so werden diese direkt wieder aus dem PACS zurückgeholt und erneut mit aktuellerer Zugriffszeit im Cache Server abgelegt.

Dieser Workflow kann weiter optimiert werden, indem man Image Document Source und Consumer, wie in Abbildung 3.14 dargestellt, direkt in das PACS integriert. Dadurch wird die Größe des Caches auf das Maximum erhöht, da der Cache so grundsätzlich direkten Zugriff auf alle Bilder im PACS hat. Außerdem vereinfacht diese Kopplung die Transaktionen zwischen Imaging Document Source, Imaging Document Consumer,

PACS und Image Viewer, da alle Aktoren in einem System integriert sind und die Kommunikation schneller als über die standardisierten XDS-Schnittstellen abläuft.

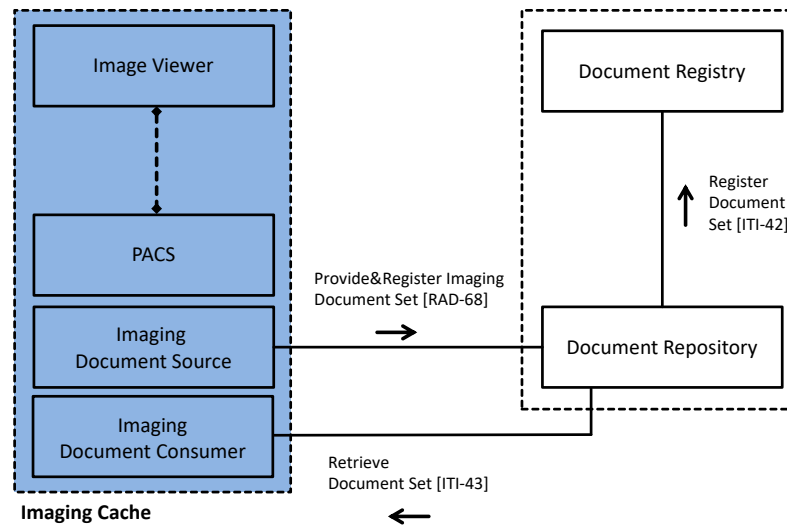


Abbildung 3.14.: Erweiterter Imaging Cache mit integriertem Image Viewer für DICOM-Daten

Auch bei Verwendung des Imaging Caches mit integriertem DICOM-Viewer ist es immer noch möglich, einzelne Studien zum Beispiel direkt via DICOM Q/R oder WADO von der Document Source abzufragen und so die Bilder auf einem externen System zur Anzeige zu bringen. Weiterhin ist an dedizierten Workstations ein Export oder Versand der DICOM-Daten für die Auswertung problemlos möglich.

3.4.4. Request-Broker für verteilte Bildablage

Wie oben dargestellt, bietet die Kopplung von Imaging Document Source und Consumer neben dem Caching Mechanismus noch zusätzlich eine erweiterte Streaming Funktionalität. Im regulären XDS-Workflow ruft ein Imaging Document Consumer meist die komplette Studie via DICOM Q/R oder WADO von der Imaging Document Source ab, bevor die Bilder in einem speziellen DICOM-Viewer zur Anzeige gebracht werden können. Obwohl dies weiterhin möglich ist, insbesondere um hier Standardkonformität mit anderen Systemen zu ermöglichen, kann der Cache-Server auch einen vollständigen und flexiblen webbasierten DICOM-Viewer ausliefern, in dem die Bilder angezeigt werden

können. Unter Verwendung dieses Webviewers ist es möglich, anstatt der vollständigen Studie nur den Teil der Bild-Studie zu übertragen (engl. streamen), welcher aktuell benötigt beziehungsweise betrachtet wird. Dies hat einen enormen Performancegewinn zur Folge und steigert die Nutzerakzeptanz aufgrund der verkürzten Wartezeiten, bis einzelne Bilder einer Studie zur Befundung dargestellt werden können.

Da eine XDS Affinity Domain grundsätzlich aus mehr als einer einzelnen Image Document Source und meist auch aus mehr als einem Krankenhaus beziehungsweise Krankenhausnetzwerk besteht, wurde das Konzept eines Image Request-Brokers etabliert. Der Request-Broker erlaubt den sicheren Zugriff auf Bilder in unterschiedlichen Krankenhäusern und ermöglicht außerdem einen sicheren Zugriff über das Internet (Abbildung 3.15).

Anstatt die Anfrage nach dem DICOM-Viewer direkt an einen Document Consumer weiterzuleiten, verarbeitet der Request-Broker alle Verbindungen zum Document Repository und extrahiert die wesentlichen Informationen aus den angefragten KOS-Objekten. Neben den Referenzen zu den DICOM-Studien enthält das KOS außerdem die Quelle der ursprünglichen Daten. Mit diesen Informationen ist es dem Request-Broker möglich, einen generellen DICOM-Viewer auszuliefern, der die Bilddaten direkt aus den entsprechenden Document Sources beziehungsweise Imaging Caches der einzelnen Standorte überträgt. Die Verbindung ist hierbei über einen Reverse Proxy sowie eine Web Application Firewall (WAF) gesichert, wodurch Verbindungen immer nur durch die Demilitarisierte Zone (DMZ) und nie direkt auf den betreffenden Cache Servern stattfinden.

Dieses Konzept erlaubt einen schnellen und sicheren Zugriff auf alle Bilder des Netzwerks über restriktive Firewalls und Security Policies, da die Kommunikation, ausschließlich per HTTPS gesichert, über eine DMZ erfolgt.

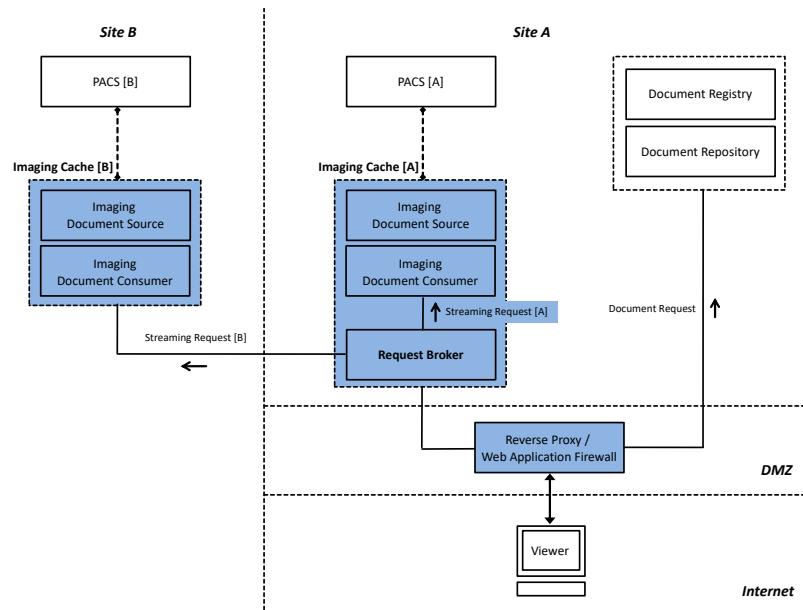


Abbildung 3.15.: Bild-Workflow unter Verwendung des Request-Brokers

3.5. Mobile Bildbetrachtung und Single-Sign-On mit IHE XDS

Für professionelle Anwender wie Ärzte und insbesondere Radiologen gibt es im Bereich der Bildbetrachtung zahlreiche PACS-Viewer, mit denen DICOM-Bilder in Befundqualität angezeigt werden können. Diese Viewer können sowohl direkt vom PACS-Hersteller an das eigene PACS angebunden sein oder über standardisierte Schnittstellen zum Beispiel via DICOM Q/R auf die Daten zugreifen. Solche Viewer bieten eine Vielzahl an befundungsrelevanten Basisfunktionen wie Zoomen, Verschieben (engl. panning), Invertieren, Fenstern (Kontraständerung an radiologischen Bildaufnahmen) und Messen als auch Spezialfunktionen wie die multiplanare Reformatierung (MPR), Maximumintensitätsprojektion (MIP), 3D-Darstellung oder Curved MPR, bei der der Rekonstruktionspfad frei gewählt werden kann, um so zum Beispiel Gefäße oder andere Strukturen darstellen zu können (Kumar, 2017; Dalrymple et al., 2005).

Neben diesen professionellen, meist eigenständigen Bildbetrachtern mit mächtigem Funktionsumfang existieren auch Basis-Viewer mit reduziertem Funktionsumfang, welche Bilder meist nicht in Befundqualität liefern können, aber für den gelegentlichen Ge-

brauch mit einem Tablet oder Smartphone ausreichende Bildqualität auch für klinische Anwender oder Patienten bieten.

Um jede Art von Viewer einfach in bestehende Strukturen einbinden zu können, wurde durch den Autor ein System für ein standardisiertes Single-Sign-On mit XDS-Komponenten konzipiert und implementiert.

3.5.1. CHILI/Mobile

Parallel zu der Erstellung dieser Arbeit entstand auch der Bildbetrachter CHILI/Mobile, welcher als Zero-Footprint-Viewer vollständig auf HTML5 und JavaScript basiert. Der Viewer kann daher in jedem Browser sowohl auf dem Desktop als auch auf einem Tablet wie zum Beispiel einem iPad oder einem Smartphone verwendet werden (Abbildung 3.16).



Abbildung 3.16.: CHILI/Mobile mit direktem Aufruf im Browser (links) oder auf dem Smartphone (rechts).

Um den Viewer ohne größere Anpassungen in verschiedenen Browsern sowie Tablet- und Smartphone-Betriebssystemen verwenden zu können, wurde bei der Entwicklung ausschließlich HTML5 und JavaScript eingesetzt. Um auf spezielle Hardware wie zum Beispiel den Touchscreen oder die Kamera eines Smartphones zuzugreifen und die Web-

Applikation nahtlos in das Betriebssystem zu integrieren, kamen entsprechende Frameworks wie Sencha Touch (<https://www.sencha.com>, 10.06.2019) und PhoneGap (<https://phonegap.com>, 10.06.2019) beziehungsweise Apache Cordova (<https://cordova.apache.org>, 10.06.2019) zum Einsatz. Durch die ausschließliche Verwendung von Web-Technologien ist der Viewer ohne die Verwendung eines App-Stores immer sofort einsetzbar, sofern eine Verbindung zum Server besteht.

Dies ist grundsätzlich keine Einschränkung, da eine Offline-Funktion des Viewers nicht vorgesehen ist, weil alle DICOM- und nicht-DICOM-Bilder per WADO-Protokoll vom Server ausgeliefert werden. Hierbei werden die Daten von DICOM nach JPEG konvertiert, um eine flüssige Anzeige auch auf älteren mobilen Geräten gewährleisten zu können. Durch diese Art der Bildkompression und durch die Anzeige direkt im Browser des Geräts kann nicht sichergestellt werden, dass die Daten immer in der korrekten Qualität angezeigt werden, da die meisten Browserhersteller aus dem Consumer-Bereich kommen und die Anzeige von Bildern unter Umständen selbst noch einmal optimieren und komprimieren. Daher kann CHILI/Mobile selbst bei korrekter Kalibrierung eines Tablets nicht zur Befundung verwendet werden (Kapitel 2.3.2).

3.5.2. Single-Sign-On

Um das CHILI/Mobile in beliebige andere Anwendungen integrieren zu können, wurde im Rahmen dieser Arbeit durch den Autor ein Single-Sign-On (SSO) Verfahren auf Basis der Security Assertion Markup Language (SAML) implementiert (OASIS Security Services TC, 2008) und in den Viewer integriert.

SAML ist ein XML-basiertes Framework, um Authentifizierung und Autorisierung zwischen zwei Entitäten, dem Service Provider und dem Identity Provider, zu realisieren. Der Service Provider vertraut dem Identity Provider die Authentifizierung der Nutzer, Knoten oder Systeme an, und im Gegenzug erstellt der Identity Provider sogenannte Authentication Assertions, die bestätigen, dass sich der Nutzer oder das System beim Identity Provider authentifiziert hat. Im Gegensatz zu anderen proprietären tokenbasierten Authentifizierungsverfahren ist SAML ein standardisiertes SSO-Format, bei dem die

Authentifizierungsinformationen mittels XML-Dokumenten übertragen werden (Hardt et al., 2014), welche mit Hilfe von X.509-Zertifikaten digital signiert wurden (Pedersen, 2005; Cooper et al., 2008). Durch das standardisierte Format ist es leicht möglich, eine Vertrauensbasis zwischen Entitäten unterschiedlicher Hersteller aufzubauen. Weiterhin ist es durch die lose Kopplung mit Hilfe von SAML nicht nötig, die Benutzerinformationen in beiden Applikation zu verwalten, da die aufgerufene Applikation nicht den eigentlichen Benutzer, sondern nur dessen Rolle und Rechte kennen muss.

Abbildung 3.17 stellt die Schritte der Authentifizierung mittels SAML Token dar.

1. Der Benutzer beziehungsweise Client oder Dienst authentifiziert sich mit seinen Zugangsdaten (zum Beispiel Benutzername und Passwort) gegenüber dem Identity Provider.
2. Der Identity Provider erzeugt ein SAML Token für den Nutzer und signiert es digital mit einem X.509 Zertifikat.
3. Der Nutzer sendet nun einen Request an den Service Provider, von dem er einen Dienst in Anspruch nehmen will. Dem eigentlichen Request fügt er das vom Identity Provider erzeugte und signierte Token an.
4. Der Service Provider prüft das mitgelieferte Token anhand der Signatur des Identity Providers und liefert bei Erfolg den Service beziehungsweise die angefragten Daten ohne weitere Prüfung von Benutzername und Passwort an den Nutzer zurück.

Hierbei findet keinerlei Kommunikation zwischen Identity Provider und Service Provider statt, alle Kommunikation geht ausschließlich vom Nutzer beziehungsweise Client aus.

Listing 3.26 zeigt ein einfaches SAML Token, welches von einem Identity Provider für den Nutzer 'dr_test' ausgestellt und digital signiert wurde. Das Token soll bis zu 30 Sekunden nach der Ausstellung gültig sein und dem Nutzer authentifizierten Zugriff auf die Applikation des Service Providers gewähren.

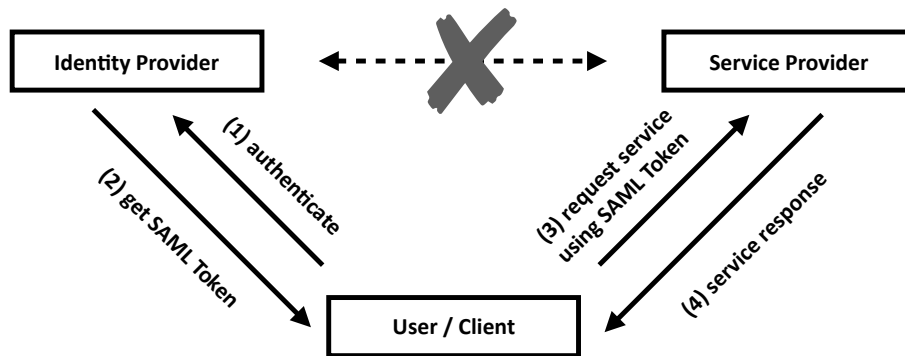


Abbildung 3.17.: Authentifizierung von Nutzern und Diensten mittels SAML Token.

Listing 3.26: Aufbau eines SAML Token

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
3   ID="_0xa8c060a1.1683057746.1505649330769.0" IssueInstant="2018-09-17T11:55:28.318Z" Version="2.0">
4   <saml2:Issuer>http://chili-radiology.com</saml2:Issuer>
5   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
6     <ds:SignedInfo>
7       <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
8       <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
9       <ds:Reference URI="#_0xa8c060a1.1683057746.1505649330769.0">
10        <ds:Transforms>
11          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
12          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
13        </ds:Transforms>
14        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
15        <ds:DigestValue>nEckRjCoh3/HAV9e5orp7+TzZnE=</ds:DigestValue>
16      </ds:Reference>
17    </ds:SignedInfo>
18    <ds:SignatureValue>Ho7s9pjt/8wdsee6waEmmnuIS/hEh...</ds:SignatureValue>
19    <ds:KeyInfo>
20      <ds:X509Data>
21        <ds:X509Certificate>MIIHATCCBVGgAwIBAgIDEAAvMA0GCSqGSIb3DQEBBQUAMIGgBQUAMIGg34
22          CBMSQmFkZW4gV3VlcnR0ZW1iZXJnMREwDwyYDVQHEwhXYWxsZG9yZjEMMAoGA1UEChMDSUNXMR4w
23          HAYDVQLExVDZXJ0aWZpY2F0ZSBDbXR0b3JpdHgg7xVvVwP8iHLxkz38hXYWxsZG9yZjEMMb3D...
24        </ds:X509Certificate>
25      </ds:X509Data>
26    </ds:KeyInfo>
27  </ds:Signature>
28  <saml2:Subject>
29    <saml2:NameID>dr_test</saml2:NameID>
30    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
31  </saml2:Subject>
32  <saml2:Conditions NotBefore="2018-09-17T11:55:28.318Z" NotOnOrAfter="2018-09-18T11:55:58.318Z">
33    <saml2:AudienceRestriction>
34      <saml2:Audience>http://chili-radiology.com</saml2:Audience>
35    </saml2:AudienceRestriction>
36  </saml2:Conditions>
37  <saml2:AuthnStatement AuthnInstant="2018-09-17T11:55:28.318Z">
38    <saml2:AuthnContext>
39      <saml2:AuthnContextClassRef>
40        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
41      </saml2:AuthnContextClassRef>
42    </saml2:AuthnContext>
43  </saml2:AuthnStatement>
44 </saml2:Assertion>

```


3.5.3. Tokenbasierter Aufruf

Die Verwendung des oben beschriebenen Mechanismus ermöglicht, das CHILI/Mobile tokenbasiert aus jeder anderen Anwendung aufzurufen beziehungsweise die Webanwendung in andere Anwendungen nahtlos einzubetten. Der Aufruf erfolgt mittels eines HTTP POST-Requests zum Server, welcher dann eine vollständige parametrisierte Webanwendung zurückliefert (Listing 3.27).

Listing 3.27: Beispielaufruf des CHILI/Mobile mittels SAML Token und übergebenen Parametern

```

1 <?xml version='1.0' encoding='UTF-8'?>
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" 'http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd'>
3 <html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en'>
4   <body onload='document.forms[0].submit()'>
5     <form method='POST' action='http(s)://[server-address](:[port])/chili/servlet/doChiliWebClient?client=[Clientname]'>
6       <input type='hidden' name='Clienttype' value='[mobile|applet]' />
7
8       <input type='hidden' name='SAMLResponse' value='[BASE64-encoded]' />
9       <input type='hidden' name='StudyInstanceUIDs' value='[uid1,uid2,...]' />
10
11       <input type='hidden' name='[parameter]' value='[value1,value2,...]' />
12     </form>
13 </body>
14 </html>

```

Bei einem Aufruf werden alle benötigten Parameter als POST-Parameter übergeben. Das SAML Token wird hierbei mittels Base64 codiert (Josefsson, 2006) und als 'SAML-Response' übergeben. Basisparameter sind hierbei:

Clientname gibt den Namen des Clients an und beschreibt damit die auf dem Server hinterlegte Konfiguration für den Aufruf. Hierdurch können verschiedene Viewer mit unterschiedlichen Basiskonfigurationen (zum Beispiel mit Plugin für Versand oder Druck) geladen werden.

Clienttype legt den Typ des Clients fest. Hierdurch kann zwischen mobiler Applikation, Java Applet, WebStart oder lokaler Installation unterschieden werden.

SAMLResponse übermittelt das SAML Token, welches die Berechtigung des Benutzers beziehungsweise der aufrufenden Applikation beinhaltet (Base64-codiert).

Als Aufrufparameter und zur Steuerung des CHILI/Mobile können auch beliebige weitere Parameter wie zum Beispiel eine StudyInstanceUID für den initialen Aufruf einer DICOM-Studie übergeben werden.

Signierter Aufruf

Da das SAML Token nur die Berechtigung des Benutzers für diesen Request transportiert, kann dadurch vom Empfänger nicht geprüft werden, ob der Aufruf ohne Manipulation der Parameter übermittelt wurde. Ein Angreifer könnte also beispielsweise den Request abfangen und das SAML Token verwenden, um eine valide Abfrage für eine völlig andere StudyInstanceUID zu generieren. Die Kommunikation zwischen Client und Server findet zwar grundsätzlich via HTTPS und damit auch verschlüsselt statt, aber auch hier sind Man-in-the-Middle (Mallik et al., 2019) Angriffe bekannt (Dacosta et al., 2012).

Aus diesem Grund wurden dem Aufruf zur Absicherung des Request noch eine Signatur der verwendeten Parameter hinzugefügt (Listing 3.28).

Listing 3.28: Aufruf mittels SAML Token und signierten Parametern

```

1 <?xml version='1.0' encoding='UTF-8'?>
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" 'http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd'>
3 <html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en'>
4   <body onload='document.forms[0].submit()'>
5     <form method='POST' action='http(s)://[server-address](:[port])/chili/servlet/doChiliWebClient?client=[Clientname]'>
6       <input type='hidden' name='Clienttype' value='[mobile|applet]' />
7
8       <input type='hidden' name='SAMLResponse' value='[BASE64-encoded]' />
9       <input type='hidden' name='StudyInstanceUIDs' value='[uid1,uid2,...]' />
10
11      <input type="hidden" name="NormalizedInput"
12        value="SAMLResponse,StudyInstanceUIDs,NormalizedInput,PublicCertificate,SignatureMethod" />
13
14      <input type="hidden" name="PublicCertificate" value="[BASE64-encoded]" />
15      <input type="hidden" name="SignatureMethod" value="http://www.w3.org/2000/09/xmlsig#rsa-sha1" />
16      <input type="hidden" name="SignatureValue" value="[BASE64-encoded]" />
17    </form>
18  </body>
19 </html>

```

Alle für den Aufruf relevanten Parameter werden miteinander verkettet und anschließend mit dem privaten Schlüssel des Aufrufers unterschrieben.

NormalizedInput enthält eine kommaseparierte Liste aller Felder, die Teil der Signatur sind. Hierbei ist wichtig, dass auch das Feld 'NormalizedInput' selbst in der Liste enthalten ist, da dies sonst wieder Ziel für Manipulationsversuche sein kann.

PublicCertificate enthält das öffentliche Zertifikat des Aufrufers. Hierdurch kann sichergestellt werden, dass der Aufrufer wirklich im Besitz des passenden öffentlichen und privaten Schlüsselpaars ist und der Request wirklich von ihm kam.

SignatureMethod beschreibt die Signaturmethode (zum Beispiel rsa-sha1), die zur Signatur verwendet wurde.

SignatureValue enthält die eigentliche Signatur der im Feld 'NormalizedInput' angegebenen Parameter.

Durch diese Erweiterung des Aufrufs ist sichergestellt, dass auf dem Transport zwischen Sender und Empfänger keine Manipulation der übergebenen Parameter stattfinden kann.

Tokenbasierter Aufruf und IHE XDS

Um zusätzlich zum Aufruf von DICOM-Daten via StudyInstanceUID das CHILI/Mobile auch als XDS Consumer verwenden zu können, wurde als Ergänzung zu den Standardaufrufparametern des PACS Viewers die Option zur Übergabe eines XDS DocumentSetRequests implementiert.

Listing 3.29: Beispiel eines XDS DocumentSetRequest

```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
3   <DocumentRequest>
4     <HomeCommunityId>1.2.840.113619.20.2.42.9</HomeCommunityId>
5     <RepositoryUniqueId>1.2.840.113619.20.2.42.9</RepositoryUniqueId>
6     <DocumentUniqueId>xds.6922442060180590602</DocumentUniqueId>
7   </DocumentRequest>
8 </RetrieveDocumentSetRequest>

```

Der DocumentSetRequest (Listing 3.29) gibt mit den drei Parametern HomeCommunityId, RepositoryUniqueId und DocumentUniqueId das XDS-Dokument, welches im Viewer zur Anzeige gebracht werden soll, eindeutig an.

HomeCommunityId: Die ID der Community (Affinity Domain), in der der Request gültig ist beziehungsweise in der sich das DocumentRepository befindet.

RepositoryUniqueId: Die eindeutige ID des Repositories, in dem sich das Dokument beziehungsweise KOS-Objekt befindet.

DocumentUniqueId: Die ID des Dokuments, welches abgerufen beziehungsweise angezeigt werden soll.

Der 'documentSetRequest' kann dann bei Aufruf des Viewers als Base64-codierter POST-Parameter übergeben werden (Listing 3.30).

Listing 3.30: Input-Feld des DocumentSetRequest bei Aufruf des CHILI/Mobile

```

1 <input type='hidden' name='documentSetRequest' value='PD94bWwgdmVyc2lvbj0iMS4wI
2 iBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InlleyI/PjxSZXRyaWV2ZURvY3VtZW50U2V0UmVx
3 dWVzdCB4bWxucz0idXJuOmloZTppdGk6eGRzLWI6MjAwNyI+ICA8RG9jdW11bnRSZXF1ZXN0PiAgICA
4 8SG9tZUNvbW11bml0eUlkPjEuMi44NDAAuMTEzNjE5LjIwLjIuNDIuOTwvSG9tZUNvbW11bml0eUlkPi
5 AgICA8UmVwb3NpdG9yeVVuaXF1ZUIkPjEuMi44NDAAuMTEzNjE5LjIwLjIuNDIuOTwvUmVwb3NpdG9ye
6 VVuaXF1ZUIkPjAgICA8RG9jdW11bnRVbmlxdWVJZD54ZHMuNjkyMjQ0MjA2MDE4MDU5MDYwMjJwvRG9j
7 dW11bnRVbmlxdWVJZD4gIDwvRG9jdW11bnRSZXF1ZXN0PjwvUmV0cmlldmVEb2N1bWVudFNldFJlcXV
8 lc3Q+' />

```

Ein vollständiges Beispiel für den Aufruf des Viewers mit SAML Token und XDS DocumentSetRequest befindet sich im Anhang A.7.

3.6. Workfloworientierte Vernetzung und Portale

Im Bereich der Teleradiologie findet heute die Kommunikation vorwiegend elektronisch statt. Der DICOM-Standard hat die Grundlage für die Teleradiologie geschaffen, und Interoperabilität ist dank standardisierter Übertragung in den überwiegenden Fällen gegeben. Sobald es aber zur Anforderung einer Untersuchung per Teleradiologie kommt, wird der Workflow meist noch analog abgebildet. Die Untersuchungsanforderung der MTRA wird per Telefon übermittelt, und die Rechtfertigende Indikation (RI) des Teleradiologen wird dann per Fax zusammen mit der Untersuchungsanordnung zurückgeschickt. Der elektronische Workflow setzt erst bei der Übermittlung der Bilder und der Befundschreibung ein, wobei der fertige Befund dann teilweise noch per Fax übermittelt wird.

Ähnlich sieht es bei der Befundübermittlung zum Patienten und der Weitergabe seiner Bilder an ihn selbst oder an ärztliche Kollegen aus. Der Befund wird zuweilen noch ausgedruckt und dem Patienten auf dem Postweg zugesendet. Bilder werden zwar elektronisch aufgenommen, aber dann entweder ausgedruckt oder zumindest auf CD dem Patienten mitgegeben. Der Zuweiser des Patienten ist meist nicht direkt per Teleradiologie mit der Klinik beziehungsweise Radiologie verbunden und erhält somit die Bilder und den Arztbrief auch nur durch den Patienten als Überbringer.

Um hier eine Lösung für die Teleradiologie zu schaffen, wurde das bestehende Produkt CHILI/Medizinakte weiterentwickelt. Bei der Medizinakte handelt es sich nicht in erster Linie um eine klassische Patienten- oder Gesundheitsakte (Haas and Bertelsmann Stiftung, 2017; Warda, 2005) beziehungsweise eine EFA oder EPA (Kapitel 2.4.3), sondern vielmehr um eine konfigurierbare Lösung, mit der beliebige Akten-Systeme frei konfiguriert werden können.

Neben einem Einsatz als Studiendokumentationssystem für klinische Studien (Bougatf et al., 2012a) lässt sich die Medizinakte auch flexibel als Patientenportal oder Zuweiserportal für den externen Zugriff auf Daten durch Ärzte oder Patienten konfigurieren.

Die Medizinakte ist mandantenfähig und stellt ein Gruppen/Rechte/Rollen-Konzept zur Benutzerverwaltung bereit. Einzelne Typen von Akteneinträgen, Felder und Ausprägungen der Einträge können zur Laufzeit frei definiert werden. Neben einem Upload für nicht-DICOM- sowie DICOM-Daten ist auch eine Integration des befundfähigen DICOM-Viewers bereits vorhanden. Weiterhin existiert eine Integration des TMF-PID Generators, um Patientendaten auch anonymisiert beziehungsweise pseudonymisiert speichern zu können (TMF ToolPool Gesundheitsforschung, 2005; Faldum and Pommereining, 2005).

Die CHILI/Medizinakte ist aufgrund ihrer flexiblen Konfiguration bereits mehrfach als Aktensystem für klinische Studien im Einsatz (Müller-Mielitz et al., 2010; Bougatf et al., 2012b).

Durch ihre zahlreichen Konfigurationsmöglichkeiten eignet sich die CHILI/Medizinakte als Grundsystem für ein Teleradiologie- oder Patientenportal, muss aber um

workflowspezifische Komponenten erweitert werden, um alle Aspekte eines Portals abdecken zu können. Weiterhin war es nötig, das Userinterface mit einem modernen Web-Framework neu zu implementieren, um Entwicklungen in aktuellen Browsern und Mobilgeräten berücksichtigen zu können.

3.6.1. Umstellung auf ein aktuelles Web-Framework

Im Rahmen der Bachelorarbeit 'Konzeption und Implementierung der Migration verschiedener Web-Frameworks am Beispiel der CHILI/Telemedizinakte und PrimeFaces' (Jungmann, 2016) wurde das bestehende Frontend der Medizinakte untersucht und verschiedene Web-Frameworks evaluiert. Ziel der Arbeit war es, unter Beibehaltung des existierenden Backend ein modernes Framework für die Medizinakte zu wählen, welches dem aktuellen Stand der Technik entspricht und mit dem sich auch zukünftige Erweiterungen und Weiterentwicklungen einfach realisieren lassen.

Ist-Zustand der Medizinakte

Die Medizinakte basiert im Backend auf Oracle Java (<https://www.java.com>, 04.04.2019) und dem Database Management System (DBMS) PostgreSQL (<https://www.postgresql.org>, 04.04.2019). Zusätzlich kommen folgende weiteren Technologien, Frameworks und Erweiterungen zum Einsatz:

JSP: JavaServer Pages werden verwendet, um Java Code in Webseiten einzubetten und so das Userinterface mit dem Backend zu verbinden (Bergsten, 2003).

JSF: JavaServer Faces bieten ein Abstraktionslayer, um mittels Templating JSP Code zu erzeugen (Bergsten, 2004).

Apache MyFaces: MyFaces ist eine Referenzimplementierung der JavaServer Faces Spezifikation. In der Medizinakte wird aktuell Version 1.1 eingesetzt (The Apache Software Foundation, 2004).

MyFaces Tomahawk: Tomahawk ist eine Komponentenbibliothek, die MyFaces um zusätzliche (Workflow-)Komponenten erweitert (The Apache Software Foundation, 2007).

Ajax4Jsf: Um clientseitige Validierung und andere Ajax-Funktionalität in der Medizinakte zu ermöglichen, wird aktuell Ajax4Jsf verwendet (Katz, 2008).

Apache Tomcat: Als Applikationsserver für die Medizinakte kommt aktuell ein Apache Tomcat Version 7 zum Einsatz (Vukotic and Goodwill, 2011).

Auswahl der einzusetzenden Technologien

Bei einer Auswahl der Technologien wurden zwei Kernpunkte untersucht, zum einen die Performance und Leistungsfähigkeit der Technologie im Hinblick auf große Datenmengen und deren Visualisierung im Frontend, zum anderen die Migrationsfähigkeit der Lösungen durch eine Literaturrecherche und Prototyping, um einen reibungslosen Übergang gewährleisten zu können.

Neben gängigen JSF-Frameworks wie PrimeFaces (<https://www.primefaces.org>, 04.04.2019), ICEfaces (<http://www.icesoft.org>, 04.04.2019) und RichFaces (<https://richfaces.jboss.org>, 04.04.2019) wurden auch reine JavaScript-Frameworks wie AngularJS (<https://angularjs.org>, 04.04.2019) und React (<https://reactjs.org>, 04.04.2019) betrachtet.

Durch die Gegenüberstellung der unterschiedlichen Lösungen und Lösungsansätze wurde klar, dass ein Umstieg auf eine andere Technologie wie ein JavaScript-Framework neben einer Umstellung des Userinterface auch eine Neuimplementierung des Backends erforderlich machen würde. Somit wurde entschieden, die grundsätzliche Technologie beizubehalten, ein modernes JSF-Framework zu wählen und gleichzeitig die darunterliegende JSF Implementierung auf eine aktuelle Version (JavaServer Faces 2.2) anzuheben.

Eine Evaluation der in Frage kommenden JSF-basierten Frameworks (PrimeFaces, ICEfaces und RichFaces) wurde auf Basis von Geschwindigkeitsmessungen der unterschiedlichen Frameworks mit konkreten Testdaten aus bestehenden Installationen der

Medizinakte durchgeführt (Jungmann, 2016). Hauptsächlich aus Performancegründen fiel die Wahl auf die Bibliothek PrimeFaces (Varaksin and Caliskan, 2013).

Umsetzung

Um eine reibungslose Migration zu gewährleisten, wurde das Frontend der Medizinakte sukzessive auf die neue Technologie umgestellt. Zuerst wurden nötige Anpassungen am Backend vorgenommen und Komponenten wie Apache Tomcat und MyFaces auf eine aktuelle Version umgestellt. Im Anschluss wurde unter Beibehaltung der Backendfunktionalität parallel zum existierenden Frontend der Medizinakten ein zweites Frontend implementiert, welches auch bei existierenden Installationen zeitgleich mit der bestehenden Version betrieben werden konnte.

Durch die Migrationen konnten folgende Kernpunkte erreicht werden:

- Modernes LookAndFeel mit responsivem Design für mobile Endgeräte (Abbildung 3.18)
- Durchgehende Verwendung von Ajax im Frontend für clientseitige asynchrone Requests
- Performanccsteigerung gegenüber der bestehenden Medizinakte
- Schaffung der Grundlage für aktuelle REST-Webschnittstellen zu anderen Komponenten und Fremdsoftware
- Umstellung von JSP auf JSF mit Implementierung eines Templating auf Basis von JSF 2.2 für alle Webseiten
- Vereinfachung der Benutzer- und Rechteprüfung für Webseiten der Medizinakte
- Vereinfachung der Implementierung und Wartung durch Refactoring und Abbau von technischen Schulden (Fowler, 2002)

3.6.2. Integration eines mobilen Bildbetrachters und Uploaders

Um die Medizinakte vollständig auf mobilen Endgeräten einsetzen zu können, wurden neben der Umstellung auf ein responsives Design (Glassman and Shen, 2014; Peng and Zhou, 2015) auch der neu entwickelte mobile Bildbetrachter (Kapitel 3.5.1) sowie ein auf HTML5-basierender Uploader für DICOM- und nicht-DICOM-Daten integriert, welcher im Rahmen der Masterarbeit 'Konzeption und Entwicklung eines plattformunabhängigen Patienten-CD-Uploads' (Krentzlin, 2017) entwickelt wurde.

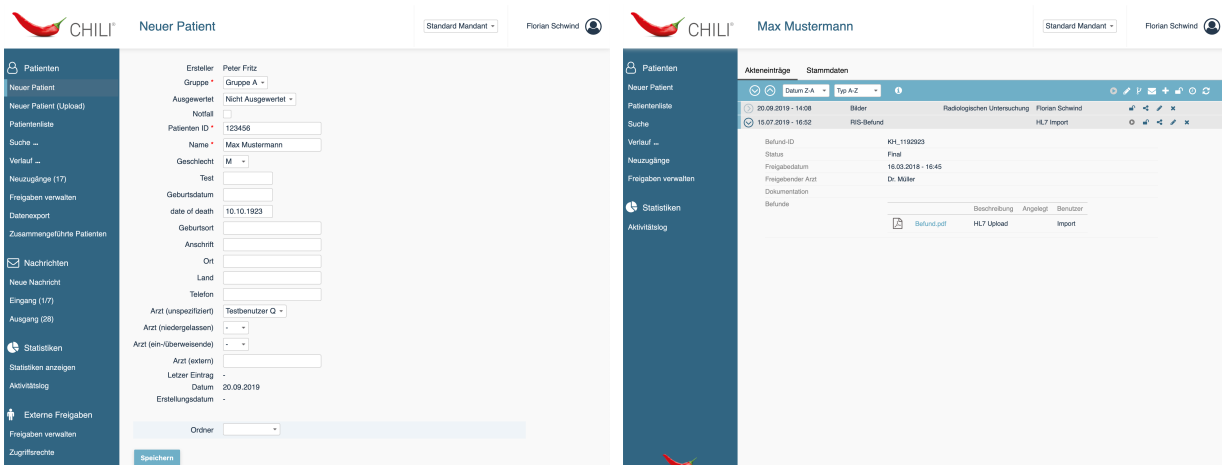


Abbildung 3.18.: CHILI/Medizinakte mit neuem Userinterface zum Erstellen (links) und Anzeigen (rechts) von Einträgen.

3.6.3. Schnittstellen

Einträge in der Medizinakte können durch einen Benutzer mit entsprechender Berechtigung eingesehen und erstellt werden. Um die Medizinakte nach außen zu öffnen und dadurch das automatisierte Erstellen von Einträgen zu erlauben, wurden unterschiedliche Schnittstellen für die verschiedenen Subsysteme im Krankenhaus implementiert (Abbildung 3.19).

Neben der manuellen Eingabe durch Benutzer können Akteneinträge auch über folgende Schnittstellen erstellt und bearbeitet werden:

HTTP: Eine neue Akte oder ein Akteneintrag kann durch Verwendung der REST-Schnittstelle via HTTP angelegt werden. Diese Variante wird von den meisten

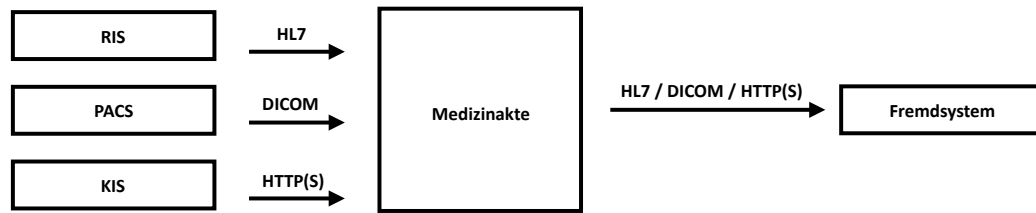


Abbildung 3.19.: Schnittstellen der Medizinakte zu unterschiedlichen Systemen

KIS-Herstellern unterstützt, da diese bereits heute einen ULN-Aufruf in ihr System integriert haben und so neue Akten mit Parametern aus den Patientenstammdaten anlegen können. Der REST-Aufruf dient weiterhin als Basisvariante und ermöglicht so den einfachen Anschluss einer Vielzahl von Fremdsoftware ohne DICOM- oder HL7-Schnittstellen.

HL7: Durch ein Mapping von HL7-Feldern und -Segmenten können Akteneinträge auch per HL7 gefüllt werden. Dies kommt insbesondere bei der Kommunikation mit einem RIS oder über einen Kommunikationsserver zum Einsatz. Neben Einträgen in Akten können auf diese Weise auch PDF- oder Text-Befunde von einem RIS oder KIS in die Akte übermittelt werden.

DICOM: Neben der Übermittlung und Speicherung von DICOM-Bildern und -Befunden in der Medizinakte können durch ein Mapping auch Akteneinträge auf Basis von Metadaten aus dem DICOM-Header erstellt werden.

IMPORT: Zusätzlich zu den standardisierten Schnittstellen wie DICOM und HL7 können auch Dateien über ein Austauschverzeichnis in die Akte importiert und so einem Akteneintrag hinzugefügt werden.

Alle Schnittstellen, die zur Eingabe in die Akte verwendet werden können, wurden auch als Ausgabeschnittstellen der Medizinakte implementiert. Weiterhin ist die Medizinakte in der Lage, durch ein Mapping zwischen den unterschiedlichen Formaten (DICOM, HL7, HTTP) zu übersetzen. Sie kann dadurch zum Beispiel aus den Header-Feldern eines importierten DICOM-Bildes zusammen mit den durch Benutzer eingegebenen

nen Einträgen aus der Medizinalakte (Abbildung 3.18) eine HL7-Nachricht für ein externes System erzeugen.

3.6.4. Workflowsteuerung

Um Workflows in der Medizinalakte abbilden zu können, wurde das Konzept der Workflowsteuerung eingeführt. Per Konfiguration kann so ein Workflow für Akteneinträge hinterlegt werden. Dabei wird beschrieben, in welcher Reihenfolge und durch welche Benutzer die Akteneinträge erstellt werden können.

Nach jedem Schritt wird der aktuelle Status des Workflows in der Akte angezeigt (Abbildung 3.20) und der Benutzer durch eine Benachrichtigung aufgefordert, den nächsten Eintrag zu erstellen.

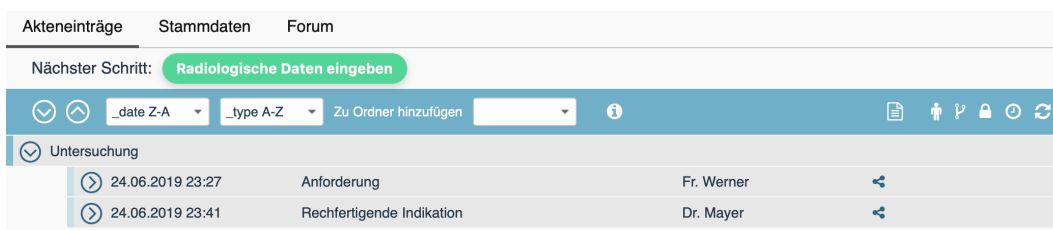


Abbildung 3.20.: Beispiel der Workflowsteuerung in der Medizinalakte

Bei strikter Workflowsteuerung müssen alle Schritte in der konfigurierten Reihenfolge abgearbeitet werden. Verfügen Benutzer über die entsprechenden Rechte, dann ist es auch möglich, einzelne Schritte zu überspringen oder zu einem vorherigen Schritt zurückzukehren.

Die konkrete Modellierung eines Workflows liegt im Aufgabenbereich der Klinik beziehungsweise des Betreibers und ist bei Einsatz einer Medizinalakte (zum Beispiel als Teleradiologieportal) bereits vorhanden. Das Portal ermöglicht vielmehr die vollelektronische Abbildung der bereits bestehenden analogen Workflows, eine neue Workflowdefinition ist hier nicht notwendig.

3.6.5. Zugriffssteuerung und Freigaben

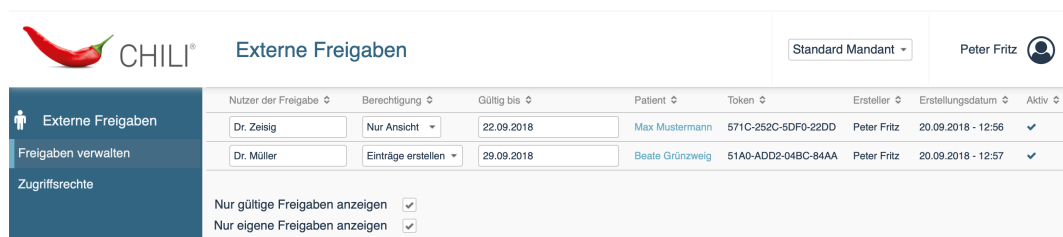
Um die Weitergabe von Akten zu erleichtern, wurde ein neues Freigabekonzept für die Medizinakte entwickelt. Dies ermöglicht es, je nach Berechtigung Akten oder Akteneinträge mit anderen Benutzern oder Benutzergruppen zu teilen. Hierbei wurden die folgenden Szenarien implementiert:

Sperren: Das Sperren von Akten für das Bearbeiten durch Benutzer (zum Beispiel nach Abschluss der Behandlung)

Weitergabe: Die Weitergabe von Akten oder Akteneinträgen zwischen registrierten Benutzern (Konsilfunktion)

Freigabe: Die Freigabe von Akten oder Akteneinträgen für interne oder externe Benutzer (tokenbasiert)

Werden Akten oder Akteneinträge für externe Benutzer freigegeben, so ist über eine Oberfläche jederzeit ersichtlich, welche Akte durch welchen Benutzer eingesehen werden kann. Je nach Konfiguration erhält der Nutzer dann lesenden oder schreibenden Zugriff auf die Akte und kann so weitere Einträge erstellen oder Dokumente hinzufügen. Weiterhin können externe Freigaben mit einem Ablaufdatum versehen werden. Die Gültigkeit einer Freigabe kann jederzeit über eine Weboberfläche eingesehen werden, und Freigaben können hier verlängert oder deaktiviert werden (Abbildung 3.21).



Nutzer der Freigabe	Berechtigung	Gültig bis	Patient	Token	Ersteller	Erstellungsdatum	Aktiv
Dr. Zeisig	Nur Ansicht	22.09.2018	Max Mustermann	571C-252C-5DF0-22DD	Peter Fritz	20.09.2018 - 12:56	✓
Dr. Müller	Einträge erstellen	29.09.2018	Beate Grünzweig	51A0-ADD2-04BC-84AA	Peter Fritz	20.09.2018 - 12:57	✓

Nur gültige Freigaben anzeigen
 Nur eigene Freigaben anzeigen

Abbildung 3.21.: Freigabeverwaltung in der Medizinakte

3.6.6. Auswertung und Export

Um die Integration in externe Datenverarbeitungssysteme zu unterstützen, wurde ein Auswertungs- und Exportmodul in die Medizinakte integriert. Dies ist wichtig, um Daten

zum Beispiel zu Abrechnungszwecken an externe Systeme übergeben zu können. Weiterhin können auf diesem Weg Daten für medizinische Studien an Expertensysteme zur Auswertung weitergegeben werden. Über eine Benutzeroberfläche können frei konfigurierbare Abfragen auf Basis der Datenbank der Medizinakte erstellt werden (Abbildung 3.22).



Abbildung 3.22.: Datenexport und Auswertungsfunktionen in der Medizinakte

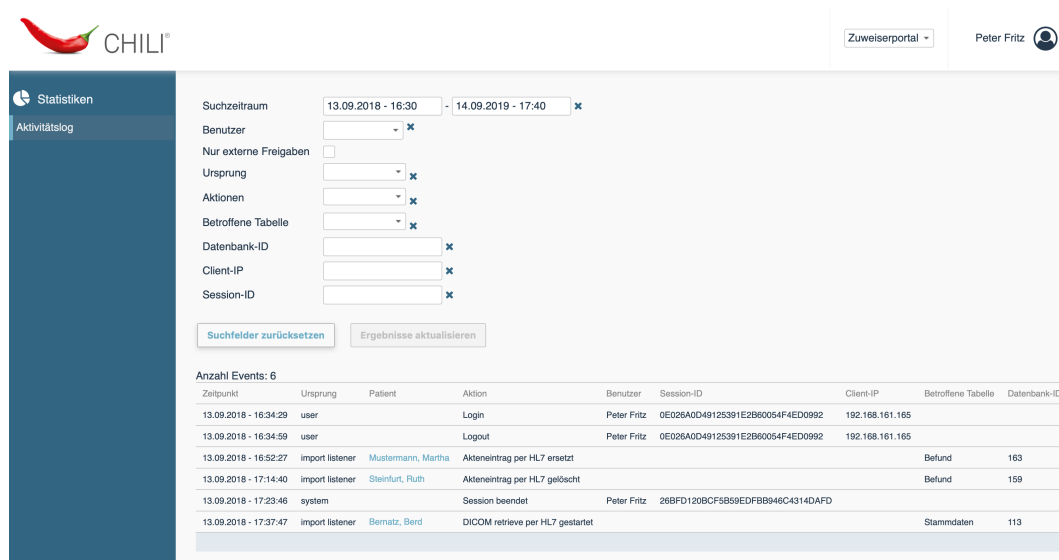
Neben der Anzeige in der Medizinakte ist es auch möglich, die Auswertung per Datenexport im CSV- oder Excel-Format für die Weiterverarbeitung bereitzustellen.

3.6.7. Protokollierung

Im Rahmen von Sicherheitserweiterungen wurde eine vollständige Protokollierung in die Medizinakte implementiert. Jegliche Zugriffe beziehungsweise Änderungen an Akteneinträgen können so über die Benutzeroberfläche durch berechtigte Benutzer nachvollzogen werden (Abbildung 3.23). Neben den Zugriffen von Benutzern werden auch Änderungen, die durch die implementierten Schnittstellen (Kapitel 3.6.3) an der Akte vorgenommen werden, in der Datenbank gespeichert.

Zusätzlich zur internen Zugriffsprotokollierung in der Medizinakte können Zugriffe auf Patienten- und insbesondere Bilddaten auch über das IHE-Profil 'Audit Trail and Node Authentication' (ATNA) zentral in einem Repository gespeichert werden (Bresser et al., 2014).

Neben der Protokollierung kann die Medizinakte auch als IHE ATNA Secure Application beziehungsweise das Gesamtsystem als Secure Node betrieben werden. Jegliche Kommunikation findet dann verschlüsselt statt.



The screenshot shows the CHILI (CHILI Accounting) interface. At the top left is the CHILI logo (a red chili pepper). The top right shows a user profile for Peter Fritz. The main area is a search filter with the following fields:

- Suchzeitraum: 13.09.2018 - 16:30 - 14.09.2019 - 17:40
- Benutzer: [dropdown]
- Nur externe Freigaben: [checkbox]
- Ursprung: [dropdown]
- Aktionen: [dropdown]
- Betroffene Tabelle: [dropdown]
- Datenbank-ID: [input]
- Client-IP: [input]
- Session-ID: [input]

Buttons: Suchfelder zurücksetzen, Ergebnisse aktualisieren

Activity Log Table:

Zeitpunkt	Ursprung	Patient	Aktion	Benutzer	Session-ID	Client-IP	Betroffene Tabelle	Datenbank-ID
13.09.2018 - 16:34:29	user		Login	Peter Fritz	0E026A0D49125391E2B60054F4ED0992	192.168.161.165		
13.09.2018 - 16:34:59	user		Logout	Peter Fritz	0E026A0D49125391E2B60054F4ED0992	192.168.161.165		
13.09.2018 - 16:52:27	import listener	Mustermann, Martha	Akteneintrag per HL7 ersetzt				Befund	163
13.09.2018 - 17:14:40	import listener	Steinfurt, Ruth	Akteneintrag per HL7 gelöscht				Befund	159
13.09.2018 - 17:23:46	system		Session beendet	Peter Fritz	26BFD120BCF5859EDFB8946C4314DAFD			
13.09.2018 - 17:37:47	import listener	Bernatz, Bernd	DICOM retrieve per HL7 gestartet				Stammdaten	113

Abbildung 3.23.: Protokollierung von Nutzer- und Systemaktionen in der Medizinakte

3.7. Qualitätssicherungswerkzeuge für teleradiologische Systeme

Im Rahmen der Diplomarbeit 'Entwicklung eines Überwachungsmoduls für die Teleradiologie' wurde bereits ein System zur Überwachung von Teleradiologiekomponenten durch den Autor entwickelt und implementiert (Schwind, 2008). Das CHILI/Accounting ermöglicht es jedem Client oder Server in einem Netzwerk, Daten wie beispielsweise die aktuelle CPU-Auslastung oder den belegten Speicherplatz zu erheben. Das Überwachungssystem mit zahlreiche Standardmodule kann durch einen Plugin-Mechanismus um server-, projekt- oder kundenspezifische Module erweitert werden. Die so gesammelten Daten können direkt auf dem Server angezeigt oder als Graph zum Beispiel für CPU- oder Speicherauslastung über einen Zeitraum visualisiert werden.

Neben dem eigentlichen Sammeln von Daten kann das System auch Warn- oder Fehlermeldungen über den Zustand des Systems an ausgewählte Benutzer versenden. Weiterhin agiert jedes Accounting-System gleichermaßen als Sender und Empfänger, und so können die von den Modulen erzeugten Daten zwischen den einzelnen im Grunde gleichberechtigten Knoten über ein Peer-to-Peer-Konzept ausgetauscht werden. Durch diesen Mechanismus lassen sich bereits Gruppen von Servern bilden, die ihre Daten mit-

einander teilen und alle Daten über einen zentralen Knoten sammeln und Warnungen beziehungsweise Nachrichten über den Zustand der Server in einem Netzwerk an den zuständigen Administrator oder die Supportabteilung senden.

Im Rahmen dieser Arbeit wurde das bestehende System durch den Autor konzeptionell erweitert und durch verschiedene Abschlussarbeiten weiterentwickelt.

3.7.1. Erweiterungen für Performancemessungen und Konstanzprüfung

Neben den auf dem Server durch das Accounting selbst generierten Daten sind auch die Daten anderer unabhängiger Testwerkzeuge für den täglichen Betrieb und die Überwachung der Server interessant, um die Auslastung und Performance von Teleradiologiesystemen besser beurteilen zu können.

Aus diesem Grund wurden Werkzeuge zur Performancemessung von Teleradiologieservern sowie ein Werkzeug zur Geschwindigkeitsmessung zwischen Client und Server integriert beziehungsweise implementiert. Hierbei handelt es sich um Bonnie++, PGbench und Speedtest.

Bonnie++

Bonnie++ (<https://doc.coker.com.au/projects/bonnie>, 04.04.2019) ermöglicht es, die Lese- und Schreibgeschwindigkeit des Dateisystems zu testen. Bei Verwendung von Bonnie++ können neben den eigentlichen Zugriffszeiten für unterschiedliche Blockgrößen auch die Latenzen für den Zugriff gemessen werden. Das weit verbreitete Tool (Tarasov et al., 2011; Gillam et al., 2013) wurde mit Referenzmessungen für unterschiedliche Serverarten (Hardware, Virtualisierung) und unterschiedliche Festplattentypen in das Accounting integriert (Abbildung 3.24).

PGbench

PGbench ist ein Werkzeug zur Geschwindigkeitsmessung von Datenbankoperationen im Zusammenspiel mit dem DBMS PostgreSQL (<https://www.postgresql.org/docs/10/>

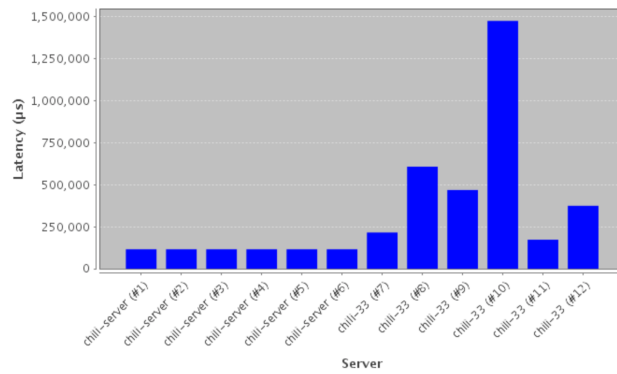


Abbildung 3.24.: Auswertung der durch Bonnie++ erhobenen Daten zur Ermittlung der Festplattenperformance des Teleradiologieservers

pgbench.html, 04.04.2019). Mit PGbench kann über die reine Lese- und Schreibgeschwindigkeit der Festplatten hinaus auch eine Aussage über die Leistung der Datenbank durch Messung der durchgeführten Transaktion pro Sekunde (TPS) getroffen werden. Auch hier wurden Referenzmessungen für unterschiedliche Server und Dateisysteme im System hinterlegt (Abbildung 3.25).

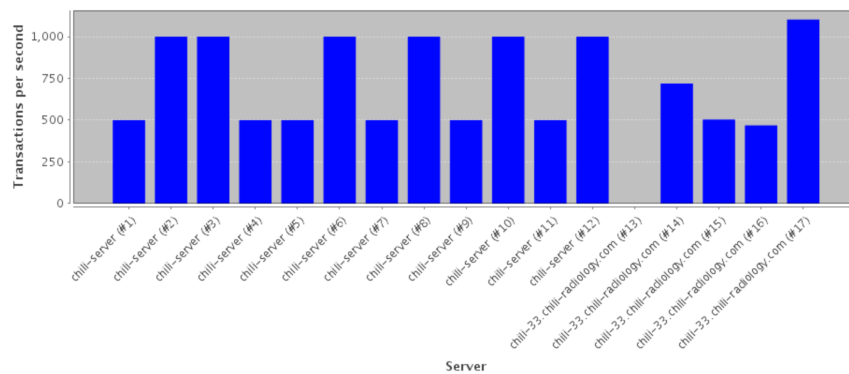


Abbildung 3.25.: Auswertung von PGbench-Daten zu Ermittlung der Transaktionsgeschwindigkeit des DBMS

Speedtest

Um insbesondere in der Teleradiologie eine Aussage über die Erreichbarkeit und Geschwindigkeit der Verbindung zwischen dem Teleradiologieclient beziehungsweise dem DICOM-Viewer und dem Server treffen zu können, wurde analog zu einem Geschwindigkeitstest für einen Internetanschluss, wie ihn beispielsweise die Bundesregierung (<http://www.bundesregierung.de>):

//breitbandmessung.de, 04.04.2019) anbietet, ein Verfahren zur Bandbreitenmessung in den DICOM-Client implementiert.

Jeder Client ist mit einem Server verbunden und kann entweder Daten von diesem empfangen oder Daten zu diesem senden. Um die Bandbreite zwischen Client und Server zu messen, wurde serverseitig ein Webservice implementiert, der Daten sowohl in einem HTTP-Request empfangen als auch in einer HTTP-Response zurückliefern kann.

Der Webservice ist unter folgender URL zu erreichen:

```
http(s)://<server>/chiliadmin/servlet/ServiceServlet?serviceServletId=
    CHILIACC&serviceServletAlias=SpeedTest
```

Das implementierte Servlet kann die beiden Parameter 'testmode' und 'size' entgegennehmen.

Testmode legt die Art der Prüfung fest (UPSTREAM oder DOWNSTREAM).

Size gibt die Größe des zu versendenden Datensatzes in KB an.

Bei einem Upload generiert der Client einen zufälligen Datenblock in gewünschter Größe und sendet diesen unter Verwendung der entsprechenden Parameter an den Server. Der Server empfängt die Daten und sendet in der Antwort die Dauer und die Anzahl der empfangenen Bytes in einem XML-Dokument zurück (Listing 3.31). Sollte die Anzahl der empfangenen Bytes nicht mit der erwarteten Anzahl aus dem Request übereinstimmen, erhält der Client eine Fehlermeldung (Listing 3.32).

Listing 3.31: Beispiel für eine erfolgreiche Bandbreitenmessung

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <speedtest_response> <!-- Bandbreite: 39.96 Mbit/s -->
3 <bytecount>1048576</bytecount> <!-- 1024 KB = 1 MB -->
4 <duration>205</duration> <!-- 205 ms -->
5 </speedtest_response>
```

Listing 3.32: Beispiel einer fehlerhaften Bandbreitenmessung

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <speedtest_response>
3 <error>Error: 500</error>
4 <errorDescription>Bytecount differs. (received: 1049600, expected: 1048576)</errorDescription>
5 </speedtest_response>
```

Im Fall des Download sendet der Client einen Request mit der Größe des gewünschten Datenblocks an den Server. Der Server antwortet mit einem zufällig generierten Datenpaket gewünschter Größe. Der Client überprüft auch hier die Anzahl der empfangenen Bytes, um Fehler auszuschließen.

Um ein Caching der Daten durch einen Webserver oder Proxy zu verhindern, werden die entsprechenden Cache-Control HTTP-Header gesetzt und zusätzlich ein Parameter 'preventcaching', welcher mit einem Zufallswert gefüllt wird, im HTTP-Request mitgesendet.

Auf diese Weise können sowohl die Upload- als auch Downloadgeschwindigkeit für verschiedene Datenpakete ermittelt werden. Unter Einbeziehung der Größe des Datenpakets lässt sich so auf einfache Weise die zur Verfügung stehende Bandbreite ermitteln.

Da die Bandbreite für den Empfang und Versand stark von der Größe des verwendeten Datensatzes abhängt, wurde zusätzlich ein mehrstufiges Verfahren implementiert. Der Client startet mit einer definierten Größe zum Beispiel von 64 KB. Sollte die Übertragung innerhalb einer definierten Zeit (zum Beispiel fünf Sekunden) möglich sein, dann verdoppelt der Client die Größe des Datenpakets und sendet es erneut. Dieser Prozess wird so lange fortgeführt, bis der konfigurierte Schwellwert überschritten ist und das Datenpaket nicht in der vorgegebenen Zeit übertragen werden kann. Das gleiche Verfahren wird anschließend auch für den Download angewendet. Aus den so erhaltenen Daten kann dadurch leicht eine mittlere Bandbreite errechnet werden, und durch die wachsenden Datenpakete mit definierter Zeitschwelle ist sichergestellt, dass der Test sowohl für schnelle als auch langsame Leitungen in kürzest möglicher Zeit durchgeführt werden kann.

3.7.2. Datenübertragung

Alle durch die oben beschriebenen Performancemessungen auf den Teleradiologiesystemen ermittelten Daten als auch die durch die Multiknotenstatistik (Kapitel 3.2) erstellten Abnahme- und Konstanzprüfungsprotokolle für die Teleradiologie können durch eine Erweiterung des Accounting zwischen allen beteiligten Partnern ausgetauscht werden.

Weiterhin können durch das Accounting Daten über die konkrete Installation, den Server und die installierte Software gesammelt und übertragen werden.

3.7.3. Auswertung und Aufbereitung der gesammelten Daten

Durch das Accounting war es bisher nur möglich, Daten auf einzelnen Servern zu erheben und die gesammelten Daten zwischen allen beteiligten Systemen auszutauschen. Um das Accounting um die Möglichkeit einer Datenaufbereitung und Datenauswertung zu erweitern, musste eine Schnittstelle für Auswertesysteme geschaffen werden. Aus diesem Grund wurde ein MessageProcessor Interface für das Accounting-System entwickelt (Listing 3.33).

Listing 3.33: MessageProcessor-Schnittstelle für das Accounting

```
1 public interface MessageProcessor {  
2  
3     public void setLog(Log log);  
4  
5     public void messageReceived(AccMessage accMessage, int connectionId, String connectionType);  
6  
7     ...  
8 }
```

Ein externes oder internes System kann so eine Erweiterung (Addon) für das Accounting erstellen, indem das Interface *MessageProcessor* implementiert wird. Die so erstellte Anwendung wird durch einen Plugin-Mechanismus im Accounting-Dienst registriert. Geht nun eine Nachricht über das Accounting auf dem Server ein, so werden alle registrierten Addons über den Eingang der Accounting-Nachricht informiert und können diese bei Bedarf verarbeiten. Zusätzlich zur eigentlichen Nachricht wird auch die Information über die Art der Verbindung sowie die Verbindungs-ID übergeben, so dass Addons die empfangenen Daten einer konkreten Verbindung zuordnen und diese bei Bedarf herausfiltern können.

Anwendungsszenarien

Durch die implementierte Addon-Schnittstelle können unterschiedliche Szenarien abgedeckt werden. Zum einen kann der reine Empfang von Nachrichten von einer bestimm-

ten Verbindung mit einem Timestamp gespeichert werden, um so den letzten aktiven Kontakt zwischen den Systemen zu dokumentieren. Dadurch ist es möglich, die Erreichbarkeit von Systemen darzustellen und auszuwerten.

Weiterhin können bestimmte Nachrichten herausgefiltert und ausgewertet werden. Dies bietet zum Beispiel die Möglichkeit bei Erhalt einer Accounting-Nachricht, die den aktuellen Festplattenfüllstand oder interne Fehlermeldungen übermittelt, diese aus dem Accounting heraus auch in andere Applikationen wie zum Beispiel Nagios (<https://www.nagios.org>, 04.04.2019) zu übergeben und dort alle angeschlossenen Server zu überwachen und auszuwerten.

Zusätzlich können alle durch die Konstanzprüfung und Performanceanalyse gesammelten Daten zentral in einem externen System aufbereitet, verwaltet und archiviert werden.

Zugriffssteuerung

Die Berechtigung und der Zugriff der einzelnen Addons lässt sich über das Accounting steuern. Hier kann festgelegt werden, welches Addon auf welche Daten Zugriff erhält und in der Nachverarbeitung auswerten darf.

3.8. Umsetzung der beschriebenen Methoden

Alle in diesem Kapitel aufgeführten Methoden wurden im Rahmen dieser Arbeit konzipiert, entwickelt und implementiert:

- Erweiterung von DICOM E-Mail um Qualitätssicherungsmechanismen zur Nachverfolgung des Datenverkehrs
- Implementierung einer herstellerunabhängigen Administration von großen DICOM E-Mail Netzwerken
- Entwicklung einer Multiknotenstatistik zur Datenanalyse in heterogenen Netzwerken mit mehreren unabhängigen Versandknoten

- Standardisierung von DICOM E-Mail in Anlehnung an IHE XDM
- Entwicklung von Komponenten zur performanten intersektoralen Vernetzung mit IHE XDS für den Routinebetrieb
- Mobile Bildbetrachtung und Single-Sign-On in IHE XDS Netzwerken
- Erweiterung von Akten- und Portallösungen zur workfloworientierten Vernetzung
- Entwicklung von Qualitätssicherungswerkzeugen und Monitoring für teleradiologische Systeme

Die Methoden zur Erweiterung von qualitätsgesicherten DICOM E-Mail Netzwerken sowie die Standardisierung im Bereich von IHE XDM und DICOM E-Mail wurden in Zusammenarbeit mit der Arbeitsgruppe Informationstechnologie der Deutschen Röntgen-gesellschaft entwickelt. Die so erarbeiteten Lösungsmöglichkeiten wurden exemplarisch in das CHILI PACS implementiert.

Die Entwicklungen zur performanten intersektoralen Vernetzung mit IHE XDS und mobilen Bildbetrachtung wurden im Rahmen des INFOPAT-Projekts (Infopat MRN, 2018) entworfen, implementiert und evaluiert (Kapitel 4.5).

Die in diesem Kapitel vorgeschlagenen und umgesetzten Methoden bilden die Basis zur Unterstützung von Prozessen der intersektoralen Vernetzung mit medizinischen Bildern und bieten eine Weiterentwicklung und Standardisierung von Teleradiologiekomponenten unter Berücksichtigung der Qualitätssicherung. Alle erarbeiteten Werkzeuge und Methoden zur Qualitätssicherung und Vernetzung kommen mittlerweile in größeren Netzwerkinstallationen zum Einsatz und haben sich im Routinebetrieb bewährt.

Neben den administrativen Anwendern profitieren auch ärztliche Nutzer, Gesundheitseinrichtungen und schlussendlich die Patienten von der qualitätsgesicherten intersektoralen Vernetzung, welche die Stabilität und Geschwindigkeit der Datenübertragung und damit auch der Behandlung direkt beeinflusst.

Auf die Umsetzung der erarbeiteten Methoden und implementierten Softwarelösungen sowie deren Nutzen für Anwender und Patienten wird im folgenden Kapitel 4 detailliert eingegangen.

4. Ergebnisse

Die im Rahmen dieser Arbeit beschriebenen Methoden und Weiterentwicklungen unterschiedlicher Standards im Bereich der Qualitätssicherungen und Teleradiologie sowie die Softwareentwicklungen im Bereich der Telemedizin und schlussendlich der intersektoralen Vernetzung unterstützen den Arbeitsablauf der medizinischen als auch administrativen Anwender. Mit Hilfe der etablierten Lösungen kann ein reibungsloser Ablauf und das Zusammenspiel verschiedener Komponenten in heterogenen Netzwerken auch unter dem Gesichtspunkt der Qualitätssicherung gewährleistet werden.

Dieses Kapitel stellt den Einsatz der in Kapitel 3 vorgestellten Methoden und Lösungen vor. Die implementierten Lösungen werden einzeln besprochen und bieten jede für sich eine Verbesserung der Vernetzung und Qualitätssicherung sowohl für administrative als auch ärztliche und nicht-ärztliche Nutzer sowie Patienten beziehungsweise Bürger.

4.1. Administration von DICOM E-Mail Netzwerken

Um der in Deutschland weit verbreiteten DICOM E-Mail Vernetzung auch mit wachsender Größe der Netzwerke gerecht zu werden, wurden bestehende DICOM E-Mail Netzwerke um die in Kapitel 3.1.1 beschriebenen Service Part E-Mails erweitert.

4.1.1. Anbindung neuer Nutzer

Soll ein neuer Teilnehmer in ein bestehendes DICOM E-Mail Netzwerk aufgenommen werden, so muss dieser jetzt nicht mehr einzeln jedem anderen Teilnehmer mit E-Mail-

Adresse sowie PGP/GPG-Schlüssel bekannt gemacht werden. Unter Verwendung der entwickelten DICOM E-Mail Service Parts genügt es, den neuen Partner bei einem einzigen vertrauenswürdigen Teilnehmer des Netzwerks anzulegen beziehungsweise zu konfigurieren. Dieser sendet anschließend eine signierte Service Part E-Mail vom Typ ADDRESSUPDATE (Abbildung 4.1) sowie KEYUPDATE (Abbildung 4.2) an alle ihm bekannten Benutzer des Netzwerks.

The screenshot shows the 'Service Part' configuration window in the PACS/Mail system. The 'Typ' is set to 'ADDRESSUPDATE' and the 'Aktion' is 'SET'. The configuration includes the following fields:

- Empfänger-Adresse: mailtest <mailto@mail>
- Empfänger-KeyID: AF17E965
- Nachricht signieren: Chillvm26 Server (10026702)
- Verbindungs-ID: ad593283-ed26-4ce9-a82e-980ec551b976
- Verbindungsname: Radiologie Musterstadt
- Mailserver: mail.musterklinik.de
- Port: 465
- E-Mail-Adresse: rad-musterstadt@musterklinik.de
- GPG-KeyID: 672A03E4B1DB923F

Buttons for 'Absenden' and 'Zurücksetzen' are visible at the bottom.

Abbildung 4.1.: Adressupdate mittels Service Part E-Mail. Versand eines Adressupdates aus der Verwaltungsoberfläche des Teleradiologiesystems unter Angabe aller relevanten Informationen.

The screenshot shows the 'Service Part' configuration window in the PACS/Mail system. The 'Typ' is set to 'KEYUPDATE' and the 'Aktion' is 'SET'. The configuration includes the following fields:

- Empfänger-Adresse: mailtest <mailto@mail>
- Empfänger-KeyID: AF17E965
- Nachricht signieren: Chillvm26 Server (10026702)
- GPG-Schlüssel: A long alphanumeric string representing a public key, starting with '-----BEGIN PGP PUBLIC KEY BLOCK-----' and ending with '-----END PGP PUBLIC KEY BLOCK-----'.

Buttons for 'Absenden' and 'Zurücksetzen' are visible at the bottom.

Abbildung 4.2.: Schlüsselupdate mittels Service Part E-Mail. Versand eines Schlüsselupdates aus der Verwaltungsoberfläche des Teleradiologiesystems.

Nach Erhalt einer solchen Service Part E-Mail obliegt es nun dem Empfänger, diese entweder vollautomatisch oder manuell seinem Adressbuch hinzuzufügen. Hierbei kann

eine Whitelist mit vertrauenswürdigen Partnern gepflegt und angewendet werden, welche es erlaubt, detaillierte Berechtigungen auf Basis der E-Mail-Signatur in Kombination mit der auszuführenden Aktion zu erstellen. In Abbildung 4.3 ist die Konfiguration eines solchen Systems dargestellt, welche automatische Adressupdates nur von einem ausgewählten Partner zulässt.

The screenshot shows the configuration interface for Service Parts. The 'Versand' (Outgoing) section is active, showing fields for 'Absender' (servicepart@chilvm26), 'Benachrichtigung anfordern' (checked), 'X-Telemedizin-Benachrichtigung anfordern' (checked), 'Benachrichtigungsadresse' (postfach@esthost (chilvm26)), and 'X-Telemedizin-Benachrichtigungsschlüssel' (Chilvm26 Server (10026702)). A 'Speichern' button is visible. The 'Empfang' (Incoming) section is also active, showing 'Unbekannte verwerfen' (checked), 'Ausführung' (Automatisch), and 'Signatur erforderlich' (checked). Below these are checkboxes for 'Chilvm26 Server (10026702)' (unchecked) and 'Service Master - chilvm27 (C17C0DE1)' (checked). A table at the bottom lists actions for incoming messages:

Name	Action	Ausführung	Filter
ADDRESSUPDATE	SET	Automatisch	
ADDRESSUPDATE	REMOVE	Automatisch	
KEYUPDATE	SET	Manuell	

Abbildung 4.3.: Konfiguration des Empfangs von Service Part E-Mails mit Einschränkung auf Signatur und der auszuführenden Aktion. In dieser Konfiguration werden Adressupdates automatisch und Schlüsselupdates nur nach vorheriger Bestätigung ausgeführt.

Wird eine E-Mail mit einem PGP/GPG-Schlüsselupdate empfangen, so erhält der Administrator des Systems eine Benachrichtigung und muss das Schlüsselupdate explizit freigeben und manuell ausführen (Abbildung 4.4). Alle weiteren empfangenen Service Part E-Mails werden bei der vorliegenden Konfiguration (Abbildung 4.3) schon vor der Verarbeitung herausgefiltert und verworfen. Durch die eingeführten X-Telemedicine-Servicepart Tags kann diese Filterung auch schon durchgeführt werden, ohne den Inhalt der E-Mail zu entschlüsseln, wodurch weniger Rechenleistung notwendig ist.

Durch den Einsatz der DICOM E-Mail Service Parts wird somit grundsätzlich jeder Teilnehmer in einem DICOM E-Mail Netzwerk in die Lage versetzt, dem Netzwerk neue Partner hinzuzufügen. Durch das Whitelist-basierte Berechtigungskonzept und den Filtermechanismus auf Basis des Typs der Service Part E-Mail kann so die Verwaltung des Teleradiologieservers detailliert auf die Bedürfnisse des Betreibers und Administrators angepasst werden.

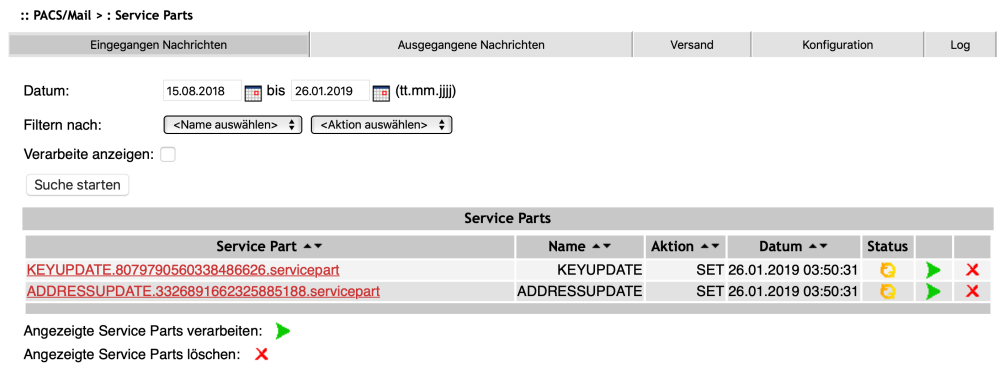


Abbildung 4.4.: Verwaltungsoberfläche für eingehende Service Part E-Mails. Die empfangenen Nachrichten können nach Kontrolle manuell ausgeführt, zurückgestellt oder verworfen werden.

Alle sowohl manuell als auch automatisch durchgeführten Aktionen unterliegen einer detaillierten Protokollierung. So ist sichergestellt, dass alle relevanten Änderungen an dem Teleradiologieserver lückenlos nachvollzogen (Abbildung 4.5) und bei Bedarf ausgewählte Änderungen rückgängig gemacht werden können.

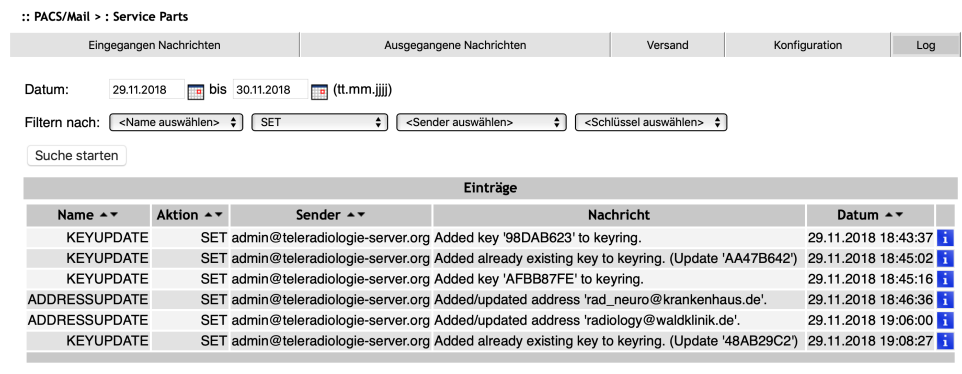


Abbildung 4.5.: Benutzeroberfläche zur Analyse von ausgeführten Service Part E-Mails. Durchgeführte Aktionen werden hier protokolliert und können mit ihren Details eingesehen werden.

4.1.2. Aktualisierung bestehender Verbindungen

Neben dem Hinzufügen von neuen Partnern zu einem Netzwerk wird durch die Implementierung der DICOM E-Mail Service Parts auch jeder Teilnehmer in die Lage versetzt, Änderungen an seinen eigenen Daten ad hoc an alle anderen Teilnehmer des Netzwerks zu kommunizieren. Zu diesem Zweck wurde eine Funktion zur Übermittlung

der geänderten Daten sowohl in die Adress- als auch in die Schlüsselverwaltung auf dem Teleradiologiesystem implementiert.

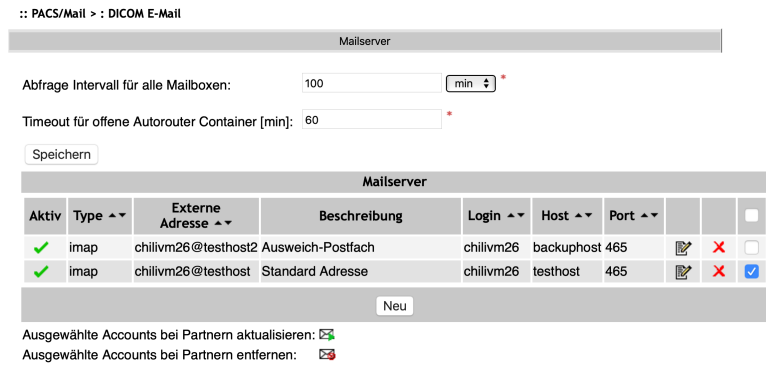


Abbildung 4.6.: Update der eigenen Verbindungsdaten via Service Part E-Mails mit direkter Integration in die Verwaltungsoberfläche des Teleradiologiesystems.

Nach Änderungen an den eigenen Kommunikationsdaten ist es so per Knopfdruck möglich, diese an alle konfigurierten Partner des DICOM E-Mail-Netzwerks zu verteilen (Abbildung 4.6). Gleiches gilt auch für die implementierte Verwaltung der PGP/GPG-Schlüssel mittels DICOM E-Mail Service Parts.

Sollte ein Empfänger kurzzeitig nicht erreichbar sein, werden Service Part E-Mails analog zu regulären DICOM E-Mails auf dem Mailserver zwischengespeichert und bei Erreichbarkeit zugestellt. Durch die gleichzeitige Verwendung der erweiterten Empfangsbestätigung für DICOM E-Mail können der Empfang und die Verarbeitung der Adressänderungen auf der Gegenseite durch den Sender beziehungsweise dem Administrator des Netzwerks nachvollzogen und bei Bedarf neu angestoßen werden. Es ist jeder Zeit ersichtlich, welcher Knoten im DICOM E-Mail Netzwerk die Änderungen erhalten und angewendet hat.

4.1.3. Erweiterte Empfangsbestätigungen

Auf Basis der in Kapitel 3.1.6 beschriebenen erweiterten Empfangsbestätigung für DICOM E-Mail in Kombination mit den bestehenden X-Telemedicine-Set Header-Tags ist es möglich, den Transfer von DICOM-Objekten via DICOM E-Mail sowohl auf Seiten des Senders als auch des Empfängers zu überwachen.

Die Implementierung der DICOM E-Mail Service Parts für die erweiterte Empfangsbestätigungen erlaubt es dem Sender, den Erhalt der versendeten Daten, auch wenn diese über mehrere E-Mails verteilt gesendet wurden, nachzuvollziehen. Informationen zum Transfer können sowohl in der Administrationsoberfläche des Teleradiologiesystems als auch direkt im verwendeten PACS-Viewer angezeigt werden (Abbildung 4.7).

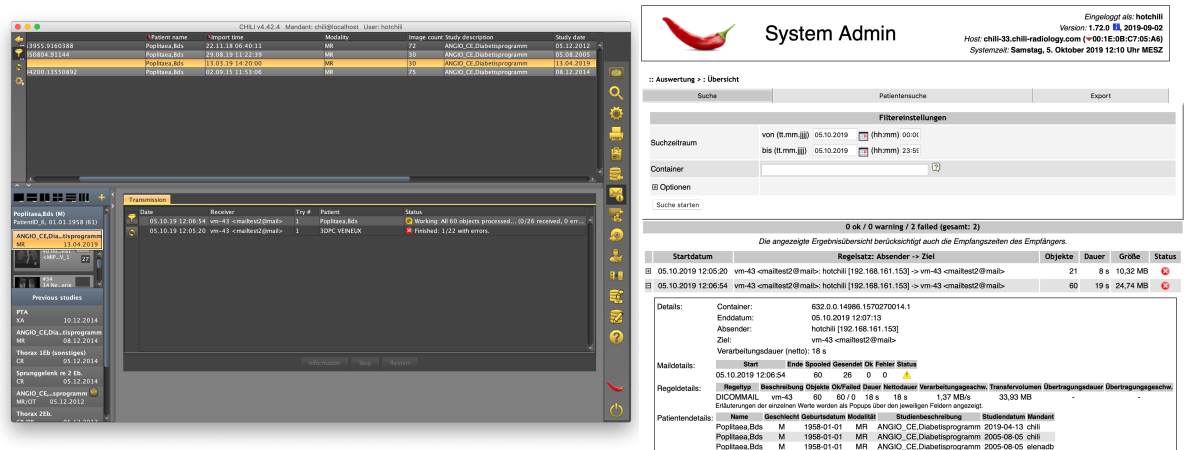


Abbildung 4.7.: DICOM E-Mail Empfangsbestätigung mit Anzeige im Teleradiologieclient (links) und Administrationsoberfläche (rechts).

Die hier entwickelten und implementierten Empfangsbestätigungen stellen die Basis für eine automatisierte Konstanzprüfung und die Verwendung von DICOM E-Mail Service Parts zur Administration von DICOM E-Mail Netzwerken dar.

4.2. Automatisierte Konstanzprüfung in der Teleradiologie

Die Implementierung der in Kapitel 3.1.7 beschriebenen Service Parts zur Konstanzprüfung ermöglicht eine halb- oder vollautomatische Konstanzprüfung eines DICOM E-Mail Netzwerks.

Um diese durchführen zu können, müssen im ersten Schritt geeignete Prüfdatensätze ausgewählt werden. Diese können, wie in Abbildung 4.8 dargestellt, aus der Routine des PACS-Betriebs entnommen werden.

:: Auswertung > : TR Konstanzprüfung

Studienauswahl		Prüfdatensätze / Profile			Ergebnisse / Protokolle		
Prüfdatensätze / Profile							
Datum	Beschreibung	M	Testdatensatz DICOM E-Mail	Bilder	Patient	Größe	
<input type="checkbox"/> 11.04.2013	Handaufnahme	CR	CR EXTREMITIES	1	FUJI,HAND (M) 1901-01-01 [FM06]	3,54 MB	<input checked="" type="checkbox"/>
<input type="checkbox"/> 24.04.2018	4 MR 3 MRT LWS	MR	<nicht zugeordnet>	207	Mustermann,Max (M) 1948-06-11 [44411]	130,83 MB	<input checked="" type="checkbox"/>
<input type="checkbox"/> 19.09.2000	Source Two Study 1	CT	CT ABDOMENT	242	Source,Two (M) 1952-03-07 [S2213]	103,77 MB	<input checked="" type="checkbox"/>

Original StudyInstanceUID: 1.2.3.4.5.6.7.8.9.22.999999

Testdatensatz DICOM E-Mail:

Es wurde noch kein Profil angelegt.

Abbildung 4.8.: Auswahl und Zuordnung der Datensätze für die Konstanzprüfung mittels DICOM E-Mail Service Parts

Die Prüfdatensätze werden dazu entsprechend den Anforderungen aus der Abnahmebeziehungweise Konstanzprüfung ausgewählt, anonymisiert und anschließend mit den im Teleradiologienetzwerk gültigen und definierten Testdatensatz-IDs versehen. Die eigentlichen Datensätze können sich hierbei für jeden Teilnehmer im Netzwerk unterscheiden.

4.2.1. Durchführung der Konstanzprüfung

Die gesamte Prüfung der Teleradiologiestrecke kann nun ausschließlich unter Verwendung von DICOM E-Mail Service Parts durchgeführt werden.

Der Administrator des Netzwerks stößt die Prüfung mittels einer Service Part TESTTRANSFER E-Mail an. In diesem ServicePart sind, wie in Listing 3.11 dargestellt, alle notwendigen Transferinformationen enthalten. Hier sind sowohl der zu verwendende Testdatensatz als auch die Adressdaten (E-Mail-Adresse und PGP/GPG-Schlüssel) des Datenempfängers angegeben.

Der Empfänger des Service Part TESTTRANSFER sendet daraufhin die spezifizierten Daten an den gewünschten Empfänger und fordert eine erweiterte Empfangsbestätigung an, um so die korrekte Übermittlung der Daten als auch die Transferzeit protokollieren zu können. Nach Abschluss des Transfers generiert der Sender das Protokoll mit allen ermittelten Daten (Listing 3.12) und sendet es an den im Service Part TESTTRANSFER

angegebenen Protokollempfänger (meist der Administrator des Netzwerks). Der gesamte Workflow ist in Abbildung 4.9 dargestellt.

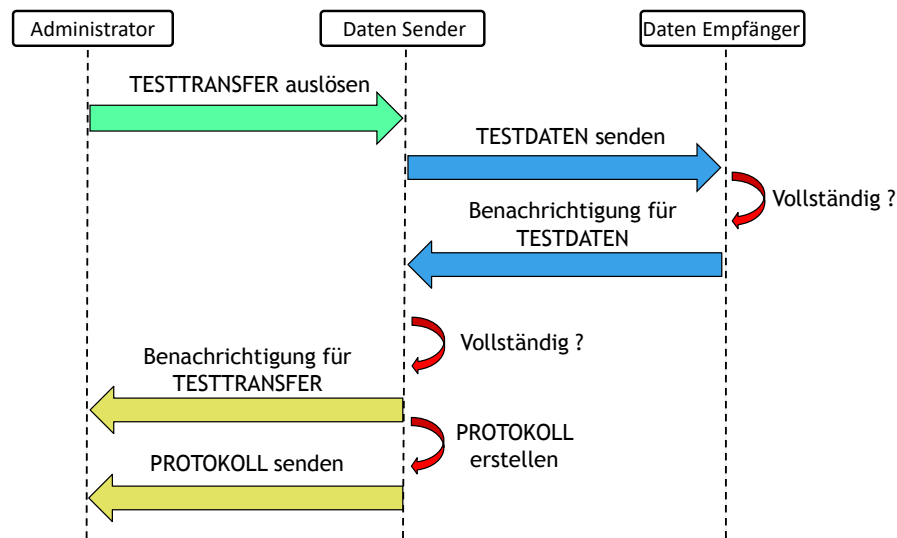


Abbildung 4.9.: Workflow der Konstanzprüfung unter Verwendung von DICOM E-Mail Service Parts

Sollte es zu Problemen während des Transfers kommen, so werden diese auch im Protokoll dokumentiert. Der Anforderer des TESTTRANSFERS hat weiterhin die Möglichkeit, einen Timeout anzugeben, nach dessen Ablauf er auf jeden Fall ein Protokoll erhalten möchte, auch wenn noch nicht alle Daten zwischen den beiden Testpartnern versendet beziehungsweise verarbeitet wurden. Dies ist notwendig, um auch bei einem Fehler in der Teleradiologiestrecke zeitnah eine Rückmeldung zu erhalten und darauf reagieren zu können.

4.2.2. Überwachung und Protokollerstellung

Da der Administrator (Abbildung 4.9) nicht zwingend ein aktiver Teil des Teleradiologienetzwerks sein muss, kann der oben beschriebene Mechanismus sowohl zur generellen Überwachung und Funktionsprüfung als auch zur Konstanzprüfung für die Teleradiologie nach RöV verwendet werden.

Um die Funktion und Erreichbarkeit des gesamten Netzwerks zu überwachen, kann der Administrator die verschiedenen Partner in regelmäßigen Abständen anweisen, einen

relativ kleinen Datensatz per DICOM E-Mail miteinander auszutauschen. Bei korrekter Konfiguration beeinträchtigt dieser zusätzliche Datenverkehr die Funktionsweise des Netzwerks nicht, gibt aber kontinuierlichen Aufschluss über die Erreichbarkeit aller Partner.

Bei einer Konstanzprüfung nach RÖV wählt der Administrator den entsprechenden Datensatz der Untersuchungsart, für die die Teleradiologiestrecke beantragt wurde, aus. Dieser Datensatz wird dann zwischen den angegebenen Partnern versendet, und der Administrator erhält im Anschluss das maschinenlesbare Protokoll der Übertragung, aus welchem er ein Prüfprotokoll für die Ärztliche Stelle generieren kann.

4.3. Multiknotenstatistik

Das in Kapitel 3.2 vorgeschlagene Statistikprotokoll wurde implementiert und kommt mittlerweile in zahlreichen Teleradiologienetzwerken zum Einsatz. Das System ermöglicht es, automatisch Statistiken zu erstellen und die Konstanz der beteiligten Systeme kontinuierlich zu überwachen. Dies ist durch die gewählte Architektur auch für komplexe und wechselnde Routen über mehrere, nicht zeitsynchrone Knoten mit verschiedenen Übertragungsprotokollen möglich (Abbildung 4.10).

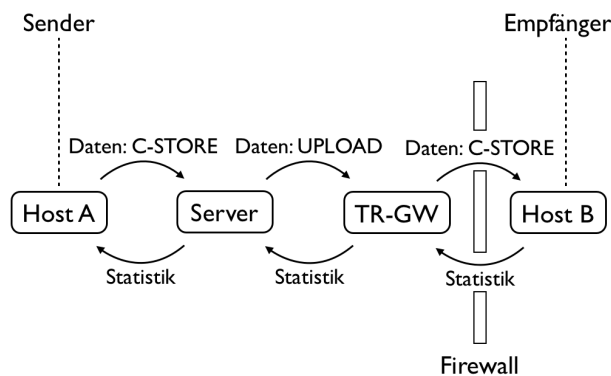


Abbildung 4.10.: Transferkette eines Teleradiologietransfers über mehrere Server unter Verwendung unterschiedlicher Übertragungsprotokolle

Endnutzern und Administratoren des Teleradiologiesystems ist es möglich, auf einen Blick zu sehen, ob die Bilddaten vom Sender zum Endsystem in den von der DIN 6868-

159 für die Teleradiologie geforderten 15 Minuten übertragen wurden (Abbildung 4.11). Durch die detaillierte Aufschlüsselung des Transfers ist es sehr einfach ein Flaschenhals in der Teleradiologiestrecke zu finden und fehlerhafte Knoten zu identifizieren.

Die medizinischen Anwender können außerdem leicht direkt im PACS-Viewer überprüfen, ob die per Teleradiologie gesendeten Bilddaten komplett und fehlerfrei zum Empfänger übertragen werden konnten (Abbildung 4.12). Liegt hier ein Übertragungsfehler über eine bestimmte Teilstrecke vor, so können die Daten direkt aus der Oberfläche über eine mögliche Ausfallroute gesendet werden. Weiterhin können, falls die eingestellten Grenzwerte überschritten wurden, automatisierte Warnungen versendet werden. Dadurch ist es möglich, eine Teleradiologiestrecke proaktiv zu überwachen. Eine Verschlechterung der Bandbreite oder Überlastung des Netzwerks kann mit Hilfe der kontinuierlichen Überwachung schnell identifiziert und behoben werden.

Startdate	Ruleset: Sender -> Destination	Objects	Duration	Bandwidth	Status																																
04.01.2011 15:24:42	Upload TR-Gateway: truser [rdp:130.124.255.255] -> gateway	70	4:01 m	149.60 KB/s																																	
Details: Container: 6.0.0.17406.1294151082.1 Enddate: 04.01.2011 15:28:44 Sender: truser [rdp:130.124.255.255] Destination: upload gateway																																					
Rule details: <table border="1"> <thead> <tr> <th>Ruletyp</th> <th>Description</th> <th>Objects</th> <th>OK/Failed</th> <th>Duration</th> </tr> </thead> <tbody> <tr> <td>UPLOAD</td> <td>gateway</td> <td>70</td> <td>70 / 0</td> <td>13 s</td> </tr> </tbody> </table>						Ruletyp	Description	Objects	OK/Failed	Duration	UPLOAD	gateway	70	70 / 0	13 s																						
Ruletyp	Description	Objects	OK/Failed	Duration																																	
UPLOAD	gateway	70	70 / 0	13 s																																	
Transfer details: Transferid: 0xa8c060a1.943447228.1294151082877.0 Sendtime: 04.01.2011 15:24:42 Receivetime: 04.01.2011 15:28:44 Duration: 4:01 m (149.92 KB/s)																																					
<table border="1"> <thead> <tr> <th>Transfer</th> <th>Destination AET</th> <th>Objects</th> <th>OK/Failed</th> <th>Sendtime</th> <th>Receivetime</th> <th>Duration</th> <th>Bandwidth</th> </tr> </thead> <tbody> <tr> <td>UPLOAD: Host_A -> Host_B</td> <td>TRGATEWAY1</td> <td>70</td> <td>70 / 0</td> <td>04.01.2011 15:24:42</td> <td>04.01.2011 15:24:58</td> <td>16 s</td> <td>2247.13 KB/s</td> </tr> <tr> <td>C-STORE: Host_B -> Host_C</td> <td>TRGATEWAY2</td> <td>70</td> <td>70 / 0</td> <td>04.01.2011 15:25:01</td> <td>04.01.2011 15:25:16</td> <td>14 s</td> <td>2448.76 KB/s</td> </tr> <tr> <td>C-STORE: Host_C -> Host_D</td> <td>WORKSTATION</td> <td>70</td> <td>68 / 2</td> <td>04.01.2011 15:25:18</td> <td>04.01.2011 15:28:44</td> <td>3:25 m</td> <td>175.86 KB/s</td> </tr> </tbody> </table>						Transfer	Destination AET	Objects	OK/Failed	Sendtime	Receivetime	Duration	Bandwidth	UPLOAD: Host_A -> Host_B	TRGATEWAY1	70	70 / 0	04.01.2011 15:24:42	04.01.2011 15:24:58	16 s	2247.13 KB/s	C-STORE: Host_B -> Host_C	TRGATEWAY2	70	70 / 0	04.01.2011 15:25:01	04.01.2011 15:25:16	14 s	2448.76 KB/s	C-STORE: Host_C -> Host_D	WORKSTATION	70	68 / 2	04.01.2011 15:25:18	04.01.2011 15:28:44	3:25 m	175.86 KB/s
Transfer	Destination AET	Objects	OK/Failed	Sendtime	Receivetime	Duration	Bandwidth																														
UPLOAD: Host_A -> Host_B	TRGATEWAY1	70	70 / 0	04.01.2011 15:24:42	04.01.2011 15:24:58	16 s	2247.13 KB/s																														
C-STORE: Host_B -> Host_C	TRGATEWAY2	70	70 / 0	04.01.2011 15:25:01	04.01.2011 15:25:16	14 s	2448.76 KB/s																														
C-STORE: Host_C -> Host_D	WORKSTATION	70	68 / 2	04.01.2011 15:25:18	04.01.2011 15:28:44	3:25 m	175.86 KB/s																														
<small>* The times for the transfer details are relative to the local system time. The values (objectcount, ok, failed, etc.) are receiver based.</small>																																					
Patient details: <table border="1"> <thead> <tr> <th>Name</th> <th>Sex</th> <th>Birthdate</th> <th>Modality</th> <th>Studydescription</th> <th>Studydate</th> <th>Database</th> </tr> </thead> <tbody> <tr> <td>Jane Doe</td> <td>F</td> <td>1951-06-05</td> <td>CT</td> <td>80 ml Ultravist,venous kidneys</td> <td>2010-11-18</td> <td>patiendb</td> </tr> </tbody> </table>						Name	Sex	Birthdate	Modality	Studydescription	Studydate	Database	Jane Doe	F	1951-06-05	CT	80 ml Ultravist,venous kidneys	2010-11-18	patiendb																		
Name	Sex	Birthdate	Modality	Studydescription	Studydate	Database																															
Jane Doe	F	1951-06-05	CT	80 ml Ultravist,venous kidneys	2010-11-18	patiendb																															

Abbildung 4.11.: Darstellung der Multiknotenstatistik in der Administrationsoberfläche des Teleradiologiesystems

Datum	Empfänger	Vers.	Patient	Status
17.05.2011 14:27:09	chilmv27	1	Schädel,Sascha	Beendet: Alle 2 Objekte erfolgreich verarbeitet
17.05.2011 14:24:07	chilmv			
17.05.2011 14:22:58	chilmv			
17.05.2011 14:22:07	chilmv			
17.05.2011 13:44:17	chilmv			
17.05.2011 13:33:45	chilmv			
17.05.2011 13:29:40	chilmv			

Patient	Geb.Dat.	Studiendatum	Beschreibung	Modality	Anzahl Bilder
Schädel,Sascha	10.01.1973	29.12.2010	Schädel,02_CCT_Trauma (Erwachsener)	CT	2

Transfer	AET	Start	Ende	Dauer	ok/failed
DICOMSEND: 192.168.161.96 -> 192.168.161.97	CHILNM27	2011-05-17 14:27:09	2011-05-17 14:27:12	2 s	2/0
UPLOAD: 192.168.161.97 -> vm-43	VM-43	2011-05-17 14:27:10	2011-05-17 14:27:12	1 s	2/0

Abbildung 4.12.: Darstellung der Multiknotenstatistik direkt im PACS-Viewer

Die Multikontenstatistik unterstützt die Anwender bei der Erstellung von statistischen Auswertungen und der Generierung von Protokollen zur Dokumentation der Abnahme- und Konstanzprüfung, die in Deutschland zur Qualitätssicherung nötig sind und zu diesem Zweck bei der Genehmigungsbehörde vorgelegt werden müssen.

4.4. DICOM E-Mail und IHE XDM

DICOM E-Mail ist mit dem Whitepaper der Arbeitsgruppe Informationstechnologie der Deutschen Röntgengesellschaft (@GIT) und insbesondere mit den in Kapitel 3.1.1 beschriebenen Service Part E-Mails eine starke Basis für die Vernetzung in der Teleradiologie in Deutschland. Zwei große Netzwerke, das Teleradiologieprojekt Rhein-Neckar-Dreieck (Teleradiologie RND, 2015) sowie der Westdeutsche Teleradiologieverbund (MEDICON Telemedizin GmbH, 2018), basieren ausschließlich auf DICOM E-Mail und verwenden die entwickelten Techniken in Routine.

Um die etablierten Techniken und Verfahren auch über Deutschland hinaus zu verbreiten und verfügbar zu machen, wurde in Zusammenarbeit mit der IHE Deutschland und der @GIT das IHE-Profil Quality Controlled Image Transfer (QCIT) entwickelt. Hierbei wurde das gesamte auf DICOM E-Mail basierte Whitepaper überarbeitet und die folgenden essentiellen Teile beibehalten und herausgearbeitet.

ZIP over Email: Für den Versand und Empfang von DICOM- und nicht-DICOM-Daten via E-Mail.

ZIP over Email Enhanced Response beinhaltet sowohl einfache als auch erweiterte Empfangsbestätigungen für DICOM E-Mails.

ZIP over Email QC Request: Ein Verfahren zur Konstanzprüfung der Teleradiologiestrecke in einem DICOM E-Mail Netzwerk.

Bei der Erstellung des IHE Drafts zu QCIT wurde auf das bestehende IHE-Profil XDM für den Transfer der DICOM- und nicht-DICOM-Daten zurückgegriffen. Dadurch wird auf der einen Seite der bewährte DICOM E-Mail Workflow unterstützt, auf der

anderen Seite lässt sich durch die Verwendung von XDM ein DICOM E-Mail-Partner nahtlos in eine XDS-Infrastruktur integrieren.

Um besser auf die internationalen Anforderungen einzugehen, wurde das Verschlüsselungsverfahren für E-Mail insofern geändert, dass das in Deutschland gebräuchliche PGP/GPG-Verfahren durch das im IHE-Kontext bereits etablierte S/MIME Verfahren abgelöst wurde.

Die erweiterte Empfangsbestätigung wurde analog dem DICOM E-Mail Service Part DISPOSITIONNOTIFICATION umgesetzt und erlaubt so zusammen mit den X-IHE-QCIT-SET Header-Tags eine Kontrolle der Übermittlung von DICOM E-Mails sowohl auf Seiten des Senders als auch des Empfängers.

Weiterhin wurde die im DICOM E-Mail Whitepaper beschriebene Konstanzprüfung auf das IHE QCIT Profil übertragen und adaptiert, um auch hier eine automatische Konstanzprüfung und Überwachung des Teleradiologienetzwerks zu ermöglichen.

Die im Whitepaper beschriebenen Möglichkeiten zur Administration eines DICOM E-Mail Netzwerks wurden nicht in das QCIT Profil überführt, um sich im ersten Schritt auf die Übertragung der Inhalte und nicht auf die technische Administration zu fokussieren.

Der Draft des Profils wurde Anfang 2016 durch IHE Deutschland und die @GIT im IHE Radiology Planning Committee eingereicht. Trotz der Bemühungen der Arbeitsgruppen wurde der Entwurf leider nicht in den Prozess zur Aufnahme in das Technical Framework angenommen. Hier zeigte sich der Unterschied in der Vernetzung zwischen Deutschland und den Netzwerken in der USA. Während in Deutschland vor allem die einfache und schnelle Vernetzung von einzelnen Partnern untereinander im Vordergrund steht, bilden sich in den USA größere Netzwerke auf Basis von XDS beziehungsweise sind bereits etabliert. Aus diesem Grund legt die IHE ihren Fokus eher auf die XDS-basierte Vernetzung und hat keine Verwendung für die schnelle Ad-hoc-Teleradiologie, die in Deutschland mit DICOM E-Mail ermöglicht wird.

Da die Arbeitsgruppe die erarbeiteten Ergebnisse dennoch weiter voranbringen wollte, wurde erwogen, Teile des Drafts für QCIT über IHE Deutschland als nationale Erweiterung des IHE-Profiles XDM umzuarbeiten und diesen erneut einzureichen. Dies ge-

staltete sich aber schwierig, und so wurde als erster Schritt ein Change Proposal in die IHE-Domäne Radiologie eingereicht (CP-RAD-408), welches unter 'Best Practice for the Grouping of PDI with XDM' die Verknüpfung der beiden IHE-Profile XDM und PDI beschreibt. Dadurch wird ermöglicht, sowohl DICOM- als auch nicht-DICOM-Daten in einem XDM/XDS-basierten Netzwerk per E-Mail übertragen zu können, was im Kern immer noch dem Grundgedanken von QCIT entspricht.

Das Change Proposal 408 'Best practice for the grouping of PDI with XDM' wurde durch das IHE-Komitee angenommen und Mitte 2018 zum Final Text. So konnten die Änderungen bereits auf dem IHE Connect-a-thon, welcher 2019 in Rennes (Frankreich) stattfand, von einzelnen Herstellern erfolgreich getestet werden.

Durch die Erweiterungen von IHE XDM und PDI ist es jetzt möglich, DICOM- und nicht-DICOM-Objekte wie zum Beispiel PDFs auf einem Transportmedium wie einer Patienten-CD oder E-Mail zusammengehörend zu übermitteln. Damit ist die erste Hürde, DICOM E-Mail Funktionen in das Technical Framework der IHE aufzunehmen, überwunden. Es wurde ein standardisierter Weg für den IHE-konformen Austausch behandlungsrelevanter (Bild-)Daten per E-Mail geschaffen.

4.5. Intersektorale Vernetzung unter Verwendung von IHE-Profilen

Unter Verwendung der Methoden aus Kapitel 3.4 wurde im Rahmen des BMBF (BMBF, 2017) geförderten INFOPAT-Projekts (Infopat MRN, 2018; Universitätsklinikum Heidelberg, 2018) eine persönliche, einrichtungsübergreifende elektronische Patientenakte realisiert, welche sowohl medizinischen Anwendern wie Ärzten und Pflegepersonal als auch den Patienten selbst Zugang zu allen wichtigen Daten gibt.

Da IHE-basierte Kommunikation auch in Deutschland und insbesondere im Bereich der Teleradiologie immer wichtiger wird (Bergh et al., 2015), setzt das Projekt im Bereich des Bildmanagements auf IHE XDS-I und die dazugehörigen Profile. Hierbei war eine der größten Herausforderungen auch nicht-IHE XDS-fähige Systeme in das Netzwerk

einzubinden und die Daten performant und ohne große Wartezeit auf dem Bildschirm der Anwender zur Anzeige zu bringen, egal in welchem Repository oder Primärsystem sie sich befinden. Die Erstellung eines XDS-Adapters war auch deshalb nötig, weil das Projekt parallel zum Klinikbetrieb ohne größere Änderungen an der Infrastruktur oder dem bestehenden PACS lauffähig sein musste, um während des Projektverlaufs agil auf neue Anforderungen reagieren zu können.

4.5.1. XDS-Adapter

Im ersten Schritt wurde durch den Autor ein vielseitig einsetzbarer XDS-Adapter entwickelt, der es erlaubt, nicht-IHE-fähige Systeme anzuschließen und die von ihnen gelieferten Metadaten durch ein konfigurierbares Mapping auf XDS Value Sets abzubilden. Hierbei wurden je nach Verfügbarkeit auf Daten des DICOM-Headers oder HL7-Nachrichten zugegriffen. Im Rahmen des Projekts wurden die beteiligten PAC-Systeme der angeschlossenen Kliniken auf diese Weise angebunden.

Der Prozess der Registrierung wird durch den Patienten selbst im Rahmen seiner Einwilligung zur PEPA angestoßen. Im Falle der Einwilligung sendet das KIS eine HL7-Nachricht mit entsprechendem Status an den XDS-Adapter. Dieser holt die Bilddaten auf Basis der Accession-Number und Patienten-ID via DICOM Q/R aus dem Primär-PACS, erstellt das entsprechende KOS-Objekt mithilfe der DICOM-Metadaten und Informationen aus der HL7-Nachricht und registriert es mit den erstellten Value Sets im XDS Registry (siehe Abbildung 3.12). Weiterhin fungiert der Adapter zusätzlich als XDS Consumer und wird in dieser Rolle für die Kommunikation mit dem Repository und zur Bildanzeige verwendet. Nicht-XDS-fähige Akteure können den Adapter via URL-Aufruf ansprechen und so die zuvor registrierten Bilder mit dem integrierten DICOM-Viewer zur Anzeige bringen.

Um die Kommunikation mit den beteiligten Systemen so einfach wie möglich zu gestalten, wurde weiterhin ein Single-Sign-On-Verfahren auf Basis von IHE Cross-Enterprise User Assertion (XUA) beziehungsweise Security Assertion Markup Language (SAML) implementiert.

Im Rahmen der Projektlaufzeit von 2012 bis 2017 und anschließend bis heute sind die Anwender- und Studienzahlen der PEPA stetig gestiegen, immer mehr Patienten willigen in die Speicherung ihrer Daten in die PEPA ein.

Tabelle 4.1.: Patienteneinwilligung zur Speicherung ihrer Daten in der PEPA über den Projektzeitraum hinaus bis 2019

Patienteneinwilligung	2014	2015	2016	2017	2018	2019
Ja	3963	3681	6171	6443	7565	7983
Nein / Keine Angaben	21849	21792	19035	18600	16203	16208
Gesamt	25812	25473	25206	25043	23768	24191

Tabelle 4.2.: Anzahl der registrierten DICOM-Studien in der PEPA über den Projektzeitraum hinaus bis 2019

Studien	2014	2015	2016	2017	2018	2019
	1080	35676	34751	48056	77452	82485

Wie in Tabelle 4.1 zu sehen ist, steigt die Zahl der Patienten, die der Nutzung der PEPA zustimmen, von 3962 im Jahr 2014 auf 7983 im Jahr 2019 stetig an, wobei die Gesamtanzahl der Patienten nahezu konstant bleibt. Trotz der gleichen Anzahl an Patienten erhöht sich jedoch die Summe der registrierten Studien kontinuierlich, von 1080 bei Projektstart auf 82485 im Jahr 2019. Der Anstieg der registrierten Studien zeigt die immer größeren Bilddatenmengen, die von der PEPA verwaltet werden müssen.

Die Zustimmung der Patienten wurde auf Basis von HL7 MDM-Nachrichten eingeholt. Im Projektverlauf empfing der XDS-Adapter neben den teilnehmenden Abteilungen der Klinik auch HL7-Nachrichten von anderen Abteilungen, in denen die PEPA noch nicht ausgerollt war. Da im KIS der Kliniken 'Keine Angabe' grundsätzlich als 'Nein' gewertet und übermittelt wird, ist so die hohe Zahl der ablehnenden Patienten zu erklären. Eine interne Umfrage in zwei teilnehmenden Kliniken hat weiterhin gezeigt, dass die Patienten, welche über einen zentralen Aufnahmeprozess (Thoraxklinik Heidelberg) kommen, zu einem hohen Prozentsatz einwilligen. Bei einer dezentralen Aufnahme auf Station

(Universitätsklinikum Heidelberg) unterscheidet sich die Zahl der Patienten, die nicht zustimmen kaum, allerdings ist die Zahl der nicht ausgefüllten Einwilligungen höher, was unter Umständen auf fehlende Aufklärungsbögen zurückzuführen ist (Abbildung 4.13).

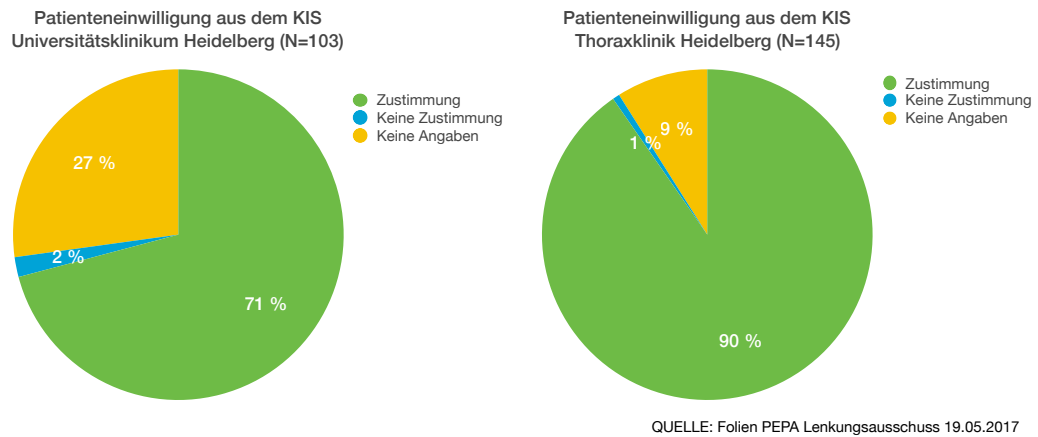


Abbildung 4.13.: Stichprobe der Patienteneinwilligung in die Nutzung der PEPA

Hier hat sich gezeigt, dass der Faktor Mensch trotz ausgefeilter Technik und einem in die Systeme integrierten Einwilligungsmanagement immer noch entscheidend ist und man die Patienten entsprechend aufklären und Hilfestellung leisten muss, um eine Teilhabe am Behandlungsprozess zu ermöglichen.

4.5.2. Imaging Cache

Im Rahmen der Projektlaufzeit zeigte sich, dass ein reiner XDS-Adapter für den Zugriff auf die Daten aus den Primärsystemen zwar grundsätzlich in der Lage ist, die technischen Anforderungen an die XDS-basierte Infrastruktur zu erfüllen, die Geschwindigkeit des Gesamtsystems aber stark von der Verbindung zwischen Adapter und Primärsystem abhängt. Da alle Bilddaten sowohl zur Erstellung des KOS-Objekts und zur Registrierung im XDS Registry als auch später zur zeitversetzten Anzeige per DICOM Q/R aus dem PACS geholt werden müssen, stellt dies einen erheblichen Flaschenhals dar.

Aus diesem Grund wurde ein Imaging Cache entwickelt und in den XDS-Adapter integriert. Der Imaging Cache hat einen dedizierten Speicher für DICOM-Daten und hält je nach Größe des Speichers die per DICOM Q/R empfangenen Bilddaten eine gewisse

Zeit vor. Dies hat zur Folge, dass Daten, die gerade registriert wurden, auch direkt vom Anwender ohne Zeitverzögerung geladen werden können. Der Bildcache verwaltet den ihm zugeteilten Speicher und löscht bei Erreichen eines konfigurierten Füllstands selbstständig die ältesten Studien. Hierbei wird zusätzlich der Zeitpunkt des letzten Zugriffs auf die Bilddaten berücksichtigt, so dass Daten, die sich vor kurzem im Zugriff befanden, eine längere Zeit im Cache verbleiben. Sollte nach Löschen der Daten ein erneuter Zugriff auf die Bilder erfolgen, so werden sie wie zuvor erneut per DICOM Q/R aus dem Primärsystem geladen und dem Nutzer mit etwas Verzögerung angezeigt.

Tabelle 4.3.: Retrievedauer für den erfolgreichen Retrieve mittels DICOM Q/R der häufigsten Modalitäten innerhalb eines Jahres. (Zeit wurde in ms gemessen. Anzeige gerundet)

Modalität	Retrieves	Dauer min.	Dauer max.	Dauer \emptyset	Dauer σ
CT	9617	2.8 s	1h 3 min 25 s	1 min 52 s	2 min 2 s
US	8719	2.9 s	9 min 14 s	23 s	25 s
CR	8035	2.8 s	5 min 8 s	9 s	6 s
MR	5595	2.9 s	15 min 6 s	1 min 15 s	1 min 37 s
DX	2212	3.7 s	52 s	8 s	3 s
XA	2023	2.9 s	9 min 32 s	28 s	46 s

Tabelle 4.3 zeigt die Anzahl der erfolgreichen DICOM Retrieves der häufigsten Modalitätentypen auf Studienebene. Die Retrievezeiten schwanken hier zwischen wenigen Sekunden bis hin zu Stunden. Im Durchschnitt benötigt der Retrieve einer CT-Studie ca. 1:52 Minuten. Schlüsselst man dies weiter auf, so sieht man, dass von den 14510 per DICOM Q/R angefragten Studien (Tabelle 4.4) lediglich 9617 erfolgreich geholt werden konnten. Die fehlerhaften Retrieves sind auf Verbindungsprobleme bei der DICOM-Kommunikation sowie krankenhausinterne Netzwerkprobleme zurückzuführen, welche unter Anwendung des Cachings weniger stark ins Gewicht fallen.

Um die Ladezeit weiter zu beschleunigen, wurde zusätzlich ein Streaming-Mechanismus in den DICOM-Viewer implementiert, der es erlaubt, auch Teile von Studien anzusehen, selbst wenn diese noch nicht vollständig auf dem Server vorliegen. Je nach Untersuchungsart ist es unter Umständen nicht nötig, alle Serien einer Studie anzuzeigen. Dies gilt insbesondere für Schnittbildaufnahmen wie die von CT- oder MR-Modalitäten, bei

Tabelle 4.4.: Transfergröße für empfangene Studien mittels DICOM Q/R der häufigsten Modalitäten innerhalb eines Jahres. (Studiengröße wurde in Byte gemessen. Anzeige gerundet)

Mod.	Anzahl	Bilder				Größe			
		min.	max.	\emptyset	σ	min.	max.	\emptyset	σ
CT	14510	1	9709	935	914	0 KB	3437 MB	282 MB	574 MB
US	10258	1	253	29	25	20 KB	1916 MB	83 MB	211 MB
CR	8418	1	8	2	1	370 KB	143 MB	10 MB	13 MB
MR	8497	1	7589	725	923	320 KB	2950 MB	114 MB	349 MB
DX	2355	1	667	1	14	2 MB	185 MB	5 MB	10 MB
XA	3876	1	3093	343	112	760 KB	3066 MB	223 MB	586 MB

denen oft nur einzelne Serien benötigt werden. Durch den oben beschriebenen Cache-Mechanismus sind dem Server grundsätzlich alle durch ihn registrierten Studien mit ihren Metainformationen bekannt, so kann dem Nutzer angezeigt werden, wie viele Bilder schon auf dem Server verfügbar sind und welche im Hintergrund noch geladen werden müssen.

Tabelle 4.5 zeigt die Ladezeit von bereits im System beziehungsweise Cache vorhandenen Bildern. Die mittlere Ladezeit beträgt hier 50 ms, eine durchschnittliche CT-Studie kann mit ihren 935 Bildern so innerhalb von 46,8 Sekunden vollständig zur Anzeige gebracht werden. In den meisten Fällen wird nicht die komplette Studie, sondern nur einzelne Serien einer Studie benötigt, so dass nie alle Bilder zwischen Client und Server übertragen werden müssen, was die Ladezeit und Performance weiter beschleunigt.

Tabelle 4.5.: Bildladezeit für auf dem Server vorliegende DICOM-Studien. (Zeit wurde in ms, Bildgröße in Byte gemessen. Anzeige gerundet)

Dauer				Größe			
min.	max.	\emptyset	σ	min.	max.	\emptyset	σ
0 ms	9 s	50 ms	129 ms	5 KB	38 MB	451 KB	1 MB

Durch die Etablierung des Imaging Caches konnte die Akzeptanz der Nutzer weiter gesteigert werden, da Bilder schnell und ohne lange Wartezeit im DICOM-Viewer angezeigt werden können. Trotzdem ist das System noch vollständig kompatibel zu IHE

XDS-I. DICOM-Bilder können auch ohne Verwendung des Imaging Caches aus dem XDS Repository und dem primären PACS geholt werden.

4.5.3. Request-Broker

Da sich die Anwender des Systems in den Netzwerken unterschiedlicher Kliniken befinden und teilweise auch über das Internet auf die Daten zugegriffen wird, musste ein System entwickelt werden, welches es ermöglicht, den Imaging Cache auch für verteilte Anfragen und über mehrere Standorte hinweg einzusetzen.

Hierzu wurde ein Request-Broker implementiert, welcher Anfragen aufgrund der im KOS-Objekt referenzierten Studien zu dem für die Daten zuständigen XDS-Adapter beziehungsweise Imaging Cache weiterleitet. Dieser Request-Broker steht in der Hauptdomäne der PEPA und ist gegen das Internet durch eine Web Application Firewall (WAF) abgesichert, welche in der demilitarisierten Zone (DMZ) des PEPA-Netzes steht.

Der Request-Broker nimmt HTTP- beziehungsweise HTTPS-basierte Anfragen zu Bilddokumenten von den angeschlossenen Subsystemen wie KIS, RIS oder der Patientenakte in Form einer XDS Dokumenten-ID entgegen. Die angefragten Dokumente (im Falle von DICOM also KOS-Objekte) werden daraufhin aus dem entsprechenden XDS Repository geholt und ausgewertet. Das KOS-Objekt enthält sowohl die eigentlichen Studien- und Bildinformationen als auch den Speicherort der Bilddaten in Form eines RetrieveLocationAET (Application Entity Title). Die bekannten Speicherorte sind in Form einer Mappingtabelle auf dem Request-Broker hinterlegt, so werden die eigentlichen Anfragen nach Auswertung des KOS-Objekts an den für die Bilder zuständigen Imaging Cache des jeweiligen Krankenhauses weitergeleitet.

Durch diesen Mechanismus bietet der Request-Broker einen zentralen Einstiegspunkt für alle nicht XDS-I fähigen Aktoren im Netzwerk und leitet deren Anfragen an den jeweils für die Bilder zuständigen Imaging Cache der einzelnen Kliniken weiter. Hierbei kommt ein Reverse Proxy Mechanismus zum Einsatz, so dass Anfragen für den Aufrufer transparent, durch die WAF abgesichert, weitergeleitet werden. Der Request-Broker

kann dabei auch selbst als Imaging Cache eingesetzt werden und Anfragen nach Bildern bei Bedarf auch eigenständig beantworten.

DICOM-Export

Obwohl alle Daten über die PEPA eingesehen werden können, gibt es die Notwendigkeit, einzelne Datensätze zur weiteren Analyse in Spezialsysteme oder generell in das Primärsystem eines anderen Krankenhauses zu übertragen, falls der Patient dort behandelt werden sollte. Hierzu wurde in den Request-Broker eine Exportschnittstelle für DICOM-Daten implementiert, welche es bei entsprechender Berechtigung des Nutzer erlaubt, die Daten direkt aus dem Viewer des Imaging Caches per DICOM C-Store in das Primär-PACS des Krankenhauses zu übertragen. Dadurch können Radiologen die Bilder nicht nur im Viewer des Imaging Caches, sondern auch in ihrer gewohnten Arbeitsumgebung befunden.

4.6. Mobile Bildbetrachter für Ärzte, Patienten und den Ad-hoc-Zugriff

Um sowohl Ärzten als auch Patienten im Rahmen der PEPA (Kapitel 4.5) einen einfachen und schnellen Zugang zu den für sie relevanten Bilddaten zu ermöglichen, wurde der bestehende mobile Zero-Footprint Viewer CHILI/Mobile um die Funktion eines standardisierten SSO mittels SAML erweitert.

Die Verwendung des SSO ermöglicht es den Benutzern der PEPA, direkt aus ihrem Bereich der Akte, im Falle von ärztlichen Nutzern aus dem Professional Portal und im Falle von Patienten aus dem Patientenportal, ohne erneute Eingabe ihres Benutzernamen und Passwort auf ihre Bilder zuzugreifen.

Da Bilddaten bei der Verwendung von XDS-I nicht direkt aus einem Repository geladen werden können, musste hier auch der Imaging Cache um den XDS-basierten SSO-Aufruf des CHILI/Mobile erweitert werden.

Abbildung 4.14 stellt die Schritte zur Auslieferung des mobilen Bildbetrachters mittels SAML Token und XDS Retrieve dar. Diese Schritte werden nachfolgend beschrieben:

1. Der Nutzer der PEPA möchte auf Bilder der aktuellen Akte zugreifen und ist bereits in der PEPA angemeldet. Die Akte generiert ein SAML Token für den Zugriff auf den Bildbetrachter, welcher zusammen mit dem XDS DocumentSetRequest an den Imaging Cache in einem HTTP-Request gesendet wird. Hierbei ist keine Abfrage des XDS Registry nötig, da der Nutzer in der Akte bereits alle benötigten Daten über HomeCommunityId, RepositoryUniqueId und DocumentUniqueId vorliegen hat.
2. Der Imaging Cache erhält und prüft das SAML Token auf Gültigkeit. Weiterhin werden alle im Request übermittelten Parameter ausgewertet, um die Konfiguration des konkreten Bildbetrachters aufgrund der im Token übergebenen Nutzerdaten zu laden.
3. Der Imaging Cache lädt das im Request angegebene KOS-Objekt auf Basis der RepositoryUniqueId und DocumentUniqueId aus dem entsprechenden XDS Repository.
4. Der Imaging Cache überprüft, ob die referenzierten DICOM-Daten noch im Cache vorhanden sind.
5. Bei Bedarf werden die DICOM-Daten erneut von dem im KOS-Objekt angegebenen primären PACS geladen.
6. Sobald das erste Bild der DICOM-Studie im Imaging Cache verfügbar ist, wird der parametrisierte mobile Viewer in der HTTP-Response zum Request aus Schritt 1 an den Nutzer zurückgeliefert. Der Nutzer kann somit schon Bilder im Viewer betrachten, auch wenn noch nicht alle Bilder der Studie vollständig aus dem Primärsystem abgeholt worden sind.

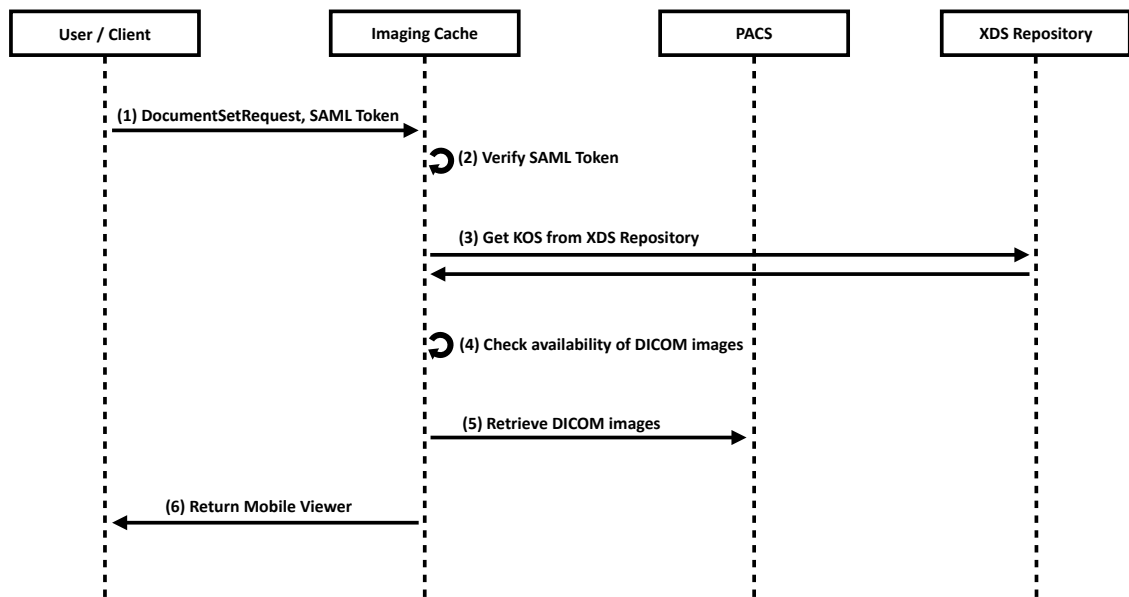


Abbildung 4.14.: Ablauf des SAML-basierten Zugriffs auf Bilddaten in einem XDS Repository mittels SSO und CHILI/Mobile.

Diese Lösung versetzt Nutzer nun in die Lage, aus der PEPA direkt auf alle für sie verfügbaren Bilder zuzugreifen, ohne sich erneut zu authentifizieren oder wissen zu müssen, in welchem Repository beziehungsweise primären PACS die Bilder wirklich liegen.

Im Rahmen der PEPA wurde den ärztlichen und insbesondere radiologischen Nutzern aus dem Professional Portal ein direkter Zugriff auf die Bilddaten mit Befundungsqualität in einem vollständigen DICOM-Viewer ermöglicht. Patienten und andere ärztliche Nutzer erhalten primär den einfachen Zero-Footprint Viewer zum Zugriff auf die Daten erhalten. Da beide Bildbetrachter aber über den Imaging Cache und die in Kapitel 4.5 beschriebenen Methoden des Request-Brokers ausgeliefert werden, ist es auch möglich, nahtlos ohne erneuten Login zwischen den beiden Viewern zu wechseln. Weiterhin kann je nach verfügbarem Endgerät, also Desktop PC oder Tablet beziehungsweise Smartphone, immer der bestmögliche Bildbetrachter an den Nutzer ausgeliefert werden.

4.7. Portale für Ärzte und Patienten

Durch das Refactoring und die Migration der CHILI/Medizinakte (Kapitel 3.6) auf aktuellen Web-Technologien wurde die Basis für die Erstellung zahlreicher Portale für die

Vernetzung zwischen Ärzten sowie Ärzten und Patienten geschaffen. Die Weiterentwicklungen im Bereich der Workflowsteuerung, die Schnittstellen zu Fremdsystemen und das Freigabemodul gestatten, eine Vielzahl an telemedizinischen Anwendungsfällen abzudecken. Die Auswertungs- und Protokollierungswerkzeuge ermöglichen eine detaillierte Nachverfolgung des Datenflusses und erlauben die Nachverarbeitung von Daten in externen Programmen.

4.7.1. Teleradiologieportal

Mit Hilfe des Teleradiologieportals ist es möglich, den Workflow der teleradiologischen Anforderung und Befundung vollständig elektronisch abzubilden. Der Ablauf von Anforderung einer Untersuchung bis hin zum fertigen Befund kann vereinfacht folgendermaßen dargestellt werden:

1. Anlage einer Anforderung (MTRA)
2. Prüfung der rechtfertigenden Indikation (Teleradiologe / Arzt)
3. Durchführung der Untersuchung (MTRA)
4. Bilddatenversand (MTRA)
5. Befundung (Teleradiologe / Arzt)
6. Befundanzeige (MTRA)

Im ersten Schritt legt die MTRA eine Anforderung direkt im Teleradiologieportal an. Der Radiologe wird durch eine Benachrichtigung über die Anforderung informiert und kann nun die rechtfertigende Indikation (RI) prüfen. Sollte er der Untersuchung zustimmen, wird ein Auftrag erstellt und die MRTA durch eine Benachrichtigung darüber informiert. Nach Durchführung der Untersuchung werden die Bilder automatisch an den Radiologen übermittelt, und dieser kann direkt über den Befund-Client im Portal die

Bilder ansehen und den Befund nahtlos im Portal diktieren. Ist die Befundung abgeschlossen, so erhält die MTRA eine Benachrichtigung und kann den Befund im Portal ansehen.

Alle durchzuführenden Schritte werden durch die implementierte Workflowsteuerung unterstützt, und die Benutzer werden somit durch den Prozess geleitet. Es ist der MTRA also zum Beispiel nicht möglich, die Untersuchung durchzuführen, solange die rechtfertigende Indikation und der Untersuchungsauftrag des Radiologen noch aussteht.

Der gesamte Workflow kann vollständig im Portal abgedeckt werden, aber es ist auch möglich, ein RIS sowohl zur Anforderung auf Seiten der MTRA als auch zur Stellung der RI und Befundschreibung per HL7 zu integrieren. Neben dem in das Portal integrierten Befund-Client können die Bilddaten auch per DICOM zum Radiologen übertragen werden, so dass dieser die Befundung mit seinem gewohnten PACS-Viewer durchführen kann.

Wird sowohl auf Seiten der MTRA als auch beim Radiologen ein RIS mit HL7-Schnittstelle eingesetzt, so kann das Portal auch als transparente Workflowkomponente eingesetzt werden, weder die MTRA noch der Radiologe müssen sich in das Portal einloggen und können vollintegriert in ihren bekannten Systemen arbeiten (Abbildung 4.15).

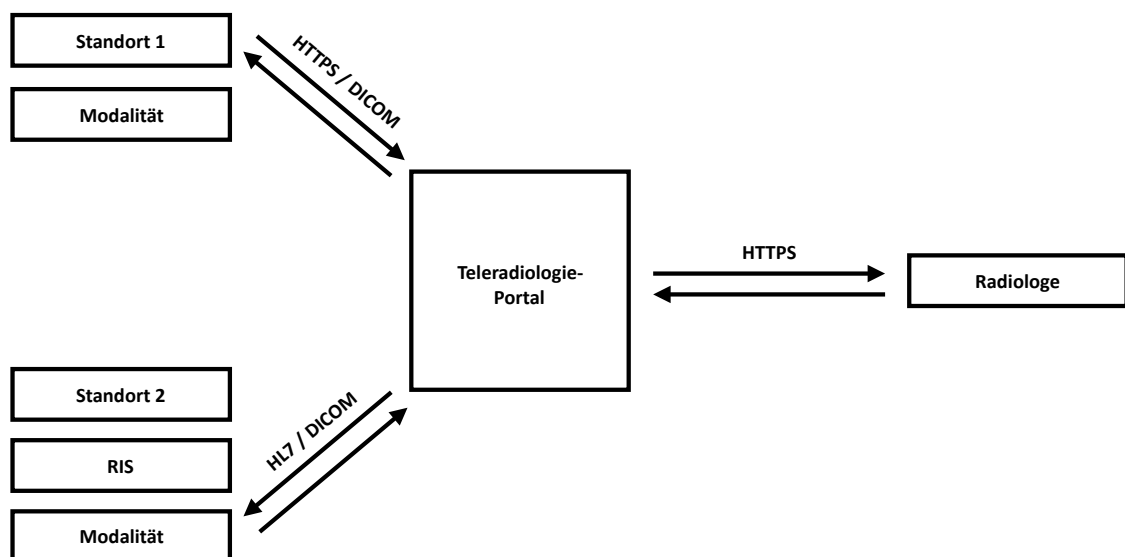


Abbildung 4.15.: Workflow der Befundung mit Teleradiologieportal

Durch den erweiterten Datenexport können alle im Portal angefallenen Daten vollständig ausgewertet werden. Dies kann sowohl zur Prozessoptimierung zum Beispiel bei der Auswertung der Untersuchungsdauer und von Antwortzeiten auf eine Anforderung als auch zur Abrechnung der Untersuchungen eingesetzt werden.

Die in dieser Arbeit beschriebenen Teleradiologieportale sind mittlerweile in mehreren Installationen zur Workflowsteuerung im Einsatz und werden aktiv zur Unterstützung der Teleradiologie verwendet. Beispielhaft für diverse Installationen zeigt Abbildung 4.16 die Nutzung des Teleradiologieportals in einem größeren deutschen Klinikkonzern zur Sicherstellung der teleradiologischen Befundung in der Nacht und am Wochenende. Seit Projektbeginn im Jahr 2016 ist dort die Anzahl der verarbeiteten DICOM-Studien von 207 auf 2821 im Jahr 2019 kontinuierlich angestiegen. Bei 253 verarbeiteten Studien im Januar 2020 lässt sich weiterhin ein Anstieg der durchgeführten teleradiologischen Befundungen erkennen, der bei linearem Wachstum bis Ende 2020 auf über 3000 Befunde pro Jahr anwachsen wird.

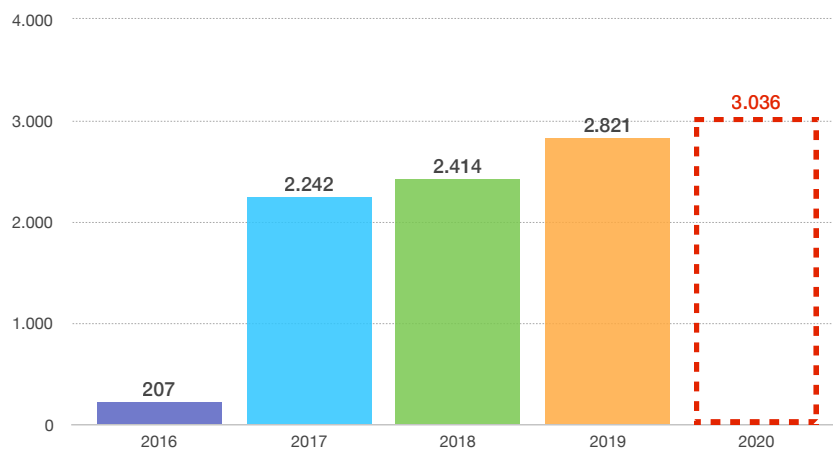


Abbildung 4.16.: Anzahl der verarbeiteten DICOM-Studien im Teleradiologieportal pro Jahr mit linearer Projektion bis 2020.

Wie diese Zahlen zeigen ist die Teleradiologie mittels Teleradiologieportal also bereits jetzt ein fester Bestandteil der Patientenversorgung. Auch andere Installationen von vergleichbarer Größe zeigen ein ähnliches Bild.

Dienstplan

Um den Workflow der teleradiologischen Befundung mit mehr als einem Befunder abbilden zu können, wurde in das Teleradiologieportal ein Dienstplanmodul integriert. Hier kann zeit- und gruppengesteuert jedem Standort beziehungsweise jeder Modalität eines Standorts ein Befunder zugewiesen werden (Abbildung 4.17). Gibt es technische Probleme oder fällt ein Befunder kurzfristig aus, so kann dieser mühelos über die Oberfläche getauscht werden.

		< KW 38/52 (2018) >		Aktuelle Woche		Neuer Eintrag		Vorlage		Befunder	
		Gruppe	Modalität	Montag 17.09.2018	Dienstag 18.09.2018	Mittwoch 19.09.2018	Donnerstag 20.09.2018	Freitag 21.09.2018	Samstag 22.09.2018	Sonntag 23.09.2018	
Krankenhaus A CT	00:00 - 07:59	bert		00:00 - 07:59	anor	00:00 - 07:59	meyt	00:00 - 07:59	mos	00:00 - 07:59	nora
	08:00 - 16:59			08:00 - 16:59		08:00 - 14:59		08:00 - 16:59		08:00 - 16:59	
	17:00 - 23:59	anor		17:00 - 23:59	meyt	15:00 - 16:59	eis	17:00 - 23:59	werh	07:00 - 07:59	aura
						17:00 - 21:59	seil		08:00 - 14:59		
						22:00 - 23:59	moer		15:00 - 16:59		
									17:00 - 23:59		
									08:00 - 14:59		
									15:00 - 16:59		
									17:00 - 23:59		
									08:00 - 14:59		
									15:00 - 16:59		
									17:00 - 23:59		
									08:00 - 14:59		
									15:00 - 16:59		
Krankenhaus B MRT	00:00 - 07:59	bert		00:00 - 07:59	anor	00:00 - 07:59	meyt	00:00 - 07:59	mos	00:00 - 07:59	nora
	08:00 - 16:59			08:00 - 16:59		08:00 - 16:59		08:00 - 16:59		08:00 - 16:59	
	17:00 - 23:59	anor		17:00 - 23:59	meyt	17:00 - 21:59	seil	17:00 - 23:59	werh	07:00 - 07:59	aura
						22:00 - 23:59	moer		08:00 - 16:59		
									17:00 - 23:59		
									08:00 - 16:59		
									17:00 - 23:59		
									08:00 - 16:59		
									17:00 - 23:59		
									08:00 - 16:59		
									17:00 - 23:59		
									08:00 - 16:59		
									17:00 - 23:59		
									08:00 - 16:59		

Abbildung 4.17.: Dienstplan zur zeitlichen Zuordnung von teleradiologischen Befundern zu Krankenhausstandorten und Modalitäten.

Je nach Standort und Tageszeit können so im Teleradiologieportal die Nachrichten und Bilder zwischen dem Krankenhaus und dem aktuell zuständigen Teleradiologen ausgetauscht werden.

Dieses System ist mittlerweile bei einem großen Befundungsnetzwerk im Einsatz. Es leitete 2017 die radiologischen Bilddaten von mehr als 80 angeschlossenen Krankenhäusern zuverlässig zu den jeweilig diensthabenden Teleradiologen. Diese werden aus einem Pool von über 37 hoch spezialisierten Notfall-Befundern in ganz Deutschland und

Österreich (e-health com, 2017) je nach Verfügbarkeit flexibel durch den Dienstplan zugeordnet. Mittlerweile besteht das Netzwerk aus weit mehr als 100 Kliniken, die ihre teleradiologische Befundung in der Nacht und am Wochenende auf diese Weise durch mehr als 50 Radiologen durchführen lassen.

4.7.2. Zuweiser- und Patientenportal

Durch die flexible Konfiguration der CHILI/Medizinakte ist es möglich, diese auch als Zuweiser- oder Patientenportal einzusetzen und so gleichwohl Ärzten als auch Patienten einen elektronischen Zugriff auf behandlungsrelevante Daten zu ermöglichen.

Das Zuweiserportal befindet sich im Normalfall unter der Kontrolle der Klinik und wird in deren IT-Infrastruktur betrieben. Zuweiser, die regelmäßig mit der Klinik beziehungsweise dem Portal arbeiten, erhalten einen personalisierten Zugang. Hierüber ist es möglich, Bilddaten und andere Dokumente wie zum Beispiel Laborbefunde, Arztberichte und Voruntersuchungen oder eine Einwilligungserklärung vorab in das Portal hochzuladen. Der Zuweiser kann eine neue Akte anlegen und diese selbstständig mit Daten füllen. Dabei bietet die Medizinakte neben dem Upload von Dokumenten und der Eingabe von Text in Freitextfeldern auch die Möglichkeit zur strukturierten Erfassung von Daten mittels Fragebogenelementen. Sind alle relevanten Daten in das Portal eingepflegt, wird eine Mitteilung an die entsprechende Abteilung der Klinik gesendet und der Behandlungsablauf gestartet.

Wird der Patient zur Behandlung in die Klinik aufgenommen, so ist es durch die Integration mit den Subsystemen der Klinik einfach möglich, die durch den Zuweiser bereitgestellten Daten direkt via DICOM- oder HL7-Schnittstelle in das krankenhauseigene KIS, RIS und PACS zu übernehmen.

Dokumente und Bilder, die während der Behandlung des Patienten in der Klinik entstehen, können über die gleichen Schnittstellen in das Portal gesendet werden, und der Zuweiser erhält eine Benachrichtigung über die Aktualisierung der Akteninhalte. Durch die Integration des mobilen Bildbetrachters kann der Zuweiser neben den Dokumenten auch DICOM-Bilder direkt in der Medizinakte betrachten (Abbildung 4.18).

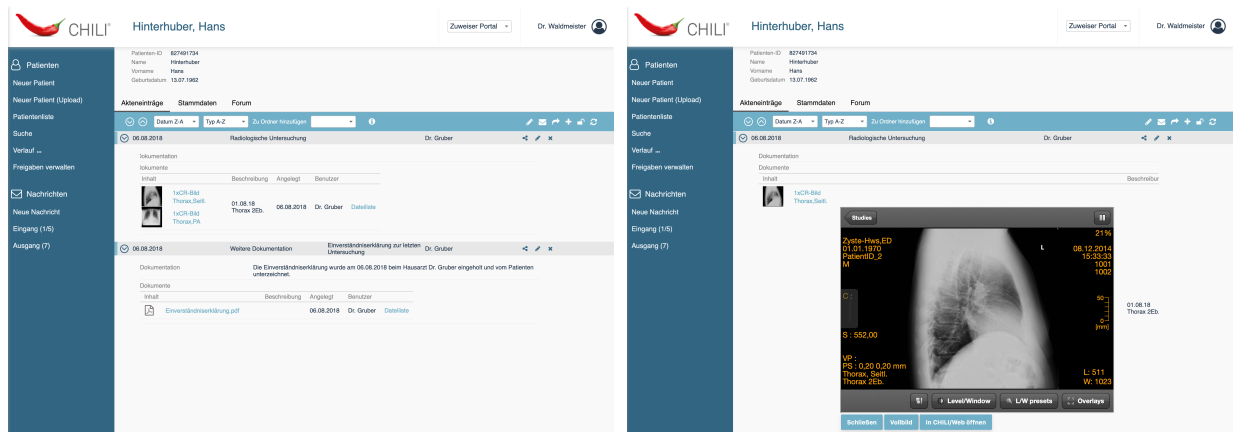


Abbildung 4.18.: CHILI/Medizinakte mit Konfiguration für das Zuweiserportal. Aktenansicht des Patienten (links) und integrierter mobiler Viewer (rechts).

Um die DICOM-Bilder auch in Befundungsqualität anzeigen zu können, wurde in das Portal auch ein vollständiger DICOM-Viewer integriert. Zwischen dem mobilen Viewer und dem DICOM-Viewer kann nahtlos unter Beibehaltung des Kontextes gewechselt werden. Weiterhin ist es möglich, die Daten der Akte sowohl als PDF als auch im JPEG- oder DICOM-Format zu exportieren, um sie auf diesem Weg in das Arztpraxissystem zu übernehmen und mit dem vorhandenen Viewer anzuzeigen.

Wird die Medizinakte als Patientenportal betrieben, so existiert meist kein personalisierter Zugriff für die Patienten. In diesem Fall wird die Akte durch die Klinik angelegt, und der Patient erhält über einen personalisierten Security-Token Zugriff auf seine Akte. Dies kann bereits im Vorfeld der Behandlung geschehen, so dass der Patient selbst Bilddaten, Vorbefunde und weitere behandlungsrelevante Dokumente in die Akte hochladen kann. Auch hier wird das Krankenhaus über den Eingang neuer Dokumente elektronisch benachrichtigt.

Auch im Falle eines Patientenportals ist es möglich, dieses vollständig mit den Subsystemen des Krankenhauses zu integrieren. Ist die Behandlung abgeschlossen, werden in der Klinik entstandene Dokumente und Bilder direkt in der Akte des Patienten gespeichert. Auch hier kann ein Security-Token für den Zugriff erstellt und beispielsweise auf den Entlassungsbericht aufgedruckt werden, so dass keine Notwendigkeit für die Erstellung einer DICOM-CD mehr gegeben ist. Der Zugriff auf die Daten kann durch

das Berechtigungskonzept der Medizinakte gesteuert werden, und die personalisierten Tokens mit einer Ablaufzeit versehen werden. Befinden sich die Daten nicht mehr im Zugriff, so werden sie wieder aus dem Zuweiserportal entfernt, da dieses nur als temporärer Speicher dient und die relevanten Bild- und Befunddaten in den Primär- und Archivsystemen der Klinik weiter vorgehalten werden.


Ein kombinierter Einsatz, der sowohl Zuweisern als auch Patienten Zugriff auf die Behandlungsdaten ermöglicht, kann mit der Medizinakte durch Konfigurationsanpassung ebenso realisiert werden.

4.8. Überwachung von Teleradiologiesystemen

Mit den Methoden aus Kapitel 3.7 ist es möglich, Teleradiologiesysteme kontinuierlich zu überwachen und Fehlerzustände proaktiv zu erkennen. Das Accountingsystem mit allen beschriebenen Erweiterungen wird aktuell auf mehr als 500 Servern aktiv betrieben und ist in den Supportworkflow vollständig eingebunden.

Es kann so jederzeit und auf einen Blick festgestellt werden, ob Kundensysteme, die sich in der Fernwartung befinden, noch erreichbar sind (Abbildung 4.19) beziehungsweise wann zum letzten Mal Daten übertragen wurden. Im Fehlerfall wird der Support per E-Mail über den Ausfall eines Teleradiologiesystems informiert.

:: Accounting > : Kunden Rechner

Rechner 

Nur Accounting Rechner anzeigen:

Nur aktive Accounting Rechner anzeigen:

Erreichbar (< 6h): 484 | Wartend (< 24h): 0 | Nicht Erreicht (> 24h): 3 | Unbekannt: 0

Kunde	Ort	Hostname	Machinelid	Empfangen	Aktiv
			7C:8B:CA:03:71:6B	19.09.2019 ja	X
			F4:03:43:06:21:2E	19.09.2019 ja	X
			vmware:00:0C:29:41:2A:DD	19.09.2019 ja	X
			vmware:00:0C:29:A6:35:52	19.09.2019 ja	X
			28:80:23:90:89:D8	19.09.2019 ja	X

Abbildung 4.19.: Übersicht der aktiven Kundensysteme unter proaktiver Überwachung.

4.8.1. Bandbreitenmessung von Teleradiologiestrecken

Um Leitungsstörungen bei der Teleradiologie nach dem Pull-Modell auszuschließen, ist es sinnvoll, bei der Analyse von Problemen im ersten Schritt die tatsächlich verfügbare Bandbreite des Teleradiologieclients zu messen. Die üblichen Messwerkzeuge, die Internetprovider dafür anbieten, testen allerdings nur die Leitungsgeschwindigkeit des Clients mit einem speziell dafür präparierten Server im Internet, um möglichst gute Werte für den Internetanschluss zu erhalten. Diese Werte geben zwar einen ersten Anhaltspunkt für die Leitungsgeschwindigkeit, können allerdings keine Aussagen für die Übertragungen zwischen einem Client und dem Teleradiologieserver treffen.

Um die konkrete Bandbreite zwischen Client und Server messen zu können, wurde die in Kapitel 3.7.1 beschriebene und implementierte Bandbreitenmessung für Teleradiologiesysteme in das CHILI/Diagnost integriert. Dadurch können Bandbreitenmessungen direkt zwischen Client und Server durchgeführt werden. Hierbei wird auch berücksichtigt, dass die Daten unter Umständen durch ein VPN oder über einen Proxy-Server geleitet werden, welcher die Verarbeitung auch verzögern kann. Die Messung kann direkt durch den Anwender aus dem Client gestartet werden (Abbildung 4.20).

Auch für die Teleradiologie nach dem Push-Modell kann mit Hilfe der Multiknotenstatistik (Kapitel 3.2) oder bei der Konstanzprüfung mittels DICOM E-Mail Service Parts (Kapitel 3.1.1) die Bandbreite der Übertragung zwischen den unterschiedlichen Knoten gemessen werden. Auch hier findet die Übertragung unter realen Bedingungen zwischen dem Teleradiologieserver und Client statt, die konkrete Netzwerkstruktur des Teleradiologienetzwerks wird dadurch bei der Messung berücksichtigt.

Auswertung

Alle durchgeführten Messungen wie auch die anderen Messdaten zur Teleradiologie werden per Accounting zwischen den betroffenen Servern übertragen und können so in Summe ausgewertet werden, um einen ganzheitlichen Blick auf das Teleradiologienetzwerk und die zur Verfügung stehende Bandbreite zu erhalten. Weiterhin lassen sich auch hier

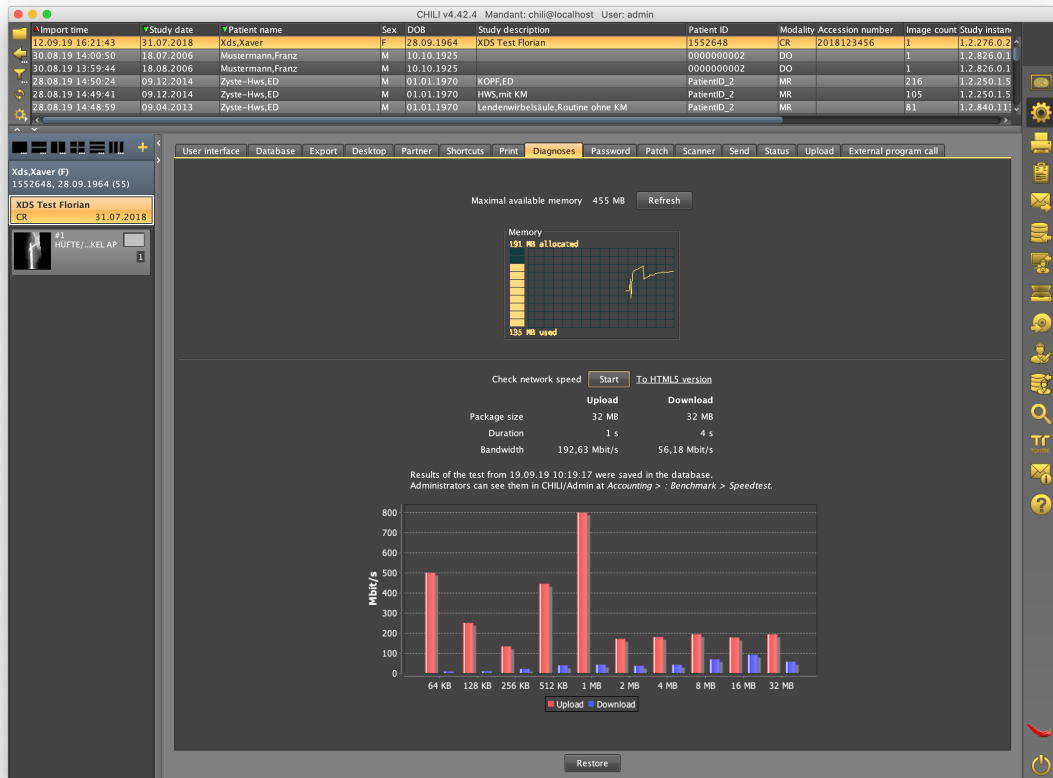


Abbildung 4.20.: Ansicht der Bandbreitenmessung direkt im Teleradiologieclient.

Schwellenwerte für Warnungen einstellen, um den Administrator eines solchen Netzwerks frühzeitig bei Verschlechterung der Übertragungsqualität zu warnen.

4.8.2. Nachverfolgbarkeit von Software

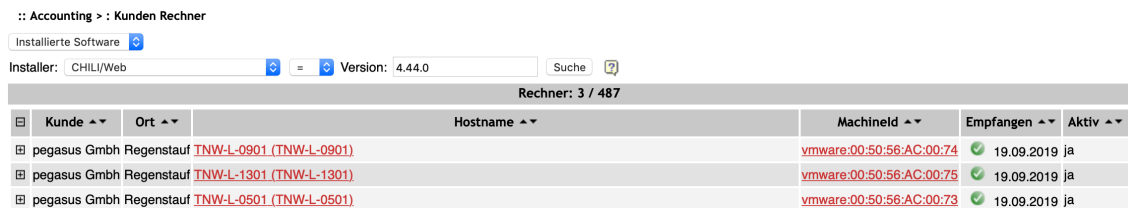
Hersteller von Medizinprodukten, auch im Bereich der medizinischen Software, sind verpflichtet, eine Liste aller von ihnen bei Kunden im Einsatz befindlichen Software vorzuhalten, um Kunden bei Problemen mit einzelnen Programmversionen direkt informieren zu können. Bisher wurden solche Listen ausschließlich in einer Excel-Tabelle oder einer Kundendatenbank gepflegt.

Um die Rückverfolgbarkeit der verschiedenen Softwareprodukte als auch Serverkonfigurationen schneller und einfacher gewährleisten zu können, wurde das Accounting um ein Plugin zur Software- und Hardwareanalyse erweitert. Dieses Plugin sammelt die

Installationsdaten aller auf einem Rechner installierten Herstellersoftware einschließlich der konkreten Version und dem Updateverlauf sowie der Versionen von Standardsoftware wie die des Web-Servers, Datenbank-Servers und weiterer zentraler Dienste. Weiterhin werden auch Daten über die Hardware wie beispielsweise die Netzwerkkonfiguration oder angeschlossene Steckkarten aufgenommen.

Alle Daten werden anschließend über den Fernwartungszugang via Accounting übertragen und durch die implementierte Addon-Schnittstelle (Kapitel 3.7.3) in eine Datenbank zur Auswertung übertragen.

Die Datenbank ermöglicht es, Abfragen auf Basis der empfangenen Daten zu erstellen, mit Hilfe derer man Nutzer, die eine spezifische Programmversion installiert haben, einfach identifizieren kann (Abbildung 4.21). Dies ist besonders im Hinblick auf die Zulassung von Software als Medizinprodukt wichtig, um hier verlässliche Daten direkt von den installierten Systemen zu bekommen und so im Fehlerfall schnell reagieren zu können.



Rechner: 3 / 487					
Kunde	Ort	Hostname	Machineld	Empfangen	Aktiv
pegasus Gmbh Regenstauf	TNW-L-0901 (TNW-L-0901)	vmware:00:50:56:AC:00:74	19.09.2019	ja	
pegasus Gmbh Regenstauf	TNW-L-1301 (TNW-L-1301)	vmware:00:50:56:AC:00:75	19.09.2019	ja	
pegasus Gmbh Regenstauf	TNW-L-0501 (TNW-L-0501)	vmware:00:50:56:AC:00:73	19.09.2019	ja	

Abbildung 4.21.: Anzeige der installierten Software auf Teleradiologiesystemen beim Nutzer.

Auf diese Weise lassen sich nicht nur bestimmte Versionen der Herstellersoftware finden, sondern zum Beispiel auch Rechner mit spezifischen Betriebssystemversionen herausfiltern, um im Bedarfsfall wie zum Beispiel dem Bekanntwerden einer Sicherheitslücke gezielt ein Update anstoßen zu können.

4.8.3. Monitoring Dashboard

Im Rahmen der Bachelorarbeit 'Konzeption und Entwicklung eines Plugins zum proaktiven Fehlermanagement externer Software am Beispiel des CHILI/Accounting' (Weisser, 2018) wurde die implementierte Addon-Schnittstelle des Accounting-Systems verwendet,

um die gesammelten Daten in das Ticket- und HelpDesk-System der Firma CHILI zu integrieren.

Alle von Kundensystemen für die Fernwartung empfangenen Daten werden dem HelpDesk-Addon übergeben. Das Addon bereitet die Daten für die spätere Visualisierung auf und speichert so den aktuellen Zustand der Systeme mit den erhaltenen Warnungen und sonstigen Meldungen in einer Datenbank. Über die Oberfläche des Dashboards (Abbildung 4.22) lassen sich so alle Meldungen einsehen, sortieren, filtern und auch bearbeiten.

The screenshot shows the CHILI HDS Help Desk System interface. At the top left is the logo and name 'HDS CHILI Help Desk System'. The user 'Florian Schwind' is logged in. The dashboard is divided into several sections:

- Navigation Menu (Left):** Tickets, Neues Ticket, Tickettliste, Suchen, Aktuelles anzeigen, Datenexport, Statistiken, Statistiken anzeigen, Entwicklung, Einstellungen, Planung, Autoresponder, Einrichten, Bereitschaft, Übersicht, Statistik, Konfiguration.
- Karte (Map):** A map showing a geographical area with a 'Kunde' popup window displaying details for a customer.
- Modulmeldungen (Module Messages):** A table listing error messages with columns for 'Zeit', 'Modul', 'Anzahl', and 'Hostname'. The table shows various error types like TRAP, DISKSPACE, ACCTASK, MAILSPOOL, and CONTAINERFAILED.
- Maschinen Erreichbarkeit (Machine Availability):** A table showing machine status with columns for 'Empfangen', 'Kunde', and 'Hostname'.

Abbildung 4.22.: Integration der empfangenen Accountingdaten in das HelpDesk-System mit Visualisierung von Fehlerzuständen.

Es wurde eine tiefe Integration in das HelpDesk-System geschaffen, und Supportmitarbeiter erhalten über diese Oberfläche einen zentralen Zugriff auf alle Statusmeldungen von Kundensystemen, die sich unter Fernwartung befinden. Über das Dashboard werden alle Meldungen eines Systems gruppiert und mit ihrem Schweregrad angezeigt. So können sofort Supporttickets zur Bearbeitung von Meldungen erstellt werden, und der Mitarbeiter erhält mit einem Klick Zugriff auf den Server, um das Problem dort genauer analysieren zu können. Dies ist insbesondere im Hinblick auf die Teleradiologie wichtig, da hier Fehler schnell erkannt und behoben werden müssen, um einen reibungslosen Ablauf gewährleisten zu können.

Anbindung zur Kundendatenbank

Über die Kundendatenbank kann eine Verknüpfung von Kundenrechner zu Kundennummer durchgeführt werden, so dass mit einem Klick in der Oberfläche direkt zum entsprechenden Eintrag des Kunden gesprungen und dieser im Bedarfsfall direkt kontaktiert werden kann. Über diese Verknüpfung können auch weitere Daten des Kunden und der Kundensysteme wie die Version der installierten Software im Dashboard angezeigt werden.

OpenStreetMap

Weiterhin wurde ein OpenStreetMap-Server installiert und angebunden (Haklay and Weber, 2008). Hierbei wurde über die Adresse des Kunden eine Rückwärtssuche zu GPS-Koordinaten implementiert, die es erlaubt, Kundenrechner auf einer Karte anzuordnen.

Zur Anzeige der Rechner mit ihrem aktuellen Status wurde die JavaScript Bibliothek LeafletJS (<https://leafletjs.com>, 04.04.2019) integriert, welche neben der reinen Anzeige auch eine Filterung der Meldungen nach Schweregrad ermöglicht. Auch aus der Kartenansicht kann direkt zum Kundensystem oder in die Kundendatenbank gesprungen werden.

4.9. Zusammenfassung der Ergebnisse

Alle in diesem Kapitel beschriebenen Ergebnisse wurden in der Software implementiert und werden heute in Routine eingesetzt. Durch ihre Entwicklung konnten die gesteckten Ziele der Arbeit umgesetzt und erreicht werden. Diese Ziele sind:

- Verbesserung des Workflows zur Unterstützung von medizinischen und nicht-medizinischen Anwendern in der Teleradiologie und der intersektoralen Vernetzung
- Teilautomatisierung der Administration und Ad-hoc-Kommunikation in großen DICOM E-Mail basierten Teleradiologienetzwerken

- Erweiterung der Qualitätssicherungsmaßnahmen im Rahmen von DICOM E-Mail sowie deren Standardisierung mit der Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft
- IHE-konforme Realisierung von teleradiologischen Netzen sowie die Weiterentwicklung von vorhandenen IHE-Profilen, insbesondere im Zusammenspiel von DICOM E-Mail und IHE XDM
- Implementierung einer Qualitätssicherung in komplexen und heterogenen Teleradiologienetzwerken mit mehreren Übertragungsknoten zwischen Sender und Empfänger
- Intersektorale Vernetzung auf Basis von IHE XDS-I und Verbesserung der Performance im Bereich des Bildmanagements durch die Erweiterung von XDS-Basiskomponenten um einen Imaging Cache sowie Request-Broker
- Integration von nicht-XDS-fähigen Komponenten durch Schaffung von Kommunikationsadaptern für die intersektorale Vernetzung
- Integration von Handheldgeräten in teleradiologische Anwendungssysteme sowie die Darstellung von DICOM-Bildern auf diesen Geräten
- Entwicklung von Portallösungen zur workfloworientierten Vernetzung zwischen Ärzten, MTRAs und Patienten
- Weiterentwicklung von Überwachungs-, Monitoring- und Qualitätssicherungswerkzeugen für teleradiologische Systeme

Die Methoden zur Qualitätssicherung und zur Administration von DICOM E-Mail Netzwerken kommen heute in großen Teleradiologieverbänden zum Einsatz und erleichtern durch ihre Funktion sowohl die Verwaltung und Fehlersuche in diesen Netzwerken als auch die Abnahme- und Konstanzprüfung, die für eine Teleradiologie nach Röntgenverordnung zwingend erforderlich ist.

Das Instrument der Multiknotenstatistik ist ein fester Bestandteil jeder PACS Installation und hilft, den Datenverkehr nachvollziehen zu können. Die Multiknotenstatistik ermöglicht auch bei dem Versand von Daten über mehrere Knoten hinweg eine verlässliche Statistik und unterstützt damit die vollautomatische Konstanzprüfung in heterogenen Umgebungen.

Die Entwicklung des XDS Imaging Cache und Request-Broker erweitert die Funktionen eines XDS Document Consumers und ermöglicht es auch, nicht-IHE XDS-fähige Komponenten in einem XDS-Netzwerk aufzunehmen und Daten performant teilen und visualisieren zu können. Auch die Weiterentwicklungen im Bereich der mobilen Bildbetrachtung bringen einen Mehrwert für XDS-basierte Netzwerke und können in Routine genutzt werden.

Die Erweiterungen und der Ausbau der flexiblen CHILI/Medizinakte bietet durch ihre Rekonfigurationsoptionen zahlreiche Möglichkeiten für verschiedenste Einsatzszenarien. Sie wird mittlerweile in unterschiedlichen Teleradiologielösungen zur Workflowsteuerung verwendet. Ihr Einsatz als Teleradiologieportal zur Unterstützung der nächtlichen Teleradiologie nach Röntgenverordnung (RöV) hat sich in mehreren Projekten bewährt und ermöglicht auch in Teleradiologienetzwerken mit mehr als 100 Kliniken und ortsunabhängigen Befundern eine lückenlose und vollständige Abbildung der teleradiologischen Prozesse von Untersuchungsanforderung über Befundung inklusive Befundschreibung bis hin zur Rückübermittlung der Ergebnisse. Ebenso kommt sie als Patienten- und Zuweiserportal zum Einsatz und ermöglicht so eine einfache Teilhabe der Patienten am Behandlungsprozess.

Abschließend bieten die Weiterentwicklungen des Monitoringsystems mit den zahlreichen Erweiterungen zur Analyse, Überwachung und Konstanzprüfung von Teleradiologiesystemen den letzten Baustein in der Qualitätssicherung von Teleradiologienetzwerken. Diese werden heute auf mehr als 500 Rechner-Knoten im täglichen Betrieb eingesetzt.

Die in dieser Arbeit entwickelten Technologien und Lösungen kommen Klinikern, niedergelassenen Ärzten, administrativen Anwendern und zu guter Letzt den Patienten direkt als auch indirekt zu Gute.

Durch eine lückenlos elektronische Abbildung der Teleradiologie nach RÖV gelangen Daten schneller zu den zuständigen Radiologen, wodurch die Patientenbehandlung beschleunigt werden kann. Die teilautomatisierte Administration erlaubt die unkomplizierte ad hoc Aufnahme von neuen Partnern in ein Teleradiologienetzwerk, wodurch eine zweite Meinung einfach eingeholt oder ein Konsil erstellt werden kann. Durch die Einbindung von weiteren Datenquellen können auch Voruntersuchungen und Ergebnisse zielgerichtet versendet beziehungsweise Voruntersuchungen angefordert und aufwändige Doppeluntersuchungen des Patienten vermieden werden.

Die herstellerunabhängigen Erweiterungen zu DICOM E-Mail und IHE XDM erlauben weiterhin einen Aufbau von großen Teleradiologienetzwerken ohne einzelne Anwender oder Hersteller auszuschließen. Außerdem ermöglichen die Weiterentwicklungen im Bereich von IHE XDS durch den Einsatz eines Imaging Cache sowie Request-Broker die IHE-konforme und performante Anbindung von bestehenden Teleradiologiekomponenten an sich langsam etablierende XDS-Netzwerke.

Die Erweiterungen zur Qualitätssicherung der Vernetzungslösungen haben indirekt eine Auswirkung auf die Patientensicherheit. Die erarbeiteten Möglichkeiten zur Überwachung und Kontrolle von Teleradiologienetzwerken erlauben ein rasches Eingreifen und eine schnelle Störungsbeseitigung durch administrative Anwender. Dadurch wird schlussendlich die zeitkritische Übertragung von Patientendaten gesichert, was in einer zeitnahen Patientenbehandlung resultiert.

Ärzte profitieren durch die Implementierung von Portallösungen und einer vollelektronische Abbildung des teleradiologischen Workflows, welcher nun ohne Medienbruch stattfinden kann. Dies vereinfacht den Behandlungsablauf, und der Fokus kann nun um so mehr auf der eigentlichen Patientenbehandlung liegen. Auch Patienten können einen Nutzen aus den erarbeiteten Portallösungen ziehen und werden mit ihrer Hilfe direkt in den Behandlungsprozess einbezogen. Durch die Weiterentwicklung der mobilen Bild-

betrachtung können Patienten selbst auf einfachen Endgeräten wie Smartphones und Tablets ihre behandlungsrelevanten Unterlagen und sogar DICOM Bilder einsehen.

5. Diskussion

Bei der weltweit stetig voranschreitenden Digitalisierung sowohl im persönlichen als auch geschäftlichen Bereich scheint die Vernetzung im medizinischen Umfeld dem Fortschritt nicht in gleichem Maß standhalten zu können. Dies ist zum einen durch den langsam wachsenden Markt an Softwareprodukten im medizinischen Umfeld und durch verschärfte Regularien wie zum Beispiel die Medical Device Regulation, das Medizinproduktegesetz, das Patientendatenschutz-Gesetz und die unzureichende Standardisierung begründet. Zum anderen spielten die Daten- und Patientensicherheit bei Medizinprodukten sowie der Datenschutz eine entscheidende Rolle, so dass nicht die gleichen Maßstäbe wie im Consumerbereich angelegt werden können. Auch der wichtige Aspekt der Qualitätssicherung insbesondere in der Teleradiologie muss berücksichtigt werden.

In dieser Arbeit wurden unterschiedliche Lösungen für die Teleradiologie beziehungsweise Telemedizin und zur intersektoralen Vernetzung insbesondere im Bereich der Kommunikation medizinischer Bilder durch den Autor konzipiert und implementiert. Weiterhin wurden alle etablierten Lösungen unter dem Gesichtspunkt der Qualitätssicherung und -verbesserung überprüft und erweitert. Sie stellen so einen Beitrag zu einer einfacheren und qualitätsgesicherten Vernetzung von Akteuren im Gesundheitswesen dar.

Mit dem fortschreitenden Netzausbau und dem stetigen Wachstum der Bandbreiten im Internet können heute auch große Datenmengen problemlos zwischen unterschiedlichen Systemen übertragen werden. Insbesondere durch den Bedarf im privaten Umfeld stehen

diese Kommunikationsverbindungen immer kostengünstiger und stabiler zur Verfügung. Eine grundsätzliche Vernetzung und Erreichbarkeit von Systemen ist heutzutage sogar häufig in entlegenen Gebieten gegeben und bilden somit die Grundlage für die Teleradiologie und Telemedizin. Dass sich die Teleradiologie auch in Deutschland mittlerweile etabliert hat, steht außer Frage (Möller, 2016).

Obwohl auf einen großen Schatz an Lösungsansätzen im privaten Umfeld zurückgegriffen werden kann, bieten dedizierte Lösungen wie WhatsApp, Threema oder ähnliche Messenger keinen ausreichenden Datenschutz und können auch nicht mit den unter Umständen sehr großen Datenmengen in der Radiologie umgehen. Weiterhin ist aus Sicherheits- und Datenschutzgründen die Kommunikation in und zwischen Krankenhäusern insbesondere über das Internet auf wenige notwendige Dienste und Ports zu beschränken. Somit erfolgt die Kommunikation in den meisten Fällen via HTTP, HTTPS sowie E-Mail. Weitere Kommunikationsverbindungen sind ausschließlich durch ein VPN möglich. Andere als die genannten Kommunikationsverbindungen werden aus Sicherheitsgründen durch die Administratoren von Kliniknetzwerken gar nicht erst geduldet.

Aus diesen Gründen hat sich in Deutschland die Verwendung des E-Mail-Protokolls bei der Übermittlung von DICOM-Daten schnell etabliert. Bilder werden bei der Übertragung via DICOM E-Mail mittels PGP/GPG verschlüsselt. Zusätzlich findet eine Leitungverschlüsselung zwischen E-Mail-Client und -Server via SSL oder STARTTLS statt. Somit sind die Daten sowohl auf dem Transportweg als auch bei der Zwischenspeicherung auf dem Mailserver ausreichend geschützt. Große Datenmengen können durch das Aufteilen der Bilder auf viele kleine E-Mails problemlos versendet werden. Durch den Bestätigungsmechanismus ist sichergestellt, dass alle Bilder vollständig übertragen wurden.

Ungeachtet ihres Alters ist die Teleradiologie via DICOM E-Mail neben XDS und XDS-I insbesondere zum einfachen Austausch von Bilddaten immer noch der empfohlene Minimalstandard der Teleradiologie und Telemedizin in Deutschland (IHE Deutschland and Deutsche Röntgengesellschaft, 2013) und ein fester Bestandteil der gesicherten Arzt-zu-Arzt-Kommunikation in diversen überregionalen Teleradiologienetzwerken.

Etablierte Verbindungen lassen sich durch die Erweiterungen zur Administration von DICOM E-Mail-Netzwerken (Kapitel 4.1) leicht anpassen, auch neue Partner können dem Netzwerk problemlos hinzugefügt werden, was eine enorme Verbesserung bei der Organisation großer E-Mail-Netzwerke mit sich bringt. Diese Lösungen kommen sowohl im Westdeutschen Teleradiologieverbund als auch im Teleradiologienetz Rhein-Neckar-Dreieck zum Einsatz.

Die neu entwickelten Methoden zur Verwaltung des DICOM E-Mail-Netzwerks setzen die gleichen E-Mail-Protokolle ein, die auch für die Kommunikation der Bilddaten zum Einsatz kommen. Dadurch lassen sich diese ohne weitere Änderungen am Sicherheitskonzept des Kliniknetzwerks verwenden, da die betreffenden Kliniknetze bereits für den E-Mail-Verkehr konfiguriert und abgesichert sind.

Neben den Vereinfachungen zur Verwaltung von DICOM E-Mail-Partnern wurden weiterhin Lösungen zur Konstanzprüfung (Kapitel 4.2) entwickelt und durch den Autor in Routine etabliert. Selbst die Prüfung eines DICOM E-Mail-Netzwerks lässt sich vollständig unter Verwendung des E-Mail-Protokolls durchführen und protokollieren, was zu einer Erleichterung des Arbeitsablaufs in der Teleradiologie und einer Verbesserung der Verbindungsqualität führt. Fehlerhafte Verbindungen werden schnell erkannt und können, wenn sie nicht einfach zu beseitigen sind, unter Verwendung der implementierten Administrationsmechanismen ausgetauscht werden.

Medizinische Daten und insbesondere Bilddaten werden meist nicht nur dediziert zwischen zwei miteinander verbundenen Partnern ausgetauscht, sondern durchlaufen eine ganze Reihe von Systemen bis zum Empfänger. Dadurch ist es nötig, die gesamte Verbindungsstrecke zu dokumentieren und zu überwachen, um sicherzustellen, dass alle Daten vollständig und auch in der entsprechenden Zeit übertragen wurden.

Seit dem 31.12.2018 gilt die neue Strahlenschutzverordnung (StrlSchV) in Kombination mit dem Strahlenschutzgesetz (StrlSchG), welche die bisherige Röntgenverordnung (RöV) ersetzt. Hier ergeben sich einige Änderungen beziehungsweise Neuerungen. Die Regelungen zur Abnahme- und Konstanzprüfung der Teleradiologie bleiben aber weiterhin unverändert bestehen (Walz et al., 2019). Vor allem die Prüfung der Verfügbarkeit

des Teleradiologiesystems ist bereits durch die Teleradiologienorm (DIN 6868-159) genau festgelegt. Dort wird detailliert beschrieben, welche Datenmengen pro Untersuchung zu erwarten sind und welche Bandbreiten theoretisch zur Verfügung stehen müssen, um die Bilddaten in den geforderten 15 Minuten zu übertragen. Werden die Daten dabei nicht nur zwischen zwei Partnern ausgetauscht, ist eine Messung der Verbindungsqualität nicht ohne Weiteres möglich. Auch heute ist eine Stoppuhr noch ein gängiges Zeitmessmittel, und es kann die Zeit zwischen Sender und endgültigem Eingang beim Empfänger manuell gemessen werden. Dies mag für die initiale Abnahmeprüfung zwischen zwei Partnern noch eine einfache Lösung sein, aber durch die immer weiter wachsenden Teleradiologienetzwerke skaliert diese Art der manuellen Prüfung bei vielen unterschiedlichen Partnern nur schlecht, auch die kontinuierliche Überwachung der Konstanz eines Teleradiologienetzwerks ist so nur schwer möglich.

Um Datenübertragungen auch über mehrere Knoten hinweg verlässlich messen zu können, wurde durch den Autor ein System zur Multiknotenstatistik konzipiert und implementiert (Kapitel 4.3). Dieses Statistikmodul erlaubt die Nachverfolgung von Datenübertragungen über mehrere Knoten. Dabei findet die zusätzliche Kommunikation der Statistikdaten zwischen den einzelnen Knoten ausschließlich per HTTP beziehungsweise HTTPS statt, wodurch in den meisten Fällen keine spezielle Netzwerkkonfiguration durchgeführt werden muss.

Die entwickelte Multiknotenstatistik ermöglicht es, den Datenverkehr über alle Knoten in einem Netzwerk hinweg auszuwerten. Hierbei spielt die Art der Verbindung (DICOM, HTTP, HTTPS) zwischen den einzelnen Partnern ebenso wenig eine Rolle wie ihre Zeitsynchronität. Durch Berechnung von Offsets zwischen den Partnern ist es nicht nötig, dass alle Knoten über eine korrekte Uhrzeit verfügen. Obwohl dies wünschenswert wäre und auch im IHE Basisprofil Consistent Time (CT) für alle IHE-Anwendungen im Bereich der Vernetzung gefordert wird, ist der Einsatz von NTP-Servern zur Zeitsynchronisation gerade durch immer wieder bekannt werdende Sicherheitslücken (Goodin, 2015; Scherschel, 2015) im Klinikbereich als kritisch zu betrachten, obwohl die Sicherheit bei richtiger Konfiguration mit neuen Methoden durchaus gegeben ist (Malhotra et al., 2017).

Die durch die Multiknotenstatistik erhobenen Daten können direkt in der Versandoberfläche des Teleradiologieclients angezeigt werden. So sehen Benutzer auf einen Blick, ob die Übertragung erfolgreich war und ob die Bilddaten fehlerfrei zum Empfänger und nicht nur zum nächsten Knoten in der Kette übertragen werden konnten. Weiterhin ist es möglich, die Auswertung zu administrativen Zwecken wie der Überwachung des Netzwerks oder zur Erstellung von Abnahme- und Konstanzprüfungsprotokollen einzusetzen. Die eingeführten Erweiterungen lassen sich dabei problemlos mit den etablierten statistischen Auswertungsmethoden von DICOM E-Mail-Netzwerken kombinieren (Kapitel 4.2) und sind mittlerweile fester Bestandteil der Qualitätssicherung in vielen Teleradiologieinstallationen.

Um die Standardisierung der in Deutschland weitverbreiteten DICOM E-Mail-Kommunikation auch international weiter voranzutreiben, wurde in Zusammenarbeit mit der Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft ein Entwurf zur Überführung des Whitepapers für DICOM E-Mail in ein IHE-Profil entwickelt (Kapitel 4.4). Das Profil 'Quality Controlled Image Transfer (QCIT)' greift dabei die Basisfunktionalität von DICOM E-Mail auf und bildet eine Erweiterung des bestehenden IHE-Profiles 'Cross-Enterprise Document Media Interchange (XDM)' zum Datenaustausch via CD oder E-Mail. Bei Erstellung des Entwurfs wurde auf möglichst viele Strukturen aus bestehenden Profilen zurückgegriffen, diese wurden um die etablierten Funktionen von DICOM E-Mail in Deutschland erweitert.

Trotz intensiver Bemühung der Arbeitsgruppe wurde QCIT nicht als eigenständiges IHE-Profil angenommen. DICOM E-Mail ist zwar insbesondere mit den Erweiterungen aus dieser Arbeit gerade in Deutschland für die schnelle Ad-hoc-Vernetzung gut geeignet, aber weltweit entstehen immer mehr Kollaborationsnetzwerke auf Basis von IHE 'Cross-Enterprise Document Sharing (XDS)' und verwandter Profile. Aus diesem Grund wurde der Kern von QCIT als Erweiterung von IHE XDM umgearbeitet und durch die @GIT unter dem Namen 'Best Practice for the Grouping of PDI with XDM' als Change Proposal (CP-RAD-408) in der IHE-Domäne Radiologie erneut eingereicht und schlussendlich auch angenommen.

Durch diesen langwierigen Prozess hat sich gezeigt, dass sich die Vernetzung im Bildbereich weltweit immer weiter in Richtung IHE XDS beziehungsweise XDS-I bewegt (Wu et al., 2017; Huang, 2018) und auch in Deutschland vorangetrieben werden sollte. Im europäischen Vergleich befindet sich Deutschland im Bereich eHealth auf einem der hinteren Plätze und damit weit ab von den nordischen Spitzenreitern wie Estland, Finnland oder Schweden (Trill and Pohl, 2016). Obwohl die Vernetzung mit XDS im Routinebetrieb noch nicht so weit vorangeschritten ist, gibt es in Deutschland zahlreiche Projekte insbesondere von Krankenkassen und Klinikketten die auf XDS-basierte Vernetzung setzen (IHE Deutschland, 2020). In der Zukunft wird es also immer wichtiger, eine Verbindung zwischen den klassischen Vernetzungsmethoden und großen XDS-Netzwerken zu schaffen, um so die Vorteile beider Welten zusammenbringen zu können.

Vor allem im Bereich der intersektoralen Vernetzung im Gesundheitswesen, also über die klassischen Grenzen der Sektoren wie niedergelassene Ärzte, Kliniken, Nachsorge- und Rehabilitationsbereiche hinaus, spielt IHE XDS und XDS-I auch in Deutschland eine immer wichtigere Rolle (Bergh et al., 2015; Bauer et al., 2019). Als Basis der Vernetzung stehen eine institutionelle elektronische Patientenakte (EPA) und eine Gesundheitsakte unter der Datenhoheit des Patienten zur Verfügung. Eine Persönliche Elektronische Patientenakte (PEPA) wurde im Projekt INFOPAT durch das Universitätsklinikum Heidelberg aufgebaut, welche es insbesondere auch ermöglicht, DICOM-Bilddaten zu kommunizieren und anzuzeigen. Im Rahmen dieser Dissertation wurden Lösungen zur einfachen und schnellen Bildkommunikation entwickelt und realisiert. Die Akte setzt hierbei vollständig auf IHE-Profile zur Realisierung der Vernetzung. Alle Transaktionen zwischen den beteiligten Akteuren finden unter Verwendung von etablierten Standards statt. Auf diese Weise konnte durch die beteiligten Projektpartner schnell eine Patientenakte zum Teilen von Dokumenten zwischen unterschiedlichen Einrichtungen und Fachabteilungen unter Kontrolle des Patienten realisiert werden.

Gerade aber im Bereich der Bildkommunikation wurde schnell klar, dass die Anbindung von Primärsystemen eine große Herausforderung im Krankenhaus darstellt. Die meisten etablierten Hersteller sind in Deutschland noch nicht auf eine andere Bildda-

tenkommunikation als DICOM eingestellt. Entwicklungen gehen auf diesem Gebiet nur langsam voran. Aus diesem Grund mussten Lösungen gefunden werden, mit denen auch klassische Systeme in die intersektorale Kommunikation aufgenommen werden können. Die im Rahmen dieser Arbeit entwickelten und implementierten Lösungen ermöglichen es solchen Alt-Systemen, an der Kommunikation teilzunehmen und als Datenquelle für den Patienten und dessen Versorgung zu dienen (Kapitel 4.5).

Ähnliche Projekte zur Vernetzung von Regionen und Krankenhäusern lassen sich auch weltweit beobachten (Zhang et al., 2014). Neben der Datensicherheit und Zugriffsbeschränkung ist hierbei die große Herausforderung nicht die grundsätzliche Vernetzung der Partner und der Austausch von Dokumenten, sondern die Sonderrolle, die medizinische Bilddaten bei der Kommunikation mittels XDS-I einnehmen. Auf Bilddaten kann nicht direkt zugegriffen werden, diese stehen erst nach erfolgreichem Abruf eines KOS-Objekts aus einem XDS Repository in einem zweiten Schritt zur Verfügung.

Obwohl die Daten grundsätzlich zugänglich sind, zeigen verschiedene Pilotstudien die Schwierigkeiten des performanten Zugriffs auf die Bilddaten (Zhang et al., 2015). In unterschiedlichen Szenarien wurde die Zugriffsgeschwindigkeit auf Bilddaten mit unterschiedlichen Zugriffsmethoden (Online vs. Nearline) sowohl in zwei Projekten in Shanghai als auch im RSNA Image Sharing Network (Langer et al., 2014) in den USA gemessen. In der Online-Variante liegen die Bilder dupliziert in einer DMZ und können so bei Zugriff durch einen XDS-Client direkt angezeigt werden. Dies hat neben Datenschutzproblemen auch einen erhöhten Speicherbedarf zur Folge, da die Daten sowohl im Primärsystem des Krankenhauses als auch in der DMZ gespeichert werden müssen. Um diese Probleme zu umgehen, wurde durch Zhang et al. (2015) eine hybride Nearline-Variante entwickelt, welche die Daten dem anfragenden Client per DICOM Q/R zur Verfügung stellt, diese aber bei Anfrage transparent per DICOM WADO aus dem primären PACS abgerufen. In diesem Szenario konnte gezeigt werden, dass dieser RAD-69/WADO-Ansatz gegenüber den Ladezeiten bei reiner online Datenhaltung nur leicht unterlegen ist. Insbesondere bei kleinen MR- oder CT-Untersuchungen ist der Unterschied vernachlässigbar. Die mittlere Ladezeit des ersten Bilds einer MR-Untersuchung wurde in dieser Studie mit 2,3 Sekunden und die einer Röntgenuntersuchung mit 3,6 Sekunden gemessen.

Auch im Projekt INFOPAT war die Verbesserung der Performance ein weiterer Schwerpunkt neben der Anbindung an das XDS-basierte Netzwerk. Im Projektverlauf zeigte sich rasch, dass die Bildverteilung zwar grundsätzlich auf standardisiertem Weg funktioniert, die Nutzerakzeptanz aber aufgrund der geringen Geschwindigkeit bei der Darstellung von großen DICOM-Schnittbildstudien wie CT oder MR sehr eingeschränkt war.

Die mittlere Abrufdauer eines CT- oder MR-Bilds lag bei 2,8 Sekunden, eine Röntgenuntersuchung konnte im Mittel in 3,7 Sekunden angezeigt werden. Im Gegensatz zum obigen hybriden RAD-69/WADO-Modell wurde hier ein anderer Ansatz durch den Autor gewählt. Um auch große Bildmengen schnell zur Anzeige bringen zu können, wurde ein intelligenter Imaging Cache mit integriertem DICOM-Viewer entwickelt (Schwind et al., 2018). Dabei liegen alle Daten online im Imaging Cache und werden bei Platzbedarf nach dem Zeitpunkt des letzten Zugriffs entfernt. So ist sichergestellt, dass sich die neuesten und zuletzt zugegriffenen Bilder immer zur schnellen Anzeige im Cache befinden und in den meisten Fällen auf ein langsames Q/R verzichtet werden kann. Durch den intelligenten Cache wird die doppelte Datenhaltung auf ein Minimum beschränkt. Der integrierte DICOM-Viewer ermöglicht außerdem einen schnellen und streamingbasierten Zugriff auf die Bilddaten, so dass die gesamte Bildstudie nie zwischen Server und Client übertragen werden muss. Unabhängig von der eigentlichen Bildgröße kann dadurch das erste Bild einer Untersuchung im Mittel innerhalb von 50 Millisekunden im Viewer angezeigt werden. Dabei spielt es keine Rolle, ob es sich hierbei um ein relativ kleines CT-Bild (~300KB) oder ein großes Röntgenbild (~10MB) handelt, da immer nur das gerade sichtbare Bild vom Imaging Cache zum DICOM-Viewer übertragen wird. Hierdurch wird insbesondere die subjektive Ladegeschwindigkeit verbessert, da Benutzer direkt mit dem ersten Bild arbeiten können, während der Rest der Studie im Hintergrund in den Viewer geladen wird.

Der im Rahmen dieser Dissertation entwickelte Imaging Cache kann sowohl für einen einzigen Standort als auch in einem föderierten System über verschiedene Standorte hinweg unter Zuhilfenahme des ebenfalls entwickelten Request-Brokers eingesetzt werden. Durch das Prefetching und Cachen der großen Bildstudien konnten die Benutzerfreund-

lichkeit (Usability) und das Benutzerverhalten (User Experience) der PEPA deutlich verbessert werden.

Zusätzlich zu dem professionellen DICOM-Viewer, der es in Verbindung mit einem kalibrierten Monitor erlaubt, Daten in Befundqualität anzuzeigen, wurde auch ein mobiler Viewer entwickelt, der durch seine Implementierung in HTML5 und JavaScript in jedem aktuellen Browser oder mobilen Endgerät lauffähig ist. Dieser Bildbetrachter zielt insbesondere auf die Patienten ab, die einen schnellen unkomplizierten Zugang zu ihren Bildern benötigen, aber auf Spezialfunktionen des DICOM-Viewers verzichten können. Um dennoch die Möglichkeit des kontextbezogenen Wechsels zwischen dem mobilen und professionellen Viewer zu ermöglichen, wurde ein Single-Sign-On in beide Viewer implementiert, deren Aufrufchnittstelle sich nahtlos in die XDS-basierte Vernetzung mit Registry und Repository einfügt.

Da sich der professionelle Anwendungsfall der PEPA schneller weiterentwickelte als das zugehörige Patientenportal, kam der mobile Viewer während der Projektlaufzeit jedoch nicht zum Einsatz. Er konnte aber in weiteren Projekten in diverse Portale zur einfachen Anzeige von DICOM-Bildern integriert werden.

Um auch ohne intersektorale Vernetzung Patienten und Zuweisern dedizierten Zugang zu Bild- und Befunddaten in einem Kliniknetzwerk geben zu können, wurden im Rahmen dieser Arbeit zahlreiche Portallösungen entwickelt und im Produktivbetrieb in verschiedenen Gesundheitseinrichtungen etabliert. Durch die Weiterentwicklung der bestehenden Medizinakte und Ergänzungen im Bereich der Workflowsteuerung, der Zugriffs- und Freigabeverwaltung sowie der Auswertungs- und Exportoptionen konnten die unterschiedlichsten Anwendungsfälle abgedeckt werden (Kapitel 4.7).

Das so entwickelte Teleradiologieportal ermöglicht die vollständige elektronische Abbildung des teleradiologischen Befundworkflows ohne analoge Hilfsmittel wie zum Beispiel einem Faxgerät. Im Portal lässt sich der komplette Workflow von der Anlage einer Anforderung und Prüfung der rechtfertigenden Indikation über die Durchführung der Untersuchung bis zum anschließenden Bilddatenversand ohne Medienbruch abbilden. Ebenso lässt sich die radiologische Befundung und spätere Befundanzeige durchgängig

im webbasierten Portal durchführen. Um die Anwender des Systems bestmöglich zu unterstützen, wurde weiterhin eine vollumfängliche Schnittstelle für alle relevanten Prozesse auf Basis von HL7, DICOM und HTTP implementiert, so dass das Portal zur Workflowunterstützung transparent im Hintergrund eingesetzt werden kann, und die Benutzer in ihrer gewohnten KIS-, RIS- und PACS-Umgebung arbeiten können.

Um die Kommunikation zwischen Zuweisern und Krankenhäusern besser zu unterstützen, wurde ein Zuweiserportal mit Anbindung an die Primärsysteme des Krankenhauses realisiert. Registrierte Ärzte können so vor dem Krankenhausbesuch ihres Patienten bereits alle relevanten Informationen in elektronischer Form der Klinik bereitstellen. Auf umgekehrtem Wege werden Zuweiser über Ergänzungen und Korrekturen der Akte des Patienten benachrichtigt und erhalten alle Mitteilungen und Bilddokumente schnell und unkompliziert in elektronischer Form. Daten können zwischen der Akte und dem PACS oder RIS der Klinik einfach auf standardisiertem Weg per HL7 oder DICOM ausgetauscht werden. Zuweiser werden durch die Integration des DICOM-Viewers in das Zuweiserportal in die Lage versetzt, DICOM-Studien direkt im Portal in Befundungsqualität anzusehen. Daneben bietet die Exportfunktion der Medizinakte Möglichkeiten, sowohl die Einträge als auch die DICOM-Daten zur Archivierung in das Arztpraxissystem zu exportieren.

Obwohl die Qualität der Patienten-CDs nach dem etablierten Testat-Prozess (Kapitel 2.1.5) weiter zugenommen hat, werden heute schon viele Rechner, insbesondere Laptops, ohne CD-Laufwerk ausgeliefert. Durch den Trend zu 'Mobile First' sind viele Benutzer aus dem Consumer-Bereich eine reibungslose Darstellung auf ihren mobilen Endgeräten gewohnt. Vor diesem Hintergrund erscheint das Brennen einer Patienten-CD geradezu obsolet. Durch die Integration des mobilen Bildbetrachters und die Weiterentwicklungen der Medizinakte im Bereich der Rechteverwaltung ist es möglich, die Datenweitergabe an Patienten vollständig elektronisch zu lösen.

Über das Patientenportal erhalten Patienten einen token-basierten Zugriff auf ihre Akte. Diese kann sowohl mit Befund- als auch Bilddokumenten befüllt und dem Nutzer zeitlich befristet zur Verfügung gestellt werden. Alle Daten können durch die Implementierung des mobilen Bildbetrachters auf einem Smartphone angezeigt werden. Patienten

haben weiterhin die Möglichkeit, selbst Daten zu exportieren und für den späteren Gebrauch zu archivieren. Die Zugriffssteuerung erfolgt durch den Betreiber der Akten. Es kann jederzeit festgestellt werden, welche Daten sich im Zugriff welcher Benutzer befinden.

Die Implementierung des Patienten- und Zuweiserportals ermöglicht somit die enge Zusammenarbeit zwischen den verschiedenen medizinischen Anwendern. Patienten können ohne große technische Hürden an ihrem Behandlungsprozess teilnehmen. Das Teilen medizinischer Daten wird trotz Einhaltung von Datenschutz und Sicherheitsbestimmungen im Krankenhaus fast so einfach und komfortabel wie das private Teilen von Bildern mit WhatsApp. Auch wenn erste Schritte in Richtung Usability gemacht sind, hängt die medizinische Industrie den großen Internetkonzernen immer noch ein Stück hinterher. Es müssen weitere Anstrengungen unternommen werden, um den Anwendern medizinischer Systeme die gleiche User Experience wie im privaten Umfeld bieten zu können.

Auch wenn mittlerweile zahlreiche internationale und nationale Unternehmen den Betrieb von Cloud-Lösungen ermöglichen, ist deren Einsatz im Rahmen von Patientenportalen oder anderer Sharing-Lösungen in Deutschland schwer vorstellbar. Selbst bei einer privaten Cloud in einem deutschen Rechenzentrum machen es die hohen Anforderungen an den Datenschutz nur schwer möglich, Daten außerhalb eines Kliniknetzwerks zu speichern. Denkbar wäre hier nur die vollständig verschlüsselte Speicherung der Daten mit Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmern. Dies ist zwar denkbar und würde den Einsatz von Apps mit Ver- und Entschlüsselung erlauben. Webbasierte Lösungen mit einem zentralen Server lassen sich auf diese Weise aber nicht realisieren. So bleibt fraglich, welcher Nutzen aus Cloud-Computing für den medizinischen Bereich wirklich gezogen werden kann, solange nicht alle Fragen zur Datensicherheit restlos geklärt sind (Shini et al., 2012). Die wahrscheinlichste Anwendung für die Zukunft ist das Software as a Service-Modell, bei dem einzelne Rechenleistungen wie zum Beispiel die Bildanalyse dediziert in die Cloud ausgelagert werden oder die Daten rein Ende-Zu-Ende-verschlüsselt gespeichert werden. Ein vollständig cloudbasiertes PACS wird es in Deutschland auf absehbare Zeit wahrscheinlich nicht geben.

Durch die immer breitere Vernetzung von Systemen und dem raschen Wachstum von Netzwerken wird es immer wichtiger, die Server und Knoten solcher Installationen konstant überwachen und analysieren zu können. Im Rahmen dieser Arbeit wurden bereits etablierte Monitoring-Systeme weiter ausgebaut und die Möglichkeit zur einfachen und schnellen Auswertung von Fehlerzuständen geschaffen (Kapitel 4.8).

Durch die wachsenden Datenmengen in der Radiologie mit immer großvolumigeren Bildstudien müssen die entsprechenden Teleradiologiestrecken durch Vergrößerung der Bandbreite mitwachsen. Trotz dedizierter Leitungen und Bandbreitenzusagen von Telekommunikationsanbietern kann die wirkliche Bandbreite einer Teleradiologiestrecke nur unter Verwendung der gleichen Verbindung gemessen werden. Aus diesem Grund wurde ein Werkzeug zur Geschwindigkeitsmessung von Teleradiologiestrecken entwickelt und direkt in den Teleradiologie-Client implementiert. Das Werkzeug kann die tatsächliche Bandbreite zwischen Client und Server unter Verwendung eines VPN, Web-Proxy oder anderer Verbindungstechnologien messen, indem es die Testdaten unter Verwendung der gleichen Methoden wie der Teleradiologieclient übermittelt. Die dadurch erhaltene Geschwindigkeitsmessung kann regelmäßig zur Kontrolle der Leitungsgeschwindigkeit, aber auch zur kurzfristigen Analyse bei Verbindungsproblemen durch den Nutzer des Teleradiologieclients eingesetzt werden. Alle Messwerte werden zentral über das Monitoring-System erfasst und können zum Vergleich zu unterschiedlichen Tages- oder Nachtzeiten oder zwischen verschiedenen Teleradiologiestrecken herangezogen werden.

Neben der Bandbreite spielt die Performance der eigentlichen Teleradiologieserver bei wachsenden Nutzerzahlen eine wichtige Rolle. Um diese zwischen den unterschiedlichen Installationen transparent vergleichen zu können, wurden Benchmarking-Werkzeuge sowohl für Dateisystemoperationen (lesen, schreiben und suchen) als auch für Datenbankoperationen in das Accounting-System implementiert. Diese Messwerte können ebenso wie die Daten der Geschwindigkeitsanalyse zwischen den Servern ausgetauscht werden. Dies ermöglicht es, einen Benchmark über alle beteiligten Server zu erstellen und diese miteinander in Relation zu setzen.

Um Fehlerzustände in Teleradiologieinstallationen schnell zu erkennen und proaktiven Support leisten zu können, wurden die Auswertefunktionen und die Visualisierung des

bestehenden Monitoring-Systems erweitert. Ein globales Nachrichten-Addon ermöglicht die zeitnahe Auswertung von Fehlerzuständen, welche direkt einer Kundeninstallation, einem Teleradiologieserver bis hin zur entsprechenden Softwarekomponente zugeordnet werden können. Dadurch werden die Verantwortlichen der Systeme in die Lage versetzt, bei auftretenden Problemen schnell und zielgerichtet handeln zu können. Neben der Visualisierung der Fehlerzustände auf einer Karte wurden auch zahlreiche Schnittstellen und Anbindungen an externe Supportsysteme geschaffen.

Zusätzlich zum Erkennen von Fehlerzuständen ermöglicht die Weiterentwicklung der Monitoring-Software auch die strukturierte Abfrage von Software- oder Betriebssystemversionen über alle angeschlossenen Server hinweg, um so alle betroffenen Installationen im Falle eines bekannten Bugs oder Sicherheitsproblems einfach identifizieren und aktualisieren zu können. Dies ist dringend notwendig, um die Sicherheit von medizintechnischen Geräten und insbesondere von Software kontinuierlich zu gewährleisten (Darms et al., 2019). Besonders vor dem Hintergrund der Einstufung von Krankenhäusern als Teil der kritischen Infrastrukturen (kurz KRITIS) und den IT-Angriffen auf Krankenhäuser (Dahmen and Krämer, 2018; Lang, 2019), über die auch in den Medien immer häufiger berichtet werden, ist gerade die Nachverfolgbarkeit von Software ein wichtiger Baustein, um Teleradiologiesysteme im Ernstfall besser schützen zu können.

Die in dieser Arbeit durch den Autor erarbeiteten Lösungen bieten jede für sich eine eigenständige Erweiterung oder Verbesserung des etablierten Workflows bei der Vernetzung medizinischer Partner. Im besten Fall ergänzen sie sich gegenseitig und unterstützen die Anwender dadurch bei der Konzeption und dem Betrieb eines Gesamtsystems für die sichere, schnelle und qualitätsgesicherte Kollaboration mit Gesundheitsdaten und tragen somit zu einer besseren Patientenversorgung bei.

Fazit und Ausblick

Im Laufe der vergangenen Jahre hat sich gezeigt, dass der Fortschritt aus dem Consumerbereich auch langsam in den medizinischen Markt vorrückt. Benutzer und insbesondere

Ärzte wollen auf den Komfort, den sie in ihrem privaten Umfeld von Webanwendungen gewohnt sind, nicht mehr verzichten. 'Mobile First' wird allmählich auch ein Paradigma im medizinischen Umfeld, die Digitalisierung hat auch längst im Gesundheitswesen Einzug gehalten (Jörg, 2018). Die Entwicklungen in diesem Bereich können allerdings mit den Fortschritten im Consumermarkt aufgrund der gesetzlichen Rahmenbedingungen nur schwer Schritt halten. Insbesondere durch den Gesetzgeber werden solche Weiterentwicklungen im Rahmen der Akte nach §291a aber forciert, und Hersteller in Deutschland sind gezwungen, sich mit neuen Technologien wie IHE XDS, XDS-I und HL7 FHIR zu befassen. Dies ist alleine schon deshalb nötig, weil die anfallenden Datenmengen immer größer werden und insbesondere die Bilddaten aufgrund ihres Platzbedarfs nicht mehr zentral gespeichert werden können. Es ist sehr wahrscheinlich, dass private Anwender Patientenakten vornehmlich auf ihren Smartphones oder anderen mobilen Endgeräten benutzen werden und hier die gleiche User Experience wie in anderen Apps erwarten. Trotz aller noch zu lösender technischer Probleme ist man hier auf einem guten Weg. Schlussendlich wird der Einsatz moderner Aktensysteme dazu führen, dass Patienten noch enger in den Behandlungsprozess eingebunden werden und so auch die Hoheit über ihre Daten erlangen.

Auch wenn diese Entwicklungen noch nicht vollständig abgeschlossen sind, profitieren Patienten schon heute von der immer besseren Vernetzung von Ärzten und Krankenhäusern. Teleradiologie ist heute fast selbstverständlich. Daten können im professionellen Umfeld unter Beachtung des Datenschutzes mittlerweile problemlos geteilt werden. Hier ist DICOM E-Mail einer der wichtigsten Standards der Vernetzung in Deutschland. Die Nachfrage und stetige Weiterentwicklung zeigen, dass dieser 2004 entwickelte Minimalstandard der Teleradiologie (Engelmann et al., 2005) auch heute noch Stand der Technik ist. Mit den Entwicklungen im Umfeld von IHE XDM und QCIT zeigt sich aber auch in diesem Bereich eine Verlagerung in Richtung internationaler Lösungen wie IHE XDS-I. Bei der Weiterentwicklung spielen vor allem die Qualitätssicherung und Konstanzprüfung der Teleradiologiestrecken eine wichtige Rolle und sind für den Betrieb einer Teleradiologie nach Röntgenverordnungen unabdingbar. Inwieweit diese etablierten und stabilen Lösungen durch die Weiterentwicklungen im Bereich der Patientenakten abge-

löst werden, bleibt fraglich. Es ist eher davon auszugehen, dass diese Technologien noch lange nebeneinander existieren und sich gegenseitig ergänzen werden.

6. Zusammenfassung

Im Rahmen dieser Arbeit wurden durch den Autor umfangreiche Lösungen für eine qualitätsgesicherte Teleradiologie nach Röntgenverordnung erarbeitet und implementiert. Durch Erweiterungen des Whitepapers für DICOM E-Mail werden Benutzer eines DICOM E-Mail-basierten Teleradiologienetzwerks in die Lage versetzt, auch die Administration eines solchen Netzwerks ausschließlich per E-Mail vorzunehmen. Dadurch kann die Verwaltung eines solchen Netzwerks über wenige zentrale Stellen erfolgen. Es müssen keine weiteren Administrationsschnittstellen neben den aktuell angewendeten Sicherheitsmaßnahmen geschaffen werden. Der Austausch eines zur Kommunikation notwendigen, aber abgelaufenen kryptographischen Schlüssels ist über diesen Mechanismus ebenso einfach möglich wie das Hinzufügen eines neuen Partners zum Netzwerk.

Ein wesentlicher Bestandteil der Arbeit ist die Implementierung einer Multiknotenstatistik, die es ermöglicht, einen Datentransfer über verschiedene Knoten hinweg nachzuverfolgen und zu überwachen. Anwender und Administratoren werden dadurch in die Lage versetzt, Fehlerzustände in teleradiologischen Transferstrecken schnell und einfach zu erkennen und zu beseitigen. Zusammen mit den Erweiterungen im Bereich von DICOM E-Mail können so automatisierte Konstanz- und Abnahmeprüfungen einfach durchgeführt werden.

Um die Konzepte der intersektoralen Vernetzung auf Basis von Cross-Enterprise Document Sharing auch mit Alt-Systemen etablieren zu können, wurden mit dieser Arbeit verschiedene Möglichkeiten geschaffen, IHE-Funktionalität in bestehende Infrastruktur zu integrieren. Die Entwicklung eines Imaging Cache und Request-Brokers mit integriertem DICOM-Viewer brachte die entscheidende Benutzerakzeptanz der Systeme im Bereich des Bildmanagements. Zusätzlich wurden mit der Implementierung eines mo-

bilen Bildbetrachters die Möglichkeiten der Persönlichen Elektronischen Patientenakte wesentlich erweitert.

Neben Maßnahmen zur intersektoralen Vernetzung wurde zusätzlich ein konfigurierbares Zuweiser- und Patientenportal geschaffen, welches die einfache Kollaboration zwischen Ärzten ermöglicht und Patienten an ihrem Behandlungsprozess teilhaben lässt. Hierfür wurde die bestehende Medizinakte um Funktionen der Zugriffs- und Freigabeverwaltung sowie um Export- und Auswertungsoptionen erweitert.

Zur vollständigen elektronischen Unterstützung des teleradiologischen Ablaufs wurde die Medizinakte außerdem mit Komponenten zur Workflowsteuerung komplettiert. Zusammen mit den implementierten Schnittstellen zu den Subsystemen im Krankenhaus lässt sich so die teleradiologische Versorgung von Patienten nahtlos und ohne Medienbruch abbilden.

Den letzten Schritt zur qualitätsgesicherten Teleradiologie bilden die Erweiterungen des Monitoringsystems, welche es erlauben, den Gesamtprozess kontinuierlich zu überwachen. Zusätzlich zu den Werkzeugen zum Benchmarking und der Performanceanalyse von Teleradiologieservern wurden unterschiedliche externe Systeme an das Monitoringsystem angeschlossen, um dadurch Warnmeldungen über alle Systeme hinweg analysieren zu können, was einen proaktiven Support von Teleradiologieinstallationen ermöglicht. Die entwickelten Lösungen helfen heute bereits in Routine, Engstellen bei der Kommunikation zwischen den unterschiedlichen Komponenten eines Teleradiologiesystems zuverlässig zu identifizieren.

Die erarbeiteten Lösungen bieten jede für sich eine eigenständige Erweiterung oder Verbesserung der etablierten Workflows in der Teleradiologie und bei der Vernetzung medizinischer Partner und Patienten. Durch die Implementierung der vorgeschlagenen Erweiterungen werden Anwender in ihrem Workflow unterstützt. Die medizinische qualitätsgesicherte Kollaboration mit Gesundheitsdaten und insbesondere mit Bilddaten wird entscheidend verbessert. Somit wurde ein wichtiger Beitrag zur besseren und qualitätsgesicherten Patientenversorgung im Rahmen der Teleradiologie, Telemedizin und der intersektoralen Vernetzung geleistet.

Literaturverzeichnis

Akhila, K., Ganesh, A. and Sunitha, C. (2016). A Study on Deduplication Techniques over Encrypted Data. *Procedia Computer Science* 87, 38–43.

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D. and Rabkin, A. (2010). A view of cloud computing. *Communications of the ACM* 53, 50.

Aryanto, K. Y. E., van de Wetering, R., Broekema, A., van Ooijen, P. M. A. and Oudkerk, M. (2013). Impact of cross-enterprise data sharing on portable media with decentralised upload of DICOM data into PACS. *Insights into Imaging* 5, 157–164.

Bauer, J., Rohner-Rojas, S. and Holderried, M. (2019). Einrichtungsübergreifende Interoperabilität. *Der Radiologe* 1.

Bender, D. and Sartipi, K. (2013). HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems IEEE*.

Bergh, B., Brandner, A., Heiß, J., Kutscha, U., Merzweiler, A., Pahontu, R., Schreiweis, B., Yüksesogul, N., Bronsch, T. and Heinze, O. (2015). Die Rolle von Integrating the Healthcare Enterprise (IHE) in der Telemedizin. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz* 58, 1086–1093.

Bergsten, H. (2003). *JavaServer Pages*. OREILLY MEDIA.

Bergsten, H. (2004). *JavaServer Faces*. OREILLY MEDIA.

Bertram, N., Püschner, F., Gonçalves, A. S. O., Binder, S. and Amelung, V. E. (2019). Einführung einer elektronischen Patientenakte in Deutschland vor dem Hintergrund der internationalen Erfahrungen. In *Krankenhaus-Report 2019* pp. 3–16. Springer Berlin Heidelberg.

BMBF (2017). Metropolregion Rhein-Neckar – Raum für Gesundheit. Online: <https://www.gesundheitsforschung-bmbf.de/de/teilprojekte-m1-p0-p2-p3-p4-p5-p7-p8-p9-4178.php>, Stand: 01.11.2017.

Bougatf, N., Kessel, K., Bohn, C., Oetzel, D., Combs, U.-P. D. S., Bendl, R., Debus, J. and Engelmann, U. (2012a). e-Health 2012. Informationstechnologien und Telematik im Gesundheitswesen Webbasierte Studiendokumentation in der Partikeltherapie mit der CHILI/Telemedizinakte, pp. 205–215. Solingen: Medical Future: Duesberg F. (Hrsg.).

Bougatf, N., Kessel, K., Oetzel, D., Bohn, C., Engelmann, U., Bendl, R., Debus, J. and Combs, S. E. (2012b). Einführung des ULICE Studiendokumentationssystems im Heidelberger Ionenstrahl-Therapiezentrum. In *GMDS 2012; 57. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik German Medical Science* GMS Publishing House.

Bresser, L., Köhler, S. and Schwaab, C. (2014). The development of an application for data privacy by applying an audit repository based on IHE ATNA. *Studies in health technology and informatics* 198, 219–225.

Bundesministerium für Gesundheit (2020). Referentenentwurf: Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur. Online: <https://www.bundesgesundheitsministerium.de/patientendaten-schutzgesetz.html>, Stand: 04.02.2020.

Chauhan, J., Makaroff, D. and Arkles, A. (2011). VM clock synchronization measurements. In *30th IEEE International Performance Computing and Communications Conference* IEEE.

Clark, J. L., Algoe, S. B. and Green, M. C. (2017). Social Network Sites and Well-Being: The Role of Social Connection. *Current Directions in Psychological Science* 27, 32–37.

Clunie, D. and Cordonnier, E. (2002). Digital Imaging and Communications in Medicine (DICOM) - Application/dicom MIME Sub-type Registration. Technical Report 3240 The Internet Society.

Clunie, D. A., Dennison, D. K., Cram, D., Persons, K. R., Bronkalla, M. D. and Primo, H. (2016). Technical Challenges of Enterprise Imaging: HIMSS-SIIM Collaborative White Paper. *Journal of Digital Imaging* 29, 583–614.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Technical report The Internet Society.

Crocker, D. (1982). Standard for the Format of ARPA Internet Text Messages. Technical report The Internet Society.

Czeschik, C. and Lindhorst, M. (2018). Weniger schlecht über IT schreiben. Dpunkt Verlag GmbH.

Dacosta, I., Ahamad, M. and Traynor, P. (2012). Trust No One Else: Detecting MITM Attacks against SSL/TLS without Third-Parties. In *Computer Security – ESORICS 2012* pp. 199–216. Springer Berlin Heidelberg.

Dahmen, U. and Krämer, N. (2018). Angriff aus der Dunkelheit: Cyberattacke auf das Lukaskrankenhaus Neuss. In *Cybersecurity Best Practices* pp. 13–21. Springer Fachmedien Wiesbaden.

Dalrymple, N. C., Prasad, S. R., Freckleton, M. W. and Chintapalli, K. N. (2005). Introduction to the Language of Three-dimensional Imaging with Multidetector CT. *RadioGraphics* 25, 1409–1428.

Darms, M., Haßfeld, S. and Fedtke, S. (2019). Medizintechnik und medizinische Geräte als potenzielle Schwachstelle. In *IT-Sicherheit und Datenschutz im Gesundheitswesen* pp. 109–128. Springer Fachmedien Wiesbaden.

DIN (2017). DIN 6868-159:2017-10, Sicherung der Bildqualität in röntgendiagnostischen Betrieben - Teil 159: Abnahme- und Konstanzprüfung in der Teleradiologie nach RöV. Beuth Verlag GmbH.

Dockweiler, C. and Hornberg, C. (2019). Mensch, Medizin, Technik – Systeme einer vernetzten Gesundheit. In *Handbuch Digitale Wirtschaft* pp. 1–20. Springer Fachmedien Wiesbaden.

e-health com (2017). Das bundesweite Teleradiologie-Netz reif & möller. Online: <https://e-health-com.de/details-unternehmensnews/das-bundesweite-teleradiologie-netz-reif-moeller-betreut-jetzt-80-krankenhaeuser-in-deutschland>, Stand: 20.03.2017.

Engelmann, U., Schütze, B., Schröter, A., Weisser, G., Walz, M., Kämmerer, M. and Mildenerger, P. (2005). Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. In *Telemed 2005* G. Steyer, K.P. Löhr, T. Tolxdorff (Hrsg).

Europäische Union (2017). Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates. Amtsblatt der Europäischen Union.

Faldum, A. and Pommerening, K. (2005). An optimal code for patient identifiers. *Computer Methods and Programs in Biomedicine* 79, 81–88.

Fielding, R. T. (2000). REST: Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation University of California, Irvine.

Fowler, M. (2002). Refactoring: Improving the Design of Existing Code. In *Extreme Programming and Agile Methods — XP/Agile Universe 2002* pp. 256–256. Springer Berlin Heidelberg.

Gillam, L., Li, B., O’Loughlin, J. and Tomar, A. P. (2013). Fair Benchmarking for Cloud Computing systems. *Journal of Cloud Computing: Advances, Systems and Applications* 2, 6.

Glassman, N. R. and Shen, P. (2014). One Site Fits All: Responsive Web Design. *Journal of Electronic Resources in Medical Libraries* 11, 78–90.

Goodin, D. (2015). New attacks on Network Time Protocol can defeat HTTPS and create chaos. Online: <https://arstechnica.com/information-technology/2015/10/new-attacks-on-network-time-protocol-can-defeat-https-and-create-chaos>, Stand: 06.09.2019.

Haas, P. and Bertelsmann Stiftung (2017). Elektronische Patientenakten. Online: <https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/elektronische-patientenakten>, Stand: 30.04.2017.

Haklay, M. and Weber, P. (2008). OpenStreetMap: User-Generated Street Maps. *IEEE Pervasive Computing* 7, 12–18.

Haque, A. K. M. B. (2019). Analysis Of Attack Techniques On Cloud Based Data Deduplication Techniques. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* 9, 01–14.

Hardt, M., Hayrapetyan, A., Millar, P. and Memon, S. (2014). Combining the X.509 and the SAML Federated Identity Management Systems. In *Communications in Computer and Information Science* pp. 404–415. Springer Berlin Heidelberg.

Hazzam, J. and Lahrech, A. (2018). Health Care Professionals’ Social Media Behavior and the Underlying Factors of Social Media Adoption and Use: Quantitative Study. *Journal of Medical Internet Research* 20, e12035.

He, Q., Li, Z. and Zhang, X. (2010). Data deduplication techniques. In 2010 International Conference on Future Information Technology and Management Engineering IEEE.

Hellmuth, D., Arends, W., Mütznier, R., Meilutat, M. and Houta, S. (2014). Handlungsempfehlungen zur Etablierung einrichtungübergreifender elektronischer Patientenakten in Deutschland. *eHealth-com* 2.

Hilbel, T., Brown, B. D., de Bie, J., Lux, R. L. and Katus, H. A. (2007). Innovation and advantage of the DICOM ECG standard for viewing, interchange and permanent archiving of the diagnostic electrocardiogram. In 2007 Computers in Cardiology IEEE.

Hilgert, J.-N., Lambertz, M. and Yang, S. (2018). Forensic analysis of multiple device BTRFS configurations using The Sleuth Kit. *Digital Investigation* 26, S21–S29.

HL7 Deutschland e.V. (2018). HL7 Deutschland. Online: <http://hl7.de/hl7/hl7-die-organisation>, Stand: 30.11.2018.

HL7 Deutschland e.V. (2019). Warum FHIR? Online: <http://hl7.de/themen/hl7-fhir-mobile-kommunikation-und-mehr/warum-fhir>, Stand: 15.11.2019.

Hounsfield, G. N. (1973). Computerized transverse axial scanning (tomography). 1. Description of system. *The British journal of radiology* 46, 1016–1022.

Huang, H. K. (2018). *Medical Image Sharing for Collaborative Healthcare Based on IHE XDS-I Profile*. Wiley.

Hussain, M. A., Langer, S. G. and Kohli, M. (2018). Learning HL7 FHIR Using the HAPI FHIR Server and Its Use in Medical Imaging with the SIIM Dataset. *Journal of Digital Imaging* 31, 334–340.

IHE Deutschland (2020). Referenzen in Deutschland. Online: <http://www.ihe-d.de/referenzen-in-deutschland>, Stand: 16.02.2020.

IHE Deutschland and Deutsche Röntgengesellschaft (2013). Positionspapier der Deutschen Röntgengesellschaft und IHE Deutschland zur Teleradiologie und Telemedizin.

Online: https://www.agit.drg.de/media/document/3618/positionspapier_telera_diologie.pdf, Stand: 10.09.2013.

IHE Europe (2018). Ready to improve Cybersecurity for health data exchange? Online: <https://www.ihe.net/wp-content/uploads/2018/12/IHE-and-Cybersecurity-V5.pdf>, Stand: 01.04.2019.

Infopat MRN (2018). Infopat Rhein-Neckar. Online: <https://www.infopat.eu>, Stand: 01.11.2018.

ITI Technical Committee (2018). Document Sharing Metadata Handbook pp. 27-29.

ITI Technical Committee (2019). IHE Radiology (RAD) Technical Framework - Volume 3 pp. 172-175.

Jin, K. and Miller, E. L. (2009). The effectiveness of deduplication on virtual machine disk images. In Proceedings of SYSTOR 2009: The Israeli Experimental Systems Conference on - SYSTOR '09 ACM Press.

Johner, C. (2019). Software als Medizinprodukt – Software as Medical Device. Online: <https://www.johner-institut.de/blog/regulatory-affairs/software-als-medizinprodukt-definition>, Stand: 14.01.2019.

Josefsson, S. (2006). The Base16, Base32, and Base64 Data Encodings. Technical report The Internet Society.

Jungmann, J. E. (2016). Konzeption und Implementierung der Migration verschiedener Web-Frameworks am Beispiel der CHILI/Telemedizinakte und PrimeFaces. Bachelorarbeit Hochschule Mannheim.

Jörg, J. (2018). Digitalisierung in der Medizin. Springer Berlin Heidelberg.

Kaczmirek, L. and Chalupa, J. (2018). Datenquellen und Standarduntersuchungen zur Online-Kommunikation. In Handbuch Organisationssoziologie pp. 11–12. Springer Fachmedien Wiesbaden.

- Kalender, W. A. (2006). Computertomographie (German Edition). Publicis.
- Katz, M. (2008). Ajax4jsf and RichFaces - historical perspective. Online: https://web.archive.org/web/20090202144946/http://www.jsfone.com/blog/max_katz/2008/08/ajax4jsf_and_richfaces__historical_perspective.html, Stand: 15.08.2008.
- Kluge, O. (2014). Dateisysteme mit Deduplizierung im Test. Online: <https://www.linux-magazin.de/ausgaben/2014/03/deduplizierung/3>, Stand: 14.01.2019.
- Koutelakis, G. V. and Lymberopoulos, D. K. (2009). WADA Service: An Extension of DICOM WADO Service. *IEEE Transactions on Information Technology in Biomedicine* *13*, 121–130.
- Krentzlin, D. (2017). Konzeption und Entwicklung eines plattformunabhängigen Patienten-CD-Uploads. Masterarbeit Fachhochschule Stralsund.
- Kumar, J. U. (2017). Application of Curved MPR Algorithm to High Resolution 3 Dimensional T2 Weighted CISS Images for Virtual Uncoiling of Membranous Cochlea as an Aid for Cochlear Morphometry. *Journal Of Clinical And Diagnostic Research* *11*, 12–14.
- Lang, M. (2019). Cyberkriminalität: Bedrohungslage unverändert. *kma - Klinik Management aktuell* *24*, 66–66.
- Langer, S. G., Tellis, W., Carr, C., Daly, M., Erickson, B. J., Mendelson, D., Moore, S., Perry, J., Shastri, K., Warnock, M. and Zhu, W. (2014). The RSNA Image Sharing Network. *Journal of Digital Imaging* *28*, 53–61.
- Lautenbur, P. C. (1973). Image Formation by Induced Local Interactions: Examples Employing Nuclear Magnetic Resonance. *Nature* *242*, 190–191.
- Lee, K., Yeuk, H., Yim, K. and Kim, S. (2016). Analysis on Manipulation of the MAC Address and Consequent Security Threats. In *Proceedings of the 2016 International Workshop on Managing Insider Security Threats - MIST '16* ACM Press.

- Leiba, B. (1997). IMAP4 IDLE command. Technical report The Internet Society.
- Lipton, P., Nagy, P. and Sevinc, G. (2012). Leveraging Internet Technologies with DICOM WADO. *Journal of Digital Imaging* 25, 646–652.
- Loose, R., Braunschweig, R., Kotter, E., Mildemberger, P., Simmler, R. and Wucherer, M. (2008). Kompression digitaler Bilddaten in der Radiologie – Ergebnisse einer Konsensuskonferenz. *RöFo - Fortschritte auf dem Gebiet der Röntgenstrahlen und der bildgebenden Verfahren* 181, 32–37.
- Madsack, B., Walz, M. and Weisser, G. (2014). Abnahme und Konstanzprüfung an Bildwiedergabesystemen – was ändert sich mit der neuen DIN V 6868-157? *Radiopraxis* 7, 195–210.
- Malhotra, A., Gundy, M. V., Varia, M., Kennedy, H., Gardner, J. and Goldberg, S. (2017). The Security of NTP’s Datagram Protocol. In *Financial Cryptography and Data Security* pp. 405–423. Springer International Publishing.
- Mallik, A., Ahsan, A., Shahadat, M. M. Z. and Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science* 3, 77–92.
- Marx, G., Beckers, R., Brokmann, J. C., Deisz, R. and Pape, H.-C. (2015). Telekooperation für die innovative Versorgung am Beispiel des Universitätsklinikums Aachen. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz* 58, 1056–1061.
- MEDECON Telemedizin GmbH (2018). Westdeutscher Teleradiologieverbund. Online: <https://www.medecon-telemedizin.de>, Stand: 01.10.2018.
- Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. Technical report National Institute of Standards and Technology.
- Mildemberger, P., Kotter, E., Riesmeier, J., Onken, M., Kauer, T., Eichelberg, M. and Walz, M. (2007). Das DICOM-CD-Projekt der Deutschen Röntgengesellschaft - eine

Übersicht über die Inhalte und Ergebnisse des Pilottests 2006. *RöFo - Fortschritte auf dem Gebiet der Röntgenstrahlen und der bildgebenden Verfahren* 179, 676–682.

Mildenberger, P., Kämmerer, M., Engelmann, U., Ruggiero, S., Klos, G., Runa, A., Schröter, A., Weisser, G., Walz, M. and Schütze, B. (2005). Teleradiologie mit DICOM E-mail: Empfehlungen der @GIT. *RöFo - Fortschritte auf dem Gebiet der Röntgenstrahlen und der bildgebenden Verfahren* 177, 697–702.

Möller, T. B. (2016). Teleradiologie in Deutschland. In *eHealth in Deutschland* pp. 295–305. Springer Berlin Heidelberg.

Müller-Mielitz, S., Ohmann, C. and A.J.W., G. (2010). Klinische Studien mit EDC und PACS. *MDI* 2, 52—55.

National Electrical Manufacturers Association (1993). *Digital Imaging and Communications in Medicine (DICOM)*.

Nivedha, B., Priyadharshini, M., Thendral, E. and Deenadayalan, T. (2017). Lossless Image Compression in Cloud Computing. In *2017 International Conference on Technical Advancements in Computers and Communications (ICTACC) IEEE*.

OASIS Security Services TC (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS.

Pedersen, T. (2005). PKIX—Public Key Infrastructure (X.509). In *Encyclopedia of Cryptography and Security* pp. 459–460. Springer US.

Peng, W. and Zhou, Y. (2015). The Design and Research of Responsive Web Supporting Mobile Learning Devices. In *2015 International Symposium on Educational Technology (ISET) IEEE*.

Pianykh, O. S. (2011). Brief History of DICOM. In *Digital Imaging and Communications in Medicine (DICOM)* pp. 19–25. Springer Berlin Heidelberg.

Reichardt, S., Schmucker, U. and Sturm, J. (2016). TKmed® Direkt – ambulante Zuweiser, Partner-Kliniken und Patienten per Mausklick zum Datenversand einladen. *Orthopädie und Unfallchirurgie - Mitteilungen und Nachrichten* 05, 612–613.

Roth, P. and Wiese, J. (2018). Nutzerzahlen: Facebook, Instagram, Messenger und WhatsApp, Highlights, Umsätze. Online: <https://allfacebook.de/toll/state-of-facebook>, Stand: 30.11.2018.

Sanjeev and Agarwal, T. (2012). Vendor neutral archive in PACS. *Indian Journal of Radiology and Imaging* 22, 242.

Scherschel, F. A. (2015). Neue Angriffe auf NTP verwirren das Klientel von Zeitservern. Online: <https://www.heise.de/security/meldung/Zeitlos-Neue-Angriffe-auf-NTP-verwirren-das-Klientel-von-Zeitservern-2853869.html>, Stand: 06.09.2019.

Schmücker, P. (2013). Digitale Archivierung – Der Schatz im Aktenkeller. Online: <https://www.kma-online.de/aktuelles/it-technik/detail/der-schatz-im-aktenkeller-a-26467>, Stand: 31.10.2019.

Schwind, F. (2008). Entwicklung eines Überwachungsmoduls für die Teleradiologie. Diplomarbeit Hochschule Mannheim.

Schwind, F., Münch, H., Schröter, A., Brandner, R., Kutscha, U., Brandner, A., Heinze, O., Bergh, B. and Engelmann, U. (2018). Long-term experience with setup and implementation of an IHE-based image management and distribution system in intersectoral clinical routine. *International Journal of Computer Assisted Radiology and Surgery* 13, 1727–1739.

Sheffer, Y., Holz, R. and Saint-Andre, P. (2015). Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). Technical report The Internet Society.

Shini, S., Thomas, T. and Chithraranjan, K. (2012). Cloud Based Medical Image Exchange-Security Challenges. *Procedia Engineering* 38, 3454–3461.

Simmon, E. and Bohn, R. (2012). An Overview of the NIST Cloud Computing Program and Reference Architecture. In *Concurrent Engineering Approaches for Sustainable Product Development in a Multi-Disciplinary Environment* pp. 1119–1129. Springer London.

Smailhodzic, E., Hooijsma, W., Boonstra, A. and Langley, D. J. (2016). Social media use in healthcare: A systematic review of effects on patients and on their relationship with healthcare professionals. *BMC Health Services Research* 16.

Staemmler, M., Walz, M., Weisser, G., Engelmann, U., Luitjens, K. D., Schmucker, U. and Sturm, J. (2014). e-Health 2014. Informationstechnologien und Telematik im Gesundheitswesen TKmed - Telekooperation für die einrichtungübergreifende Versorgung, pp. 217–220. Solingen: Medical Future: Duesberg F. (Hrsg.).

Staemmler, M., Walz, M., Weisser, G., Engelmann, U., Weininger, R., Ernstberger, A. and Sturm, J. (2012). Establishing end-to-end security in a nationwide network for telecooperation. *Studies in health technology and informatics*, 180, 512–516.

Strahlenschutzkommission (2011). Datenkompression bei Röntgenbildern - Empfehlung der Strahlenschutzkommission. Technical report, Strahlenschutzkommission.

Tao, K., Li, J. and Sampalli, S. (2008). Detection of Spoofed MAC Addresses in 802.11 Wireless Networks. In *E-business and Telecommunications*, pp. 201–213. Springer Berlin Heidelberg.

Tarasov, V., Bhanage, S., Zadok, E. and Seltzer, M. (2011). Benchmarking File System Benchmarking: It *IS* Rocket Science. In *Proceedings of the 13th USENIX Conference on Hot Topics in Operating Systems, HotOS'13*, pp. 9–9, USENIX Association, Berkeley, CA, USA.

Teleradiologie RND (2015). Das Teleradiologie-Projekt Rhein-Neckar-Dreieck. Online: <http://www.teleradiologie-rnd.de>, Stand: 01.10.2015.

The Apache Software Foundation (2004). MyFaces core 1.1. Online: <http://myfaces.apache.org/core11/index.html>, Stand: 01.05.2019.

The Apache Software Foundation (2007). Tomahawk Taglibrary. Online: <https://myfaces.apache.org/tomahawk>, Stand: 01.05.2019.

TMF ToolPool Gesundheitsforschung (2005). PID-Generator. Online: <https://www.toolpool-gesundheitsforschung.de/produkte/pid-generator>, Stand: 01.05.2019.

Traeger, D. H. and Volk, A. (2001). Netzarten, Topologien und Zugriffsverfahren. In LAN Praxis lokaler Netze pp. 87–171. Vieweg Teubner Verlag.

Trill, R. and Pohl, A.-L. (2016). Internationale Perspektiven von eHealth. In eHealth in Deutschland pp. 241–254. Springer Berlin Heidelberg.

Tschirsich, M. (2018). All Your Gesundheitsakten Are Belong To Us. In 35c3 Chaos Computer Club e.V., Online: https://media.ccc.de/v/35c3-9992-all_your_gesundheitsakten_are_belong_to_us, Stand: 27.12.2018.

Universitätsklinikum Heidelberg (2018). INFOrmationstechnologie für die PATientenorientierte Gesundheitsversorgung in der Metropolregion Rhein-Neckar. Online: <https://mis-hd.eu/projekte/infopat>, Stand: 01.11.2018.

Varaksin, O. and Caliskan, M. (2013). PrimeFaces Cookbook. Packt Publishing.

Vukotic, A. and Goodwill, J. (2011). Introduction to Apache Tomcat 7. In Apache Tomcat 7 pp. 1–15. Apress.

Walz, M. (2006). DICOM CD – Erfahrungen, Anforderungen und Perspektiven der ärztlichen Stellen. RöFo - Fortschritte auf dem Gebiet der Röntgenstrahlen und der bildgebenden Verfahren 178.

Walz, M., Wucherer, M. and Loose, R. (2019). Was bringt die neue Strahlenschutzverordnung? Der Radiologe 59, 457–466.

Warda, F. (2005). Die elektronische Gesundheitsakte in Deutschland. Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz 48, 742–746.

Weisser, G., Walz, M., Ruggiero, S., Kämmerer, M., Schröter, A., Runa, A., Mildemberger, P. and Engelmann, U. (2005). Standardization of teleradiology using Dicom e-mail: recommendations of the German Radiology Society. *European Radiology* 16, 753–758.

Weisser, S. (2018). Konzeption und Entwicklung eines Plugins zum proaktiven Fehlermanagement externer Software am Beispiel des CHILI/Accounting. Bachelorarbeit Hochschule Heilbronn.

Winkler, F. (2015). Btrfs – Das Dateisystem der Zukunft? In FrOSCon Free and Open Source software Conference e.V., Online: <https://av.tib.eu/media/19575>, Stand: 02.08.2016.

Wu, C. H., Chiu, R. K., Yeh, H. M. and Wang, D. W. (2017). Implementation of a cloud-based electronic medical record exchange system in compliance with the integrating healthcare enterprise’s cross-enterprise document sharing integration profile. *International Journal of Medical Informatics* 107, 30–39.

Zhang, J., Yang, Y., Zhang, K., Sun, J., Ling, T., Wang, T., Wang, M. and Bak, P. (2014). Medical imaging document sharing solutions for various kinds of healthcare services based on IHE XDS/XDS-I profiles. In *Medical Imaging 2014: PACS and Imaging Informatics: Next Generation and Innovations*, (Law, M. Y. and Cook, T. S., eds), SPIE.

Zhang, J., Zhang, K., Yang, Y., Sun, J., Ling, T., Wang, M. and Bak, P. (2015). Implementation methods of medical image sharing for collaborative health care based on IHE XDS-I profile. *Journal of Medical Imaging* 2, 046501.

Veröffentlichungen des Autors

Schwind, F., Münch, H., Schröter, A., Brandner, R., Kutscha, U., Brandner, A., Heinze, O., Bergh, B. and Engelmann, U. (2018a). Long-term experience with setup and implementation of an IHE-based image management and distribution system in intersectoral clinical routine. *International Journal of Computer Assisted Radiology and Surgery*, *13*, 1727–1739

Schwind, F., Münch, H., Schröter, A. and Engelmann, U. (2018b). Secure and high-performance image sharing in IHE XDS-I- based networks. In Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie. 63. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS). Osnabrück, 02.-06.09.2018. German Medical Science GMS Publishing House

Engelmann, U. and Schwind, F. (2017). E-Health-Ökonomie, Bildkommunikation in der Medizin: Vom PACS zum flächendeckenden E-Health-System, pp. 683–705. Wiesbaden: Müller-Mielitz S, Lux T (Hrsg)

Engelmann, U., Münch, H., Rimmler, B., Schwind, F., Staemmler, M. and Sturm, J. (2015). e-Health 2016. Informationstechnologien und Telematik im Gesundheitswesen TKmed Direkt: Spontaner Austausch von medizinischen Bildern und Dokumenten mit Kollegen, Zuweisern und Patienten, pp. 120–124. Solingen: Duesberg F. (Hrsg.)

Schwind, F., Münch, H., Schröter, A., Engelmann, U. and Weisser, G. (2012). e-Health 2013. Informationstechnologien und Telematik im Gesundheitswesen Ein Whitepaper zur Administration und Qualitätssicherung von DICOM E-Mail basierten Teleradiologie-Netzwerken, pp. 169–199. Solingen: Duesberg F. (Hrsg.)

Schwind, F., Münch, H., Schröter, A., Meinzer, H. and Engelmann, U. (2011a). e-Health 2012. Informationstechnologien und Telematik im Gesundheitswesen, Qualitätssicherung in heterogenen Teleradiologie-Netzwerken, pp. 218–221. Solingen: Duesberg F. (Hrsg.)

Schwind, F., Münch, H., Schröter, A., Weisser, G., Meinzer, H. and Engelmann, U. (2012). Using control messages for administrative tasks and constancy testing of DICOM e-mail based teleradiology networks. *International Journal of Computer Assisted Radiology and Surgery* 7, 98–99

Schwind, F., Münch, H., Schröter, A., Meinzer, H. and Engelmann, U. (2011c). Advanced Transfer Statistics for Acceptance and Constancy Testing of Teleradiology Networks. *International Journal of Computer Assisted Radiology and Surgery* 6, 65–66

Schwind, F., Münch, H., Schröter, A., Meinzer, H. and Engelmann, U. (2011b). Der CHI-LI Ansatz für Transferstatistiken zur Abnahme- und Konstanzprüfung in Teleradiologie-Netzwerken über mehrere Knotenpunkte. In Mainz//2011. 56. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (gmds), 6. Jahrestagung der Deutschen Gesellschaft für Epidemiologie (DGEpi). Mainz, 26.-29.09.2011. German Medical Science GMS Publishing House

Abbildungsverzeichnis

2.1. Aufbau eines DICOM E-Mail-Netzwerks	26
2.2. Aufbau einer DICOM E-Mail	27
2.3. DICOM E-Mail mit nicht-DICOM-Daten	28
2.4. Empfangsbestätigung bei DICOM E-Mail	29
2.5. DICOM E-Mail mit Message Sets	30
2.6. Der IHE-Prozess	42
2.7. Scheduled Workflow (SWF)	44
2.8. Aktoren und Transaktionen (SWF)	44
2.9. Aktoren und Transaktionen (XDS-I)	46
2.10. Cross-Community Access (XCA)	51
2.11. Netzwerktopologien	52
2.12. Mesh Netzwerk	53
2.13. Sternförmiges Netzwerk	54
2.14. Push-Modell der Teleradiologie	56
2.15. Pull-Modell der Teleradiologie	57
2.16. Medical Device Regulation	59
3.1. Ablauf der Konstanzprüfung mit DICOM E-Mail Service Parts	83
3.2. Beispiel eines heterogenen Teleradiologienetzwerks	87
3.3. Austausch von statistischen Daten	87
3.4. Ablauf der Datenübertragung bei der Multiknotenstatistik zwischen zwei Knoten	92
3.5. QCIT Aktor Diagramm mit Transaktion	96

3.6. Beispielhafter Aufbau einer XDM-Verzeichnisstruktur	99
3.7. Datenübertragung mittels QCIT	100
3.8. Erweiterte Empfangsbestätigung mittels QCIT	103
3.9. Konstanzprüfung mittels QCIT	104
3.10. Vereinfachter XDS-Workflow mit Aktoren und Transaktionen	107
3.11. Vereinfachter XDS-I Workflow für Bilddaten mit Aktoren und Transaktionen	108
3.12. PACS mit Adapter für XDS Imaging Document Source	109
3.13. XDS Imaging Cache zur Speichererweiterung und Performanceoptimierung der Document Source	115
3.14. Erweiterter Imaging Cache mit integriertem Image Viewer für DICOM-Daten	116
3.15. Bild-Workflow unter Verwendung des Request-Brokers	118
3.16. CHILI/Mobile mit direktem Aufruf im Browser oder auf dem Smartphone	119
3.17. Authentifizierung von Nutzern und Diensten mittels SAML Token	122
3.18. CHILI/Medizinakte mit neuem Userinterface zum Erstellen und Anzeigen von Einträgen.	131
3.19. Schnittstellen der Medizinakte zu unterschiedlichen Systemen	132
3.20. Beispiel der Workflowsteuerung in der Medizinakte	133
3.21. Freigabeverwaltung in der Medizinakte	134
3.22. Datenexport und Auswertungsfunktionen in der Medizinakte	135
3.23. Protokollierung von Nutzer- und Systemaktionen in der Medizinakte	136
3.24. Auswertung der durch Bonnie++ erhobenen Daten zur Ermittlung der Festplattenperformance des Teleradiologieservers	138
3.25. Auswertung von PGbench-Daten zu Ermittlung der Transaktionsgeschwindigkeit des DBMS	138
4.1. Adressupdate mittels Service Part E-Mail	146
4.2. Schlüsselupdate mittels Service Part E-Mail	146

4.3. Konfiguration des Empfangs von Service Part E-Mails mit Einschränkung auf Signatur und der auszuführenden Aktion	147
4.4. Verwaltungsoberfläche für eingehende Service Part E-Mails	148
4.5. Benutzeroberfläche zur Analyse von ausgeführten Service Part E-Mails	148
4.6. Update der eigenen Verbindungsdaten via Service Part E-Mails mit direkter Integration in die Verwaltungsoberfläche des Teleradiologiesystems	149
4.7. DICOM E-Mail Empfangsbestätigung mit Anzeige im Teleradiologieclient und Administrationsoberfläche	150
4.8. Auswahl und Zuordnung der Datensätze für die Konstanzprüfung mittels DICOM E-Mail Service Parts	151
4.9. Workflow der Konstanzprüfung unter Verwendung von DICOM E-Mail Service Parts	152
4.10. Transferkette eines Teleradiologietransfers über mehrere Server unter Verwendung unterschiedlicher Übertragungsprotokolle	153
4.11. Darstellung der Multiknotenstatistik in der Administrationsoberfläche des Teleradiologiesystems	154
4.12. Darstellung der Multiknotenstatistik direkt im PACS-Viewer	154
4.13. Stichprobe der Patienteneinwilligung in die Nutzung der PEPA	160
4.14. Ablauf des SAML-basierten Zugriffs auf Bilddaten in einem XDS Repository mittels SSO und CHILI/Mobile	166
4.15. Workflow der Befundung mit Teleradiologieportal	168
4.16. Anzahl der verarbeiteten DICOM-Studien im Teleradiologieportal pro Jahr mit linearer Projektion bis 2020	169
4.17. Dienstplan zur zeitlichen Zuordnung von teleradiologischen Befundern zu Krankenhausstandorten und Modalitäten	170
4.18. CHILI/Medizinakte mit Konfiguration für das Zuweiserportal.	172
4.19. Übersicht der aktiven Kundensysteme unter proaktiver Überwachung	173
4.20. Ansicht der Bandbreitenmessung direkt im Teleradiologieclient	175
4.21. Anzeige der installierten Software auf Teleradiologiesystemen beim Nutzer	176

4.22. Integration der empfangenen Accountingdaten in das HelpDesk-System
mit Visualisierung von Fehlerzuständen 177

Tabellenverzeichnis

2.1. Kompressionsfaktoren für DICOM-Bilder nach 'Datenkompression bei Röntgenbildern - Empfehlung der Strahlenschutzkommission'	36
3.1. Definierte Service Parts mit Name und Aktion	75
3.2. Elemente und Attribute für eine ContactUpdate-Nachricht	79
3.3. RFC 3798 konforme Statusnachrichten für Service Part E-Mails	81
3.4. QCIT - Actors and Options	97
3.5. Elemente und Attribute für eine QCIT Enhanced Response-Nachricht . .	102
3.6. Elemente und Attribute für eine QCIT QC Request-Nachricht	105
3.7. Elemente und Attribute für eine QCIT QC Protocol-Nachricht	105
4.1. Patienteneinwilligung zur Speicherung ihrer Daten in der PEPA über den Projektzeitraum hinaus bis 2019	159
4.2. Anzahl der registrierte DICOM-Studien in der PEPA über den Projektzeitraum hinaus bis 2019	159
4.3. Retrievedauer für den erfolgreichen Retrieve mittels DICOM Q/R der häufigsten Modalitäten innerhalb eines Jahres	161
4.4. Transfergröße für empfangene Studien mittels DICOM Q/R der häufigsten Modalitäten innerhalb eines Jahres	162
4.5. Bildladezeit für auf dem Server vorliegende DICOM-Studien	162

Listings

2.1. Minimalbeispiel einer HL7 ADT^A01 Nachricht	20
2.2. Minimalbeispiel einer DICOM E-Mail (multipart/mixed)	25
2.3. IHE Value Sets - Beispiel für unterschiedliche Codes	48
3.1. XML-Struktur eines Service Part	74
3.2. Service Part zum Erstellen/Ändern von Adressdaten	75
3.3. Service Part zum Löschen von Adressdaten	76
3.4. Service Part zum Bereinigen des Adressbuchs	76
3.5. Service Part zum Abfragen von Adressdaten	77
3.6. Service Part zum Anlegen eines PGP/GPG-Schlüssels	77
3.7. Beispiel eines PGP/GPG-Schlüsselupdates	77
3.8. Beispiel eines einfachen Kontakt-Updates	78
3.9. Service Part zum Abfragen von Verbindungsdaten	80
3.10. Empfangsbestätigung mit der Verwendung von Service Part E-Mails . . .	81
3.11. Service Part TESTTRANSFER für die Konstanzprüfung nach DIN 6868- 159	82
3.12. Service Part PROTOCOL für die Konstanzprüfung nach DIN 6868-159 .	84
3.13. Service Part QUERY/FIND zur Abfrage eines Adressverzeichnisses . . .	85
3.14. Service Part QUERY/RESULT als Antwort auf eine Adressanfrage . . .	86
3.15. XML-Struktur einer Transferstatistiknachricht	88
3.16. Beispiel einer Statistiknachricht	90
3.17. Beispiel einer Fehlernachricht	90
3.18. Beispiel einer Transfernachricht	91

3.19. Beispiel einer Anfragenachricht der Multiknotenstatistik	93
3.20. Beispiel einer Antwortnachricht der Multiknotenstatistik	94
3.21. Beispiel einer erweiterten Bestätigung mit QCIT	102
3.22. Beispiel einer QC Anforderung mit QCIT	104
3.23. Auszug eines DICOM-Dumps für RetrieveAETitel und RetrieveLocationUID eines KOS-Objekts	110
3.24. Auszug aus der codes.xml für XDS Document.TypeCode	112
3.25. Auszug aus der mappings.xml für Mapping von DICOM Modality nach XDS Document.TypeCode	113
3.26. Aufbau eines SAML Token	122
3.27. Beispielaufruf des CHILI/Mobile mittels SAML Token und übergebenen Parametern	123
3.28. Aufruf mittels SAML Token und signierten Parametern	124
3.29. Beispiel eines XDS DocumentSetRequest	125
3.30. Input-Feld des DocumentSetRequest bei Aufruf des CHILI/Mobile	126
3.31. Beispiel für eine erfolgreiche Bandbreitenmessung	139
3.32. Beispiel einer fehlerhaften Bandbreitenmessung	139
3.33. MessageProcessor-Schnittstelle für das Accounting	141
A.1. Beispiel einer Service Part E-Mail (Zeilen mit % sind PGP/GPG verschlüsselt)	225
A.2. Vollständiger Service Part zum Anlegen von Kontaktdaten	226
A.3. Vollständiges Beispiel für die Abfrage eines Adressverzeichnisses (Suche nach Teilnehmern in Mannheim und Heidelberg)	227
A.4. Vollständiges Beispiel einer Antwort eines Adressverzeichnisses (mit Connection- und ContactID)	227
A.5. Vollständiges Beispiel einer Statistik Anfrage-Nachricht (mit Informationen über die TR-Strecke und der aktuellen Zeit zur Offsetberechnung)	228
A.6. Vollständiges Beispiel einer Statistik Antwort-Nachricht mit drei Knoten	229

A.7. Vollständiges Beispiel eines Viewer-Aufrufs mit SAML Token und XDS	
DocumentSetRequest	230

A. Anhang

A.1. Service Part - Beispiel-E-Mail

Listing A.1: Beispiel einer Service Part E-Mail (Zeilen mit % sind PGP/GPG verschlüsselt)

```
1 From: from@test.de
2 To: to@test.de
3 Message-ID: <08154711@ABC>
4 Subject: Service Part Example
5 Date: Fri, 1 Feb 2019 08:48:23 +0000
6 Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
7   boundary="-----boundary_A"
8 X-TELEMEDICINE-SERVICEPART: KEYUPDATE
9 X-TELEMEDICINE-VERSION: 1.7.0
10
11 -----boundary_A
12 Content-Type: application/pgp-encrypted
13 Content-Transfer-Encoding: 7bit
14
15 Version: 1
16 -----boundary_A
17 Content-Type: application/octet-stream
18 Content-Transfer-Encoding: 7bit
19
20 -----BEGIN PGP MESSAGE-----
21
22 %Content-Type: multipart/mixed; boundary="-----boundary_B"
23 %
24 %-----boundary_B
25 %Content-Type: text/xml; charset=UTF-8
26 %Content-Transfer-Encoding: 7bit
27 %Content-Id: KEYUPDATE_10_13e9de5c461_4ec769a13e580e63
28 %
29 %<?xml version="1.0" encoding="UTF-8"?>
30 %<ServicePart action="SET" name="KEYUPDATE" timestamp="2019-02-01T08:48:23Z">
31 % <PublicKeyASCIIData>
32 % -----BEGIN PGP PUBLIC KEY BLOCK-----
33 % 0Wh7seClfszkKVpniVY+thZmFw2r/odGXPLl88dXK7mzF8bFv1DmtrMG2mjzyk7MXX3eEZ
34 % kRD+Uj5B/DKuLbOIMwphEvu8+RGmEMPiB+wDMrrZdZwMzeb6JDS69Rs2sGKSdr4bOU3STPc
35 % geokWVS1A0qUOoljbkuWBrZPLuU21D3MJZVZcMeXW5GoOXkwMMfkUJzZ2Jq2QljT1hnV/lJ
36 % inNPLSb9GCDD2xqKJMj5pSS0+gGg75UCtUPr6RXtSpkB+DHW4lsN6C9eaZvnAmoqY4eSJVA
37 % ncNDKevCqb0LQfuFf2Mtv8VHhmfWr11jN7uFTmrtpsD7apEjwe12C5BQlwQcUAJ3DVHYa4e
38 % -----END PGP PUBLIC KEY BLOCK-----
39 % </PublicKeyASCIIData>
40 % </ServicePart>
41 %-----boundary_B--
42
43 -----boundary_A--
```

A.2. Service Part - Kontaktupdate

Listing A.2: Vollständiger Service Part zum Anlegen von Kontaktdaten

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="CONTACTUPDATE" action="SET" timestamp="YYYY-MM-DDThh:mm:ssZ">
3   <ContactID />
4   <ConnectionID />
5   <Comment />
6   <Role />
7   <Unit />
8   <Specialty />
9   <Title />
10  <Sex />
11  <GivenName />
12  <Name />
13  <ContactInformation order="[i]">
14    <RealLifeEmailAddress />
15    <Fax />
16    <Mobile />
17    <Phone />
18    <Pager />
19    <Website />
20    <Comment />
21  </ContactInformation>
22  <Address order="[i]">
23    <Comment />
24    <Street_1 />
25    <Street_2 />
26    <City />
27    <ZipCode />
28    <State />
29    <Country />
30  </Address>
31  <RelatedID />
32  <ContainerID />
33  <Custom identifier="[string]" version="1.2.3"> ...</Custom>
34 </ServicePart>
```


A.3. Service Part - Adressanfrage

Listing A.3: Vollständiges Beispiel für die Abfrage eines Adressverzeichnisses (Suche nach Teilnehmern in Mannheim und Heidelberg)

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="QUERY" action="FIND" timestamp="2019-01-02T08:42:23Z">
3   <Search maxCount="5" >
4     <Filter>
5       <City>Mannheim</City>
6       <City>Heidelberg</City>
7     </Filter>
8   </Search>
9   <ResultSet filtered="true">
10    <ContactID />
11    <ConnectionID expand="false">
12  </ResultSet>
13 </ServicePart>

```

A.4. Service Part - Adressantwort

Listing A.4: Vollständiges Beispiel einer Antwort eines Adressverzeichnisses (mit Connection- und ContactID)

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <ServicePart name="QUERY" action="RESULT" timestamp="2019-01-02T08:48:23Z">
3   <ResultSet>
4     <Result>
5       <ConnectionID>a2029a1d-0ea2-4e08-b3fc-b4fda26f3a75</ConnectionID>
6       <ContactID>2deace9e-f74d-4b16-be7a-c3e5fdf95434</ContactID>
7     </Result>
8     <Result>
9       <ConnectionID>7e71f14c-6c0f-43e4-bea4-e647dd147553</ConnectionID>
10      <ContactID />
11    </Result>
12    <Result>
13      <ConnectionID>a4186454-68d4-4d2f-8aef-1810382bfa7c</ConnectionID>
14      <ContactID />
15    </Result>
16  </ResultSet>
17 </ServicePart>

```

A.5. Statistik Request

Listing A.5: Vollständiges Beispiel einer Statistik Anfrage-Nachricht (mit Informationen über die TR-Strecke und der aktuellen Zeit zur Offsetberechnung)

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <statisticmessage version="1.71.0">
3   <head>
4     <macid>DE:AD:BE:EF:23:42</macid>
5     <hostname>sender</hostname>
6     <hostaddress>192.168.1.28</hostaddress>
7     <type>TRANSFER</type>
8   </head>
9   <body>
10    <transfer>
11      <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
12      <type>CSTORE</type>
13      <remotedata>true</remotedata>
14      <sender>
15        <macid>DE:AD:BE:EF:23:42</macid>
16        <name>sender</name>
17        <address>192.168.1.28</address>
18        <container>de23e6d7-76c9-4b40-bc17-51c645f149db</container>
19        <time>1550927907000</time>
20        <destinationaet>TRGATEWAY</destinationaet>
21      </sender>
22    </transfer>
23  </body>
24 </statisticmessage>
```

A.6. Statistik Response

Listing A.6: Vollständiges Beispiel einer Statistik Antwort-Nachricht mit drei Knoten

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <statisticmessage version="1.71.0">
3   <head>
4     <macid>AB:CD:EF:12:34:56</macid>
5     <hostname>receiver</hostname>
6     <hostaddress>192.168.161.23</hostaddress>
7     <type>DATA</type>
8   </head>
9   <body>
10    <transfer>
11      <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
12      <type>CSTORE</type>
13      <remotedata>>true</remotedata>
14      <sender>
15        <macid>DE:AD:BE:EF:23:42</macid>
16        <name>sender</name>
17        <address>192.168.1.28</address>
18        <container>de23e6d7-76c9-4b40-bc17-51c645f149db</container>
19        <time>1550927907000</time>
20        <destinationaet>TRGATEWAY</destinationaet>
21      </sender>
22      <receiver>
23        <macid>AA:BB:08:15:47:11</macid>
24        <name>gateway</name>
25        <address>10.1.23.17</address>
26        <container>1309fe39-7e36-4e4f-b47d-c19756e0d756</container>
27        <time>1550928073000</time>
28        <objects>144</objects>
29        <failed>0</failed>
30        <size>72837</size>
31        <offset>23731</offset>
32      </receiver>
33    </transfer>
34    <transfer>
35      <transferid>4317728f-b064-4a29-93f6-acd2d9482220</transferid>
36      <subid>f5a7a7b1-dd13-429f-8763-a0d894986ed3</subid>
37      <type>HTTPS</type>
38      <remotedata>>true</remotedata>
39      <sender>
40        <macid>AA:BB:08:15:47:11</macid>
41        <name>gateway</name>
42        <address>10.1.23.17</address>
43        <container>1309fe39-7e36-4e4f-b47d-c19756e0d756</container>
44        <time>1550928074623</time>
45        <destinationaet>RECEIVER</destinationaet>
46      </sender>
47      <receiver>
48        <macid>AB:CD:EF:12:34:56</macid>
49        <name>receiver</name>
50        <address>192.168.161.23</address>
51        <container>5d8c1d51-f0ee-4105-aece-cf77fff3b9bd</container>
52        <time>1550928162000</time>
53        <objects>144</objects>
54        <failed>1</failed>
55        <size>72837</size>
56        <offset>62832</offset>
57      </receiver>
58    </transfer>
59  </body>
60 </statisticmessage>

```


Lebenslauf

PERSONALIEN

Name und Vorname: Florian Schwind
Geboren: 05.06.1981 (Speyer am Rhein)
Familienstand: verheiratet
Eltern: Beate U. Schwind, Norbert Schwind

SCHULISCHER WERDEGANG

1987 - 1991 Grundschole Nord, Schifferstadt
1991 - 2000 Friedrich-Magnus-Schwerd Gymnasium, Speyer
Abitur: 15.06.2000

AUSBILDUNG / BERUF

2000 - 2001 Zivildienst als Rettungssanitäter
2001 - 2008 Nebenberufliche Tätigkeit als Rettungssanitäter/-assistent
2003 Ausbildung zum Rettungsassistent, Wörth-Maximiliansau
Abschluss: 26.09.2003

UNIVERSITÄRER WERDEGANG

WS 2001/2002 Beginn des Studiums der Informatik an der
Universität Karlsruhe (TH)
WS 2003/2004 Beginn des Studiums der Informatik an der
Hochschule für Technik und Gestaltung Mannheim
WS 2007/2008 Diplomarbeit: Entwicklung eines Überwachungsmoduls
für die Teleradiologie
Diplom: Dipl.-Inform. (FH), 12.03.2008, Mannheim
ab 2008 Softwareentwickler bei der CHILI GmbH, Heidelberg

Danksagung

Ich danke Herrn Prof. Dr. Paul Schmücker für die Möglichkeit der Erstellung dieser Dissertation, die akademische Betreuung im Rahmen des Promotionsverfahrens sowie die über viele Jahre aufgebrachte Geduld.

Herrn Dr. Uwe Engelmann danke ich für die regelmäßigen Gespräche und Impulse sowie die Möglichkeit zur Teilnahme an Fachkonferenzen, Arbeitsgruppentreffen und der konstanten Unterstützung und den Hinweisen bei der Erstellung von wissenschaftlichen Publikationen.

Mein Dank gilt außerdem Herrn Prof. Dr. Gerald Weisser für die Zusammenarbeit während der Promotion.

Ebenso bedanke ich mich bei Herrn Dr. Heiko Münch, der mich durch viele Diskussionen und Gespräche stets unterstützt und mich durch herausfordernde Aufgaben motiviert und meinen Ehrgeiz geweckt hat.

Besonders danke ich meiner Frau Katrin, die mir in den schwierigen Zeiten dieser Arbeit stets zur Seite stand.

Abschließend danke ich meinen Eltern Beate und Norbert, ohne deren positive Art und Unterstützung ich im Leben nie so weit gekommen wäre.