Aus dem Institut für Medizinische Informatik
der Medizinischen Fakultät Charité - Universitätsmedizin Berlin

DISSERTATION

Sichere und fehlertolerante DICOM-Bildübertragung in medizinischen Grid-Infrastrukturen

zur Erlangung des akademischen Grades
Doctor rerum medicarum (Dr. rer. medic.)

vorgelegt der Medizinischen Fakultät
Charité - Universitätsmedizin Berlin

von
Michal Vossberg

aus Nienburg

Gutachter: 1. Prof. Dr. rer. nat. Th. Tolxdorff

2. Prof. Dr. med. P. Mildenberger

3. Prof. Dr. med. M. Taupitz

Datum der Promotion: 18. September 2009

Danksagung

Mein Dank gilt Herrn Prof. Dr. rer. nat. Thomas Tolxdorff, Geschäftsführender Direktor des Instituts für Medizinische Informatik, für die Betreuung und die Unterstützung dieser Arbeit.
Ganz besonders bedanken möchte ich mich auch bei Frau Dr. rer. nat. Dagmar Krefting für die zielgerichtete Unterstützung, die intensiven, fachlichen Diskussionen, sowie die unermüdliche Arbeit bei der Modulleitung im Projekt MediGRID, in dessen Rahmen diese Arbeit entstand und ohne das sie nicht möglich gewesen wäre.
Weiterhin bedanken möchte ich mich auch bei allen Mitarbeitern aus dem Projektumfeld, allen voran Herrn Dipl. Geophys. Andreas Hoheisel für seine immerwährende fachliche Unterstützung im Bereich Workflow-Management, sowie allen Kollegen und Kolleginnen aus dem Institut für Medizinische Informatik für Ihre Hilfe und Diskussionsbereitschaft.

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Grid-Computing

„Grid-Computing“ bezeichnet das Rechnen auf verteilten Systemen, auch über organisatorische Grenzen (wie beispielsweise Universitäten oder Kliniken) hinweg. Das Ziel ist, die verteilten Ressourcen zu einem virtuellen Großcomputer zu bündeln und die Leistung für Nutzer bereitzustellen, ohne dass diese sich mit den technischen Einzelheiten auseinander setzen müssen. Die Vision ist, Rechenleistung so einfach wie Strom aus der Steckdose zu beziehen.

Erste Formen des Grid-Computing entstanden schon Anfang der neunziger Jahre in rechenintensiven Fachbereichen wie Astro- oder Teilchenphysik. Dort stand man vor dem Problem, enorme Datenmengen speichern und auswerten zu müssen, die weit über die Kapazitäten eines einzelnen Rechners hinausgingen. Bisherige Lösungen ermöglichten es, die Daten auf mehre Rechner zu verteilen, indem man die Rechner zu einem Verbund zusammenschloss, einem sogenannten „Cluster“. Ein Cluster verbindet allerdings nur Rechner in einer einzelnen Institution unter der gleichen Administration. Gerade bei kleinen Instituten waren die Grenzen auch hier schnell erreicht. Zusätzlich wollte man die Daten auch auf möglichst einfache Weise anderen Organisationen zugänglich machen. Als Lösung verband man nicht nur die lokalen Rechner zu einem Cluster, sondern auch die Cluster der einzelnen Organisationen untereinander.

Ende der neunziger Jahre begründete Ian Foster zuerst in seinem vielbeachteten Artikel „Anatomy of the Grid“ [1, 2] und später in seinem Buch „Grid 2: The Blueprint for a new Computing Infrastructure“ [3] das Grid-Computing so wie es heute verstanden wird. Die zunehmend gute Vernetzung des Internets als standardisiertes und öffentliches Netz, machte es möglich, verteiltes Rechnen nicht nur auf das eigene Institut zu begrenzen, sondern weltweit auszudehnen. Die Probleme, die es dabei zu bewältigen gab, entstanden weniger durch die technische Vernetzung sondern mehr durch die Zusammenarbeit der Organisationen. Die Arbeit auf fremden Rechnern sollte sich möglichst transparent gestalten, gleichzeitig ausreichend sicher sein und eine Möglichkeit bieten, die Kosten abzurechnen. Foster führte das Konzept der

„Virtuellen Organisationen“ ein. Virtuelle Organisationen bezeichnen eine dynamische Organisationsstruktur, die ein gemeinsames Interesse haben und sowohl ihre Mitglieder als auch ihre Ressourcen ohne ein zentrales Organ (also einen zentralen Administrator) verwalten können.

Dabei zeigte sich, dass die ursprüngliche Vorstellung „*des* Grids“, also einer einzelnen großen Grid-Infrastruktur im Sinne von „*dem* Internet“, nicht sinnvoll ist, da sich die Anforderungen und Interessen der einzelnen Organisationen zu stark unterschieden. So war es in der Astrophysik beispielsweise nicht nötig im gleichen Maße auf Datensicherheit zu achten wie in der Medizin. Andererseits aber benötigten die Physiker eine möglichst effiziente Datenverteilung, um allen beteiligten Gruppen einfachen Zugriff auf die erstellten Daten zu gewähren, was wiederum in der Medizin selten gewünscht ist. Dementsprechend unterscheidet man heute zwischen vielen, kleineren Grids, die eine Infrastruktur für eine virtuelle Organisation bereitstellen, beispielsweise „AstroGrid“ für die Astrophysik oder „AeroGrid“ für die Institute der Klimaforschung. Entsprechend ist der Begriff „Grid“ heute nicht mehr scharf definiert und gerade auch durch die modernen Weiterentwicklungen der letzten Jahre, wie „Peer-to-Peer“ Netze oder „Cloud-Computing“ erweitert worden. Nach Foster spricht man von einem Grid, wenn die beteiligten Ressourcen die folgenden drei Eigenschaften besitzen:

1. dynamisch,
2. verteilt,
3. autonom.

Im ursprünglichen Sinne sind mit „Ressourcen“ meistens noch Rechner gemeint und die parallele Verteilung von aufwändigen Berechnungen auf mehrere, verteilte Rechner ist das Hauptziel eines Grids. Dabei handelt es sich im Allgemeinen um eine sogenannte „grob-granulare“ Parallelisierung. Im Unterschied zur “fein-granularen“ Parallelisierung werden dabei nur Programmabläufe parallel gestaltet, die völlig unabhängig voneinander laufen und keine Kommunikation - beispielsweise den Austausch von Zwischenergebnissen - untereinander benötigen. Nicht immer geht es bei einem Grid jedoch um Parallelisierung. Oftmals kann es schon vorteilhaft sein, sich für die Anwendungen eines einzigen fremden Rechners zu bedienen, wenn es sich dabei beispielsweise um einen Hochleistungsrechner eines Rechenzentrums handelt.

Heute sind mit dem Begriff „Ressourcen“ oft nicht mehr nur Rechnersysteme gemeint. Im Unterschied zu dem ursprünglichen Ziel, mehr Rechenleistung bereitzustellen, verfolgt man mit Grids aktuell eine erweiterte Zielstellung. So soll eine möglichst einfache Verwaltung von verteilten Datenspeichern der zunehmenden Menge von erstellten Daten, etwa beim neuen Large Hadron Collider (LHC) des CERN, Platz bieten. Gleichzeitig sollen es die neuen organisatorischen Strukturen ermöglichen, Programme und Dienste für eine weit verteilte Anwendergruppe nutzbar zu machen. Diese lokal entwickelten Programme müssen dann nicht mehr aufwändig installiert und gewartet werden, sondern können einfach, ohne Details kennen zu

müssen, im Grid genutzt werden. Ganz allgemein versteht man also heute bei Grids eine Infrastruktur für die gemeinsame Nutzung von Ressourcen unter denen man Rechenleistung, Speicherplatz, aber auch Programme oder Geräte verstehen kann.

1.2 Grid-Computing in der Medizin

Durch die großen Vorteile und die Vielfalt von Grid-Infrastrukturen in den „traditionellen“ Gebieten begann man schnell, sie auch auf andere Anwendungsbereiche, wie beispielsweise die Medizin, zu übertragen. Gerade in der medizinischen Bildverarbeitung sind diese Vorteile von besonderem Nutzen. Dort stellen der Einsatz von modernen 3D- und 4D-Techniken, die kontinuierliche Verbesserung der räumlichen und zeitlichen Auflösung, sowie der immer höhere Druck zur Kooperation im Gesundheitswesen, herkömmliche Rechnerstrukturen zunehmend vor Probleme. Dieser potentielle Nutzen für die biomedizinische Forschung ist in der letzten Zeit von verschiedenen Institutionen und Forschergruppen erkannt worden, so dass eine steigende Zahl von nationalen und internationalen medizinischen Grid-Projekten, sogenanten „Healthgrids“, zu verzeichnen ist. Die derzeit größten, beziehungszweise bekanntesten Gruppen sind:

1. „Mammogrid“: Ein europäisches Verbundprojekt zum verteilten Zugriff und Verarbeitung von digitalen Mammographien [4],

2. „fightAIDS@home“: Der Zusammenschluss tausender privater Computer bei dem Forschungsgrid zur Bekämpfung von AIDS [5],

3. „Cancer Biomedical Informatics Grid (caBIG)“: Ein US-weites Gridprojekt aller nationalen Krebsinstitute zur kollaborativen Krebsforschung [6],

4. „Medical Imaging and Computing for Unified Information Sharing (MEDICUS)“: Ein U.S. amerikanisches Projekt um bildverarbeitende Ressourcen für klinische und Forschungsanwendungen zu verbinden [7],

5. „Enabling Grids for E-Science (EGEE)“: Das größte Europäische Gridnetzwerk mit verteilten Bilddatenbanken, Anwendungen für rechenintensive „Computer Aided Diagnosis (CAD)“ und statistische Studien über große Bilddaten [8],

6. D-Grid/MediGRID: In Deutschland wurde im Rahmen der D-Grid Initiative des Bundesministeriums für Bildung und Forschung im Jahr 2005 das MediGRID-Projekt mit dem Ziel gestartet, eine Grid-Infrastruktur für die bundesweite biomedizinische Forschung zu entwickeln und zu betreiben. Neben Anwendungen aus der Bioinformatik liegt ein Schwerpunkt aufgrund der großen Datenmengen und des hohen Rechenbedarfs auf der medizinischen Bildverarbeitung [9, 10].

Dabei unterscheiden sich die Anforderungen von Healthgrids deutlich von denen der „traditionellen“ Einsatzgebiete, wie beispielsweise der Astrophysik. Medizinische Daten unterliegen im Allgemeinen strengen Sicherheitsanforderungen und die Anwendungen werden von Medizinern mit Patientenverantwortung anstelle von Wissenschaftlern benutzt. Healthgrids stellen daher in der Medizin besonders hohe Anforderungen an Sicherheit, Zuverlässigkeit und Bedienbarkeit.

1.3 „Grid-Middleware“

Grids unterscheiden sich nicht nur in den unterschiedlichen Anforderungen, sondern auch in der Art und Weise, wie diese technisch umgesetzt werden. Als „Grid-Middleware“ fasst man diejenige Software zusammen, welche die Basisfunktionen zum Betrieb eines Grids bereitstellt, also das „Betriebssystem“ des Grids. Die Middleware muss sowohl von Rechnern, die sich als Ressource anbieten, und damit das Grid bilden, als auch von Rechnern, die ein Grid nutzen wollen, betrieben werden. Damit vereinheitlicht sie die Unterschiede zwischen den einzelnen Systemen und stellt eine einheitliche Plattform dar. Zu den Basisfunktionen dieser Plattform gehören unter anderem die Benutzerverwaltung, ein Sicherheitsstandard, Datentransfer und Programmausführung auf fremden Rechnern. Damit die Middleware möglichst einfach auf möglichst vielen Systemen betrieben werden kann, sollte sie offene und akzeptierte Standards benutzen. Aus der Grid-Forschung der letzten zwei Jahrzehnte entstanden verschiedene Middleware-Zusammenstellungen, die mittlerweile in vielen Fachgebieten als etablierte Software sowohl den wissenschaftlichen, als auch kommerziellen Routinebetrieb einer Grid-Infrastruktur ermöglichen. Im Wesentlichen unterscheidet man heute dabei zwischen den folgenden drei Systemen:

1.3.1 Unicore

*Uni*form *I*nterface to *Co*mputing *Re*sources ist eines der ältesten Grid-Systeme. Es wurde Anfang der neunziger Jahre in diversen vom BMBF geförderten Projekten entwickelt. Obwohl die aktuellen Entwicklungen die neuesten Standards berücksichtigen, basierte es lange Zeit auf eigenen, proprietären Verfahren, die Zusatzentwicklungen erschwerten. Dies ist der Hauptgrund, warum es sich international nicht durchgesetzt hat. Verwendung findet es vor allem in den (astro)physikalischen Teilgebieten von D-Grid [11]. Die Sicherheitsverfahren basieren, ähnlich wie bei Globus (siehe unten, „Globus Toolkit“) auf Zertifikaten, sind aber weniger standardisiert und bieten auch nicht die Zusatzfunktionalität, wie beispielsweise die Weiterleitung der Benutzeridentifikation.

1.3.2 LCG/gLite

LHC Computing Grid (LCG) entstand aus einem Gridprojekt des CERN „Large Hadron Collider“ Teilchenbeschleuniger mit einem starken Fokus auf Teilchenphysik. Im Rahmen des oben beschriebenen europaweiten Gridnetzwerkes *EGEE* wurde es erweitert und wird dort aktuell mit dem Namen „gLite“ als grundlegende Middleware betrieben. Eingeflossen ist dabei auch die ursprünglich bei Mammogrid entwickelte Software „Alien“. Als Sicherheitsinfrastruktur wurden mittlerweile die von Globus entwickelten, standardisierten Sicherheitsverfahren übernommen (siehe unten). Ein Vorteil von gLite ist die ausgeprägte Vielseitigkeit durch die vielen Einflüsse aus früheren Projekten. Andererseits ist es dadurch auch sehr komplex, so dass Grids mit diesem System sehr aufwändig zu betreiben sind [12].

1.3.3 Globus Toolkit

Das „Globus Toolkit“ ist eine der umfangreichsten Grid-Lösungen und bildet den heutigen de facto Standard für die meisten Gridnetzwerke. Diese Entwicklung einer Kooperation führender U.S. amerikanischer Institute, der „Globus-Alliance“, unter Mitarbeit von Ian Foster, bietet mit vielen Bausteinen einen Werkzeugkasten mit den wichtigsten Funktionen, die sich im Rahmen von offenen Standards auch international durchgesetzt haben [13]. Der von Globus entworfene Sicherheitsstandard, das „Globus Security Interface (GSI)“, ist mittlerweile weltweit anerkannt und größtenteils übernommen worden [14]. Er basiert auf standardisierten Zertifikaten, die als digitale Ausweise fungieren und Personen oder Systeme eindeutig identifizieren können. Ein Zertifikat ermöglicht es außerdem, ein Dokument digital zu signieren oder zu verschlüsseln. Aus diesem Grund werden diese Zertifikate auch beim Deutschen Signaturgesetz oder der neuen Gesundheitskarte, bzw. dem Heilberufeausweis, eingesetzt. Das GSI bietet durch die Verwendung dieser Zertifikate auch bei unbekannten Benutzern oder Systemen eine eindeutige und vertrauenswürdige Identifizierung. Weiterhin bietet der Sicherheitsstandard viele Funktionen, die über die reine Verschlüsselung bei herkömmlichen Netzwerken hinausgehen. Er ermöglicht beispielsweise das Weiterleiten einer einmal durchgeführten Benutzeridentifikation an alle Systeme im Grid. Dies ist bei einer Verteilung auf viele Systeme besonders wichtig, da sich sonst der Benutzer an jedem einzelnen System mit seinem Zertifikat neu anmelden müsste. Auf Grund seiner Standardisierung und großen Verbreitung wird das Globus Toolkit auch als Grundlage bei caBIG und vielen Teilbereichen von D-Grid, beispielsweise MediGRID, als grundlegendes „Betriebssystem“ eingesetzt.

1.4 Erweiterungen für die medizinische Bildverarbeitung

Die beschriebene Middleware stellt nur die grundlegenden Funktionen für ein Grid bereit. Für spezielle Anforderungen, beispielsweise die Integration von Geräten mit dem Bildüber-

tragungsstandard „Digital Imaging and Communication in Medicine (DICOM)“, müssen, basierend auf diesen Grundfunktionen, spezifische Anpassungen und Erweiterungen vorgenommen werden.

Die folgenden Projekte aus dem medizinischen Umfeld beschäftigen sich speziell mit der Entwicklung von Grid-Middleware für die medizinische Bildverarbeitung:

1. MEDICUS: Als ein aktuelles „Globus Alliance Incubator“ Projekt, also ein gefördertes Projekt der Globus Alliance, repräsentiert es den neuesten Stand der Technik für Bildintegration in Globus-basierten Grids. Kernstück ist dabei der entwickelte „Dicom Globus Interface Service (DGIS)“. Dieses System erlaubt die Bildverteilung von DICOM-kompatiblen Geräten zu verteilten Datenspeichern im Grid, welche dann allen beteiligten Kliniken zugänglich sind.

2. EGEE: Als ein Teil des europäischen Grid-Projektes EGEE-2 haben die bildverarbeitenden Gruppen den „Medical Data Manger (MDM)“ entwickelt [15]. Dieser basiert auf den Erfahrungen aus den Vorgängerprojekten EGEE-1 und DataGrid. Ähnlich zum DGIS erlaubt das System die Verteilung und Speicherung von Bilddaten im Grid, sowie den gesicherten Zugriff für medizinische Anwendungen. Technisch stützt es sich dabei allerdings hauptsächlich auf die gLite-Middleware, die bei EGEE zum Einsatz kommt.

3. Mammogrid: Als eines der ersten Healthgrid-Projekte startete es ursprünglich mit einer komplett eigenen Grid-Middleware „Alien“, die dann aber später größtenteils in LCG und gLite von EGEE-1 übernommen wurde. Mammogrid steht stellvertretend für viele frühere Gridprojekte, die mit nicht-standardisierter Middleware eine einfache DICOM-Bildübertragung für medizinische Anwendungen erreichten.

Im Folgenden werden für die medizinische Bildverarbeitung grundlegende Funktionalitäten in den Bereichen DICOM-Kompatibilität, Sicherheit und Fehlertoleranz deutlich gemacht und die bislang verfügbaren Lösungen diskutiert:

1.4.1 DICOM-Kompatibilität

Für die medizinische Bildverarbeitung unerlässlich ist die Unterstützung des DICOM-Standards. Dieser spezifiziert nicht nur die erlaubten Bildformate, sondern auch die zur Kommunikation notwendigen Sicherheits- und Übertragungsverfahren. Damit bildet er die Grundlage für jede medizinische Bildübertragung zwischen bildverarbeitenden Systemen [16]. Dies sind üblicherweise Radiologie-interne Systeme wie bilderzeugende Geräte (Modalitäten wie Computed Tomography (CT) oder Magnetic Resonance Tomography (MRT)), Langzeitarchive („Picture Archiving and Communication System (PACS)“) oder radiologische Arbeitsplätze. Der Bildtransfer ist damit begrenzt auf ein lokales Netzwerk und dadurch hinreichend sicher und zuverlässig. Der DICOM-Standard ist bisher nur für solche, herkömmliche Netze definiert und bietet

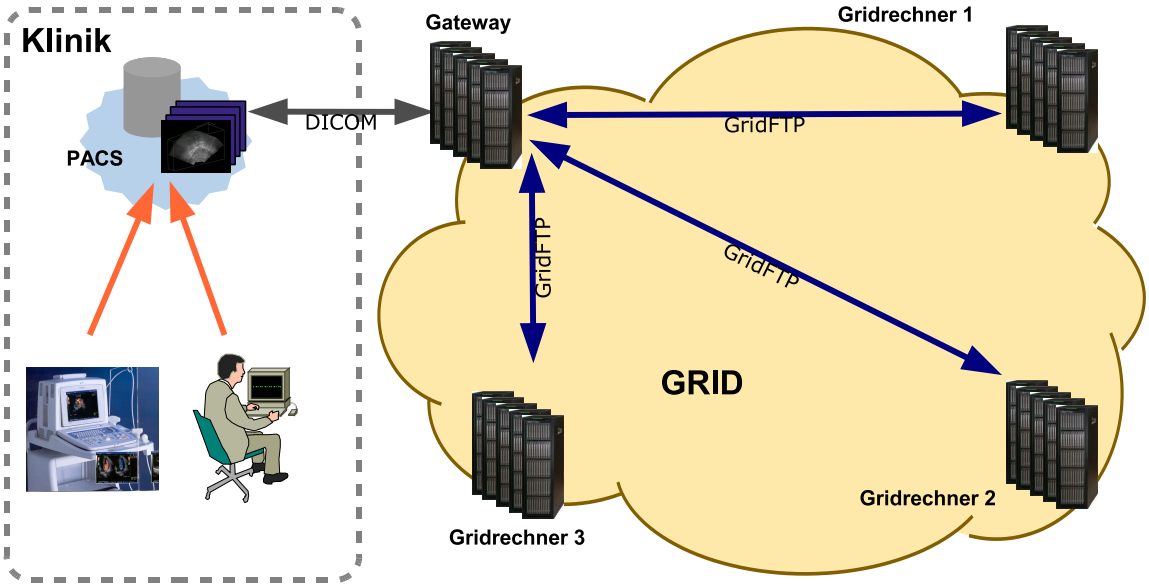


Abbildung 1.1: Schematische Darstellung der medizinischen Bildübertragung aus einem Kliniknetz in eine Grid-Infrastruktur bei bestehenden Lösungen unter Verwendung von DICOM und dem allgemeinen Dateiübertragungsprotokoll „GridFTP“.

auch nur begrenzte Sicherheits- und Zuverlässigkeitsmechanismen. Den bildverarbeitenden Systemen ist es daher nicht möglich, über ein Gridnetzwerk zu kommunizieren.

Als Abhilfe übertragen alle bisherigen medizinischen Grid-Projekte die Bilder in zwei Schritten: zunächst mit DICOM und für die eigentliche Gridverbindung dann mit einem generischen Übertragungsverfahren der Grid-Middleware wie zum Beispiel mit „GridFTP“ des Globus-Toolkits [17] (siehe auch Abbildung 1.1). Nach diesem Prinzip arbeiten sowohl die älteren Projekte, wie Mammogrid, aber auch aktuelle, wie der „MDM“ oder der „DGIS“ aus dem MEDICUS-Projekt.

Der Vorteil dieser Lösung ist, dass auf standardisierte und bewährte Methoden aus der Middleware zurückgegriffen wird. Der Nachteil ist, dass durch die Kombination der unterschiedlichen Verfahren viele Vorteile des eigentlichen DICOM-Standards verloren gehen:

1. Bilder müssen exportiert und am Gateway (siehe Abbildung 1.1) zwischengespeichert werden, was sich nachteilig auf die Leistung und Datensicherheit auswirken kann.

2. Zwei DICOM-Systeme können nicht direkt miteinander kommunizieren (zum Beispiel kann ein Arbeitsplatz nicht direkt ein im Grid lokalisiertes Bildarchiv abfragen).

3. Die Interaktivität des Benutzers geht verloren (zum Beispiel kann er länger dauernde Such- oder Übertragungsvorgänge nicht mehr kontrolliert abbrechen).

1.4.2 Datensicherheit

Gridnetzwerke zu benutzen bedeutet, temporär Rechner aus fremden Organisationen, wie Kliniken oder Rechenzentren, zusammenzuschließen und für die eigenen Berechnungen zu benutzen. Die Daten werden dabei auf die fremden Rechner kopiert, ohne dass der Anwender eine genaue Kenntnis des Systems oder der Organisation hat.

Der Sicherheitsstandard des Globus-Toolkit, der auch von den anderen Middleware-Lösungen übernommen wurde, bietet zwar Sicherheitsmaßnahmen während des Transports der Daten, wie beispielsweise Verschlüsselung, nicht aber, wenn sie einmal das Ziel erreicht haben. Es ist unabdingbar, dass gerade in der Medizin besondere Sicherheitsmaßnahmen auch nach dem Kopieren zum Schutz der personenbezogenen Daten in den Bildern getroffen werden müssen. Die bisherigen Lösungen nutzen dazu die im DICOM-Standard Teil 15 definierte „Attribute Level Confidentiality (ALC)“, eine selektive Pseudonymisierung beziehungsweise Anonymisierung der Patientendaten. Dabei werden einzelne Attribute in den Bilddaten wie „Name“ oder „Geburtsdatum“, als verschlüsselte Sequenz an das Bild angehängt und durch Standardwerte (beispielsweise „anonymisiert“) ersetzt. Der Nachteil ist, dass eine Zuordnung zu den Originaldaten, wie sie bei der Berechnung von Sekundärbildern oft notwendig ist, nur bei Entschlüsselung der kompletten Daten-Sequenz möglich ist. Dies muss aber auf den öffentlichen Gridrechnern unbedingt vermieden werden. MEDICUS, als aktuellstes Projekt, welches patientenbezogene Bilder in einem Grid überträgt, integriert einen zusätzlichen, mehrschichtigen Sicherheitsmechanismus zum Schutz der Patientendaten [7]. Dieser entspricht größtenteils den Vorschriften nach den strengen Regeln des amerikanischen Standards „Health Insurance Portability and Accountability Act (HIPAA)“ [18], birgt aber zwei Nachteile: erstens bedingt er die Nutzung eines aufwändigen, zusätzlichen Sicherheitssystems, „Shibboleth“, das aufgrund seiner Komplexität nicht in jedem Grid eingesetzt wird [19]. Zweitens werden Tabellen mit Zuordnungen zwischen den echten und den pseudonymisierten Patientendaten in den, zwar geschützten, aber dennoch öffentlichen Bereich des Grids gespeichert. Dies birgt das Risiko, dass im Fall eines Systemeinbruchs die kompletten Daten kompromittiert werden könnten.

1.4.3 Zuverlässigkeit und Fehlertoleranz

Der dynamische Zusammenschluss vieler kleinerer Informationssysteme, wie er in einem Gridnetzwerk erfolgt, erhöht nicht nur die Rechenleistung, sondern auch die Zahl der möglichen Fehlerquellen. Mit jeder möglichen Fehlerquelle erhöht sich aber auch die Unsicherheit bei der Ausführung von Berechnungen im Grid. Da die Zuverlässigkeit eines Grids ein wesentlicher Faktor im medizinischen Umfeld oder der kommerziellen Nutzung darstellt, rückt dieses Thema zunehmend in den Mittelpunkt des Interesses. Dabei beschäftigt sich die Forschung derzeit hauptsächlich mit Verfahren, welche die Programmausführung auf fremden Rechnern überwachen und sichern können. Voraussetzung für eine zuverlässige Ausführung von Pro-

grammen ist aber zunächst eine zuverlässige und sicherere Bereitstellung der Daten. Dai et. al. haben gezeigt, dass mit wachsender Größe der Gridnetzwerke insbesondere die Datenübertragung bei der Zuverlässigkeit eine entscheidende Rolle spielt [20]. Nach Schulz [21] und Kosar et al. [22] lassen sich die Hauptprobleme zurückführen auf temporäre Ausfälle (bis zu einer Stunde) durch

1. Überlastungen der Gridrechner,
2. Unterbrechungen bei der Übertragung durch Netzwerkprobleme,
3. Ausfälle der Dienste auf den Gridrechnern.

Es ist undenkbar, dass der Benutzer selbst an seinem Arbeitsplatz alle möglichen Fehlerquellen analysieren und gegebenenfalls beheben kann. Diese Aufgabe kann nur ein Computersystem erledigen, welches die Übertragungen automatisch überwacht und selbständig auf Fehler reagiert, also „fehlertolerant“ ist. Die Art und Weise, wie auf Fehler reagiert wird, kann dabei sehr unterschiedlich sein und richtet sich nach den Ansprüchen der Benutzer, beziehungsweise der Anwendung. Eine reine Forschungsanwendung braucht im Allgemeinen weniger Sicherheit bei der Übertragung als zum Beispiel eine Anwendung zur Operationsplanung. Die Bandbreite möglicher Fehlerstrategien ist deshalb groß und reicht von einer einfachen Fehlermeldung an den Benutzer bis zu effektiveren Methoden, wie die Auswahl alternativer Bildquellen. Bei der genannten Grid-Middleware existiert bisher lediglich im Globus-Toolkit ein einfaches Verfahren zur fehlertoleranten Dateiübertragung, der „Reliable File Transfer (RFT)“ [23]. Dieser genügt den allgemeinen Ansprüchen, indem er den Erfolg einer Dateiübertragung überwacht und im Fehlerfall die gesamte Übertragung wiederholt. Eine ähnliche Methode wurde im MEDICUS-Projekt umgesetzt, das einzige System, welches Fehlertoleranz bei der Bildübertragung berücksichtigt. Dort wird die Zwischenspeicherung der Bilder und die Komprimierung in ein Dateiarchiv als Aufgabe in einer Datenbank vermerkt und solange wiederholt, bis sie erfolgreich ausgeführt wurde. Da in der medizinischen Bildverarbeitung aber oft größere, zusammenhängende Bildserien übertragen werden, sind hier flexiblere und fortgeschrittene Verfahren wünschenswert, die zum Beispiel gezielt den Transfer einzelner, fehlgeschlagener Bilder einer Serie wiederholen.

Im Unterschied zu den allgemeinen Funktionen, die mit den vorgestellten Gridsystemen wie dem „Globus Toolkit“ entwickelt und gut erforscht sind, existieren damit in den Bereichen „DICOM-Kompatibilität“, „Datensicherheit“ und „Fehlertoleranz“ zurzeit keine zufriedenstellenden Lösungen beim Einsatz von Gridnetzwerken in der medizinischen Bildverarbeitung. Dies ist ein maßgeblicher Grund, warum keines der genannten Gridprojekte bisher das Forschungsstadium verlassen hat und Gridnetzwerke derzeit keinen Einsatz in der klinischen Routine finden. Erfolgreiche Lösungen in diesen drei Themen können die Akzeptanz von Grids in der Medizin deutlich erhöhen und einen entscheidenden Beitrag zu einem Einsatz in der klinischen Routine ermöglichen.

Kapitel 2

Motivation und Zielsetzung

2.1 Motivation

Grid-Infrastrukturen können gerade auch in der medizinischen Bildverarbeitung einen entscheidenden Beitrag für das moderne, IT-gestützte Gesundheitswesen leisten. So könnten auch kleinere Kliniken oder radiologische Praxen auf aufwändige Informationssysteme oder Software zugreifen, ohne hohe Investitionen leisten zu müssen. Das Konzept der virtuellen Organisationen und die damit verbundene Interoperation in Grids ist prädestiniert für das immer stärker werdende Thema eHealth und Telematik im Gesundheitswesen, in Deutschland genauso wie in anderen Ländern. Die Bandbreite der möglichen Einsatzgebiete von Grids ist dabei groß:

- Anwendungen, die eine große Rechenleistung aus einem Grid beziehen: Dazu gehören mittlerweile viele Berechnungen zur Bildverarbeitung von komplexen 3D- und 4D-Bildern, wie beispielsweise die funktionelle Kernspintomographie oder 3D-Simulationsberechnungen wie bei der virtuellen Operationsplanung, die durchaus mehrere Tage zur Berechnung brauchen können.
- Speicherung großer Datenmengen im Grid: Die modernen bildgebenden Verfahren produzieren immer größere Datenmengen. Durch die gemeinsame Nutzung von Bildarchiven in anderen Organisationen oder den Zusammenschluss kleinerer, verteilter Archive bieten Grids nahezu unbegrenzten Datenspeicher ohne größere Investitionen (GridPACS).
- Kooperation: Zunehmend werden Grids nicht zur Bündelung von Rechenleistung oder Speicherplatz sondern auch zum Austausch und zur Kooperation von Fachleuten eingesetzt. Dabei spielt die eingeführte Organisations- und Sicherheitsstruktur eine große

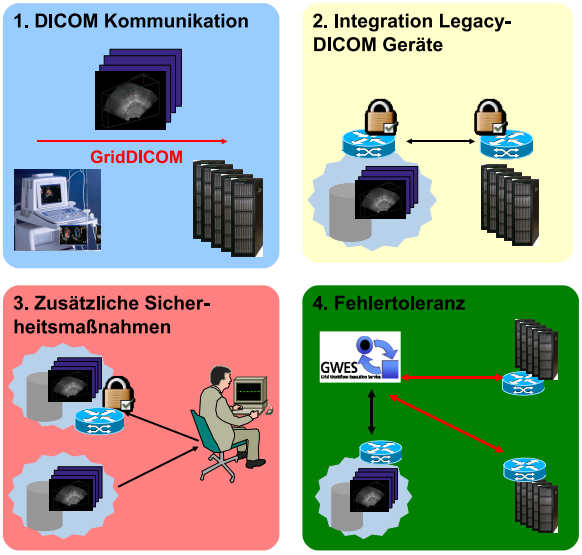


Abbildung 2.1: Eine Übersicht der vier Ziele der Arbeit, die sich so auch in den Beschreibungen wiederfindet. Jedes einzelne Ziel wird durch eine Referenzimplementierung validiert. Insgesamt ermöglicht die Lösung eine sichere und zuverlässige Bildübertragung in Grids.

Rolle. Diese Funktion erlaubt beispielsweise Konsile mit Kollegen und könnte in der Telemedizin eine große Rolle spielen oder die aufkommenden Kooperationsnetzwerke deutlich unterstützen.

Ein weiterer, großer Anwendungsbereich, dem auch aktuell in herkömmlichen Netzen eine sehr große Bedeutung zugemessen wird, ist die Nutzung von Software und Diensten („Software as a Service (SAAS)“). Dabei muss teure und aufwändige Software nicht mehr gekauft werden, sondern kann über das Grid genutzt werden, als wäre sie lokal vorhanden. Damit entfallen der Aufwand und die Pflege für die lokale Administration, sowie die nötige Hardware für anspruchsvolle Programme. Dies lohnt sich besonders für aufwändige Spezialprogramme, wie beispielsweise besondere Bildverarbeitungsverfahren, die bei der Diagnose eher selten zum Einsatz kommen. Dies gilt für kommerzielle Software genauso wie für die Wissenschaft, in der entwickelte Methoden oder Daten schnell der Forschung zur Verfügung gestellt werden können. Damit muss nicht jeder das Rad neu erfinden und hat einen schnelleren Zugang zu den neusten Entwicklungen.

Setzt man die angesprochenen Probleme als gelöst voraus, geht man allgemein davon aus, dass Healthgrids das Gesundheitswesen und die Zusammenarbeit der einzelnen Partner in Zukunft entscheidend beeinflussen werden [24].

Beispiel: Charité und MediGRID

Wie schon in der Einleitung kurz erwähnt, wird seit 2005 im Rahmen der deutschen D-Grid-Initiative das MediGRID betrieben. Ziel ist es, eine bundesweite

Grid-Infrastruktur für die biomedizinische Forschung aufzubauen und eigene Erfahrungen mit Anwendungen aus den Lebenswissenschaften zu sammeln. Das Institut für Medizinische Informatik der Charité ist maßgeblich an diesem Projekt beteiligt und leitet das Modul „Bildverarbeitung“. Dabei werden prototypisch Anwendungen aus der medizinischen Bildverarbeitung mit unterschiedlichen Ansprüchen auf dem Grid implementiert. Eine der umgesetzten Anwendungen ist „3D Ultraschall Prostatabiopsien“. Die Anwendung entsteht in enger Zusammenarbeit des Instituts mit der Urologie der Charité. Dabei handelt es sich um die räumliche Lokalisation von Prostatabiopsien durch Analyse der bei der Untersuchung aufgenommenen TRUS-Bilder (transrektaler Ultraschall). Hierbei werden die aufgenommenen 2D-TRUS Sequenzen mit den Gewebeproben mit Methoden der medizinischen Bildverarbeitung (Segmentierung und Registrierung) in einem anschließenden 3D- Übersichtsbild visualisiert. Die Berechnungen, gerade die Registrierung, sind dabei sehr rechenintensiv und können auf einem einzelnen Rechner mehrere Tage dauern. Durch die Nutzung des MediGRIDs werden die Berechnungen parallel auf mehreren Hochleistungsrechnern im Verbund gestartet und bieten so schon nach sehr kurzer Zeit das Ergebnis. Diese Anwendung befindet sich derzeit noch im Forschungsstadium. Erfolgreich umgesetzt sind bisher die Segmentierung der Biopsienadel [25, 26] und erste Algorithmen bei der Registrierung.

Obwohl Grid-Infrastrukturen in vielen Gebieten bereits sowohl in der Forschung als auch in der Industrie produktiv eingesetzt werden, ist dies in der Medizin bisher noch nicht der Fall. Der Grund sind die bisher noch nicht zufriedenstellend gelösten Probleme in den angesprochenen Bereichen "DICOM-Kompatibilität“, „Datensicherheit“ und „Fehlertoleranz“. Hier existieren zurzeit keine zufriedenstellenden Lösungen beim Einsatz von Grids in der medizinischen Bildverarbeitung. Es war das vorrangige Ziel dieser Arbeit, Verbesserungen in diesen drei Themenbereichen zu erzielen.

2.2 Ziele

Ziel der Arbeit war die Entwicklung eines Verfahrens zur sicheren und fehlerfreien DICOM-Bildübertragung in modernen Grid-Infrastrukturen, um diese in Zukunft auch für klinische Anwendungen nutzbar zu machen. Die entwickelte Lösung erfüllt die folgenden, bislang nicht oder nur unzureichend verfügbaren Funktionen, die damit die vier Kernziele der Arbeit darstellen (Abbildung 2.1):

1. Eine durchgängige DICOM-Kommunikation in Globus-basierten Grids,

2. Integration von in der Medizin verwendeten DICOM-kompatiblen Geräten in das Grid, ohne Gerätemodifikationen vornehmen zu müssen,

3. Datenschutzmaßnahmen für die patientenbezogenen Daten, die über den Transport hinausgehen und die Sicherheit auch nach Erreichen des Gridrechners gewährleisten sowie einen praktikablen Zugang zum internen PACS ermöglichen,

4. Verfahren, die automatisiert die umfangreiche Bildübertragung in Grids steuern, im Fehlerfall „intelligente“ Fehlerstrategien finden und so eine erfolgreiche Übertragung gewährleisten.

Aufbauend auf der Grid-Middleware „Globus-Toolkit“, welches die am meisten genutzte Gridsoftware mit den besten Voraussetzungen darstellt, beschäftigt sich die Arbeit zunächst mit Methoden der sicheren **DICOM-Integration**. Eine erfolgreiche Integration bietet die Möglichkeit der durchgängigen DICOM-Kommunikation in Grids, im Unterschied zu den bisherigen unsicheren Datentransfers, sowie einen **erfolgreichen Anschluss** von DICOM-kompatiblen Geräten. Entwickelt wurde hier ein Verfahren, sodass teure, bereits verfügbare Geräte ohne Änderungen in gewohnter Weise über Grids kommunizieren können.

Weiterhin erlauben es **zusätzliche Sicherheitsmaßnahmen**, Daten aus der klinischen Routine pseudonymisiert im Grid zu übertragen und zu bearbeiten. Die strengen Sicherheitsvorschriften an Kliniken erlauben meistens keine direkte Anbindung an öffentliche Netze, geschweige denn Grids. Wünschenswert waren deshalb Methoden, die in möglichst einfacher und praktikabler Weise den Austausch von Daten erlauben, und trotzdem den gängigen Sicherheitsanforderungen genügen.

In diesem Zusammenhang sei darauf hingewiesen, dass es sich bei diesem Teil um die Entwicklung von (technischen) Verfahren handelt, um die zusätzlichen Sicherheitsprobleme beim Einsatz von Grids im Vergleich zu herkömmlichen Netzen zu lösen. Es ist *nicht* der Anspruch dieser Arbeit, ein grundsätzliches Konzept für den Datenschutz beim Einsatz von Grid-Infrastrukturen zu entwickeln. Wie in dem folgenden Grundlagen-Kapitel noch ausführlich beschrieben wird, sind die Datenschutzanforderungen in der Medizin äußerst komplex und sind, wie beispielsweise mit den nötigen rollenbasierten Zugriffsrechten bei wechselnden Berechtigungen, über DICOM in Grids ebenso schwer praxisnah umzusetzen wie in herkömmlichen Netzen. Ein Konzept dieser Art ist ein komplett eigener Forschungsbereich und würde den Rahmen der Arbeit sprengen.

Ein abschließender Teil der Arbeit beschäftigt sich mit dem Thema einer **fehlertoleranten Bildübertragung**, um auf Fehler oder Ausfälle bei der Übertragung reagieren zu können. Auch in dem MediGRID-Rechnerverbund zeigen sich immer wieder Systemausfälle. Oft müssen aufwändig gestartete Experimente komplett wiederholt werden, unter anderem, weil Bilder

gar nicht oder nur unvollständig geladen wurden. Die Erfahrungen mit den bildverarbeitenden Anwendungen in MediGRID ergeben eine durchschnittliche Ausfallrate bei der Bildübertragung von etwa 5-6%. Dabei erhöht sich die Fehlerquote, je umfangreicher die übertragenen Bildserien sind. Eine Reduktion der Fehlerrate ist essentiell um einen routinemäßigen Einsatz von MediGRID zu ermöglichen.

Kapitel 3

Grundlagen

Im Folgenden werden einige der fachspezifischen Grundlagen zum besseren Verständnis der Arbeit erläutert:

3.1 Protokolle

In der Informationstechnik spielt die Vernetzung und der Datenaustausch zwischen Systemen seit jeher eine große Rolle. Durch die große Vielfalt an existierenden Betriebssystemen, Netzwerken und Programmen muss jede Kommunikation klar definiert werden. Diese Regelung übernehmen Protokolle, die auf den unterschiedlichsten Ebenen existieren. Sie schreiben vor, in welcher Art und Weise ein Verbindungsaufbau zwischen zwei Systemen zustande kommt, wie er beendet oder abgebrochen werden kann und wie im Einzelnen die Daten übertragen werden müssen, damit sie auf der Gegenseite richtig interpretiert werden können. Da die Definition von Protokollen bei Netzwerkverbindungen eine sehr komplexe Angelegenheit werden kann, werden diese in der Regel in kleinere Aufgabenbereiche unterteilt. So existieren Protokolle für die physikalische Datenübertragung, also die Signalsteuerung, in einem Medium wie einer Telefonverbindung oder einem Netzwerkkabel. Darauf aufbauend regeln „höhere“ Protokolle die Darstellung der Daten, die beispielsweise binär oder als Text dargestellt werden können. In der Netzwerktechnik sind diese Ebenen mit dem sogenannten „Open Systems Interconnection (OSI)-Schichtmodell“ genau definiert und die Übergänge zwischen den einzelnen Ebenen festgelegt. Dies hat den Vorteil, dass Protokolle der einzelnen Ebenen geändert werden können, ohne dass es die anderen Protokolle beeinflusst. Aus diesem Grund kann beispielsweise ein so weitreichendes Protokoll wie das Internet Protokoll, welches alle Rechner im weltweiten Internet verbindet, sowohl über ISDN-Telefonverbindungen als auch über Hochgeschwindigkeitsnetzwerke gleichermaßen funktionieren. Wichtige Protokolle im Rahmen dieser

Arbeit sind das

- Internet Protocol (IP): Das IP ist zuständig für die Adressierung der Rechner und die Weiterleitung von Datenpaketen im weltweiten Internetverbund [27].
- Transmission Control Protocol (TCP): Aufbauend auf dem IP, regelt das TCP die korrekte, zusammenhängende Übertragung von Datenpaketen [28].
- Transport Layer Security (TLS): Aufbauend auf dem TCP, regelt das optionale TLS eine Verschlüsselung der übertragenen Daten [29].
- Hypertext Transport Protocol (HTTP): Das HTTP-Protokoll baut auf TCP, beziehungsweise optional TLS, auf und regelt u.a. die Kommunikation zwischen einem Rechner, der Webseiten anbietet (Webserver) und einem Programm, welches diese nutzt (meistens ein Webbrowser). Damit ist es die Grundlage des WorldWideWeb [30].

Zwei weitere, wichtige Protokolle sind DICOM und das Simple Object Access Protocol (SOAP), die im Folgenden detailliert erklärt werden.

3.2 DICOM

Der DICOM-Standard [16, 31] ist ein weltweit anerkannter Standard zum Datenaustausch in der Medizin. Sein Ziel ist es, eine effiziente und korrekte Bild- und Datenübertragung zwischen bildverarbeitenden Geräten unterschiedlicher Hersteller und Systeme zu gewährleisten. Damit regelt der Standard jeglichen Bilddatenaustausch in der Radiologie und bildet, zusammen mit Health Level 7 (HL7) [32] im administrativen Bereich, die Grundlage für die digitale Kommunikation in jedem Krankenhaus. DICOM entstand ursprünglich 1992 aus dem amerikanischen ACR-Nema 2.0 Übertragungsstandard und befindet sich seitdem unter kontinuierlicher Weiterentwicklung durch die verschiedenen DICOM-Arbeitsgruppen. Von Anfang an wurde der Standard daher modular aufgebaut, sodass er möglichst einfach zu erweitern ist. Derzeit existieren 18 Module die dem Kernstandard zugerechnet werden und eine Vielzahl freigegebener Zusätze, den sogenannten „Supplements“.

Der Gesamtstandard geht dabei weit über die bloße Definition eines Bildformates hinaus. Er gibt im Detail vor, welche Daten in den jeweiligen Bildarten, beispielsweise CT, Ultraschall oder MRT, enthalten sein und wie diese interpretiert werden müssen. Gleichzeitig definiert er ein umfassendes Protokoll für die Kommunikation der jeweiligen Geräte auf Basis des Internet-Protokolls (und eines Direktverbindungsprotokolls, dies ist aber veraltet und wird nicht mehr

genutzt). Die im Protokoll enthaltenen Funktionen sind mittlerweile recht umfangreich und reichen von einer einfachen Geräteüberpüfung bis zu der Möglichkeit, Untersuchungen zu planen.

Zwei wichtige Funktionen sind dabei das sogenannte „Query/Retrieve“ und der „Storage“-Dienst, die alle Befehle zum Suchen und Übertragen von Bildern beschreiben und dementsprechend auch für diese Arbeit eine wichtige Rolle spielen. Dafür werden die folgenden Befehle definiert:

1. C-ECHO: Ein Verbindungstest von dem entfernten System. Beim C-ECHO wird nur eine Verbindung hergestellt um zu überprüfen ob das entfernte System reagiert und wie kompatibel es ist,
2. C-STORE: Sendet ein Bild zur Speicherung an einen anderen Rechner,
3. C-FIND: Über ein C-FIND lassen sich Bilder in einem System, beispielsweise einem PACS, suchen. C-FIND erlaubt es, einige der im DICOM-Bild angegebenen Daten als Suchkriterien anzugeben und eine Liste mit allen Bildnummern zurückzuerhalten, die diesen Kriterien entsprechen. Die eigentlichen Bilder müssen dann mit einem C-GET oder einem C-MOVE angefordert werden,
4. C-GET: Fordert Bilder an, welche den angegebenen Kriterien entsprechen. Dabei wird keine neue Verbindung aufgemacht, sondern die Bilder werden direkt als Antwort auf der gleichen Verbindung zurückgesendet,
5. C-MOVE: Weist ein Quellsystem an, Bilder, die den angegebenen Kriterien entsprechen, an dritte Systeme zu übertragen. Dabei macht das Quellsystem eine eigene Verbindung zu dem Drittsystem auf und gibt am Ende einen Gesamtstatus der Übertragung an den Auftraggeber zurück.

Bei allen DICOM-Funktionen ist der grundlegende Datenaufbau immer gleich und hierarchisch organisiert: Im Gegensatz zum fallbasierten HL7, bei dem ein Patient mehrere Fälle mit Untersuchungen besitzt, werden in DICOM einem Patienten gleich die Untersuchungen („Studies“) zugeordnet. Eine Untersuchung besteht dabei aus ein bis mehreren Bildserien („Series“), die von unterschiedlichen Modalitäten kommen können. Eine Bildserie setzt sich, je nach Modalität, aus einem Einzelbild (beispielsweise Computed Radiography (CR)), oder einigen hundert Bildern (wie einem 3D-MRT-Scan) zusammen. Alle Untersuchungen, Serien und Einzelbilder werden dabei mit einer permanenten, weltweit eindeutigen Identifikationsnummer versehen, der „Unique Identification (UID)“. Da die UID eine Kennzeichnung der erzeugenden Systeme und Organisation enthält, lassen sich erzeugte DICOM-Bilder jederzeit auf ihren Ursprung zurückführen, was bei dem Versand in öffentlichen Netzen ein datenschutzrechtliches Problem darstellt.

Der Kernstandard selbst bietet nur wenige Sicherheitsmechanismen. Im Wesentlichen handelt es sich dabei um die optionale Möglichkeit, einzelne Werte im Bild („Attribute“), wie beispielsweise den Patientennamen, zu pseudonymisieren. Dieses Vorgehen ist im Kapitel „Methodik: zusätzliche Sicherheitsmaßnahmen“ ausführlicher erläutert. Weiterhin ist im Modul 15 eine verschlüsselte Übertragung über die Protokolle TLS (und das ältere Integrated Secure Communication Layer (ISCL) [33]) definiert. Als Drittes ist in dem „Supplement 99“ die Möglichkeit definiert, eine Benutzeridentifikation bei dem Verbindungsaufbau mit anzugeben. Diese Verfahren sind aber nur für herkömmliche Netzwerke gedacht und erfüllen wesentliche Voraussetzungen für eine Nutzung im Grid, wie der Authentizität oder der Weiterleitung von Benutzeridentifikationen, nicht (siehe auch das Kapitel 4 „Methodik: DICOM-Kommunikation“).

3.3 SOAP: Web- und Gridservices

Ein „Webservice“ ist ein Synonym für einen standardisierten, Internet-basierten Dienst. Ähnlich zu den im WorldWideWeb angebotenen Webseiten für eine interaktive Bedienung, wie beispielsweise die Online-Abfrage des Wetters, sind Webservices Internet-basierte Anwendungen, die von Programmen selbständig ohne weitere Einwirkungen von Personen aufgerufen werden können. Auch die Ergebnisse können von den aufrufenden Programmen selbständig eingelesen und verarbeitet werden. Dazu bedarf es zusätzlich zu dem Web-Protokoll HTTP eines besonderen Protokolls, SOAP, welches die automatische Kommunikation regeln kann und die Übergabe und Interpretation von Ein- und Ausgabedaten definiert [34]. Das Anbieten von bisher integrierten Programmfunktionen als ausgegliederte Webservices hat den Vorteil, dass diese besser (öffentlich) zugänglich gemacht werden können und sich damit auch die Wartbarkeit, Skalierbarkeit und Effektivität von komplexen Systemen erhöht. Man spricht dabei von einer „dienste-orientierten Architektur“, oder englisch „Service Oriented Architectur (SOA)“.

Das SOA-Konzept hat die modernen Grid-Infrastrukturen stark beeinflusst, da sie für eine Umsetzung dynamisch verteilter Anwendungen wie geschaffen sind. Jedoch haben die ursprünglichen Webservices für eine Anwendung im Grid zwei Defizite: Erstens nutzen sie nicht die im Grid angewandte Sicherheitsinfrastruktur, zweitens sind sie „zustandslos“. Dies bedeutet, dass sie keine Daten über längere Zeit speichern können, was gerade bei den lange laufenden Anwendungen im Grid ein Problem werden kann. In Grid-Infrastrukturen wurden daher zwei Erweiterungen für die allgemeinen Webservices definiert, so dass erstens die gängige Sicherheitsinfrastruktur genutzt werden kann und zweitens Zustände gespeichert werden können (Webservice Resource Framework (WSRF) [35]). Im Allgemeinen spricht man bei Webservices dieser Art dann von „Gridservices“.

3.4 Verschlüsselung, Signatur und Zertifikate

Moderne Verfahren zur Verschlüsselung und zur elektronischen Signatur von Dokumenten basieren fast ausschließlich auf einer asynchronen „Publik-Key-Infrastruktur (PKI)“. Im Unterschied zu synchronen Verfahren, bei denen jeder Teilnehmer die Daten mit dem gleichen Schlüssel ver- und entschlüsselt, besitzt hierbei jeder Teilnehmer ein eigenes Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Mit dem öffentlichen Schlüssel können Daten verschlüsselt werden, die nur mit dem passenden privaten Schlüssel, also von dem entsprechenden Teilnehmer, wieder gelesen werden können. Dieses Verfahren hat den Vorteil, dass niemals ein geheimer Schlüssel über öffentliche Kanäle transportiert werden muss wo er eventuell kompromittiert werden könnte. Nachteilig ist, dass die Verschlüsselungsalgorithmen im Vergleich zu synchronen Verfahren sehr viel mehr Zeit benötigen und die Authentizität des öffentlichen Schlüssels von dem jeweiligen Teilnehmer gewährleistet sein muss.

Technisch kann es sich bei einem Teilnehmer um natürliche Personen, aber auch um Computersysteme, wie beispielsweise Modalitäten, handeln. Zusätzlich zur Verschlüsselung können Teilnehmer Daten mit dem privaten Schlüssel digital signieren. Die digitale Signatur bezeugt die Herkunft und Unveränderlichkeit von Daten und kann von jedem mit dem öffentlichen Schlüssel des Teilnehmers verifiziert werden. Dabei ist die digitale Signatur, als ein technisches Verfahren, zu unterscheiden von der elektronischen Signatur. Diese stellt, als ein rechtlicher Begriff, die Analogie zur herkömmlichen Unterschrift dar und unterliegt weiteren Einschränkungen. So darf sie beispielsweise nur von natürlichen Personen angewandt werden. Bei dem Verfahren der digitalen Signatur ist es wichtig, dass der öffentliche Schlüssel auch wirklich dem signierenden Teilnehmer zugeordnet werden kann. Diese Aufgabe übernehmen Zertifikate, die einen öffentlichen Schlüssel eindeutig einer bestimmten Person oder System zuordnen. Bei dem Format der Zertifikate hat sich der sogenannte X.509-Standard [36] durchgesetzt, der daher sowohl beim Deutschen Signaturgesetz als auch der neuen Gesundheitskarte oder dem Heilberufeausweis angewandt wird [37, 38]. Der X.509-Standard beruht auf einer Zertifikatshierarchie: ein einzelnes Zertifikat wird von einer Organisation bestätigt („Certificate Authority (CA)“). Das Zertifikat dieser Organisation wird eventuell wiederum von einer höheren Instanz bestätigt. Als letztes bestätigt eine Organisation, die allgemein bekannt ist und der man vertraut, wie beispielsweise der Bundesregierung oder einer großen wissenschaftlichen Einrichtung. Diese Zertifikatskette hat den Vorteil, dass man den Zertifikaten einer großen Benutzermenge vertrauen kann, ohne jedes einzeln überprüfen zu müssen. Alternativen zu dieser hierarchischen Struktur ist das sogenannte „Web-of-Trust“, das „Netz des Vertrauens“. Dabei werden die Zertifikate nicht von einer übergeordneten Organisation, sondern von den anderen, vertrauenswürdigen Teilnehmern bestätigt. Dieses Verfahren ist weniger aufwändig, aber auch nur für kleine, vorab definierte Benutzergruppen sinnvoll, wes-

halb die hierarchische Form im Allgemeinen bevorzugt wird.

3.5 Datenschutz in der Medizin

Patientenbezogene medizinische Daten unterliegen zu Recht höchsten Datenschutzanforderungen. Diese gelten insbesondere bei der Übertragung von Daten über öffentliche Netze, aber auch bei der Datenspeicherung für klinische Studien oder der elektronischen Fall- oder Patientenakte. In Deutschland ist dabei die oberste Richtlinie das Bundesdatenschutzgesetz [39]. Weiterhin existieren zahlreiche Datenschutzkonzepte vom „Bundesamt für Sicherheit in der Informationstechnik (BSI)“, wie beispielsweise [40], oder von nationalen Interessensgruppen wie dem Verein „Telematikplattform für medizinische Forschungsnetze (TMF)“ [41]. Grundlegende Bedeutung hat auch der in Nordamerika seit 2005 bindend eingeführte und speziell für das Gesundheitswesen ausgelegte HIPAA [18]. Allen Vorgaben gemeinsam sind die folgenden, grundlegenden technisch-organisatorischen Sicherheitsziele [42]:

- Integrität, Authentizität und Vertraulichkeit: Es muss sichergestellt werden, dass die abgespeicherten Daten dem Urheber zugeordnet werden können und unverfälscht sind. Für die Sicherstellung der Vertraulichkeit können Verschlüsselungsverfahren eingesetzt werden.
- Benutzer- und aufgabenbezogenes Berechtigungskonzept: Es muss ein differenziertes Berechtigungskonzept erarbeitet werden, das basierend auf der Organisationsstruktur der Institution für alle Benutzer die zur Aufgabenerfüllung benötigten Rechte festlegt.
- Verfügbarkeit: Die Verfügbarkeit beschreibt die Fähigkeit eines Systems, überhaupt zu kommunizieren und die dem System zugerechnete, operative Aufgabe in adäquaten Zeitrahmen zu erledigen.
- Protokollierung und Revisionsfähigkeit: Aus Gründen der Revisionsfähigkeit muss für sämtliche patientenbezogenen Daten nachvollziehbar sein, wer welche Daten zu welchem Zeitpunkt verarbeitet hat.

.

Kapitel 4

Methodik

Entsprechend der vier Kernziele der Arbeit, unterteilen sich die Methoden in die folgenden vier Bereiche:

4.1 Durchgängige DICOM-Kommunikation

Im Unterschied zu den bisherigen Lösungen, die verschiedene Verfahren kombinieren und dadurch den DICOM-Funktionsumfang effektiv begrenzen, ermöglicht eine durchgängige DICOM-Kommunikation, den vollen Umfang des DICOM-Standards zwischen den kompatiblen Endgeräten zu nutzen. Damit bleiben die Vorteile, wie die Asynchronität des Protokolls oder die eindeutige Identifizierung von Bildern, erhalten. Zusätzlich werden die Bilder nicht mehr zwischengespeichert, was Einbußen bei der Leistung und der Datensicherheit verhindert.

4.1.1 Ansatz

Für eine durchgängige Kommunikation im Grid ist das DICOM-Protokoll an die im Grid eingesetzten Sicherheitsverfahren anzupassen. Da die meisten Grids als Sicherheitsstandard das beschriebene GSI des Globus-Toolkits verwenden, erfolgt die Anpassung an diesen Standard.

Grundsätzlich beschreibt das GSI Funktionen in den folgenden vier Bereichen:

1. *Authentifikation:* Die Kommunikationspartner müssen sich untereinander identifizieren können. Diese sichere Identifikation gilt sowohl für Personen als auch für Systeme und muss auch für größere und weit verteilte Benutzergruppen, wie sie bei Grids vorkommen,

möglichst einfach administrierbar und anwendbar sein.

2. *Autorisierung:* Im Unterschied zur Authentifikation, die überprüft, wer der Kommunikationspartner ist, regelt die Autorisierung, was der jeweilige Partner darf. In Grids hängen die Zugriffsrechte stark von der jeweiligen Anwendung und Ressource ab. So gibt es beispielsweise für den Zugriff auf verteilte Daten andere Zugriffsrechte als für die Ausführung einer Anwendung. Im Unterschied zu einheitlichen Ressourcen in herkömmlichen Netzen, macht dies eine grundlegende Regelung der Zugriffsrechte schwieriger.

3. *Verschlüsselung und Integrität:* Bei der Verschlüsselung wird der Datenstrom für Fremde unlesbar gemacht, wohingegen bei der Integrität sichergestellt wird, dass die Daten nicht durch Dritte verändert werden können. Der Sicherheitsstandard legt fest, welche Verfahren und welche Algorithmen jeweils für die Verschlüsselung und Datenintegrität angewendet werden sollen.

4. *„Single-Sign-On“:* Einer der wichtigsten Sicherheitsfunktionen in Grids, die es von herkömmlichen Netzen unterscheidet, ist das sogenannte „Single-Sign-On“. Dies bezeichnet die Möglichkeit, sich nur einmal dem Grid gegenüber identifizieren zu müssen, aber danach beliebig viele verteilte Systeme gleichzeitig im Grid nutzen zu können. Dies ist nötig, da die Kommunikation in Grids naturgemäß über viele verteilte Rechner stattfindet. Dabei werden die Daten des Benutzers oft ohne seinen weiteren Einfluss zur schnelleren Berechnung von einem System auf zusätzliche weitere verteilt.

Wie in den Grundlagen beschrieben, ist der DICOM-Standard in einzelne Module unterteilt, die jeweils genau abgegrenzte Themenbereiche beschreiben. Diese Modularisierung erlaubt eine einfache Erweiterung des Standards um neue Verfahren. Das Modul 15, „Sicherheitsprofile“, beschreibt dabei die Verwendung zusätzlicher Sicherheitsstandards beim Verbindungsaufbau. Bisher ist hier lediglich die Verwendung des TLS-Protokolls zur Verschlüsselung des Datentransfers enthalten. Nach Abschnitt 6.2 muss ein solches Profil die folgenden Punkte enthalten:

1. Beschreibung des Protokoll-Rahmens und der Mechanismen für die gegenseitigen Vereinbarungen.

2. Beschreibung der Authentifikations-Mechanismen, welche die Anwendung unterstützen sollen, insbesondere

   (a) das Identitätsformat der zu authentifizierenden Teilnehmer.

   (b) das Verfahren, mit dem sich die Teilnehmner identifizieren.

   (c) spezielle Anforderungen für eine Audit-Unterstützung.

3. Beschreibung der unterstützten Verschlüsselungsverfahren, insbesondere das Verfahren zur Verteilung von Session-Schlüssels und das Verschlüsselungsprotokoll mit den relevanten Parametern.

4. Beschreibung der unterstützen Mechanismen zum Integritätscheck.

Als Grundlage für eine durchgehende DICOM-Kommunikation muss ein solches Profil „Grid-DICOM“ erstellt und standard-konform beschrieben werden. Dies bedeutet im Einzelnen die Durchführung der folgenden Schritte:

1. Analyse der Verfahren beim GSI.

2. Definition des DICOM-Verbindungsaufbaus unter Verwendung der GSI-Funktionen.

3. Beschreibung der relevanten Verfahren für das Profil gemäß Modul 15 des DICOM-Standards analog zu den bereits existierenden Profilen. Das fertige Profil kann als Vorschlag zur Einbringung in den Standard dienen.

4.1.2 Referenzimplementation und Tests

Das neue Sicherheitsprofil wird mit einer Referenzimplementation validiert. Die Implementation muss den folgenden Entwicklungskriterien genügen:

1. *Aufbau von GSI-gesicherten DICOM-Verbindungen:* Anwendungen sollen mithilfe der Implementation in der Lage sein, GSI-gesicherte Verbindungen auf Basis einer vorhandenden GSI-Infrastruktur aufzubauen und Bilder zwischen Gridrechnern auszutauschen. Die vorhandene GSI-Infrastruktur beinhaltet insbesondere die Authentifizierung und Autorisierung der am Grid beteiligten Partner.

2. *Wiederverwendung bereits existierender Software:* Da es sich bei dem neuen Profil größtenteils um eine Erweiterung handelt, soll die Software nicht gänzlich neu entwickelt, sondern möglichst an eine bestehende DICOM-Implementation angepasst werden. Das gleiche gilt für die Implementation der GSI-Funktionen, wie beispielsweise der Verschlüsselung. Hierfür soll möglichst eine bestehende Software verwandt werden, die die GSI-Grundfunktionen bereitstellt.

3. *Plattformunabhängigkeit:* Die Software soll ohne weitere Änderungen auf möglichst vielen von den in Grids genutzten Rechnerarchitekturen und Betriebssystemen einsatzfähig sein.

Abbildung 4.1: Mögliche Testumgebung für die GridDICOM-Implementation. Für praxisnahe Tests sollen die Testrechner aus dem MediGRID-Verbund eine möglichst breite unterschiedliche geographische Verteilung repräsentieren.

Getestet wird diese Implementation durch manuelle DICOM-Übertragungen zwischen ausgewählten Rechnern aus dem MediGRID-Verbund. Um realistische Bedingungen in Hinblick auf einen späteren Grid-Einsatz zu testen, werden die Rechner mit einer möglichst unterschiedlichen geographischen Bandbreite ausgewählt. Ähnlich zu Erberich et al. bei ihren Tests der DGIS-Lösung [7] wird in fünf unterschiedlichen Grid-Regionen unterschieden (siehe auch Abbildung 4.1):

1. *Campus:* Die Kommunikationspartner befinden sich im gleichen Institut, bzw. auf dem gleichen Campus.
2. *City:* Die Kommunikationspartner sind in der gleichen Stadt.
3. *Region:* Die Kommunikationspartner befinden sich in der näheren Region.
4. *Greater Region:* Die Kommunikationspartner befinden sich überregional in mittlerer Entfernung.
5. *Country:* Die Kommunikationspartner befinden sich landesweit in großer Entfernung.

Gleichzeitig sollen die Rechner unterschiedliche Systemarchitekturen besitzen um die Flexibilität der Software zu gewährleisten.

Für die Tests werden Anwendungen entwickelt, die auf Basis der erweiterten GridDICOM-Software manuell Bilder übertragen können. Diese Anwendungen werden auf den Testrechner installiert. Sie übertragen durch den DICOM-Befehl C-STORE ausgewählte, öffentliche Testbildserien unterschiedlicher Modalitäten an die anderen Gridrechner. Die Testbildserien unterscheiden sich möglichst in ihrer Struktur. So bestehen sie beispielsweise sowohl aus Studien

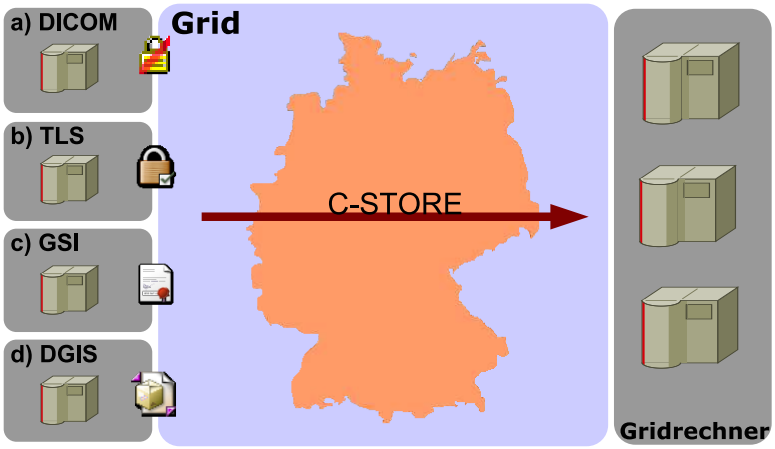


Abbildung 4.2: Testszenario für die Tests der durchgängigen DICOM-Kommunikation: Über ein DICOM-C-STORE-Befehl werden Bildserien von einem Gridrechner zu unterschiedlich entfernten Gridrechnern gesendet. Verglichen werden a) die herkömmliche, direkte DICOM-Kommunikation, b) eine herkömmliche TLS-verschlüsselte DICOM-Kommunikation, c) die neue GridDICOM-Kommunikation und d) die bisherige DGIS-Lösung.

mit vielen, kleineren Einzelbildern als auch aus vielen Serien mit wenigen, aber größeren Bildern. In den Tests werden die Übertragungsraten bei der Versendung der unterschiedlichen Bildserien auf den verschiedenen Distanzen ermittelt und mit den bisher existierenden Verfahren verglichen (siehe auch Abbildung 4.2).

4.2 Integration von vorhandenen DICOM-kompatiblen Systemen

Da die Akzeptanz und die Bekanntheit von Grids in der Medizin noch relativ gering ist, ist nicht zu erwarten, dass die erweiterten Sicherheitsprofile in naher Zukunft in den DICOM-Standard offiziell übernommen werden. Damit werden auch die Hersteller von DICOM-kompatiblen Geräten die zusätzlichen, Grid-spezifischen Sicherheitsprofile nicht zeitnah umsetzen. Es wurde deshalb eine Lösung entwickelt um herkömmliche DICOM-Geräte in das Grid zu integrieren, ohne Änderungen an den Geräten oder ihrer Software vornehmen zu müssen.

4.2.1 Ansatz

Als Lösung wird ein System konzipiert, welches zwischen dem herkömmlichen DICOM-Gerät und den Grid-Systemen „übersetzt“. Ein solcher Ansatz ist auch als „Router“ bekannt und kommt in der Netzwerktechnik bei der Umsetzung von verschiedenen Transportmethoden zum Einsatz [43]. Router arbeiten nach dem Verfahren der transparenten, bi-direktionalen Um-

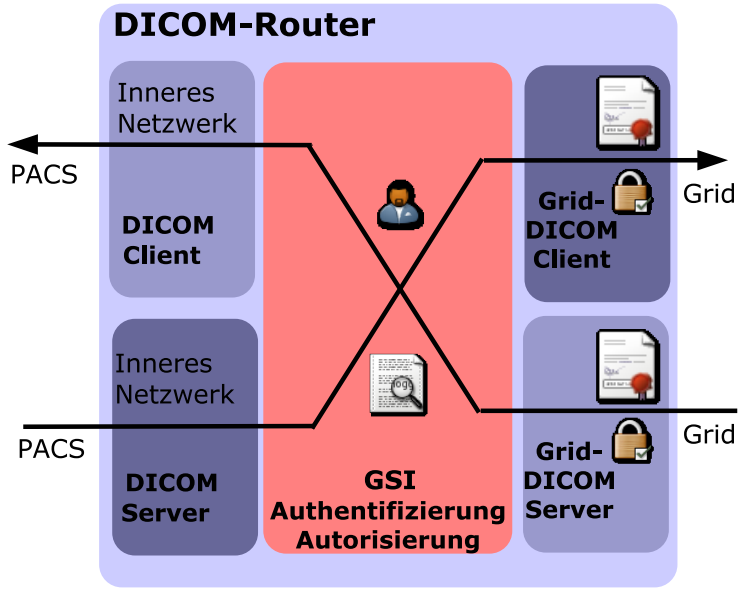


Abbildung 4.3: Architektur des DICOM-Routers: Zur einen Seite kommuniziert das System mit einem PACS, zur anderen Seite mit dem Grid. Eingehende DICOM-Nachrichten vom PACS werden angenommen, den GSI-Sicherheitsüberprüfungen unterzogen, und über eine GridDICOM-Verbindung ins Grid weitergeleitet. Gleichermaßen arbeitet das System in der entgegengesetzten Richtung.

wandlung von Datenströmen. Dabei übernehmen sie oft auch die Funktion einer „intelligenten“ Überprüfung und Weiterleitung der einzelnen Datenpakete und steuern so den Datenverkehr im Netz.

Im Unterschied zur Netzwerktechnik arbeitet der Router hier nicht auf der unteren Netzwerkebene, sondern auf der oberen DICOM-Ebene mit explizitem Zugriff auf die Inhalte der DICOM-Daten. Damit entspricht der Begriff „Router“ nicht ganz der herkömmlichen Definition aus der Netzwerktechnik. Jedoch erfüllt das System eine „Routing“-Funktion im übergeordneten Grid-Kontext, weshalb der Begriff hier gewählt wurde. Dabei kommuniziert der Router zur einen Seite mit DICOM-Geräten (beispielsweise einem PACS) und zur anderen Seite mit GridDICOM-gesicherten Systemen aus dem Grid. Eingehende DICOM-Daten vom PACS werden angenommen und über eine GridDICOM-Verbindung ins Grid weitergeleitet. Gleichermaßen arbeitet das System in der entgegengesetzten Richtung (siehe Abbildung 4.3).

Ein alternativer Lösungsansatz zu einem solchen DICOM-Router wäre die Möglichkeit, die Verbindungen auf der Netzwerkebene weiterzuleiten, also auf TCP/IP-Ebene. Ein solches Verfahren, bekannt als „Socket-Forwarding“ existiert bereits [44] und ließe sich auch für GSI anpassen. Der Nachteil bei diesem Verfahren aber ist, dass diese Methode nur Zugriff auf die Datenpakete auf Netzwerkebene bietet. Die DICOM-Objekte werden zwar mit diesen Paketen transportiert, können aber nicht als solche erkannt werden, da sie auf einer viel abstrakteren Ebene verarbeitet werden. Der vorgeschlagene Router dagegen nimmt explizit die einzelnen DICOM-Nachrichten an und leitet sie weiter. Damit hat er Zugriff auf die Inhalte der DICOM-

Objekte bei der Übertragung. So können beim Durchlauf durch den Router die Zugriffsrechte überprüft werden (beispielsweise auf Basis der in den Bilder eingetragen behandelnden Arztnamen), Weiterleitungen anhand der DICOM-Systemkennungen durchgeführt werden oder Veränderungen an den Inhalten vorgenommen werden (wie eine Pseudonymisierung).

Entscheidend bei der Konzeption von Routern ist der Aufbau eines solches Systems. Es muss in der Lage sein, jegliche Kommunikation in beide Richtungen auch unter hohem Datenaufkommen technisch fehlerfrei und möglichst ohne Zeitverlust umzusetzen. Hierzu werden zwei Ansätze untersucht:

1. Ein klassisches, monolithisches System

   Bei klassischen Ansätzen besteht die Router-Software aus einem einzigen Programm, welches alle Funktionen integriert und einmal gestartet wird. Der Vorteil ist, dass solche Programme einfach zu implementieren und administrieren sind. In der Praxis zeigen sich solche Systeme aber oft als sehr ineffizient oder schnell ausgelastet, da sie nicht in der Lage sind, sich hohen und wechselnden Belastungen anzupassen. Im weiteren Verlauf wird dieses System als das „monolithische“ System referenziert.

2. Eine moderne, modulare Architektur nach dem sogenannten „MBean“- und dem „J2EE“-Standard

   „MBeans“ sind standardisierte Programmmodule, die dynamisch von einem Kontrollsystem verwaltet werden. Der „Java2 Enterprise Edition (J2EE)“-Standard ist ein moderner Standard zur Entwicklung verteilter, hochperformanter Anwendungen, der wichtige Programmfunktionen, wie beispielsweise Datenbankoperationen, als solch skalierbare Module bereitstellt [45]. Im Gegensatz zu den herkömmlichen Verfahren kann das Routersystem so jederzeit die ein- und ausgehenden Verbindungsanfragen auf eine beliebige Anzahl von laufenden Modulen verteilen. Damit ist es flexibler und der jeweils aktuellen Belastung besser gewachsen (siehe auch Abbildung 4.4). Zwar ließe sich diese Lastverteilung grundsätzlich auch mit mehreren monolithischen Anwendungen erreichen, jedoch ist dann die Kommunikation untereinander nicht mehr gegeben. Diese ist aber entscheidend in den Router-Szenarien, beispielsweise um Zertifikate über mehrere Verbindungen hinweg weiterleiten zu können. Zusätzlich sind diese Entwicklungen standardisiert und können von jedem konformen Kontrollsystem betrieben werden, wodurch sie auch in anderen Grid-Projekten besser genutzt werden können. Dieses System wird im Folgenden als das „modulare“ System bezeichnet.

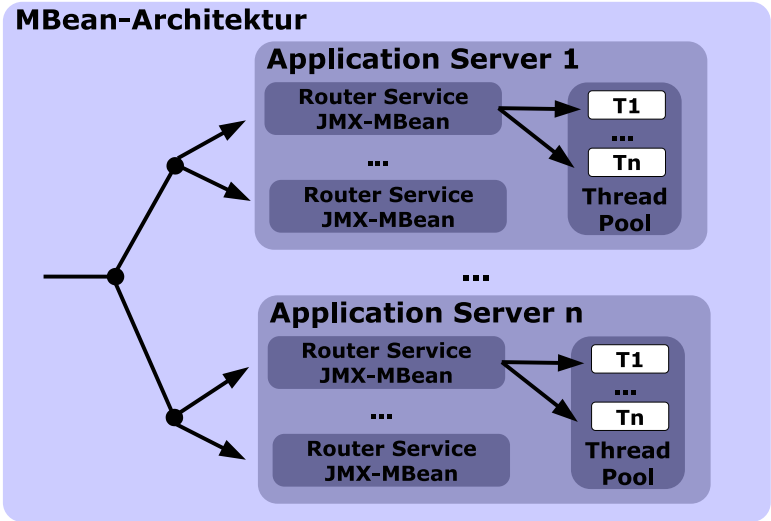


Abbildung 4.4: Modulare Architektur eines Systems. Im Unterschied zu einem monolithischen System können die Anfragen dynamisch auf beliebig viele Module verteilt werden, wodurch das Gesamtsystem flexibler und leistungsstärker ist.

Authentifizierung und Autorisierung

Der DICOM-Kernstandard definiert keine besonders sicheren Authentifizierungs-Maßnahmen. Die kommunizierenden Anwendungen tauschen bei der Verbindungsanfrage lediglich eine Kennung, den sogenannten „Application Entity Title (AET)“, aus. In einer Ergänzung zum Standard, dem „Supplement 99“, wird die Möglichkeit definiert, eine Authentifizierung auf Basis von Benutzernamen durchzuführen. Dieses Verfahren hat im Grid-Zusammenhang jedoch zwei Nachteile: Erstens ist es nur optional und daher nicht verlässlich überall verfügbar. Zweitens regelt es nicht das Grundproblem im Grid der Vertrauenswürdigkeit und Identifikation von unbekannten Benutzern. Dies wird erst über die Nutzung des gridweiten GSI erreicht. Anfragen nach dem ungesicherten DICOM-Standard, die ins Grid weitergeleitet werden sollen, muss daher für eine verlässliche Authentifizierung ein Zertifikat zur Umsetzung in GridDICOM zugewiesen werden. Ein besonderes Kriterium bei der Funktionsweise der Router ist deshalb die Frage, ob die Weiterleitung der Zertifikate unterstützt wird um eine durchgehende Authentifizierung zu gewährleisten, selbst bei Drittanfragen wie beispielsweise dem DICOM-C-MOVE.

4.2.2 Referenzimplementation und Tests

Für die Untersuchungen werden jeweils ein DICOM-Router-Programm nach monolithischem Ansatz und eines nach dem modularisierten MBean- bzw. J2EE-Standard entworfen und entwickelt. Die Router nehmen die gängigen DICOM-Befehle zur Bildübertragung an und setzen sie in GridDICOM um. Die gleichen Befehle können sie von Systemen aus dem Grid verarbeiten und an die DICOM-Geräte weiterleiten.

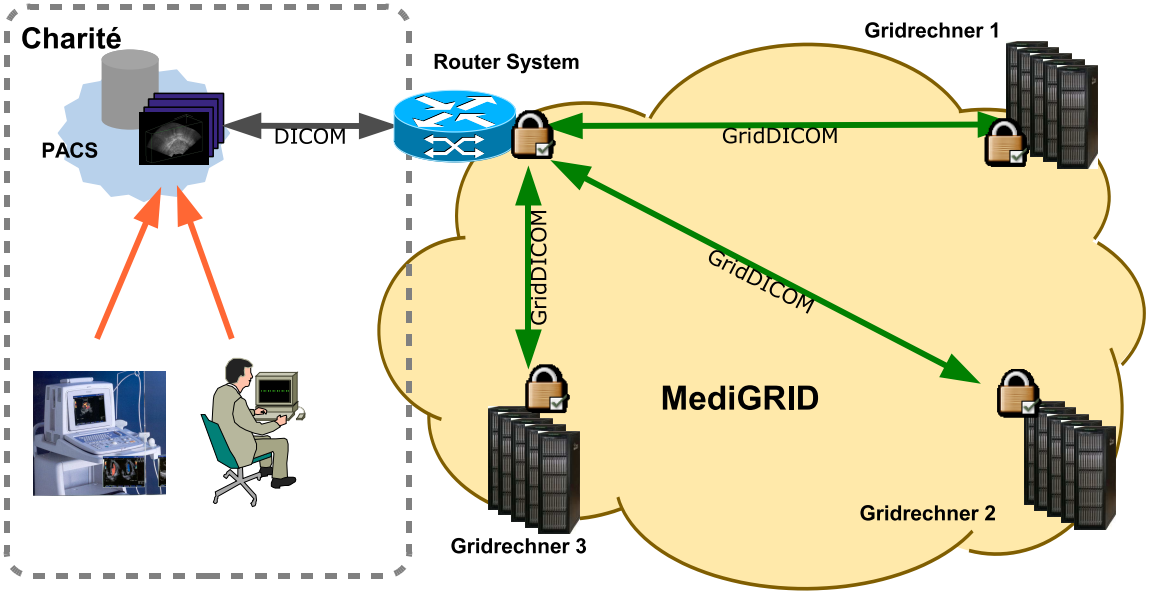


Abbildung 4.5: Aufbau der DICOM-Router: Die Router werden jeweils zwischen dem PACS und dem Grid installiert und übersetzen transparent den DICOM-Datenverkehr in GridDICOM und umgekehrt.

Evaluiert werden die beiden Systeme wie in 4.1.2 durch Tests mit Gridrechnern aus dem MediGRID-Verbund. Um Unregelmäßigkeiten durch die Netzwerkverbindungen auszuschließen, sollen diesmal allerdings nur diejenigen Rechner gewählt werden, die geographisch, bzw. von der Netzwerkverbindung, sehr nahe zusammenstehen. Beide Routerlösungen werden jeweils zwischen dem PACS und dem Grid auf einem gängigem Arbeitsplatzrechner installiert (siehe Abbildung 4.5). Die Router werden sowohl in ihrer Funktion als auch in der Übertragungsleistung evaluiert:

Bei den **Funktionstests** soll die fehlerfreie Umsetzung über den Router verifiziert und mit der direkten Übertragung ohne einen zwischengeschalteten Router verglichen werden. Dabei werden drei typische Szenarien der Bildübertragung getestet:

1. Das Storage-Szenario aus 4.1.2 bei dem Bilder von einem Arbeitsplatz direkt an verschiedene Gridrechner ohne Router gesandt werden (Abbildung 4.2).

2. Das Speichern zwischen zwei Geräten, die über GridDICOM-Router verbunden sind, beispielsweise das Senden von einem Arbeitsplatzrechner zu einem Grid-PACS (Abbildung 4.6 links).

3. „C-MOVE“: Das Beauftragen von einem Arbeitsplatzrechner aus, Bilder von einem Grid-PACS zu einem anderen zu senden (Abbildung 4.6 rechts).

Bei den **Leistungstests** soll vor allem die zeitliche Leistung der Router bei der Bearbei-

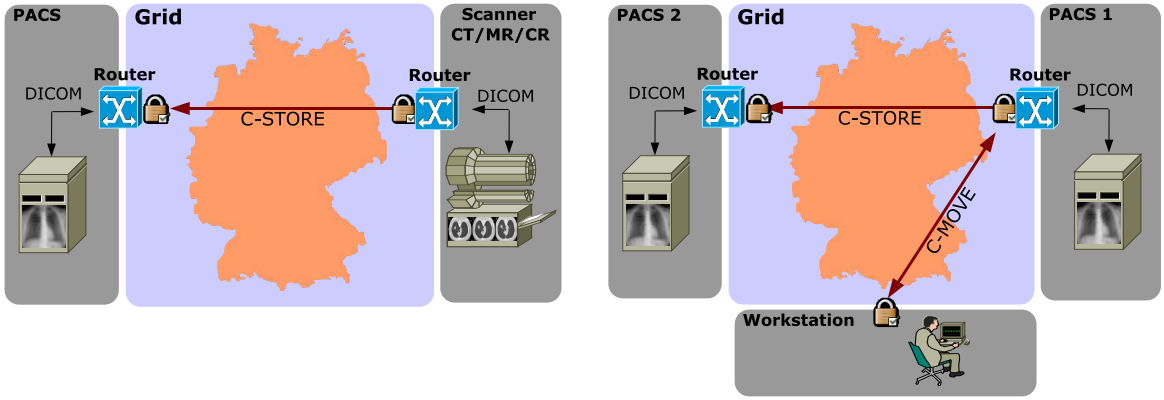


Abbildung 4.6: Testszenarien für die DICOM-Router. Links: Das Speichern zwischen zwei Geräten, die über GridDICOM-Router verbunden sind, beispielsweise das Senden von einem Arbeitsplatzrechner zu einem Grid-PACS. Rechts: Das Beauftragen von einem Arbeitsplatzrechner aus, Bilder von einem Grid-PACS zu einem anderen zu senden (C-MOVE).

tung von parallel gesendeten Bildserien verglichen und auf ihre Skalierbarkeit hin überprüft werden. Gut skalierbare Systeme zeigen bei steigender Belastung ein entsprechend lineares Antwortverhalten. In der Praxis bedeutet dies, dass das System unter jeder Last berechenbar und damit einfach erweiterbar ist. Skaliert ein System schlecht, zeigt es unter steigender Belastung ein unerwartetes Verhalten (im schlimmsten Fall bricht es zusammen) und ist damit für einen Einsatz in der Praxis nicht zu gebrauchen.

4.3 Zusätzliche Sicherheitsmaßnahmen

Zur Berechnung in einem Grid werden die Bilder in der Regel auf fremde Rechner kopiert. Daher müssen die patientenbezogenen Inhalte nicht nur auf dem Transport, sondern auch nach Erreichen des Zielrechners besonders geschützt werden. Weiterhin ist ein direkter, automatischer Zugriff auf ein internes Klinik-PACS, selbst nach den beschriebenen Sicherheitsverfahren, in den meisten Kliniken nicht erlaubt. Es wurde daher eine Lösung zum Schutz der Patientendaten jenseits des eigentlichen Transports zusammen mit einen sicheren Zugriff auf das klinikinterne PACS entwickelt.

4.3.1 Ansatz

Zum Schutz der patientenbezogenen Daten werden die Bilder vor dem Übergang in das öffentliche Grid pseudonymisiert. Dabei werden die Originaldaten in dem Bild verschlüsselt und durch Pseudonyme ersetzt. Im Unterschied zu der rein verschlüsselten Übertragung sind die Daten damit auch über den Transport hinaus geschützt. Erst nach einer eventuellen Rück-

übertragung vom Grid in das private Kliniknetz, werden sie wieder identifiziert.

Wie schon in den Grundlagen kurz beschrieben, wird in dem Modul 15 des DICOM- Standards ein Verfahren definiert, welches die Verschlüsselung von sicherheitsrelevanten Daten, den Attributen, erlaubt. Diese „Attribute Level Confidentiality (ALC)“ schreibt dabei nicht vor, welche Daten zu schützen sind, sondern gibt nur eine technische Beschreibung über das Vorgehen. Alle zu schützenden Attribute werden zusammengefasst und als ein großer Block verschlüsselt an das Bild angehängt. Um die Konformität zu erhalten, werden die ursprünglichen Daten durch unkritische Werte, wie beispielsweise „anonym“ als Patientennamen, ersetzt. Dieses Verfahren hat den Nachteil, dass der Zugriff auf einzelne Original-Attribute die Entschlüsselung des kompletten Blocks bedingt. Gerade bei der medizinischen Bildverarbeitung in Grids kommt es aber oft vor, dass auf den fremden Rechner einzelne Original-Attribute referenziert werden müssen. Beispielsweise müssen berechnete Bilder eine Referenz auf das Originalbild enthalten, damit diese später im PACS zusammen angezeigt werden können. Dies ist ohne die Entschlüsselung der Originaldaten, was man unbedingt vermeiden will, aber nicht möglich.

Als Alternative wird daher ein im Rahmen eines Promotionsvorhabens von Andreas Thiel am Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und -Systeme (OFFIS) entwickeltes Verfahren „SecureDicom“ überprüft [46]. Diese Erweiterung verschlüsselt nicht alle Einzeldaten zusammen in einem großen Block, sondern hängt die Werte einzeln verschlüsselt an das Bild an. Dies erlaubt auch ohne Entschlüsselung des kompletten Datenblocks den Zugriff auf einzelne Werte und damit eine eindeutige Referenzierung. Für die Überprüfung wird zunächst die Erweiterung „SecureDICOM“ analysiert, mit der bisher verfügbaren Methode ALC verglichen und dann auf eine mögliche Verwendung im Grid-Umfeld hin überprüft. Für eine erfolgreiche Verwendung in Grids muss sichergestellt sein, dass alle relevanten Daten pseudonymisiert werden und trotzdem auf einzelne, verschlüsselte Original-Attribute zugegriffen werden kann.

Für einen sicheren Zugang zum internen Klinik-PACS wird ein Konzept für die Systemintegration in der Klinik entwickelt und auf seine Machbarkeit hin überprüft. Eine Bildübertragung vom Grid zum internen Klinik-PACS und zurück ist im Allgemeinen nur möglich, wenn die Bildübertragungen a) nicht automatisiert und b) nur zu den internen, eingetragenen Arbeitsplatzrechnern der Benutzer stattfinden. Als Ansatz wird daher ein zusätzliches Standard-PACS als Zwischenspeicher in einer externen, weniger gesicherten Netzwerkzone eingeführt. Dieses externe PACS ist über einen GridDICOM-Router an das Grid angeschlossen und erlaubt explizit automatische Bildübertragungen zu und von den einzelnen Gridrechnern. Als Quellbilder enthält es aber nur diejenigen Bilder, die manuell von einem internen Benutzer aus dem Original-PACS zur Bearbeitung ausgewählt und entsprechend der „SecureDICOM“ Erweiterung pseudonymisiert wurden (siehe Abbildung 4.7). Im Rahmen der Untersuchung wird das

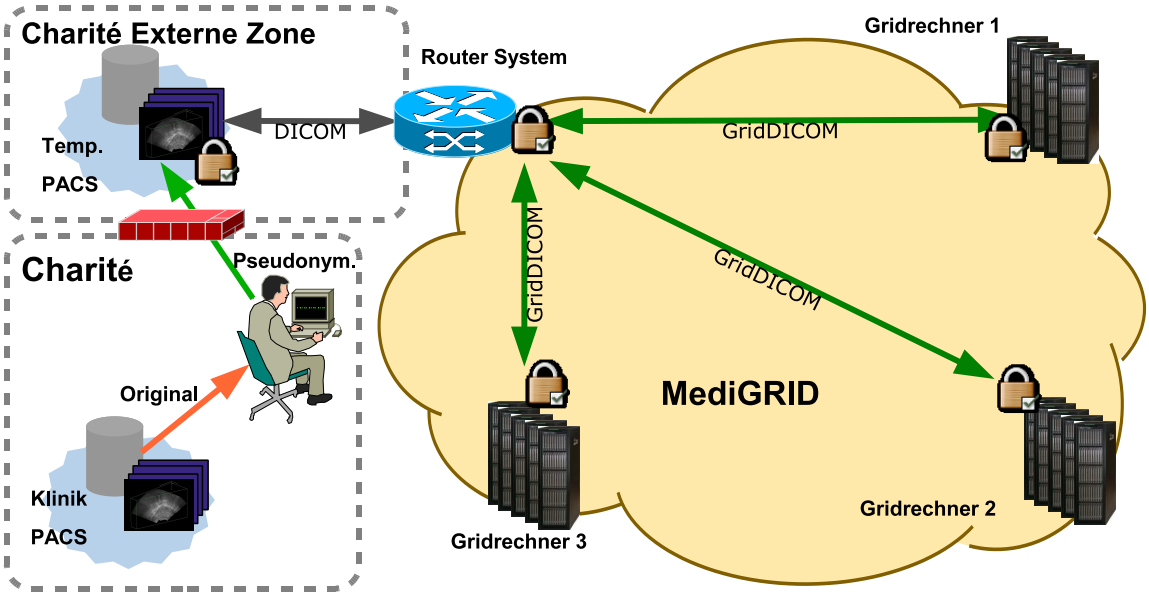


Abbildung 4.7: Schematische Darstellung des PACS-Zugangs. Die manuelle, nutzergesteuerte Bereitstellung von pseudonymisierten Daten bei voller Erhaltung der Bildhierarchien wird durch ein zusätzliches PACS in der externen Zone des Kliniknetzes realisiert.

Konzept konkret entwickelt und auf den Datenfluss zwischen den einzelnen Systemen hin analysiert.

4.3.2 Referenzimplementation und Tests

Die beiden beschriebenen zusätzlichen Sicherheitsmaßnahmen werden exemplarisch in einem realen Grid-Umfeld validiert. Dazu eignet sich besonders die beschriebene 3D-Ultraschall-Anwendung der Charité im MediGRID-Verbund, da sie Standard-Arbeitsabläufe der Bildverarbeitung enthält. Entsprechend dem Konzept werden die zusätzlichen Systeme in der Charité installiert und eingerichtet. Dies sind insbesondere das zusätzliche PACS in der externen Netzwerkzone der Charité und die DICOM-Router als Zugangspunkte für dieses PACS. Als Zugang zum MediGRID dient ein deutschlandweit betriebenes Zugangsportal, welches dem Benutzer von jedem internetfähigen Arbeitsplatz aus eine intuitive, webbasierte Benutzeroberfläche zur Verfügung stellt. Um eine möglichst praktikable Möglichkeit zu schaffen, Bilder aus dem internen Original-PACS bei gleichzeitiger Pseudonymisierung manuell in das externe PACS und umgekehrt zu kopieren, wird ein bestehendes Java-Programm (ebenfalls entwickelt von Andreas Thiel von OFFIS) verwandt und in diese Benutzeroberfläche integriert. Dem Benutzer steht dadurch ein und dieselbe webbasierte Benutzeroberfläche mit folgenden Funktionalitäten zur Verfügung, die in einem Testdurchlauf überprüft werden:

1. Selektion der zu verarbeitenden Ultraschall-Bildserien,
2. Übertragung der Bilder in das externe Grid-PACS bei gleichzeitiger Pseudonymisierung und Verschlüsselung nach der „SecureDICOM“ Erweiterung,
3. Starten der entsprechenden 3D-Ultraschall Bildverarbeitungsanwendung im Grid und
4. Auswahl und eventuelle Rückübertragung der Ergebnisse aus dem externen PACS bei gleichzeitiger Reidentifizierung.

4.4 Fehlertoleranz und Zuverlässigkeit

Eines der Hauptziele der Arbeit ist eine Lösung zur automatisierten Bildübertragung, die selbständig und fehlertolerant Bildserien zwischen den Systemen in einem Grid übertragen kann. Eine wesentliche Voraussetzung dabei ist die entwickelte durchgängige Kommunikation zwischen DICOM Systemen im Grid. Im Unterschied zu den bisher verfügbaren Lösungen reduziert die durchgängige Kommunikation nicht nur die Anzahl der möglichen Fehlerquellen, sondern bietet auch mehr Möglichkeiten, fortgeschrittene Fehlerstrategien umzusetzen.

4.4.1 Ansatz

Methodisch sollte ein modell-basierter Ansatz verfolgt werden, bei dem komplexe dynamische Prozesse zunächst mathematisch modelliert werden. Das Modell bildet eine formale Beschreibung der einzelnen Prozessschritte, ihrer Zusammenhänge und möglichen Zustände. Danach können die aus dem Modell gewonnenen Informationen genutzt werden um die Arbeitsabläufe, beispielsweise die Bildübertragung, geregelt und automatisiert (von Programmen) ausführen zu lassen (Kopplung des Modells an das System).

Modellierung

Die Modellierung der DICOM-Kommunikationsmuster wird mithilfe von „High-Level Petri-Netzen (HLPN)“ vorgenommen. Petri-Netze sind mathematische Repräsentationen von diskreten, verteilten Systemen und sind ideal beschaffen, um lose gekoppelte Grid-Systeme zu modellieren und darzustellen [47]. Sie bestehen aus einer Menge von Plätzen P, dargestellt durch Kreise „$\bigcirc$“, Transitionen T, dargestellt durch Rechtecke „$\square$“ und Flussbeziehungen $F \subseteq (P \times T) \cup (T \times P)$, repräsentiert durch gerichtete Pfeile von Plätzen zu Transitionen „$\bigcirc \rightarrow \square$“

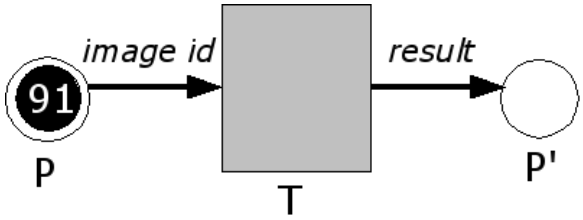


Abbildung 4.8: Einfaches Petri-Netz bestehend aus einem Eingabeplatz P mit 91 Token, einer Transition T und einem Ausgabeplatz P'.

oder von Transitionen zu Plätzen „$\square \rightarrow \bigcirc$“. Ein Netz N ist ein geordneter, zweiteiliger, gerichteter Graph der durch das Triple definiert ist $N = (P, T, F)$ mit $P \cup T \neq \emptyset$ und $P \cap T = \emptyset$. Die *Eingabeplätze* einer Transition $t \in T$ sind definiert als ${}^\bullet t = \{p \in P | (p, t) \in F\}$ und die *Ausgabeplätze* als $t^\bullet = \{p \in P | (t, p) \in F\}$. Zusätzlich können Plätze versehen werden mit einer *Kapazitätsbeschränkung* $c : P \rightarrow \mathbb{N} \cup \{\infty\}$ mit dem Standardwert ∞, der die maximale Anzahl von Token auf einem Platz festlegt. Abbildung 4.8 zeigt ein einfaches High-Level Petri-Netz (HLPN) mit einem Eingabeplatz mit 91 Token, einer Transition und einem Ausgabeplatz.

Im Unterschied zu regulären Petri-Netzen, sind die Token von High-Level Petri-Netzen unterscheidbar und können benutzt werden um Werte auf hoher Ebene zu modellieren, wie beispielsweise reale Ein- und Ausgabewerte, Referenzen zu Dateien oder logische Werte die Seiten-Effekte repräsentieren. Die Verteilung der Token auf den Plätzen nennt man „Marking“ und sie repräsentiert den Zustand des verteilten Systems. Das *Initiale Marking* $m_0 : P \rightarrow \mathbb{N}_0$ genügt $\forall p \in P : m_0(p) \leq c(p) \vee c(p) = \infty$. Eine Transition $t \in T$ ist *aktiv* bei einem „Marking“ m wenn $\forall p \in {}^\bullet t \Rightarrow m(p) \geq 1$ und $\forall p \in t^\bullet \Rightarrow m(p) + 1 \leq c(p)$. Eine aktive Transition t kann *eintreten* (oder *feuern*) was zu dem nachfolgenden Marking m' führt, definiert durch: $\forall p \notin {}^\bullet t \cup t^\bullet : m'(p) = m(p)$; $\forall p \in {}^\bullet t : m'(p) = m(p) - 1$; und $\forall p \in t^\bullet : m'(p) = m(p) + 1$. Dies bedeutet, dass ein Eingabe-Token verarbeitet wurde von jedem Eingabeplatz (der Eingabedaten hält) und ein neues Ausgabe-Token erzeugt wurde auf jedem Ausgabeplatz (das Ausgabedaten hält). Das Eintreten einer Transition, die eine externe Aktivität anstösst, verändert den Zustand des Systems ($m \xrightarrow{t} m'$). Zur Vereinfachung drückt die Bezeichnung „Marking“ in der Definition oben nur die Anzahl der Token auf jedem Platz aus, obwohl jedes Token selbst spezifische und individuelle Daten modelliert. Die komplette Definition von High-Level Petri-Netzen, die in ISO/IEC 15909-1 [48] standardisiert ist, definiert ein „Marking“ formaler als eine Funktion, die eine Anzahl von Token vom richtigen Typ mit jedem Platz assoziiert ($m : P \rightarrow \bigcup_{p \in P} \mu Typ(p)$ so dass $\forall p \in P : m(p) \in \mu Typ(p)$).

Um High-Level Petri-Netze nicht nur zur Modellierung und Simulation, sondern auch zur Ausführung von Prozessabläufen („Workflows“) zu nutzen, werden die Notation von Kantenbeschriftungen und Bedingungen erweitert, um reale Ein- und Ausgabedaten in der Ablauflogik zu betrachten. Obwohl normalerweise Kantenanschriften als Wichtungsfunktionen genutzt

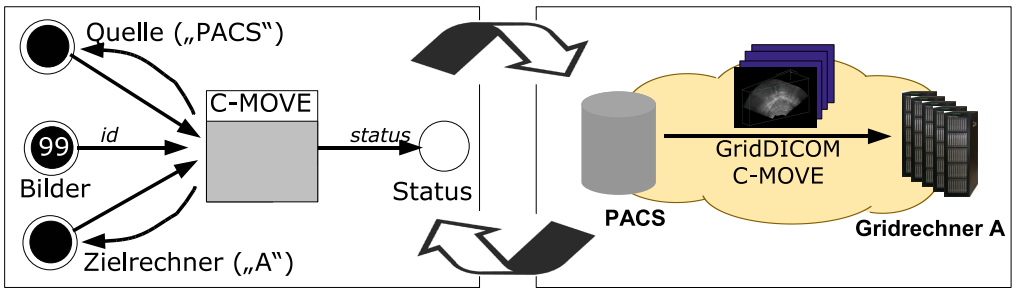


Abbildung 4.9: Ein einfaches Transfer-Petri-Netz. Links: Das transferbasierte Modell stellt die Übertragung von 99 Bildern zwischen zwei beteiligten Gridrechnern dar. Die Eingabe-Token repräsentieren das Quell-PACS, den Zielrechner „A“ sowie die Bild-IDs, die zu übertragen sind. Rechts: Das abstrakte Modell wird an das reale Grid gekoppelt und auf das echte PACS und den Gridrechner „A“ abgebildet. Bei der Transition wird die DICOM-Aktivität „C-MOVE“ ausgeführt.

werden, wird in diesem Fall eine konstante Gewichtsfunktion $w = 1$ angenommen und die Kantenanschriften benutzt, um Eingabe-Token an Variablen zu binden und Ausgabe-Token mit dem XPath 1.0 Standards auszuwerten. Zusätzlich können Transitionen mit Bedingungen verknüpft werden. Dabei werden Transitionen nur ausgeführt („feuern“), wenn alle Bedingungen erfüllt sind. Im Gegensatz zu den sogenannten „mehrfarbigen Petri-Netzen“, bei denen die Token einen begrenzten Satz von Datentypen repräsentieren, können durch diesen Ansatz willkürliche Daten behandelt und dargestellt werden.

Abbildung 4.9, links, zeigt ein Beispiel für ein einfaches Transfer-Petri-Netz. Es stellt die Übertragung von 99 Bildern zwischen zwei beteiligten Gridknoten dar. Die Eingabe-Token repräsentieren den Quell- und den Zielrechner sowie die Bild-IDs, die zu übertragen sind. Abbildung 4.9, rechts, zeigt die Zuordnung von dem abstrakten Modell zu dem realen Grid-System, was in dem nachfolgenden Abschnitt „Grid-Kopplung“ erklärt ist.

Bei der Modellierung werden zwei mögliche Ansätze untersucht:

1. Netzwerkbasierte Modelle: Hier repräsentiert ein Petri-Netz das gesamte Grid-Netzwerk (siehe Abbildung 4.10 links), oder
2. Transferbasierte Modelle: Hier stellt ein Petri-Netz lediglich die zwei jeweils beteiligten Systeme aus dem Gesamtgrid dar (siehe Abbildung 4.10 rechts).

Netzwerkbasierte Modelle haben den Vorteil, dass sie zu jeder Zeit den Zustand des Gesamtgrids darstellen. Da die Graphen für das gesamte Gridnetzwerk schnell sehr groß werden können, sind vor allem bei komplexen Übertragungsabläufen transferbasierte Modelle wesentlich effizienter. Für die Untersuchung der beiden Ansätze werden jeweils ein Modell für eine einfache, bi-direktionale Bildübertragung zwischen vier Gridrechnern entwickelt und verglichen.

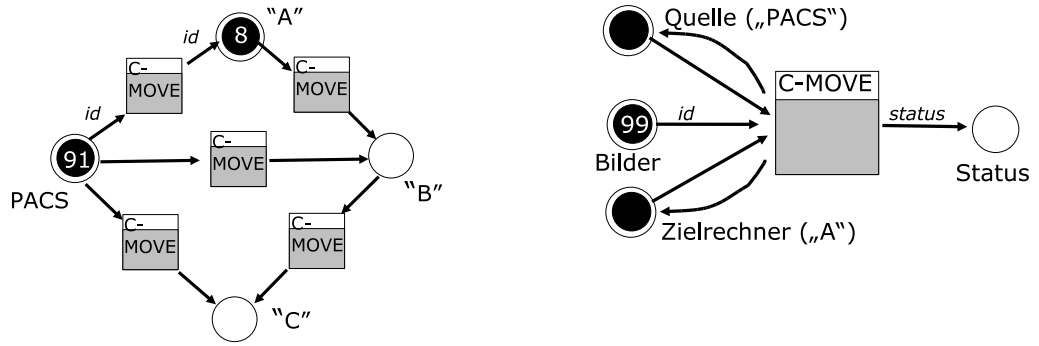


Abbildung 4.10: Zwei mögliche Ansätze der Modellierung. Links: Netzwerkbasierte Modelle, hier repräsentiert ein Modell das gesamte Grid-Netzwerk. Rechts: Transferbasierte Modelle: Hier stellt ein Petri-Netz lediglich die zwei jeweils beteiligten Systeme aus dem Gesamtgrid dar.

Grid-Kopplung

In der zweiten Phase werden die entworfenen Modelle genutzt, um ein System zu entwickeln, welches selbständig die beschriebenen Übertragungsprozesse ausführen und kontrollieren kann. Damit ein System die beschriebenen Prozesse ausführen kann, müssen die Modelle in einer Sprache beschrieben werden, die das System verstehen kann. Gleichzeitig muss sie die Modellelemente auf das reale System abbilden. Als Grundlage dient dazu die „Grid Workflow Description Language (GWorkflowDL)", die vom Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik (FIRST) zusammen mit der Universität Münster entwickelt wurde [49]. GWorkflowDL ist eine XML-basierte Sprache, die die beschriebenen graphenbasierten HLPN repräsentiert. Zusätzlich erlaubt sie es, die Transitionen der Modelle im Netz auf „Aktivitäten" im Grid abzubilden. Aktivitäten sind hauptsächlich Grid- oder Webservice-Aufrufe, die beispielsweise GridDICOM-Befehle ausführen. Dafür müssen die für die Modelle jeweils nötigen Dienste identifiziert und entwickelt werden. Dies werden die gängigsten DICOM-Befehle wie C-FIND oder C-MOVE sein, aber auch zusätzliche Dienste zur Bildverifikation. Die Datentoken auf den Plätzen im Petri-Netz entsprechen den Eingabeparametern für die Aktivitäten, wie zum Beispiel das Quell- und Zielsystem oder die DICOM-Bild-UIDs, die übertragen werden sollen.

Abbildung 4.11 zeigt ein Beispiel für eine GWorkflowDL-Prozessbeschreibung, die den einfachen Transfer des Petri-Netzes aus Abbildung 4.9 beschreibt (allerdings aus Platzgründen mit nur zwei statt 99 Bildern). Die Beschreibung bildet die Transition „moveImage" auf ein DICOM-C-MOVE Aktivität ab. Wenn er ausgeführt wird, wird der C-MOVE-Befehl an das Quellsystem gesandt, welches seinerseits dann die Bilder an das Empfangssystem überträgt und den Gesamtstatus des Transfers auf den Ausgabeplatz „result" zurückgibt.

```
<workflow xmlns="http://www.gridworkflow.org/gworkflowdl"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xmlns:xsd="http://www.w3.org/2001/XMLSchema"
          xsi:schemaLocation="http://www.gridworkflow.org/gworkflowdl
                              http://www.gridworkflow.org/kwfgrid/src/xsd/gworkflowdl_1_0.xsd"
          ID="No_ID">

<description>Simple sample RDT workflow</description>

<place ID="ImageUID">
  <token>
    <data><value xsi:type="xsd:string">1.3.6.9590.002406.331785581953714</value></data>
  </token>
  <token>
    <data><value xsi:type="xsd:string">1.3.6.9590.002406.331785581953715</value></data>
  </token>
</place>

<place ID="Source">
  <token>
    <data><value xsi:type="xsd:string">archive</value></data>
  </token>
</place>

<place ID="Destination">
  <token>
    <data><value xsi:type="xsd:string">nodeA.medigrid.de</value></data>
  </token>
</place>

<place ID="result"/>

<transition ID="moveImage">
  <description>issues a C-MOVE command</description>
  <property name="priority">1</property>
  <inputPlace placeID="ImageUID" edgeExpression="id"/>
  <inputPlace placeID="Source" edgeExpression="source"/>
  <inputPlace placeID="Destination" edgeExpression="destination"/>
  <outputPlace placeID="result" edgeExpression="result"/>
  <operation>
    <ws:WSClassOperation xmlns:ws="http://www.gridworkflow.org/gworkflowdl/wsclassoperation">
      <ws:WSOperation wsdl="http://localhost:8080/RDTjbossws/RDTService?wsdl"
                      operationName="moveImage" selected="true" />
    </ws:WSClassOperation>
  </operation>
</transition>

</workflow>
```

Abbildung 4.11: Beispiel für eine GWorkflowDL-Prozessbeschreibung: Der Prozessablauf bildet die Transition „moveImage“ auf ein DICOM-C-MOVE Aktivität ab. Wenn er ausgeführt wird, wird der C-MOVE-Befehl an das Quellsystem gesandt, welches seinerseits dann die Bilder an das Empfangssystem überträgt und den Gesamtstatus des Transfers auf den Ausgabeplatz „result“ zurückgibt.

Einzelbildbasierte und Serienbasierte Bildübertragungen

Wie in den Grundlagen schon beschrieben, sind komplette Bildserien die am häufigsten übertragenen Einheiten. In DICOM kann eine komplette Serie mit nur einem Befehl übertragen werden („Series-Level“). Eine solche Übertragung resultiert in deutlich weniger DICOM-Nachrichten als eine Übertragung auf Einzelbildbasis, bei der jedes Bild einzeln angefordert wird („Image-Level“). Auf der anderen Seite gibt DICOM keine Identifikation von fehlgeschlagenen Bildern zurück, nur einen Gesamtstatus. Eine explizite Bildverifikation ist nötig, um die fehlenden Bilder zu identifizieren und neu zu übertragen. Im Unterschied dazu ergibt eine Übertragung auf Einzelbildbasis zwar mehr Nachrichten, ist aber einfacher zu verifizieren, da sofort der Status jeder einzelnen Übertragung gemeldet wird.

Für die Untersuchungen werden daher vier verschiedene Modelle für die Kommunikation entwickelt und sowohl untereinander als auch mit der existierenden DGIS-Lösung verglichen:

1. Einfacher DICOM-Transfer einer Bildserie auf Einzelbildbasis ohne besondere Fehlerkorrektur.
2. Einfacher DICOM-Transfer einer Bildserie auf Serienbasis ohne besondere Fehlerkorrektur.
3. Fehlertoleranter DICOM-Transfer einer Bildserie auf Einzelbildbasis.
4. Fehlertoleranter DICOM-Transfer einer Bildserie auf Serienbasis.

4.4.2 Referenzimplementation und Tests

Mit einer Referenzimplementation wird das entwickelte System implementiert und in Tests validiert. Um es in die bestehende Webservice-orientierte Architektur der Grid-Middleware des Globus-Toolkits einzupassen (siehe Kapitel 1), wird es ebenfalls als ein Webservice entwickelt.

Im Wesentlichen werden dabei die folgenden vier Komponenten implementiert:

1. *Die Modell-Vorlagen:* Die bei der Modellierung zu entwickelnden Transfer-Modelle (siehe 4.4.1) sind für die Kopplung in GWorkflowDL umzusetzen, um sie für das System als Prozessvorlage lesbar und ausführbar zu machen.
2. *Der Hauptdienst:* Dies ist der Haupt-Webservice, der für eine Bildübertragung aufgerufen wird. Ihm werden die Parameter übergeben, welche Bilder zu und von welchen Systemen übertragen werden soll. Aus diesen Parametern und der Modell-Vorlage werden

dann konkrete Prozessbeschreibung erzeugt und an die „Workflow-Engine“ zur Ausführung übergeben.

3. *Die „Workflow-Engine“:* Die GWorkflowDL-Prozessbeschreibungen brauchen ein System, welches diese ausführt und kontrolliert. Als eine solche „Workflow-Engine“ wird der von FIRST entwickelte „Grid Workflow Execution Service“ (GWES) [50, 51, 52] verwendet. Neben der Steuerung von Prozessabläufen bietet der GWES zusätzlich grundlegende Möglichkeiten zur Zuverlässigkeit: „Checkpoints“ können im Ablauf gesetzt werden um erfolgreich durchlaufene Teile des Prozesses zu markieren. Weiterhin kann die gesamte Prozessbeschreibung in ihrem jeweiligen Zustand in einer Datenbank persistent gespeichert werden. Dies ermöglicht es, in Fall eines Systemfehlers des Haupt-Dienstes selbst, die Prozesse wieder zu laden und vom letzten erfolgreich durchlaufenen Checkpoint an wieder zu starten. Dies kann automatisch erfolgen, oder manuell durch die webbasierte GWES-Benutzeroberfläche. Diese bietet eine Reihe von grafischen Administrationswerkzeugen und (Echtzeit-)Visualisierungskomponenten, die sehr nützlich zur Überwachung und für Statusabfragen der Bildübertragungen sind. GWES selbst ist als standardisierter Webservice in Java implementiert und frei verfügbar (im akademischen Bereich).

4. *Die Satelliten:* Jedes an der Bildübertragung beteiligte System (PACS oder Gridrechner) soll durch einen *Satelliten-Server* an das Grid angeschlossen werden. Dieser Satellit fungiert nicht nur als GridDICOM-Router, sondern speichert auch DICOM-Bilder, die an ihn zur Berechnung gesandt werden. Zusätzlich soll er die neu entwickelten Dienste anbieten, die vom GWES bei den Transitionen aufgerufen werden können.

Das Gesamtsystem wird sowohl in einem isolierten Testgrid als auch in dem produktiven MediGRID-Verbund evaluiert. In dem Testgrid werden die Methoden der direkten Übertragung ohne Modellunterstützung verglichen mit den vier entwickelten Modellen und der bisherigen DGIS-Lösung. Dabei werden die Standard-Bildserien jeweils mit und ohne simulierten Systemstörungen übertragen und die Gesamtübertragungszeiten verglichen.

Nach den Vergleichstests werden die Modelle mit den besten Ergebnissen (jeweils eines mit und eines ohne Fehlerkorrektur) mit dem Gesamtsystem in die Produktivumgebung von MediGRID installiert. Durch einen Langzeittest mit simulierter, typischer Gridnutzung wird die Verbesserung der Fehlerraten durch einen Vergleich des einfachen und des fehlertoleranten Modells ermittelt.

Kapitel 5

Ergebnisse

5.1 Durchgängige DICOM-Kommunikation

In diesem Abschnitt werden zunächst die Ergebnisse der GSI-Analyse vorgestellt und der Verbindungsaufbau in Bezug auf DICOM erläutert. Auf dieser Basis wird ein zusätzliches Sicherheitsprofil nach Art und Vorgaben des DICOM-Standards entwickelt, welches als Vorlage für künftige Implementationen sowie zur Einbringung in den Standard selbst dienen kann.

5.1.1 Analyse des GSI

Das GSI spezifiziert konkrete Verfahren in den vier Bereichen Authentifikation, Autorisierung sowie Verschlüsselung und Integrität nach dem allgemein anerkannten Internet-Sicherheitsstandard „Generic Security Standard (GSS)“ [53]. Zusätzlich definiert es Methoden für das Grid-spezifische Problem des „Single-Sign-On“.

1. *Authentifikation:* Ähnlich wie im deutschen Signaturgesetz, basiert die Identifikation beim GSI auf dem Einsatz von X.509-Zertifikaten, die einem Kommunikationspartner einen eindeutigen Namen zuweist. Die Vertrauenswürdigkeit der Zertifikate wird über eine hierarchische Kette vertrauter Organisationen hergestellt, die für diese Zertifikate bürgen. Die konkrete Authentifikation bei einem Verbindungsaufbau wird dabei über das auch in herkömmlichen Netzen genutzte „SSL-Authentication-Protocol“ geregelt [29]. Bei diesem Protokoll werden die Parameter für die nachfolgende verschlüsselte Übertragung ausgehandelt und ausgetauscht. Im Gegensatz zu vielen herkömmlichen Anwendungen, bei denen sich dabei oft nur einer der Partner identifizieren muss, ist beim GSI die gegenseitige Identifikation beider Partner Pflicht.

```
"/C=DE/O=GridGermany/OU=Charite - Universitaetsmedizin Berlin/OU=Medizinische Informatik/CN=Michal Vossberg"
globus
...
```

Abbildung 5.1: Ausschnitt aus der GridMap-Datei, die Zertifikats-Identitäten auf lokale Benutzernamen, in diesem Fall „globus“, abbildet und so die Zugriffsrechte der jeweils lokalen Benutzersteuerung übernimmt.

2. *Autorisierung:* Die Zugriffsrechte werden im GSI nur indirekt geregelt. Der durch das Zertifikat identifizierte Kommunikationspartner wird einem Benutzer des lokalen Systems zugeordnet. Dieser lokale Benutzer besitzt dann, wie ein regulärer Benutzer des Systems, die ihm von Betriebssystem zugewiesenen Zugriffsrechte. Diese Zuordnung bestimmt die sogenannte „GridMap“-Datei auf dem lokalen Rechner, in der die jeweiligen Zertifikats-Identitäten mit lokalen Benutzernamen verknüpft sind. Ein Beispiel für einen Eintrag aus der GridMap-Datei zeigt die Abbildung 5.1. Der Vorteil dieser Methode ist, dass die jeweils auf der Ressource lokal verfügbaren Methoden zur Autorisierung genutzt werden können. Der Nachteil ist, dass durch dieses Verfahren allein keine feingranularen, rollenbasierten Zugriffsrechte, abgestimmt auf die jeweilige Aufgabe, möglich sind. Außerdem muss die Datei ständig von dem Administrator des jeweiligen Systems gepflegt und aktualisiert werden. Um diese Nachteile auszugleichen wird das Verfahren in den meisten Grids mit einer zusätzlichen Software zur zentralen Verwaltung der Benutzer der virtuellen Organisation kombiniert, beispielsweise „Virtual Organization Management Registration Service (VOMRS)“ [54]. Mit einer solchen Software können Nutzergruppen einfach verwaltet sowie die GridMap-Dateien im Grid zur Verfügung gestellt werden.

3. *Verschlüsselung und Integrität:* Für die reine Verschlüsselung und Integrität der Datenpakete nutzt das GSI das allgemein anerkannte Verschlüsselungsprotokoll TLS. Obwohl mit dem TLS-Protokoll verschiedene Verschlüsselungsalgorithmen zum Einsatz kommen können, wie beispielsweise Triple-DES oder AES, ist das GSI derzeit nur für den Triple-DES-Algorithmus definiert.

4. *„Single-Sign-On“:* Das „Single-Sign-On“, also die einmalige Identifikation gegenüber vielen, verteilten Systemen, erfolgt im GSI durch die sogenannte „Delegation“ (Weiterleitung). Dies ist eine Erweiterung des X.509-Zertifikatsstandards und erlaubt es einem Benutzer „Unterzertifikate“ auszustellen, die anstelle seines Originalzertifikats an andere Systeme weitergeleitet werden können. Diese stellvertretenden Zertifikate, auch „Proxy“-Zertifikate genannt („Proxy = Stellvertreter“), unterscheiden sich in zwei Punkten vom Originalzertifikat: zum einen enthalten sie einen neuen, temporären Schlüssel, der nicht Passwortgeschützt ist und ohne weitere Interaktion genutzt werden kann. Zum anderen sind sie nur eine sehr kurze Zeit gültig (meist eine Stunde), so dass eine Kompromittierung des Schlüssels nur begrenzt Schaden anrichten würde.

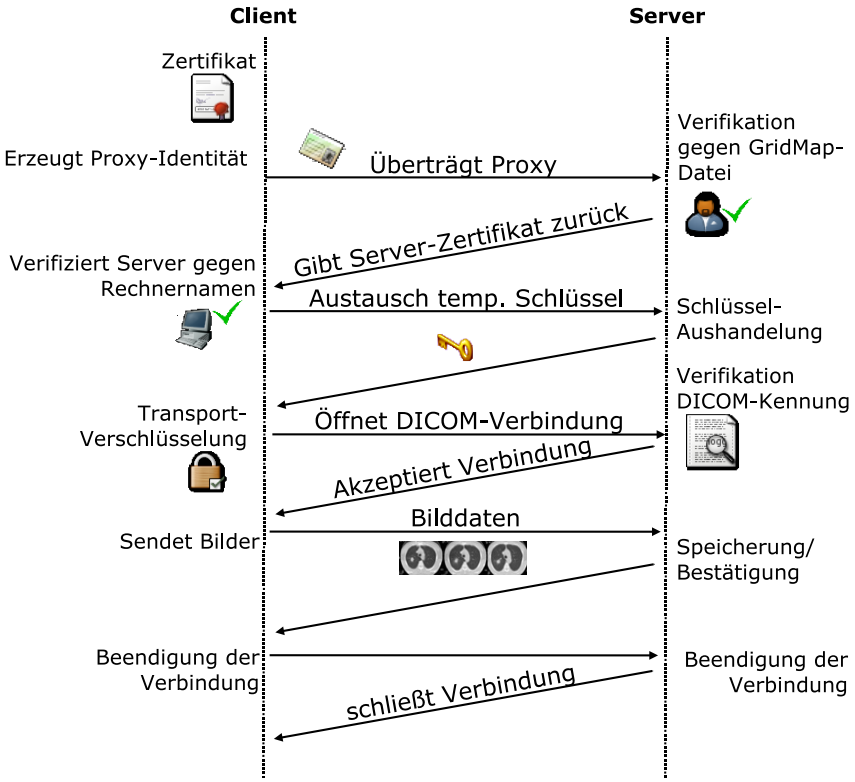


Abbildung 5.2: Ablauf eines Verbindungsaufbaus und einer DICOM-Kommunikation nach dem GSI-Standard am Beispiel des Bildersendens. Nach erfolgreicher GSI-Authentifizierung und Autorisierung findet die reguläre DICOM-Kommunikation über die gesicherte Verbindung statt.

5.1.2 Definition des DICOM-Verbindungsaufbaus

Im Folgenden werden die nötigen Schritte aufgeführt um den DICOM-Verbindungsaufbau auf TCP/IP-Basis um die Verfahren des GSI zu erweitern (siehe auch Abbildung 5.2). Da die Kommunikationspartner sowohl natürliche Personen als auch Rechnersysteme sein können, abstrahiert man bei derartigen Beschreibungen im Allgemeinen zu einem „Client“, der eine Verbindung anfragt, und einem „Server“, der diese Verbindungen annimmt.

1. Zunächst erzeugt der Client mithilfe seines ständigen Zertifikats ein temporär gültiges Proxy-Zertifikat für diese Verbindung.

2. Dieses Proxy-Zertifikat sendet der Client mit einer Verbindungsanfrage an den Server (Delegation). Der Server überprüft zunächst die Gültigkeit des Zertifikats und der eingetragenen Identität („Client-Authentifizierung“). Danach ermittelt der Server aus der systemweiten „GridMap“-Datei den Benutzernamen und die Zugriffsrechte auf dem lokalen System („Client-Autorisierung“).

3. Nach erfolgreicher Verifikation sendet der Server sein eigenes Zertifikat zurück an den Client. Der Client überprüft nun seinerseits die Gültigkeit des Zertifikats und den einge-

Unterstützte GSI-Funktion	Minimaler Mechanismus
Teilnehmer Authentifikation	RSA Zertifikate nach X.509 Standard
Teilnehmer Autorisierung	„GridMap“-Datei
Weiterleitung (Delegation)	X.509 Proxy Zertifikatserweiterung, wie in [55] definiert
Verschlüsselung	Triple DES EDE, wie bei TLS 1.0
Austausch der Session-Schlüssel	RSA, wie bei TLS
Integrität	SHA, wie bei TLS

Tabelle 5.1: Mechanismen, die beim GridDICOM-Sicherheitsprofil für die einzelnen GSI-Funktionen unterstützt werden müssen.

tragenen Rechnernamen („Server-Authentifizierung“). Da dieses Zertifikat nicht weitergeleitet wird, reicht hier das Original-Zertifikat anstelle eines Proxy-Zertifikats.

4. Nach erfolgreicher gegenseitiger Legitimation werden ein temporärer Schlüssel und ein Algorithmus für die nachfolgende Verschlüsselung der Daten vereinbart. Ab diesem Punkt werden alle nachfolgenden Datenpakete mit diesem temporären Schlüssel verschlüsselt.

5. Der Client sendet seine DICOM-Systemkennung, wie im Standard definiert. Nach der vorhergehenden, erfolgreichen GSI-Verifikation kann dieser Kennung nun vertraut werden, alleine eignet sie sich jedoch nicht, da sie sehr einfach gefälscht werden kann.

6. Akzeptiert der Server die Kennung, erfolgt die eigentliche DICOM-Kommunikation.

7. Mit dem Ende der Kommunikation endet auch die Verschlüsselung und die Verbindung wird geschlossen.

5.1.3 Beschreibung des GSI-Sicherheitsprofils

Durch den modularisierten Aufbau des DICOM-Standards, erfolgt eine Erweiterung der Sicherheitsmechanismen nicht im Kernteil des Standards, sondern im Modul 15 „Sicherheitsprofile“. Hier ist auch bereits ein Sicherheitsprofil für die verschlüsselte Übertragung über TLS, sowie das weniger bekannte ISCL beschrieben. Analog zu diesen Profilen wird nun ein neues Sicherheitsprofil „GridDICOM“ entworfen, welches die beschriebenen Funktionen des GSI nach den Regeln des DICOM-Standards beschreibt. Die Tabelle 5.1 zeigt eine Zusammenfassung der geforderten Methoden zur Unterstützung des GSI. Das vollständige Profil ist DICOM-konform in Anhang A aufgeführt und kann als Vorschlag für den Standard dienen.

Kürzel	Stadt	Distanzzone	Institut
PACS	Berlin	Campus	Charité
B	Berlin	City	Konrad-Zuse-Institut
D	Dresden	Regional	ZIH Dresden
DO	Dortmund	Überregional	Uni Dortmund
KA	Karlsruhe	Land	Uni Karlsruhe

Tabelle 5.2: Verzeichnis der an den MediGRID-Tests beteiligten Gridrechner und ihrer Institute in Deutschland. Die Rechner wurden in Hinblick auf geographisch unterschiedliche Grid-Regionen ausgewählt.

5.1.4 Ergebnisse der Referenzimplementation

Für die Referenzimplementation ist die DICOM-Software „dcm4che2“ [56] angepasst worden. Diese Software eignet sich besonders, da sie erstens eine frei verfügbare, hochperformante Implementierung des DICOM 3.0-Standards ist und zweitens in der Programmiersprache Java entwickelt wurde, was es ermöglicht, die Software auf den unterschiedlichen im Grid genutzten Recherarchitekturen und Betriebssystemen laufen zu lassen. Die Grundfunktionen des GSI, wie Zertifikatsverwaltung oder Verschlüsselungsalgorithmen, stehen mit einer ebenfalls frei verfügbaren Java-Software, dem „Java Commodity Toolkit“ [57] der Globus-Gruppe, zur Verfügung und bedürfen damit keiner Neuentwicklung.

Die meiste Netzwerkfunktionalität bei *dcm4che2* ist enthalten in den Klassen *Association* und *NetworkConnection*. Die ursprünglichen Versionen implementieren zwei mögliche Verbindungsalternativen, einmal auf Basis des unverschlüsselten DICOM-Protokolls und einmal auf Basis von TLS. Die neue Implementation erweitert diese und stellt einen sicheren GSI-Kontext her, bevor die eigentliche DICOM-Kommunikation stattfindet. Wie mit jeder Anwendung, die auf GSI basiert, setzt dies eine verfügbare Einrichtung der Zertifikate, GridMap-Datei und übergeordneten Zertifikate (CA) voraus. Der GSI-Kontext regelt die gegenseitige Authentifizierung, Autorisierung sowie die Verschlüsselung und Nachrichtenintegrität basierend auf dem jeweils gewünschten Sicherheitslevel. Weiterhin erlaubt es den Zugriff auf die jeweils ausgetauschten Zertifikate und Identitäten. Die Referenzimplementation stellt zusätzlich neue Methoden und Anwendungen bereit, um die erweiterte Autorisierung durchzuführen, wie beispielsweise die Zugriffsrechte des Benutzers aus der GridMap-Datei zu ermitteln oder die Identität an andere Rechner weiterzuleiten.

Getestet worden ist diese Implementation durch manuelle DICOM-Übertragungen zwischen ausgewählten Rechnern aus dem MediGRID-Verbund. Die Auswahl beschränkt sich dabei auf ein Rechnersystem aus jeder der beschriebenen Regionen: von sehr kurzen Entfernungen in der Stadt („City“) bis zu längeren Distanzen im ganzen Land (“Country“, siehe Abbildung 4.1). Tabelle 5.2 listet die Kürzel der beteiligten Gridrechner und ihrer Institute auf, die im Folgenden

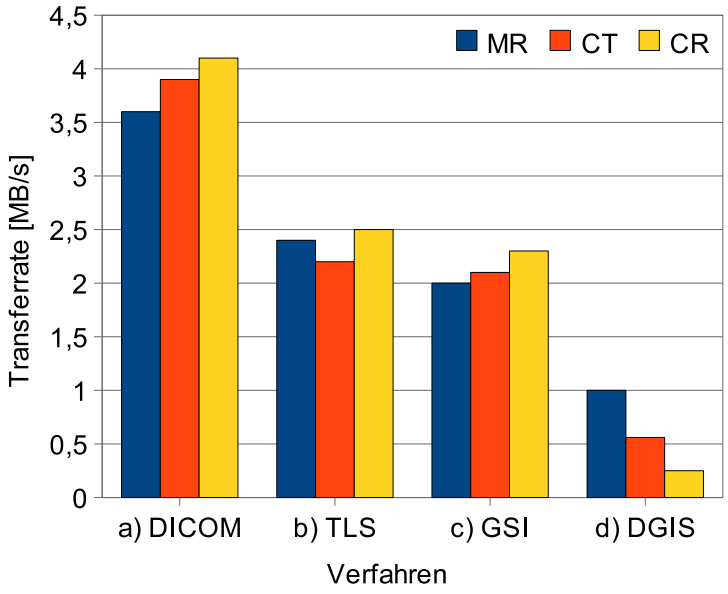


Abbildung 5.3: Durchschnittliche Transferraten der vier unterschiedlichen Verfahren zur DICOM-Kommunikation bei dem Storage-Testszenario in MB/s: a) herkömmlicher DICOM-Transfer, b) TLS-verschlüsselter DICOM-Transfer, c) GridDICOM-Transfer und d) DGIS-Transfer. Die Ergebnisse sind jeweils gemittelt über die vier Gridrechner aus Tabelle 5.3.

verwendet werden.

Für die manuelle Übertragung der Bilder wurden auf Basis der erweiterten DICOM-Software jeweils ein Programm zum Senden (*GridDcmSend*) und Empfangen (*GridDcmRcv*) von Bildern entwickelt und auf den MediGRID-Rechnern installiert. *GridDcmSend* sendet jedes Bild mit einem C-STORE Befehl an den empfangenden Rechner. Die Übertragung wurde mit drei öffentlich verfügbaren MRT-, CT- und CR-Testbildserien getestet. Die Bildserien bestehen aus einer unterschiedlichen Anzahl aus Einzelbildern von unterschiedlichen Größen: Die MRT-Study besitzt fünf Serien mit jeweils 100 Bildern (512x512, 16bit, insgesamt 250MB). Die CT-Study besteht aus 50 Serien mit jeweils zehn Bildern (512x512, 16bit, insgesamt 250MB) und die CR-Bilder setzen sich aus zehn Studies mit jeweils zehn Serien aus einem einzelnen Brust-CR (2140x1760, 16bit, insgesamt etwa 800MB). Die Übertragungsraten der GridDICOM-Lösung wurden verglichen mit einer herkömmlichen, unverschlüsselten DICOM-Übertragung, einer TLS-verschlüsselten Übertragung und mit der derzeit aktuellsten Grid-Lösung DGIS aus dem MEDICUS-Projekt.

Die Abbildung 5.3 zeigt die durchschnittlichen Transferraten einer Bildserie (MR, CT oder CR), gemittelt über alle Übertragungen zu den vier Test-Gridknoten („B“,„D“,„DO“ und „KA“) in Megabyte pro Sekunde (MB/s). Diese Transferraten sind damit unabhängig von der Distanz und entsprechen eher einer realen Gridnutzung als die Übertragungsergebnisse zu den ein-

Test	**MR**				**CT**				**CR**			
Berlin →	B	DD	DO	KA	B	DD	DO	KA	B	DD	DO	KA
a) DICOM	4.0	3.9	2.8	3.5	4.5	4.2	3.1	3.8	4.8	4.5	3.2	3.9
b) TLS	2.8	2.7	2.1	2.0	2.6	2.5	1.9	1.8	2.9	2.8	2.2	2.1
c) GridDICOM	2.4	2.3	1.7	1.6	2.5	2.4	1.8	1.7	2.7	2.6	2.0	1.9
d) DGIS	1.2	1.1	0.9	0.8	0.8	0.7	0.4	0.35	0.35	0.31	0.2	0.15

Tabelle 5.3: Durchschnittliche Transferraten der vier unterschiedlichen Verfahren zur DICOM-Kommunikation bei dem Storage-Testszenario in MB/s zu den einzelnen Rechnern der jeweiligen Grid-Region: a) herkömmlicher DICOM-Transfer, b) TLS-verschlüsselter DICOM-Transfer, c) GridDICOM-Transfer und d) DGIS-Transfer.

zelnen Gridrechnern. Der Vollständigkeit halber sind diese Einzelergebnisse aber zusätzlich in Tabelle 5.3 aufgeführt. Getestet wurden a) die herkömmliche DICOM-Übertragung, b) die DICOM-Übertragung auf Basis des TLS-Sicherheitsprofils für verschlüssselte Verbindungen, c) die Übertragung nach dem neuen GSI-Sicherheitsprofil und d) die Übertragung nach der bereits existierenden DGIS-Methode aus dem MEDICUS-Projekt. Die Testergebnisse sind wie folgt:

Test a) Herkömmmlicher DICOM-Transfer vom Arbeitsplatzrechner zum Gridknoten

Die Transferraten resultieren von einer unverschlüsselten Bildübertragung und sind damit entsprechend hoch. Sie liegen durchschnittlich bei 3.6-4.1 MB/s und entsprechen in etwa der Größenordnung, die man in einer heterogenen, weitverteilten System-Infrastruktur erwarten kann. Erwartungsgemäß zeigt sich bei den Einzelergebnissen aus Tabelle 5.3 ein deutlicher Geschwindigkeitsunterschied bei Übertragungen in die verschiedenen Regionen. Stadt-interne Übertragungen laufen in der Regel über das gleiche Netz und sind damit meistens schneller als Übertragungen in entfernte Gegenden, die zusätzlich zur größeren Distanz verschiedene Netze durchqueren müssen. Auffällig ist die niedrige Transferrate bei Bildserien mit vielen Bildern gegenüber einer hohen Transferrate bei wenigen Einzelbildern. Der Grund hierfür liegt in dem Aufbau des DICOM-Protokolls, das jedes einzelne Bild als ein Objekt in einer Nachricht überträgt. Werden weniger Einzelbilder transportiert, reduziert sich auch die Datenmenge der Nachrichten und die Transferrate steigt. Man beachte, dass diese herkömmliche DICOM-Kommunikation so in einer Grid-Infrastruktur aus Sicherheitsgründen natürlich nicht gewünscht ist. Diese Werte dienen rein als Vergleich, um die Leistungsunterschiede zu den nachfolgenden Methoden zu verdeutlichen.

Test b) Verschlüsselter DICOM-Transfer auf Basis des TLS-Sicherheitsprofils vom Arbeitsplatzrechner zum Gridknoten

Dieser Test entspricht einer herkömmlichen DICOM-Kommunikation aus Test a), allerdings unter zusätzlicher Verschlüsselung mit dem TLS-Protokoll. Der Verschlüsselungsalgorithmus

„Triple-DES“, der im Protokoll angewendet wurde, reduziert die Übertragungsrate erheblich, da er die Menge der übertragenen Daten mehr als verdreifacht. Bei großen Datenmengen, wie den CR-Bildern, macht sich dies besonders negativ bemerkbar, weshalb diese Bilder nicht so schnell übertragen werden, wie im Test a). Da die Verschlüsselung sensibel auf Rechnerlast und Datenmenge reagiert, kann die Transferrate im Vergleich zur unverschlüsselten Übertragung schwanken, beispielsweise bei der CT-Übertragung, liegt aber im Durchschnitt bei allen Bilder im Bereich 2.3-2.5 MB/s. Obwohl die Übertragung verschlüsselt ist und das TLS-Protokoll auch bei dem GSI-Standard Anwendung findet, genügt dieses Übertragungsverfahren allein nicht einer allgemeinen Gridnutzung, da es weder die Dynamik noch die Weiterleitungs-Funktion von Grids unterstützt.

Test c) GridDICOM-Transfer auf Basis des neuen GSI-Sicherheitsprofils vom Arbeitsplatzrechner zum Gridknoten

Die Transferraten bei dem neu entwickelten DICOM-Transfer nach GSI-Standard liegen mit etwa 2.0-2.3 MB/s nur leicht unter den Ergebnissen des herkömmlichen TLS-Protokolls aus Test b). Der Grund ist, dass der GSI-Standard für die reine Verschlüsselung, die einen Großteil des Zeitaufwands bei der Übertragung ausmacht, seinerseits das TLS-Protokoll verwendet. Der zusätzliche Zeitaufwand für die erweiterte Authentifizierung und Autorisierung, inklusive der möglichen Weiterleitung des GSI-Standards, fallen bei den Übertragungsraten nur unwesentlich ins Gewicht, da er nur einmalig beim initialen Verbindungsaufbau anfällt.

Test d) DICOM-Transfer vom Arbeitsplatzrechner über DGIS zum Gridknoten

Die Tests mit der momentan verfügbaren DGIS-Lösung des MEDICUS-Projekts ergeben eine sehr viel niedrigere Datenrate zwischen 0.3 und 1.0 MB/s. Dabei hängen sie stark von der übertragenen Bildserie ab. Da der DGIS alle Bilder einer Serie vor der Übertragung zu einem Archiv komprimiert, erzielt dieses Vorgehen bei Bildserien mit vielen kleineren Bildern, wie der MRT-Serie, deutlich bessere Übertragungsraten als mit wenigen großen Bildern, wie der CR-Serie, die sehr zeitaufwändig bei der Kompression sind. Insgesamt kostet gerade die Kompression und die Zwischenspeicherung deutlich Zeit und Speicherressourcen, sodass die Gesamtübertragungsrate des Verfahrens im Vergleich zur direkten Kommunikation deutlich geringer ist.

Insgesamt liegen die Übertragungsergebnisse der Referenzimplementation des GSI-Sicherheitsprofils nur unwesentlich unter der herkömmlichen Übertragung bei gleichem Verschlüsselungsalgorithmus und deutlich über der bisher verwendeten DGIS-Lösung. Die unverschlüsselte Kommunikation dient wie gesagt nur zu Orientierungszwecken und sollte nicht direkt verglichen werden.

Gleichzeitig zeigen sich in den Tests die weiteren Vorteile des umgesetzten GridDICOM-

Protokolls: Die Übertragung ist durchgängig und Bilder werden weder exportiert noch zwischengespeichert. Dies erhöht die Sicherheit und bedeutet weiterhin, dass ein Sender direkt über den Empfangsstatus informiert wird, was beispielsweise bei DGIS nicht der Fall ist, da das DICOM-Protokoll unterbrochen wird. Dieser Vorteil ist entscheidend für die Umsetzung einer möglichst fehlertoleranten Bildübertragung.

Teilergebnisse dieser Arbeit sind auch in [58] veröffentlicht. Die Referenzimplementierung wurde inklusive des Quellcodes auf der bekannten Webseite für frei verfügbare Software **griddicom.sourceforge.org** der Allgemeinheit öffentlich verfügbar gemacht.

5.2 Integration von vorhandenen DICOM-kompatiblen Systemen

Für die Untersuchungen wurden jeweils ein monolithisches und ein modulares DICOM-Router-Programm entworfen und in der Programmiersprache Java unter Verwendung der GridDICOM-Referenzimplementation entwickelt. Die Router können die gängigen DICOM-Query/Retrieve-Befehle zur Bildübertragung C-MOVE, C-GET und C-FIND, sowie den Storage-Befehl C-STORE zur Bildspeicherung verarbeiten.

Im Folgenden werden die Ergebnisse der Funktions- und Leistungstests der beiden Routerprogramme vorgestellt und verglichen. Die Funktionstests überprüfen die fehlerfreie Verarbeitung der DICOM-Nachrichten sowie den Einfluss, den die Systeme auf die Geschwindigkeit der Gesamtübertragung haben. In den Leistungstests werden beide Systeme einer hohen Last ausgesetzt, d.h. einer steigenden Anzahl gleichzeitiger Übertragungen, und die Übertragungszeiten gemessen.

Als DICOM-kompatibles PACS dient bei allen Tests das am Institut für Medizinische Informatik im Rahmen von MediGRID betriebene webbasierte PACS „dcm4chee“ [56]. Als Kontrollsystem, welches bei dem modularen System für das dynamische Ausführen der Module nötig ist, kommt der weit verbreitete, öffentlich verfügbare „J2EE-JBoss Application Server“ [59] zum Einsatz. Bei beiden Tests werden wiederum die schon im ersten Teil genutzten Testbildserien von MRT-, CT- und CR-Untersuchungen genutzt. Alle Übertragungen werden drei mal ausgeführt und die Ergebnisse jeweils über die drei Testläufe gemittelt.

5.2.1 Funktionstests

Die Funktionstests testen die drei in Kapitel 4.2.2 beschriebenen Transferszenarien, welche nachfolgend mit „S1-S3“ bezeichnet werden. Da immer nur eine Bildserie zur Zeit übertragen wird, ist die Belastung der Systeme dabei gering. In den Transferszenarien verarbeiten die Router transparent die DICOM-Nachrichten mit den eingebetteten Bildern. Das erwartete Verhalten bei einer korrekten Funktionsweise ist daher, dass sowohl die Bildserien in Anzahl und Größe in den Quell- und Zielsystemen übereinstimmen, also auch die Bilder selbst identisch mit den Ursprungsbildern sind. Gleichzeitig muss die sichere Übertragung entsprechend der GSI-Funktionalität sichergestellt sein.

Nach den Tests der drei Bildserien mit beiden Routern lässt sich feststellen, dass es in der Funktion beider Programme keine Unterschiede gibt. Unter der geringen Last bei den Funktionstests übertragen beide Programme alle DICOM-Nachrichten fehlerfrei und die durch die Router übertragenen Bilder entsprechen in allen Szenarien ihren Ursprungsbildern. Dabei werden jeweils korrekte Verbindungen nach dem GSI-Standard für die Gridübertragung mit den entsprechenden Zertifikaten aufgebaut. Hierbei gibt es zwei unterschiedliche Fälle:

1. Es handelt sich um eine Anfrage, die von einem DICOM-Gerät ohne Benutzerzuordnung initiiert wurde (Szenario *S1* und *S2*). In diesem Fall nutzt der Router das installierte Server-Zertifikat mit dem Namen des lokalen Rechners.

2. Es handelt sich um eine Anfrage, die durch eine vorherige, weitergeleitete Kommunikation initiiert wurde, beispielsweise eine C-STORE-Antwort aufgrund eines vorangegangenen C-MOVE-Befehls an das DICOM-Gerät aus dem Grid (wie bei dem dritten Szenario *S3*, bei dem der Transfer durch einen Drittauftrag ausgelöst wurde). In diesem Fall muss das gleiche Zertifikat zugewiesen werden, das die vorangegangene Verbindung initiierte. Zu diesem Zweck wird das eingehende Zertifikat zwischengespeichert und bei der ausgehenden Antwort wiederverwendet. Hierbei kann es sich sowohl um ein Nutzer-Zertifikat als auch ein Server-Zertifikat eines anderen Routers handeln. Dieses Vorgehen ist nur möglich, da der GSI-Standard im Gegensatz zu bisherigen Sicherheitsverfahren die „Delegation“, also die Weiterleitung von Zertifikaten, erlaubt.

Abbildung 5.4 zeigt die durchschnittlichen Transferraten für die drei Testszenarien *S1*-*S3* in Megabyte pro Sekunde für beide Routersysteme („Monolithisch“ und das modulare „J2EE“).

Bei den Gesamtübertragungen der Szenarien zeigt sich insgesamt, dass ein zwischengeschalteter Router die Transferrate gegenüber einer direkten Verbindung deutlich reduziert. Die Ergebnisse aus dem Szenario *S1* mit einer durchschnittlichen Transferrate im Nahbereich („City“) von 0.8-0.9 MB/s bei dem monolithischen Programm, beziehungsweise 0.7-0.8 MB/s

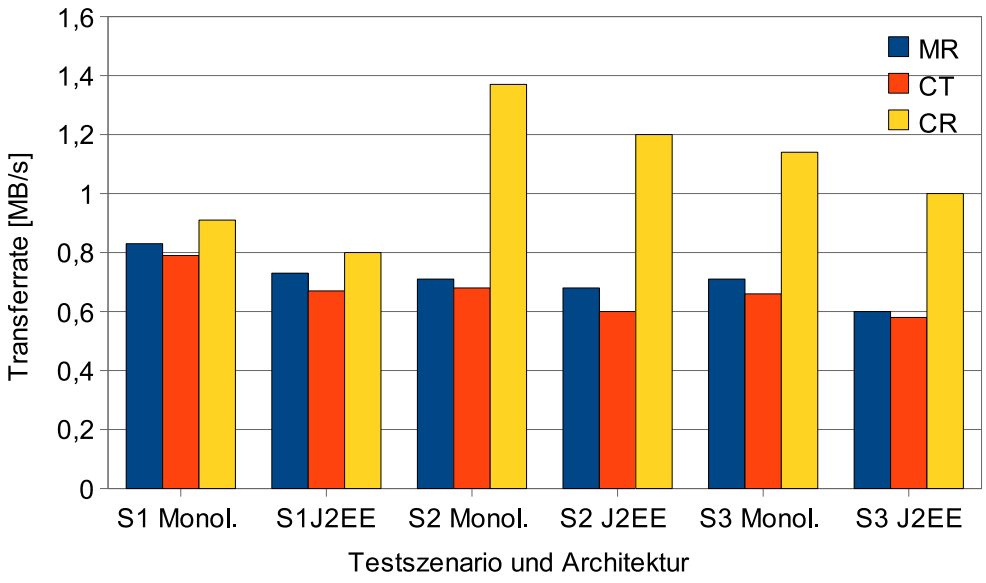


Abbildung 5.4: Durchschnittliche Transferraten der beiden Router-Systeme mit der monolithischen und der modularen (J2EE) Architektur bei den drei Testszenarien S1-S3 in MB/s.

bei der modularen Version, sind direkt vergleichbar mit der durchschnittlichen Transferrate von 2.5 MB/s aus der Tabelle 5.3 zu dem Gridknoten „B“ am Konrad-Zuse-Institut. Diese doch signifikante Reduktion in der Übertragungsgeschwindigkeit war allerdings zu erwarten, da alle ein- und ausgehenden DICOM-Nachrichten von den Routern verarbeitet und weitergeleitet werden müssen. Gleichzeitig muss angemerkt werden, dass die Leistung der Router stark von der genutzten Hardware abhängt. In diesen Tests wurden die Router auf herkömmlichen Arbeitsplatzrechnern installiert. Dies sind derzeit gängige PCs, beispielsweise mit einem Intel-3Ghz Prozessor und 512MB Speicher. Eine Nutzung entsprechend optimierter Rechner in einer Produktivumgebung würde die Leistung, und damit auch die Transferraten, deutlich beschleunigen. Die Ergebnisse können hier also nur im relativen Vergleich gesehen werden.

Im Szenario *S2*, der Übertragung zwischen zwei DICOM-Geräten, die jeweils mit einem Router verbunden sind, führt der zweite, zusätzliche Router zu einer weiteren Reduktion der Transferrate, die mit etwa 0.7 MB/s nochmal etwas unterhalb der Kommunikation mit nur einem Router liegt. Eine Ausnahme bildet hier die CR-Bildserie. Durch die im Vergleich zu den anderen beiden Bildserien geringe Anzahl von DICOM-Bildern -und damit DICOM-Nachrichten- haben die Router weniger Objekte zu verarbeiten und fallen damit bei der Übertragung nicht so ins Gewicht.

Das dritte Szenario, *S3*, eine Übertragung durch Drittaufruf, hat keinen weiteren Router zur Folge und unterscheidet sich dementsprechend nur noch geringfügig von *S2*. Die Rückgabe der Statusmeldungen der Übertragung an den Auftraggeber erfolgen zeitgleich zur Übertragung und machen sich im Vergleich zur Übertragung bei der Transferrate nicht auffallend

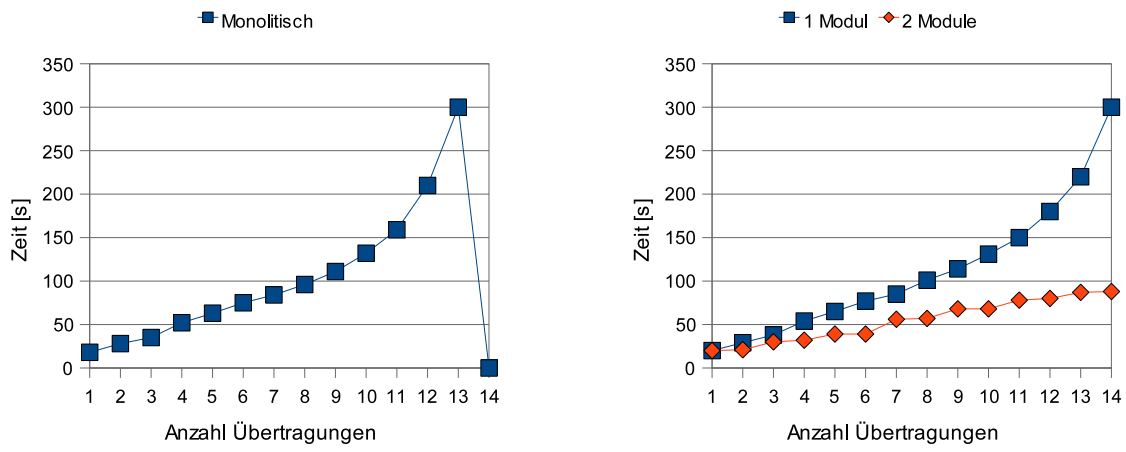


Abbildung 5.5: Ergebnisse der Router-Leistungstests: Die oberen Kurven zeigen die Gesamtübertragungszeit beider Router mit monolithischer Architektur (links) und modularer Architektur (rechts) bei einer steigenden Anzahl gleichzeitiger Übertragungen. Die untere Kurve rechts zeigt die Übertragungszeiten des modularen Systems bei der Verteilung auf zwei Module.

bemerkbar.

Das Verhältnis der beiden Router-Architekturen zueinander ist im Prinzip in allen Szenarien konstant. Es zeigt sich, dass der monolithische Ansatz bei gleicher Funktion die Transferrate um durchschnittlich etwa 0.1 MB/s beschleunigt. Dies liegt daran, dass das J2EE-Kontrollsystem, welche den modularen Router steuert, selbst etwas Rechenzeit und Speicher verbraucht und damit insgesamt die Verarbeitung etwas verlangsamt.

5.2.2 Leistungstests

Der folgende Abschnitt zeigt die Ergebnisse der Leistungstests, in denen beide Router jeweils einer steigenden Last durch eine zunehmende Anzahl von zeitgleichen Bildübertragungen ausgesetzt werden.

Abbildung 5.5 zeigt die gesamte Bearbeitungszeit in Sekunden für die steigende Anzahl paralleler Übertragungen. Die absolute Gesamtzeit der Übertragung hängt dabei, genau wie bei den Funktionstests, stark von der verwendeten Rechner-Hardware ab, auf der der Router läuft. Die Ergebnisse hier können also wiederum nur im Vergleich gesehen werden. In der Abbildung links sieht man die Übertragungsszeiten des monolithischen Systems, rechts die des modularen. Initial läuft der modulare Router mit nur einer Programm-Instanz, also in einer ähnlichen Konfiguration wie das monolithische System (obere Kurve). Man sieht deutlich, wie die Systeme auf die steigende Belastung reagieren: Bei einer geringen Anzahl von gleichzeitigen Übertragungen, bis zu 12 Clients etwa, steigt die Bearbeitungszeit gleichmäßig an. In diesem Bereich skalieren beide Router sehr gut. Das bedeutet, der Zuwachs an Bearbei-

tungszeit verhält sich direkt proportional zu der Anzahl gleichzeitiger Übertragungen. Bei einer Last von mehr als 12 Übertragungen jedoch, stoßen die Systeme an ihre Grenzen. Die Folge sind überlange Antwortzeiten und Fehler bei der Übertragung. In diesen Bereichen sind die Reaktionen der Systeme in dieser Konfiguration nicht mehr vorhersehbar.

Das monolithische System ist nun in seiner Leistung nicht mehr erweiterbar. Das modulare System dagegen ist in der Lage, sich der wachsenden Last anzupassen indem es eine zusätzliche Instanz erzeugt, auf die die Anfragen aufgeteilt werden können. Das Ergebnis sieht man in der zweiten, unteren Kurve, bei der die Antwortzeiten wieder in ein lineares, und damit berechenbares, Verhältnis rücken. Wie schon beschrieben, ließe sich grundsätzlich auch bei den monolithischen Programmen eine Lastverteilung durch das Starten über mehrere Programme erreichen. Im Unterschied zur modularen Version können diese dann aber nicht mehr untereinander kommunizieren, was entscheidende Router-Funktionen, wie beispielsweise die Weiterleitung von Zertifikaten, verhindert.

Die Ergebnisse des J2EE-Routers sind auch in [58] veröffentlicht. Die Referenzimplementierung wurde ebenfalls auf der Webseite **griddicom.sourceforge.org** der Allgemeinheit öffentlich verfügbar gemacht.

5.3 Zusätzliche Sicherheitsmaßnahmen

5.3.1 „SecureDICOM“

Um die patientenrelevanten Informationen in den DICOM-Bildern auf den fremden Gridrechnern zu schützen und aber gleichzeitig den Zugriff auf einzelne, verschlüsselte Attribute zuzulassen, ist das erweiterte Sicherheitsverfahren „SecureDICOM“ evaluiert worden. Ähnlich zu der bisher verfügbaren Methode ALC aus dem DICOM-Standard können zu schützende Daten in den DICOM-Bildern durch selbstgewählte Pseudonyme unleserlich gemacht werden. Dabei werden die Originalwerte mit einem Kennwort verschlüsselt an das Ende des Bildes angehängt und durch die jeweiligen Pseudonyme ersetzt. Die Originaldaten sind also zu jeder Zeit verschlüsselt im Bild vorhanden, an den unverschlüsselten Originalpositionen stehen aber die Pseudonyme.

Die Liste der Attribute, die zu ersetzen sind, ist derzeit nicht festgelegt, da die Vorgaben hier nicht weltweit einheitlich sind. Zurzeit wird im Standard bei der Beschreibung der ALC lediglich eine Empfehlung gegeben, welche Attribute Rückschlüsse auf den Patienten zulassen. Die Tabelle 5.4 zeigt diese Liste. Mit der sich derzeit in Bearbeitung befindenden Ergänzung zum Standard „Supplement 142 - Clinical Trials De-identification“ werden verschiedene Profile

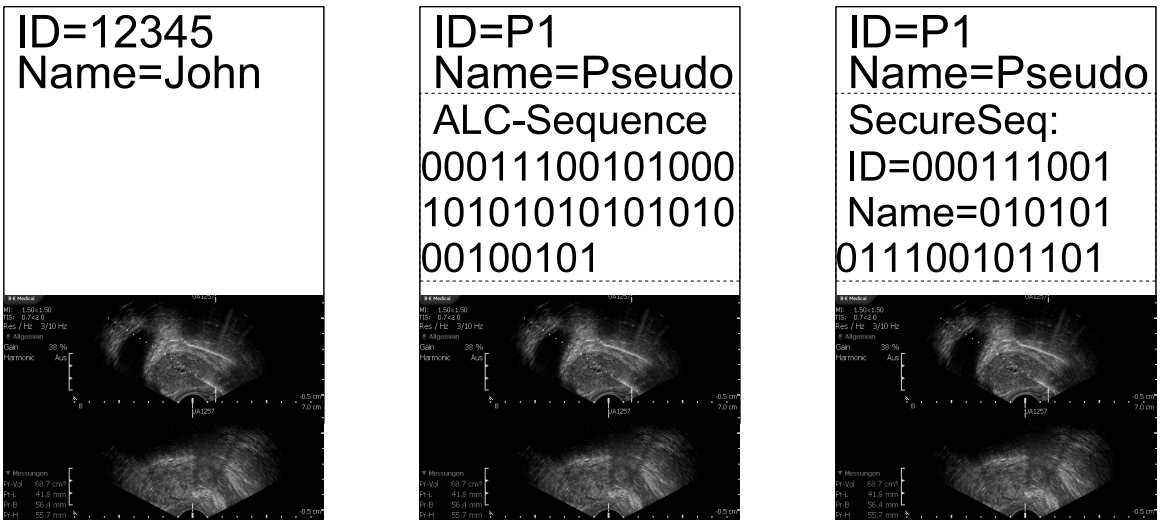


Abbildung 5.6: Schematische Darstellung des Unterschieds der DICOM-„Attribute Level Confidentiality“ (ALC) zur Abwandlung „SecureDICOM“. Alle zu schützenden Originaldaten im schematischen DICOM-Bild (links) werden bei der DICOM-ALC zu einem Block verschlüsselt (Mitte). Bei „SecureDICOM“ (rechts) werden nur die Werte selbst in einer verschlüsselten Sequenz angehängt. Dadurch kann weiterhin auf einzelne Attribute verwiesen werden ohne diese zu entschlüsseln, sodass sich beispielsweise Referenzen erhalten lassen.

definiert, die patientenrelevante Daten zu einem unterschiedlich hohen Grad schützen. Das SecureDICOM-Verfahren setzt das in diesem Dokument definierte „Basic Application Level Confidentiality Profile“ um, welches alle Attribute in der Tabelle 5.4 beinhaltet und um einige klinikinterne Angaben erweitert. Da weder das Dokument noch das Verfahren in endgültiger Form vorliegen, wird hier auf eine weitere Ausführung verzichtet. Es sei aber noch erwähnt, dass neben den Attributen auch die Pixeldaten des Bildes selbst mit verschlüsselt werden können, da diese oft „eingebrannte“ Identifikationsmerkmale besitzen, wie beispielsweise bei Ultraschallbildern.

Im Unterschied zur ALC werden bei „SecureDICOM“ die zu pseudonymisierenden Werte nicht alle zusammen in einen großen Block, sondern einzeln in einer Liste verschlüsselt. Dadurch kann auf einzelne, verschlüsselte Attribute zugegriffen werden, ohne dass es einer Entschlüsselung des kompletten Blocks bedarf. Abbildung 5.6 verdeutlicht diesen Unterschied schematisch.

Die Abbildungen 5.7 und 5.9 zeigen ein Bildschirmfoto der PACS-Konsole bei der Betrachtung eines reales Ultraschall-Bildes vor und nach der „SecureDICOM“-Verschlüsselung. In der linken oberen Ecke des Bildes sieht man jeweils die von dem Betrachtungsprogramm eingeblendeten Originaldaten des Patienten (Patient „Zeus“). Zusätzlich zeigen die Abbildungen 5.8 und 5.10 alle patientenrelevanten Daten aus dem Bild in der Textausgabe der PACS-Konsole. Auf dem Bildschirmfoto des zweiten Bildes (Abbildung 5.9) sieht man, dass die originalen Patientendaten durch das Pseudonym ersetzt wurden. Analog ist in der Textdarstellung

Attribut Name	DICOM-Tag
Instance Creator UID	(0008,0014)
SOP Instance UID	(0008,0018)
Accession Number	(0008,0050)
Institution Name	(0008,0080)
Institution Address	(0008,0081)
Referring Physician's Name	(0008,0090)
Referring Physician's Address	(0008,0092)
Referring Physician's Telephone Numbers	(0008,0094)
Station Name	(0008,1010)
Study Description	(0008,1030)
Series Description	(0008,103E)
Institutional Department Name	(0008,1040)
Physician(s) of Record	(0008,1048)
Performing Physicians' Name	(0008,1050)
Name of Physician(s) Reading Study	(0008,1060)
Operators' Name	(0008,1070)
Admitting Diagnoses Description	(0008,1080)
Referenced SOP Instance UID	(0008,1155)
Derivation Description	(0008,2111)
Patient's Name	(0010,0010)
Patient ID	(0010,0020)
Patient's Birth Date	(0010,0030)
Patient's Birth Time	(0010,0032)
Patient's Sex	(0010,0040)
Other Patient Ids	(0010,1000)
Other Patient Names	(0010,1001)
Patient's Age	(0010,1010)
Patient's Size	(0010,1020)
Patient's Weight	(0010,1030)
Medical Record Locator	(0010,1090)
Ethnic Group	(0010,2160)
Occupation	(0010,2180)
Additional Patient's History	(0010,21B0)
Patient Comments	(0010,4000)
Device Serial Number	(0018,1000)
Protocol Name	(0018,1030)
Study Instance UID	(0020,000D)
Series Instance UID	(0020,000E)
Study ID	(0020,0010)
Frame of Reference UID	(0020,0052)
Synchronization Frame of Reference UID	(0020,0200)
Image Comments	(0020,4000)
Request Attributes Sequence	(0040,0275)
UID	(0040,A124)
Content Sequence	(0040,A730)
Storage Media File-set UID	(0088,0140)
Referenced Frame of Reference UID	(3006,0024)
Related Frame of Reference UID	(3006,00C2)

Tabelle 5.4: Im DICOM-Standard vorgeschlagene Attribute, die verschlüsselt werden sollten.

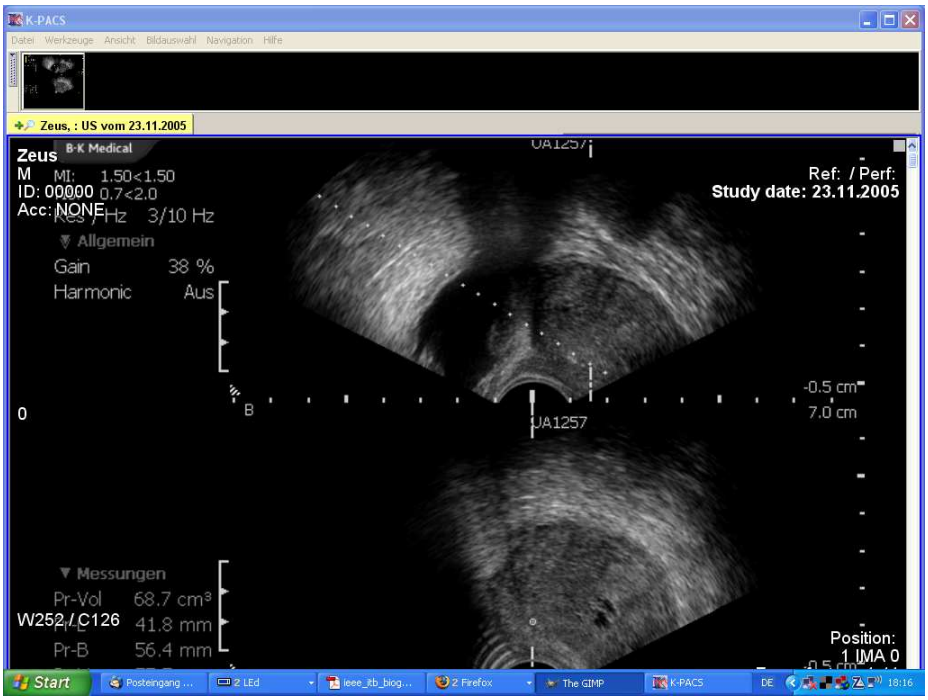


Abbildung 5.7: Bildschirmfoto bei der Betrachtung eines unverschlüsselten Ultraschall-Bildes. In der linken oberen Ecke des Bildes sieht man die von dem Betrachtungsprogramm eingeblendeten Originaldaten des Patienten (Patient „Zeus“).


```
<?xml version="1.0" encoding="ISO-8859-1"?>
<file-format>
  <Group_0008 name="">
    <Element_0008 name="ImageType" VR="CS" VM="">ORIGINAL\PRIMARY\\</Element_0008>
    <Element_0016 name="SOPClassUID" VR="UI" VM="">1.2.840.10008.5.1.4.1.1.6.1</Element_0016>
    <Element_0018 name="SOPInstanceUID" VR="UI" VM="">1.3.6.1.4.1.9590.100.1.1.331785581490704</Element_0018>
    <Element_0020 name="StudyDate" VR="DA" VM="">20051123</Element_0020>
    <Element_0023 name="ContentDate" VR="DA" VM=""></Element_0023>
    <Element_0030 name="StudyTime" VR="TM" VM="">091727.000000 </Element_0030>
    <Element_0033 name="ContentTime" VR="TM" VM=""></Element_0033>
    <Element_0050 name="AccessionNumber" VR="SH" VM="">NONE</Element_0050>
    <Element_0060 name="Modality" VR="CS" VM="">US</Element_0060>
    <Element_0070 name="Manufacturer" VR="LO" VM="">BK-Medical</Element_0070>
    <Element_0090 name="ReferringPhysiciansName" VR="PN" VM=""></Element_0090>
    <Element_1090 name="ManufacturersModelName" VR="LO" VM="">UltraPACS </Element_1090>
  </Group_0008>
  <Group_0010 name="">
    <Element_0010 name="PatientsName" VR="PN" VM="">Zeus</Element_0010>
    <Element_0020 name="PatientID" VR="LO" VM="">00000 </Element_0020>
    <Element_0030 name="PatientsBirthDate" VR="DA" VM=""></Element_0030>
    <Element_0040 name="PatientsSex" VR="CS" VM="">M </Element_0040>
  </Group_0010>
  <Group_0020 name="">
    <Element_000D name="StudyInstanceUID" VR="UI" VM="">1.2.840.113711.2.300.500.123456789.511230900</Element_000D>
    <Element_000E name="SeriesInstanceUID" VR="UI" VM="">1.2.840.113711.2.300.500.511230900</Element_000E>
    <Element_0010 name="StudyID" VR="SH" VM="">51123.0900</Element_0010>
    <Element_0011 name="SeriesNumber" VR="IS" VM="">1 </Element_0011>
    <Element_0013 name="InstanceNumber" VR="IS" VM="">0 </Element_0013>
    <Element_0020 name="PatientOrientation" VR="CS" VM=""></Element_0020>
  </Group_0020>
  <Group_7FE0 name="">
    <Element_0010 name="PixelData" VR="OB/OW" VM="1">not included in XML output</Element_0010>
  </Group_7FE0>
</file-format>
```


Abbildung 5.8: Textausgabe des unverschlüsselten Ultraschall-Bildes aus Abbildung 5.7. In den einzelnen Attributen sieht man die Originaldaten.

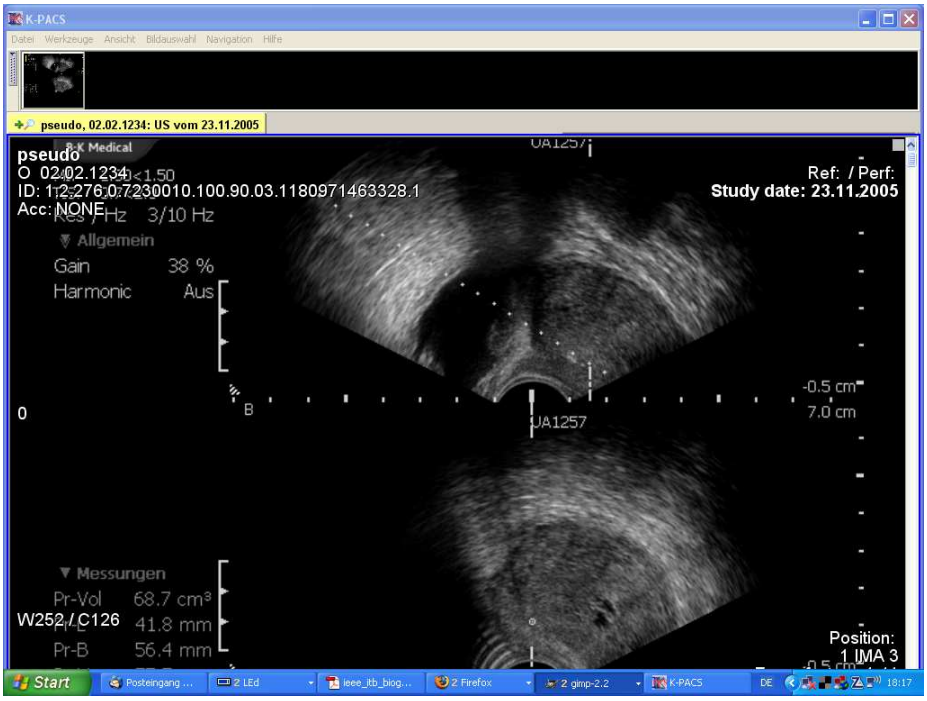


Abbildung 5.9: Bildschirmfoto bei der Betrachtung eines Ultraschall-Bildes nach der Pseudonymisierung mit dem „SecureDICOM“-Verfahren. In der linken oberen Ecke des Bildes sieht man die von dem Betrachtungsprogramm eingeblendeten ersetzten Daten Patienten (Patient „pseudo“).

(Abbildung 5.10) deutlich zu erkennen, dass alle relevanten Daten pseudonymisiert und in einer verschlüsselten Sequenz an das Bild angehängt wurden. Die Sequenz enthält mehrere Gruppen, die jeweils ein Schlüssel-Werte-Paar beinhalten. Jedes dieser Paare listet den lesbaren DICOM-Attribut-Schlüssel, wie beispielsweise „0010:0020“ für die Patienten-ID, und den nicht-lesbaren, verschlüsselten Originalwert auf. Dieser Originalwert könnte nun von einer Gridanwendung verschlüsselt in neu erzeugte Ergebnisbilder übernommen werden. Bei der Rückübertragung dieser Bilder, und der gleichzeitig stattfindenden Reidentifizierung, könnten diese dann eindeutig dem Originalbild zugeordnet werden. Bei der ALC wäre dies ohne eine Entschlüsselung der Attribute nicht möglich. Damit ist das „SecureDICOM“-Verfahren gerade für Anwendungen in Grid-Infrastrukturen, die eine Zuordnung von neuen Bildern erfordern, wie in der Bildverarbeitung, besser geeignet. Die zusätzlichen Informationen, die im Vergleich zu ALC mehr gespeichert werden müssen, liegen bei maximal einem Kilobyte und sind im Vergleich zur Gesamtgröße der Bilder vernachlässigbar.

5.3.2 Sichere Anbindung des Klinik-PACS

Wie beschrieben erlauben die allermeisten Kliniken keinen automatischen Zugang zu ihrem internen PACS. Ein Zugang ist im Allgemeinen nur für Ärzte mit den entsprechenden Zugriffs-

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<file-format>
  <Group_0008 name="">
    <Element_0008 name="ImageType" VR="CS" VM="">ORIGINAL\PRIMARY\\</Element_0008>
    <Element_0016 name="SOPClassUID" VR="UI" VM="">1.2.840.10008.5.1.4.1.1.6.1</Element_0016>
    <Element_0018 name="SOPInstanceUID" VR="UI" VM="">1.2.276.0.7230010.100.90.09.1180971463578</Element_0018>
    <Element_0020 name="StudyDate" VR="DA" VM="">20051123</Element_0020>
    <Element_0023 name="ContentDate" VR="DA" VM=""></Element_0023>
    <Element_0030 name="StudyTime" VR="TM" VM="">091727.000000 </Element_0030>
    <Element_0033 name="ContentTime" VR="TM" VM=""></Element_0033>
    <Element_0050 name="AccessionNumber" VR="SH" VM="">NONE</Element_0050>
    <Element_0060 name="Modality" VR="CS" VM="">US</Element_0060>
    <Element_0070 name="Manufacturer" VR="LO" VM="">BK-Medical</Element_0070>
    <Element_0090 name="ReferringPhysiciansName" VR="PN" VM=""></Element_0090>
    <Element_1090 name="ManufacturersModelName" VR="LO" VM="">UltraPACS </Element_1090>
  </Group_0008>
  <Group_0010 name="">
    <Element_0010 name="PatientsName" VR="PN" VM="">pseudo</Element_0010>
    <Element_0020 name="PatientID" VR="LO" VM="">1.2.276.0.7230010.100.90.03.1180971463328.1 </Element_0020>
    <Element_0030 name="PatientsBirthDate" VR="DA" VM="">12340202</Element_0030>
    <Element_0040 name="PatientsSex" VR="CS" VM="">O </Element_0040>
  </Group_0010>
  <Group_0020 name="">
    <Element_000D name="StudyInstanceUID" VR="UI" VM="">1.2.276.0.7230010.100.90.04.0900</Element_000D>
    <Element_000E name="SeriesInstanceUID" VR="UI" VM="">1.2.276.0.7230010.100.90.05.31</Element_000E>
    <Element_0010 name="StudyID" VR="SH" VM="">51123.0900</Element_0010>
    <Element_0011 name="SeriesNumber" VR="IS" VM="">1 </Element_0011>
    <Element_0013 name="InstanceNumber" VR="IS" VM="">3 </Element_0013>
    <Element_0020 name="PatientOrientation" VR="CS" VM=""></Element_0020>
  </Group_0020>
  <Group_0099 name="Private Group">
    <Element_0001 name="PrivateAttribute" VR="SQ" VM="1">
      <Item_1>
        <Group_0099 name="Private Group">
          <Element_0002 name="PrivateAttribute" VR="AT" VM="">.</Element_0002>
          <Element_0003 name="PrivateAttribute" VR="OB" VM="">.w.5.+.. G.aY.üm0P.F.Nzm..üxI.</Element_0003>
        </Group_0099>
      </Item_1>
      <Item_2>
        <Group_0099 name="Private Group">
          <Element_0002 name="PrivateAttribute" VR="AT" VM="">.</Element_0002>
          <Element_0003 name="PrivateAttribute" VR="OB" VM="">.......j4741..</Element_0003>
        </Group_0099>
      </Item_2>
      <Item_3>
        <Group_0099 name="Private Group">
          <Element_0002 name="PrivateAttribute" VR="AT" VM="">  </Element_0002>
          <Element_0003 name="PrivateAttribute" VR="OB" VM="">.£Ä.R.a..../3..WN££.....I6.Ö...</Element_0003>
        </Group_0099>
      </Item_3>
      <Item_4>
        <Group_0099 name="Private Group">
          <Element_0002 name="PrivateAttribute" VR="AT" VM="">  </Element_0002>
          <Element_0003 name="PrivateAttribute" VR="OB" VM="">......D...X..G.e.6..P....Z...\.</Element_0003>
        </Group_0099>
      </Item_4>
    </Element_0001>
  </Group_0099>
  <Group_7FE0 name="">
    <Element_0010 name="PixelData" VR="OB/OW" VM="1">not included in XML output</Element_0010>
  </Group_7FE0>
</file-format>
```


Abbildung 5.10: Textausgabe des pseudonymisierten Ultraschall-Bildes aus Abbildung 5.9. Deutlich sieht man die ersetzten Originalwerte und die angehängte verschlüsselte Sequenz.

berechtigungen von ihren Arbeitsplätzen innerhalb des Kliniknetzes aus möglich.

Um von Gridrechnern aus die Bilder für die Berechnungen automatisch selbst vom internen Klinik-PACS abfragen zu können, wurde folgendes Konzept entwickelt: Normalerweise existiert in stark gesicherten Netzwerken, wie Kliniknetzen, auch eine weniger gesicherte Netzwerkzone, die sogenannte „Demilitarized Zone (DMZ)“. Der Zugriff auf diese Zone ist ebenfalls limitiert. Im Unterschied zur internen Zone ist er aber von außen auf bestimmte öffentliche Informationssysteme, wie beispielsweise einem Webserver, explizit zugelassen. Auf den Systemen dürfen sich damit allerdings keine sensitiven Informationen befinden. In dieser DMZ wird nun ein zusätzliches Standard-PACS als Zwischenspeicher eingeführt. Da dieses PACS nur eine Kurzzeitarchivierung und damit nur begrenzten Speicherplatz und Funktionalität zur Verfügung stellen muss, genügen hier kostenfreie, öffentliche PACS-Lösungen auf einem einfachen Arbeisplatzrechner. Dies sind beispielsweise die bekannten Anwendungen „K-PACS“ für Windows-basierte Systeme [60] oder das Betriebssystem-unabhängige „dcm4chee“-PACS [56] für Linux oder andere Systeme. Dieses externe PACS wird über einen GridDICOM-Router an das Grid angeschlossen. Da der Zugriff von außen auf dieses PACS erlaubt ist, können die einzelnen Gridrechner automatisiert Bilder von und zu dem PACS übertragen.

Um Bilder von dem externen PACS aus im Grid abrufbar machen zu können, muss der Benutzer (beispielsweise der Arzt) seine Bilder explizit vom internen Klinik-PACS dorthin übertragen. Dies ist nur einem Benutzer mit entsprechender Zugriffsberechtigung sowohl für das interne PACS als auch für das Grid erlaubt. Von einem legitimierten Arbeitsplatzrechner aus kann er mit einer speziellen Übertragungsanwendung Bilder aus dem Original-PACS anfragen und über seinen Rechner an das externe PACS senden. Da das externe PACS jedoch keine sensitiven Daten enthalten darf, müssen diese Bilder nach dem „SecureDICOM“-Verfahren pseudonymisiert werden bevor sie das interne Netz verlassen. Dies wird ebenfalls durch die spezielle Übertragungsanwendung sichergestellt, die in einem Schritt die Bilder anfordert, verschlüsselt und an das externe PACS sendet. Mit der gleichen Anwendung kann ein Benutzer dann Ergebnisbilder aus dem externen PACS abfragen und unter gleichzeitiger Reidentifizierung in das interne PACS übertragen. Für zusätzliche Sicherheit erfolgt der Zugriff der Übertragungsanwendung sowohl auf das interne als auch auf das externe PACS über einen DICOM-Router.

Abbildung 5.11 zeigt die wichtigsten Systeme und den Datenfluss bei einem heutzutage typischen, gesicherten Netzwerkaufbau, wie er auch an der Charité praktiziert wird. Im Einzelnen sind dies:

1. Das interne PACS: das PACS nimmt DICOM-Verbindungen auf dem Port 104 an. Dabei überprüft es im Allgemeinen die DICOM-Kennung (AET) und die Internetadresse des anfragenden Systems. Diese müssen vorab entsprechend vom Administrator des PACS

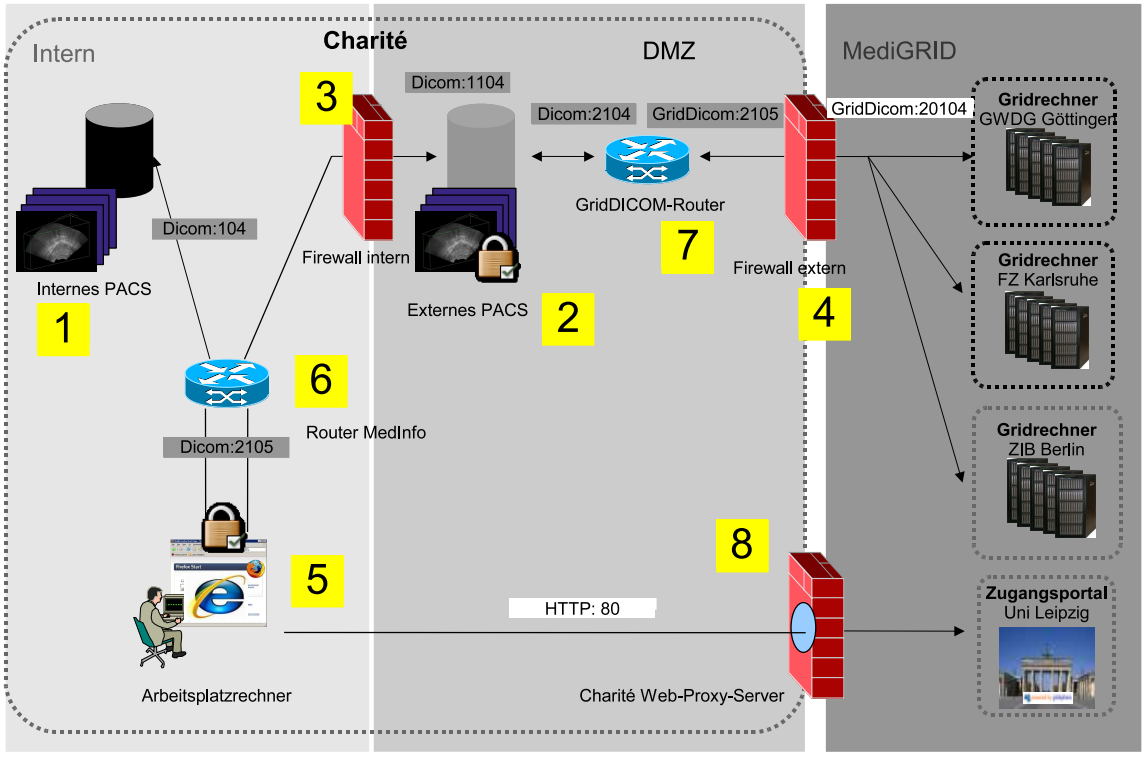


Abbildung 5.11: Systeme und Datenfluss beim MediGRID-Anschluss an der Charité: Das interne PACS (1) steht in der internen Netzwerkzone, das externe PACS (2) in der DMZ. Bilder können nur manuell vom Arbeitsplatzrechner (5) über den Router (6) verschoben werden. Der Zugriff auf die Anwendungen im Grid erfolgt mit dem Webbrowser über den Charité-Proxy (8). Gridrechner können auf das externe PACS nur über den GridDICOM-Router (7) zugreifen.

konfiguriert sein.

2. Das externe PACS: das externe PACS nimmt DICOM-Verbindungen auf dem Port 1104 an. Der Zugriff von innen kann auf einzelne Systeme beschränkt werden. Von außen erlaubt es nur GSI-gesicherte Zugriffe autorisierter Gridnutzer über den vorgeschalteten GridDICOM-Router (7). Der Router nimmt DICOM-Verbindungen von innen auf dem Port 2104 und GridDICOM-Verbindungen von außen auf 2105 an.

3. Die interne Firewall: Die interne Firewall sichert den Übergang vom internen Kliniknetz zur externen Zone (DMZ): Verbindungen sind in der Regel nur von eingetragenen Systemen von innen nach außen und nur auf eingetragene Systeme innerhalb der Zone zugelassen.

4. Die externe Firewall: Diese, etwas weniger restriktive Firewall reguliert den Übergang von der DMZ in das öffentliche Netz: Verbindungen sind in der Regel von allen Rechnern auf eingetragene Systeme in der DMZ zugelassen.

5. Arbeitsplatzrechner der Benutzer: Von den Arbeitsplatzrechnern aus werden Bilder aus dem internen PACS ins externe transportiert und umgekehrt. Eine spezielle Übertra-

gungsanwendung stellt dabei die gleichzeitige Pseudonymisierung bzw. Reidentifizierung sicher. Zur Sicherheit müssen die Arbeitsplatzrechner die Übertragungen über einen eigenen Router (6) ausführen. Dieser nimmt DICOM-Verbindungen aus allen Richtungen auf dem Port 2105 an. Der Zugriff auf die webbasierte Benutzeroberfläche des Grids erfolgt mit dem Webbrowser auf das Zugangsportal über den Standard-Proxy-Server der Charité für Webzugriffe auf Port 80 (8).

Bei der Analyse des Datenflusses und der nötigen Sicherheitsbetrachtungen zeigen sich die folgenden Beobachtungen:

1. Zugriffe auf das klinikinterne PACS erfolgen nur von einem einzigen System aus, dem DICOM-Router für die Arbeitsplatzrechner. Damit braucht auch nur dieses System im PACS eingetragen zu sein, was die Administration wesentlich erleichtert. An den Routern können entsprechende Zugriffsbeschränkungen für die Arbeitsplatzrechner eingetragen werden. Zusätzlich können durch die eingebaute Protokollierungsfunktion alle übertragenen DICOM-Nachrichten für spätere Audits in einer Datenbank protokolliert werden.

2. Zugriffe auf das externe PACS von innen erfolgen ebenfalls nur von dem Router-System mit einer festen Internetadresse. Dies erleichtert die Administration der internen Firewall, die diesen Zugriff erlauben muss. Ein dedizierter Zugriff von einem inneren System auf ein System in der DMZ stellt in aller Regel sicherheitstechnisch kein Risiko dar und wird meist erlaubt, beispielsweise zur Pflege von Webseiten auf dem Webserver.

3. Das externe PACS enthält nur pseudonymisierte Bilder, die im Allgemeinen zur Übertragung in öffentlichen Netzen zugelassen sind.

4. Ein automatisierter Zugriff erfolgt nur auf das externe PACS und nur über Verbindungen von autorisierten Gridnutzern nach dem GSI-Sicherheitsstandard.

5. Über den externen Grid-Router können die Zugriffsrechte auf die Bilder im externen PACS auf Gridnutzer beschränkt werden.

Damit kann dieses Konzept als ausreichend sicher für die Bildübertragung in eine Grid-Infrastruktur gesehen werden. Jedoch besitzt es zwei Nachteile: Erstens benötigt es, im Gegensatz zu einem direkten Zugriff, einen zusätzlichen Arbeitsschritt seitens des Benutzers und trägt damit nicht zur Benutzerfreundlichkeit bei. Da ein direkter Zugriff jedoch in aller Regel außer Frage steht, muss dies in Kauf genommen werden. Über entsprechende Anwendungen kann der zusätzliche Schritt möglichst einfach in den Arbeitsablauf integriert werden (siehe auch der folgende Test der Referenzimplementation). Zweitens ist es derzeit schwierig, benutzerbezogene und rollenbasierte Zugriffsrechte für die Bildabfrage der pseudonymisierten

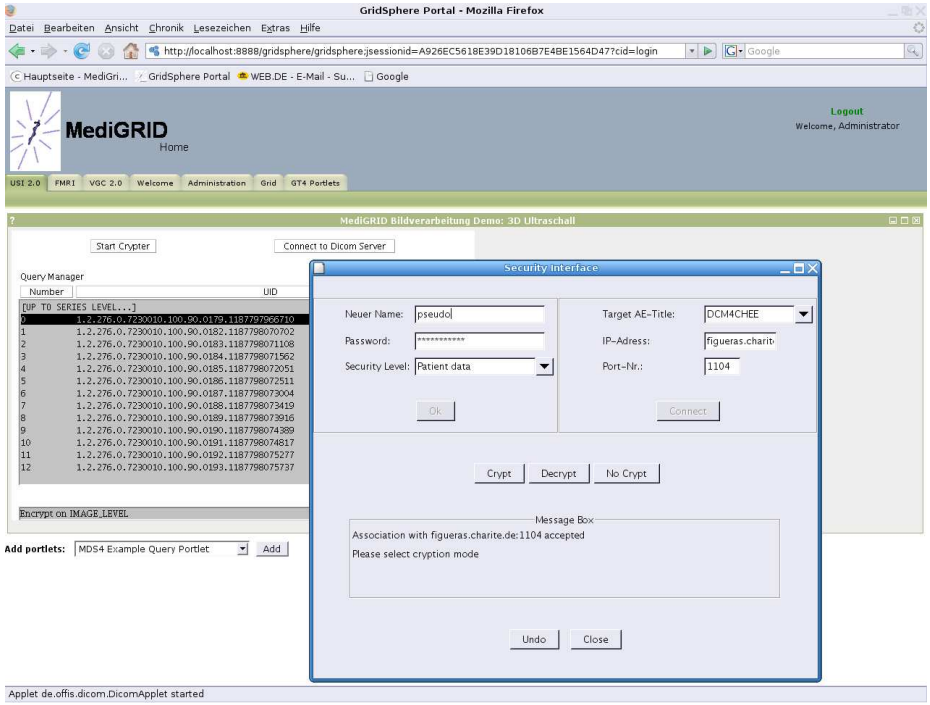


Abbildung 5.12: Ein Bildschirmfoto des SecureDICOM-Programms. Über eine DICOM-PACS-Abfrage kann eine Bildserie ausgewählt werden, danach startet das Pseudonymisierungsmodul in einem eigenen Fenster. Das Programm ist in die webbasierte MediGRID-Benutzeroberfläche integriert und kann von jedem internetfähigen Webbrowser ohne zusätzliche Installationen aufgerufen werden.

Bilder nach innen umzusetzen. Dies ist allerdings ein generelles DICOM-Problem und ließe sich nur über eine konsequente Implementierung und Umsetzung von benutzerbezogenen DICOM-Abfragen erreichen, die aber selbst in kommerziellen Systemen selten implementiert sind.

5.3.3 Referenzimplementation und Tests

Mit einem Testaufbau, wie in Kapitel 4.3.2 beschrieben, wurde das Konzept am Beispiel der 3D-Ultraschall Anwendung der Charité in MediGRID (siehe Kapitel 2 „Motivation“) umgesetzt. Als externes PACS wurde in diesem Fall das frei-verfügbare „dcm4chee“-PACS eingesetzt [56]. Dieses wurde zusammen mit einem GridDICOM-Router auf einem Standard-Arbeitsplatzrechner (Intel Pentium mit 256MB Speicher und 300GB Festplatte mit dem Linux Betriebssystem Debian „Sarge“) installiert. Der Rechner wurde vom IT-Zentrum an der Charité in der DMZ angeschlossen und der Internet-Port von dem Router für weltweite Zugriffe von außen freigegeben. Als Zugang von innen wurde entsprechend dem Konzept als einziges System ein DICOM-Router in dem Institut für Medizinische Informatik installiert und zugelassen. Alle Verbindungen zum PACS aus dem Charité-Netz heraus laufen aus Sicherheitsgründen über

dieses System.

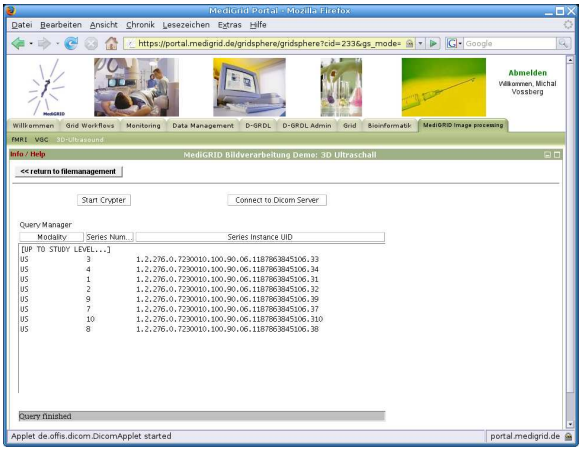
Für die manuelle Bildübertragung und Pseudonymisierung wurde ein bestehendes OFFIS-Programm verwendet. Das Programm ermöglicht es, eine Bildserie in einem Quell-PACS auszuwählen sowie ein Pseudonym und ein Kennwort anzugeben. Diese Bildserie wird dann von dem Programm über ein DICOM-C-GET angefordert, mit dem angegebenen Pseudonym nach der „SecureDICOM“-Methode im Speicher verändert und über ein DICOM-C-STORE an das externe Grid-PACS gesandt. Ursprünglich ein eigenes Programm, wurde diese Anwendung in die bestehende Weboberfläche der MediGRID-3D-Ultraschall-Anwendung integriert. Dazu wurden die in Java programmierten Oberflächen-Komponenten so angepasst, dass in dem Bereich Datenmanagement der Anwendung nun auf Knopfdruck das „SecureDICOM“-Programm in der gleichen, webbasierten Oberfläche aufrufbar ist. Abbildung 5.12 zeigt ein Bildschirmfoto der Anwendung.

Mit dieser integrierten Oberfläche wurde nun der Standard-Arbeitsablauf der Ultraschall-Anwendung mit mehreren verschiedenen Bildserien hintereinander getestet. Die Bildschirmfotos in der Abbildung 5.13 zeigen den Ablauf von der Selektion der Daten über die Pseudonymisierung bis zur Übertragung und Start der Anwendung. Insgesamt zeigt sich, dass sich über das integrierte „SecureDICOM“-Programm und das zusätzliche PACS das vorgeschlagene Konzept sicher und praktikabel umsetzen lässt. Als Nachteil ergibt sich, dass derjenige Rechner, auf dem die Weboberfläche genutzt wird, einen Zugang zum internen Kliniknetz benötigt, da die Bilder auf diesen Rechner übertragen, dort verschlüsselt und an das externe PACS weitergeleitet werden. Dies steht ein wenig im Widerspruch zu den Vorteilen der webbasierten Portallösung, die einen intuitiven Zugang unabhängig vom Standort des Arbeitsplatzes ermöglichen soll, beispielsweise auch von zuhause aus. Jedoch beschränkt sich diese Voraussetzung lediglich auf die Bildserienauswahl aus dem internen PACS. Hat der Benutzer diese Daten einmal ausgewählt und ins externe PACS übertragen, kann er die Anwendung wie bisher beliebig von überall aus steuern und die Ergebnisse kontrollieren.

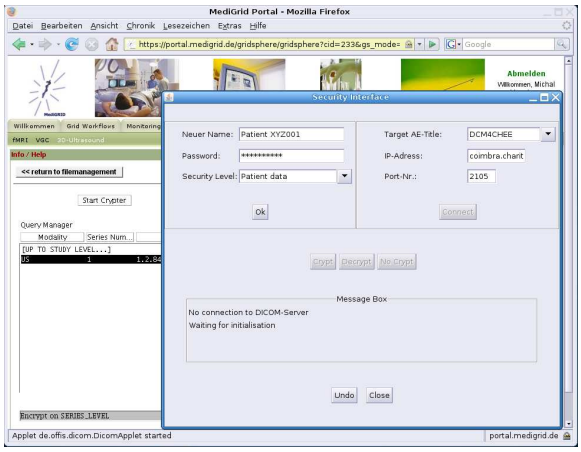
5.4 Fehlertoleranz und Zuverlässigkeit

5.4.1 Modellierung

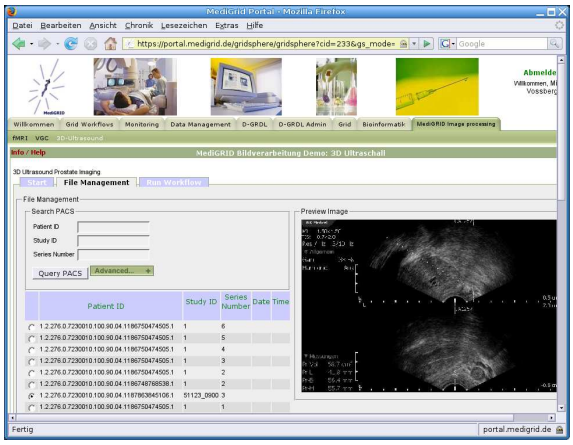
Die DICOM-Kommunikation wurde zunächst mithilfe von Petri-Netzen als Prozessablauf (ein „Workflow“) modelliert. Dabei wurden zwei unterschiedliche Ansätze überprüft: a) das netzwerkbasierte Modell und b) das transferbasierte Modell. Im Folgenden werden die entsprechend entwickelten Petri-Netze vorgestellt und diskutiert:



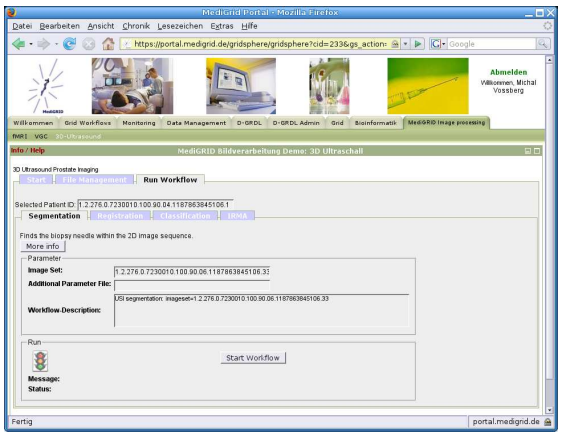
1. Auswahl Bildserien im Klinik-PACS



2. Transfer und Pseudonymisierung



3. Auswahl im Grid-PACS



4. Starten der Bildverarbeitungs-anwendung

Abbildung 5.13: Arbeitsablauf bei der 3D-Ultraschallanwendung von der Selektion der Bilddaten im Klink-PACS bis zum Start der Anwendung.

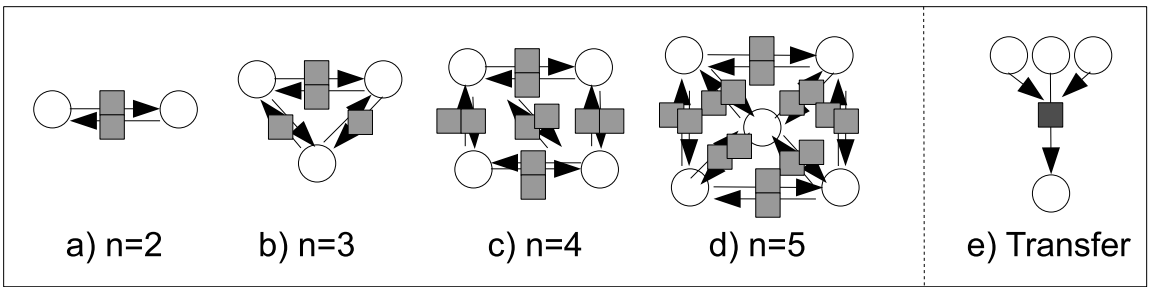


Abbildung 5.14: Netzwerkbasierte und transferbasierte Modellierung mit Petri-Netzen. Die Abbildungen a-d zeigen die Entwicklung eines Netzwerk-Modells bei n Rechnern. Abbildung e stellt das transferbasierte Modell dar. Dies besteht lediglich aus den beiden Eingabeplätzen für den Quell- und Zielrechner, einem Eingabeplatz für die Bild-IDs, und einem Ausgabeplatz für das Ergebnis der Übertragung.

Netzwerkbasiert

Die netzwerkbasierte Modellierung bildet alle vorhandenen Gridrechner jeweils als ein Platz im Petri-Netz ab und stellt alle möglichen Verbindungen durch eine Transition dar. In der Modellierung zeigte sich schon bei einfachen DICOM-Übertragungsmodellen, wie dem Senden eines Einzelbildes von einem PACS zu einem Rechner, dass die netzwerkbasierten Modelle schnell sehr aufwändig und komplex werden. Abbildung 5.14a-d verdeutlicht die Entwicklung eines Petri-Netz-Modells bei einer steigenden Anzahl von Rechnern in einer Grid-Infrastruktur. Da das Modell jeden möglichen Übertragungsweg zwischen den Rechnern abbilden muss und zusätzlich jeder Übertragungsweg aus einem Hin- und Rückweg mit jeweils zwei Transitionen und vier Kanten besteht, entwickelt sich die Anzahl der Knoten in einem Netz aus n Rechnern nach der Formel $n!$. Zwar erlaubt die Darstellung eine gute Übersicht über den Zustand der gesamten Grid-Infrastruktur und der verfügbaren Gridrechner, jedoch wird deutlich, dass dies nur für sehr kleine und einfache Netze gilt. Zusätzlich erwiesen sich die statischen Transfer-Modelle in der MediGRID-Umgebung als unpraktikabel, da sie nicht die nötige Dynamik der Grid-Infrastrukturen besaßen. So mussten für jeden Gridrechner der dem Grid hinzugefügt oder entfernt wurde, das Modell geändert werden.

Transferbasiert

Abbildung 5.14e zeigt das Petri-Netz der gleichen DICOM-Übertragung nach dem transferbasierten Ansatz. Da der transferbasierte Ansatz lediglich einen Ausschnitt des Grids mit den zwei jeweils beteiligten Rechnern zeigt, ist er unabhängig von der Größe und Dynamik der Grid-Infrastruktur und damit wesentlich praktikabler. Dies gilt vor allem auch in Hinblick auf die zu entwickelnden, komplexeren Modelle mit expliziter Fehlerkorrektur. Aus diesem Grund wurde dieser Ansatz für die weitere Modellierung verfolgt.

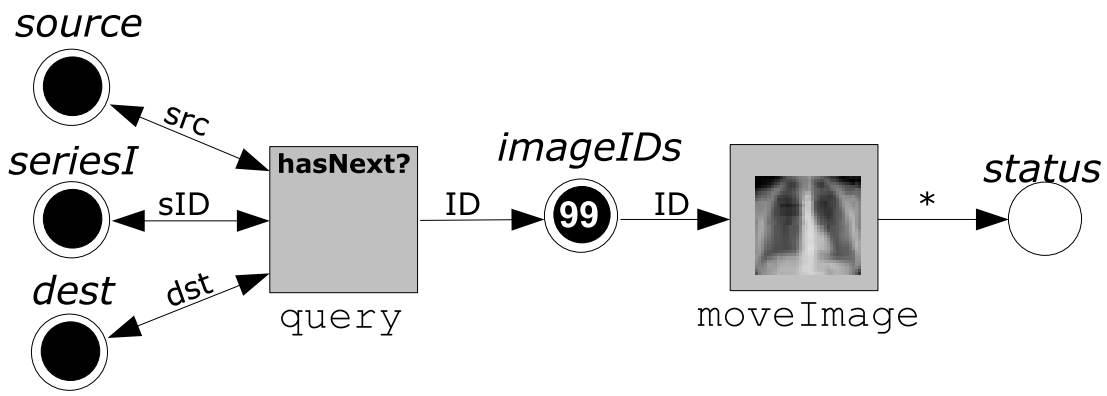


Abbildung 5.15: Petri-Netz-Modell auf Einzelbildbasis ohne Fehlerkorrektur. Zuerst werden alle Einzelbilder zu einer Serie gesucht, dann werden diese einzeln übertragen. Das Ergebnis jeder Übertragung ist direkt sichtbar. Zur besseren Übersicht wurden kleinere Detailschritte in der Darstellung ausgelassen.

Wie im Kapitel 4 „Methodik“ beschrieben, unterscheiden sich die Abläufe durch Übertragungen auf Einzelbildbasis und auf Serienbasis. Im Folgenden werden jeweils zwei Modelle mit und ohne expliziter Fehlerkorrektur für diese beiden Ansätze vorgestellt. Dazu werden die wichtigsten Schritte im Ablauf sowie das entwickelte High-Level Petri-Netz beschrieben:

Abläufe auf Einzelbildbasis

Bei den Abläufen auf Einzelbildbasis werden die Bilder einzeln beim PACS angefragt und übertragen. Der Vorteil ist, dass dabei das Ergebnis jeder Einzelbildübertragung direkt sichtbar wird und im Ablauf entsprechend reagiert werden kann. Als Nachteil erfordert dies einen wesentlich höheren Datenverkehr, da jedes Einzelbild mit einer expliziten DICOM-Nachrichten angefordert wird.

Abbildung 5.15 zeigt das Petri-Netz der Kommunikation auf Einzelbildbasis ohne Fehlerkorrektur. Der Ablauf enthält die folgenden Schritte:

1. Absetzen eines DICOM-C-FIND-Befehls an das PACS, um alle verfügbaren Bilder für diese bestimmte Bildserie zu ermitteln („query“-Transition). Für jedes Bild wird in diesem Schritt dann ein Token mit der entsprechenden Bild-ID auf dem Ausgabeplatz erzeugt.
2. Für jedes Token mit einer Bild-ID auf dem Ausgabeplatz wird ein DICOM- C-MOVE-Befehl für dieses einzelne Bild an das PACS gesendet („moveImage“-Transition).

Die Abbildung 5.16 dagegen zeigt das Petri-Netz der Kommunikation mit explizit modellierter Fehlerkorrektur. Dabei werden die einzelnen Schritte jeweils auf Erfolg oder Misserfolg überprüft und gegebenenfalls wiederholt. In diesem Fall ergeben sich die folgenden Schritte:

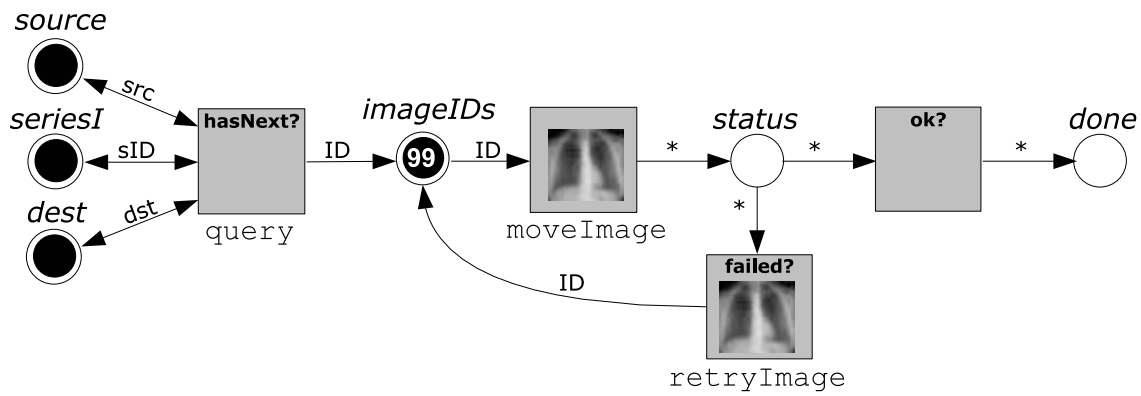


Abbildung 5.16: Petri-Netz-Modell auf Einzelbildbasis mit expliziter Fehlerkorrektur. Zuerst werden alle Einzelbilder zu einer Serie gesucht, dann werden diese einzeln übertragen. Schlägt eine Übertragung fehl, wird das Bild direkt wiederholt. Zur besseren Übersicht wurden kleinere Detailschritte in der Darstellung ausgelassen.

1. Absetzen eines DICOM-C-FIND-Befehls an das PACS um alle verfügbaren Bilder für diese bestimmte Bildserie zu ermitteln („query“-Transition). Für jedes Bild wird in diesem Schritt dann ein Token mit der entsprechenden Bild-ID auf dem Ausgabeplatz erzeugt. Im Fehlerfall, wird dieser Schritt solange wiederholt, bis das PACS erfolgreich abgefragt werden konnte oder eine einstellbare Maximalzeit erreicht wurde (beispielsweise eine Stunde).

2. Für jedes Token mit einer Bild-ID auf dem Ausgabeplatz wird ein DICOM-C-MOVE-Befehl für dieses einzelne Bild an das PACS gesendet („moveImage“-Transition).

3. Falls dieser C-MOVE-Befehl erfolgreich war, wird das Token auf den finalen Ausgabeplatz geschoben, andernfalls geht es zurück zur Bildübertragungs-Transition („retryImage“-Transition).

Abläufe auf Serienbasis

Der Ablauf auf Serienbasis überträgt eine komplette Bildserie mit einem einzigen DICOM-Befehl. Da dabei aber nur ein Gesamtstatus mit der Anzahl der erfolgreich übertragenen Bilder zurückgegeben wird, müssen die Einzelbilder für eine Fehlerüberprüfung noch einmal explizit verifiziert werden.

Die Abbildung 5.17 zeigt zunächst das Petri-Netz der Kommunikation ohne Fehlerkorrektur. Dieser besteht einfach aus dem Senden eines DICOM-C-MOVE-Befehls an das PACS um die entsprechende Bildserie zu übertragen („moveSeries“-Transition). Das Ergebnis dieses Schritts wird dabei nicht weiter überprüft.

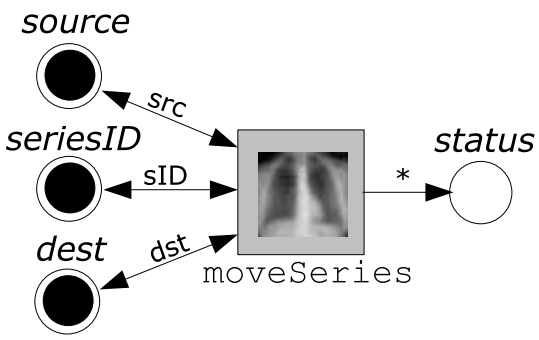


Abbildung 5.17: Petri-Netz-Modell auf Serienbasis ohne Fehlerkorrektur. Alle Bilder werden mit einem einzigen DICOM-Befehl übertragen. Das Ergebnis ist der Gesamtstatus der Übertragungen. Zur besseren Übersicht wurden kleinere Detailschritte in der Darstellung ausgelassen.

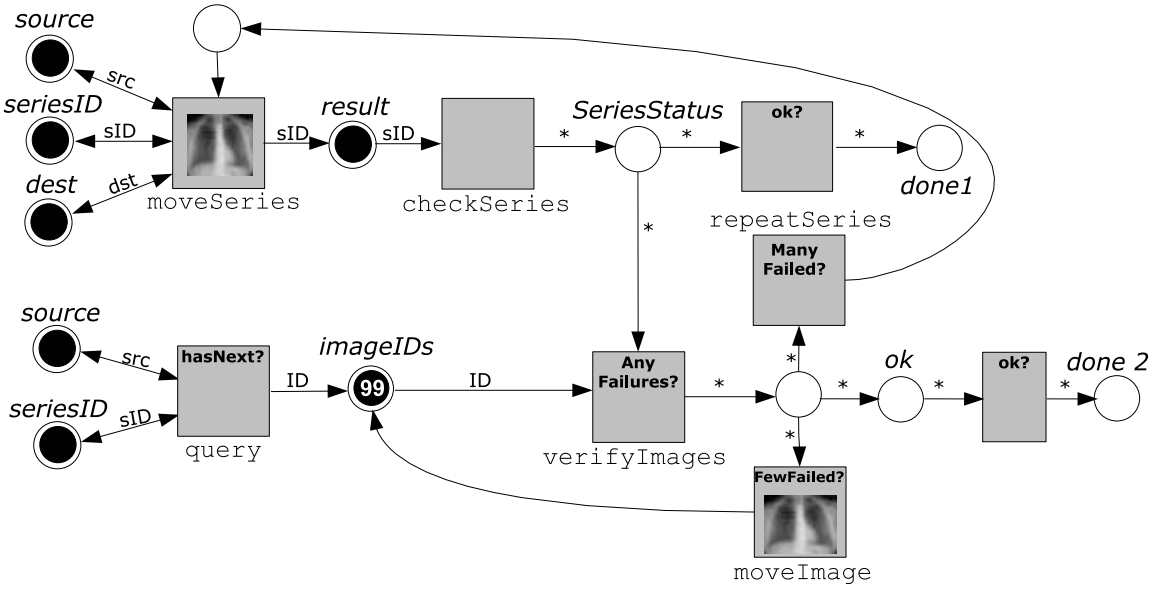


Abbildung 5.18: Petri-Netz-Modell auf Serienbasis mit expliziter Fehlerkorrektur. Alle Bilder werden mit einem einzigen DICOM-Befehl übertragen. Enthält der Gesamtstatus Fehler, werden die empfangenen Bilder im Ziel verifiziert und je nach Anzahl der fehlgeschlagenen Bilder einzeln oder komplett neu übertragen. Zur besseren Übersicht wurden kleinere Detailschritte in der Darstellung ausgelassen.

Das gleiche Netz mit explizit modellierter Fehlerkorrektur zeigt die Abbildung 5.18. Es ist wesentlich komplexer und beinhaltet die folgenden Schritte:

1. Absetzen eines DICOM-C-MOVE-Befehls an das PACS um die entsprechende Bildserie zu übertragen („moveSeries“-Transition). Im Fehlerfall wird dieser Schritt solange wiederholt, bis der Befehl erfolgreich ausgeführt werden konnte oder eine einstellbare Maximalzeit erreicht wurde (beispielsweise 1 Stunde).

2. Parallel zum ersten Schritt wird durch einen DICOM-C-FIND-Befehl an das PACS eine Liste aller Bilder in dieser Serie ermittelt („query“-Transition).

3. Sobald beide Befehle abgearbeitet sind, wird der Status der Gesamtübertragung überprüft („checkSeries“-Transition). Sind nicht alle Bilder erfolgreich übertragen, wird der Verifikations-Webservice auf dem Zielrechner aufgerufen („verifyImages“-Transition). Dieser vergleicht die Bilderliste mit dem persistenten Nachrichten-Log aller eingegangenen Bilder und gibt entweder eine Liste aller fehlenden Bilder zurück oder empfiehlt die komplette Neuübertragung der Serie, falls mehr als die Hälfte der Bilder fehlen.

4. Im Fall der Neuübertragung der Serie („repeatSeries“), startet der Ablauf wieder von vorne. Falls nur einzelne Bilder neu übertragen werden, geschieht dies ähnlich wie beim Ablauf auf Einzelbildbasis („moveImage“-Transition) bis alle Bilder erfolgreich übertragen sind.

5.4.2 Referenzimplementierung und Tests

Mit einer Referenzimplementation ist das beschriebene System prototypisch umgesetzt und getestet geworden. In Analogie zu dem Globus-Transferdienst für allgemeine Dateien, dem „Reliable File Transfer Service“ (RFT) [23], wurde das System ebenfalls als Webservice entwickelt und *Reliable DICOM Transfer Service (RDT)* genannt. Insgesamt besteht es aus den folgenden vier Komponenten (siehe auch Abbildung 5.19):

1. *Die Prozessablauf-Modelle:* Die Basis für die verschiedenen Transfer-Szenarien bilden die vier in GWorkflowDL beschriebenen Petri-Netz-Modelle: zwei einfache Bildserientransfers und zwei fehlertolerante Transfers, jeweils auf Einzelbild- und auf Serienbasis. Die Modelle liegen als abstrakte GWorkflowDL-Muster vor, die für jede Übertragung mit den jeweiligen Eingabedaten zur GWES-Ausführung konkretisiert werden können.

2. *Der RDT-Hauptdienst:* Der RDT-Dienst ist der Haupt-Webservice, der für eine Bildübertragung aufgerufen wird. Ihm werden vier Parameter übergeben: das Quellsystem, das

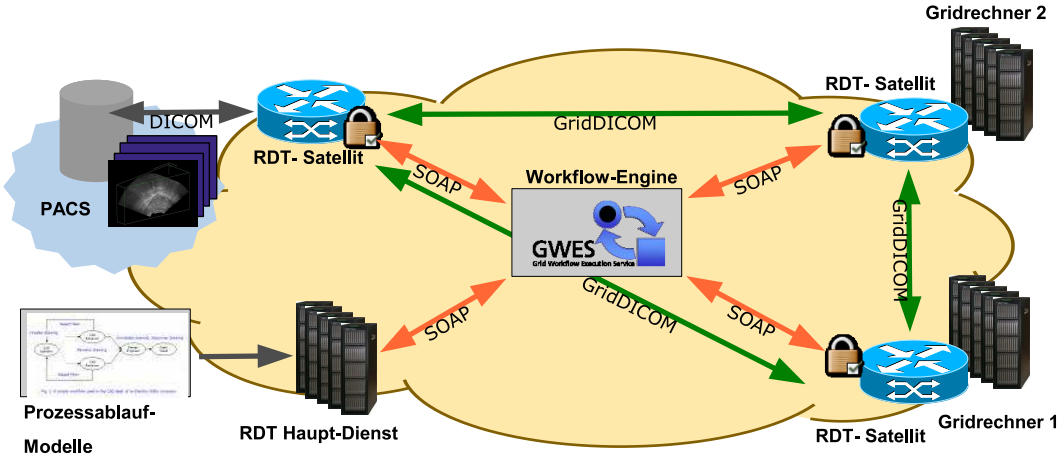


Abbildung 5.19: Aufbau und Komponenten des „Reliable DICOM Transfer“-Dienstes. Soll der Haupt-Dienst eine Bildserie übertragen, erzeugt er eine konkrete Ablaufbeschreibung aus den Vorlagen und sendet diese an die Workflow-Engine GWES, die damit die Übertragung ausführt und steuert. Der GWES kommuniziert mit den RDT-Satelliten-Servern in denen alle nötigen Funktionen bereitgestellt werden.

Zielsystem, die Bild- bzw. Serien-UID und das Transfer-Modellmuster, das benutzt werden soll. Der RDT-Dienst erzeugt dann die konkrete Prozessbeschreibung von dem Muster und übergibt sie an die „Workflow-Engine“ zur Ausführung.

3. *Die „Workflow-Engine“:* Die Prozessbeschreibungen benötigen ein System, welches die Prozesse ausführt und kontrolliert. Hierzu wird der schon beschriebene Java-Webservice GWES eingesetzt und zusammen mit dem RDT-Hauptdienst auf einem zentralen Dienste-Server im Grid betrieben. Die besonderen Vorteile der Webservice-Architektur machen den Betrieb dieses Server skalierbar und jederzeit an wechselnde Belastungen anpassbar. Im Falle eines Systemfehlers besitzt der GWES eine Persistenzschicht, die die aktuellen Prozessbeschreibungen regelmässig in einer Datenbank zwischenspeichert. Zurzeit nutzt der GWES als integrierte Datenbank die ebenfalls frei verfügbare XML-Datenbank eXist [61]. Zwischengespeicherte Übertragungsprozesse werden nach einem Neustart des System wieder vom letzten erfolgreich ausgeführten Zustand aufgenommen.

4. *Die RDT-Satelliten:* Jedes teilnehmende DICOM-Gerät (PACS oder Gridrechner) ist am Grid angeschlossen durch einen *RDT-Satelliten-Server*, oder kurz, *RDT-Satelliten*. Die Funktionalität des Satelliten ist dreifach: Zum einen agiert er als GridDICOM-Router, der das GridDICOM-Protokoll für das angeschlossene DICOM-Gerät umsetzt. Zum zweiten arbeitet er, bei Gridrechnern, als Bildspeicher-Dienst, der DICOM-Bilder annehmen und speichern kann (in DICOM-Sprache, agiert er als „C-STORE StorageClassProvider“). Als solcher ist er mit einer Persistenzschicht erweitert worden, die ein- und ausgehende DICOM-Nachrichten in einer internen Datenbank speichert, die später von einem Dienst

zur Verifikation und für Sicherheitsaudits abgefragt werden können. Zum dritten, implementiert der Server die neu-entwickelten Webservices, die vom GWES als Aktivitäten (siehe unten) bei den Transitionen aufgerufen werden können. Die Satelliten sind in Java 1.5 entwickelt und laufen in dem öffentlich-verfügbaren JBoss-System [59].

5. *Die GWES-Aktivitäten:* Für die entwickelten Modelle wurden die folgenden Funktionen und Dienste, die als Aktivitäten an den Transitionen ausgeführt werden können, identifiziert und implementiert:

   - *GridDICOM-Dienste:* Eine Umsetzung der wichtigsten DICOM-Befehle aus dem Bereich Query/Retrieve und Storage. Dies sind a) C-FIND um ein PACS auf verfügbare Bilder abzufragen, b) C-MOVE um eine von außen gesteuerte Bildübertragung zu veranlassen und c) C-STORE um Bilder auf einem System zu speichern.
   - *Verifikationsdienst:* Ein Webservice, um explizit alle Bilder einer Serie zu verifizieren, die erfolgreich auf einem Zielrechner empfangen wurden. Dieser Dienst überprüft den persistenten DICOM-Nachrichten-Log auf dem Zielsystem. Er gibt entweder eine Liste mit Bildern zurück, die wiederholt werden müssen, oder, falls mehr als die Hälfte der Bilder in der Serie nicht empfangen wurden, empfiehlt die gesamte Serie zu wiederholen. Alternativ hierzu hätte man auch die DICOM-Funktionalität „Instance Availability Notification“, die in der Ergänzung „Supplement 93“ zum DICOM-Standard definiert ist, implementieren können. Ähnlich zum Webservice lassen sich dabei die vorhandenen Bilder einer Serie über DICOM-Anfragen verifizieren. Diese DICOM-Implementierung auf Server-Seite ist aber wesentlich aufwändiger als der Webservice, der daher zunächst vorgezogen wurde. In einer späteren Version ließe sich das System mit dieser Implementation durchaus optimieren.
   - *Konfigurationsdienste:* Ein interner Webservice um spezifische, nicht-standard Konfigurationen auf dem Zielsystem zu konfigurieren (wie beispielsweise benutzerabhängige Dateiverzeichnisse zum Ablegen der Bilder).

Das RDT-Gesamtsystem wurde sowohl in einem isolierten Testgrid als auch in dem produktiven MediGRID-Verbund evaluiert. Das lokale Testgrid besteht aus dem bereits genutzten PACS, einem RDT-System und zwei Gridrechnern, alle bestehend aus Standard-Intel und AMD 32bit und 64bit-Maschinen mit Linux als Betriebssystem und Java JRE 1.5. Die Systeme sind verbunden über ein reguläres 100Mbit Ethernet Class C Netzwerk. Alle Tests wurden mehrfach mit den drei bereits verwendeten MRT-, CT-, und CR-Bildserien durchgeführt und die Ergebnisse gemittelt. Die Tabelle 5.5 zeigt zunächst diese Ergebnisse im lokalen Testgrid. Aufgeführt wird die Dauer der jeweiligen Übertragung in Sekunden von dem direkten GridDICOM-Transfer ohne modellgesteuerte-Unterstützung im Vergleich mit modell-gesteuerten Abläufen

Transfer-Methode	Kein Ausfall			Ausfall 2s			Ausfall 10s		
	CR	CT	MRT	CR	CT	MRT	CR	CT	MRT
Direktes GridDICOM	1.13	5.32	10.4	n/a			n/a		
Modell auf Einzelbildbasis	1.7	30	43.2	6.7	40	46.8	21.3	50.7	66.1
Modell auf Serienbasis	1.4	7.7	13.1	8.1	14.8	27.0	18.4	38.7	51.8
DGIS	5.2	67.3	96	8.4	86	130.6	20.1	98	145

Tabelle 5.5: Ergebnisse der Modell-Vergleichstests im lokalen Testgrid. Im Gegensatz zu den vorherigen Tests wird nicht die Transferrate, sondern die Gesamtdauer der Übertragungen dargestellt.

und der bisher existierenden DGIS-Lösung. Dabei kam die derzeit verfügbare Version der DGIS-Software „Release Candidate 1“ zum Einsatz. Bei den fehlertoleranten Modellen wurden Systemfehler durch zufälliges Abtrennen der empfangenen Gridrechner vom Grid für einmal eine kurze und einmal eine längere Unterbrechung (etwa so lang wie die eigentliche Gesamtlänge der Übertragung) simuliert. Im Unterschied zu den Ergebnissen aus Kapitel 5.1, bei der die Datentransferrate dargestellt wurde, wird hier bewusst die Gesamtzeit der Übertragungen gemessen, da die Transfers sowohl die Auswahlzeiten als auch die Wartezeiten bei den Wiederholungen beinhalten.

Bei den modell-gesteuerten Abläufen wurden sowohl Modelle auf Einzelbild- als auch auf Serienbasis aufgeführt. Dabei zeigten sich die folgenden Beobachtungen:

Direkter GridDICOM-Transfer

Der direkte GridDICOM-Transfer entspricht der manuellen Übertragung ohne Modell-Unterstützung auf Serienbasis aus den früheren Tests der GridDICOM-Router. Diese Form ermöglicht keine explizite Fehlerkorrektur, weshalb die Ausfall-Szenarien hier nicht getestet wurden. Die Transferzeiten unterscheiden sich je nach Art der übermittelten Bildserie und unterscheiden sich hauptsächlich durch die Größe der DICOM-Bilder in der Serie. Die wesentlich größeren CR-Bildserien brauchen mit knapp 10s daher entsprechend länger zur kompletten Übertragung als die kleineren CT- oder MRT-Serien, die in der Hälfte der Zeit und noch weniger übertragen werden. Die relativ hohe Übertragungsgeschwindigkeit liegt an dem isolierten lokalen Netzwerk, das eine wesentlich höhere Bandbreite zulässt als externe, öffentliche Netze.

Modellgestützte Transfers auf Einzelbildbasis

Diese Übertragungen nutzen das GWES-Prozesssystem mit den entwickelten Modellvorlagen auf Einzelbildbasis. In diesen Modellen wird jedes Bild einzeln von dem System übertragen. Dadurch ergeben sich die deutlich höheren Übertragungszeiten, die je nach Bildserien vier oder fünfmal länger dauern als bei der direkten Übertragung. Im Gegensatz dazu erlauben die

Modelle aber eine explizite Fehlerkorrektur. So werden sowohl die kurzzeitigen als auch die langfristigen Ausfälle erfolgreich überwunden und alle Bilder übertragen. Die Übertragungszeiten liegen dafür höher als ohne Fehlerkorrektur. Man beachte allerdings, dass die angegebenen Zeiten die Gesamtübertragungszeiten darstellen, also inklusive der Ausfallzeiten selbst.

Modellgestützte Transfers auf Serienbasis

Diese Übertragungen auf Serienbasis transportieren alle Bilder einer Serie mit einem einzigen GridDICOM-Befehl. Die Übertragungszeiten sind dadurch schneller als bei dem Einzelbild-Modell und nur unwesentlich langsamer als beim direkten GridDICOM-Transfer. Die zusätzlichen Sekunden im Vergleich zu diesem Transfer, kommen durch das Einlesen, Initialisieren und Ausführen der Prozessbeschreibungen zur Steuerung der Übertragungen durch das GWES System. Diese Zeit hängt wesentlich von der Komplexität der Modelle ab und der Anzahl der Datentoken (bzw. Bilder) die ihn durchlaufen. In diesem Test erhöht das RDT-System die Übertragungszeit um etwa 30% im Vergleich zu einem direkten Transfer. Diese relativ hohe Zeit entsteht aber nur einmalig bei der Initialisierung und fällt umso weniger ins Gewicht, je länger die einzelnen Übertragungen dauern. In der produktiven Grid-Umgebung ist sie daher durch die längeren Übertragungszeiten der Bilder in den öffentlichen Netzen fast vernachlässigbar.

Auch in den beiden Ausfall-Szenarien werden alle Bilder durch die explizite Fehlerkorrektur am Ende richtig und vollständig übertragen. Im Vergleich zu den fehlertoleranten Modellen auf Einzelbildbasis, sind die Gesamtübertragungszeiten aber deutlich kürzer, obwohl die Bilder in einem Extraschritt verifiziert werden müssen. Vor allem sieht man dies an dem länger dauernden Ausfall, bei dem die komplette Serie erneut mit einem Serien-basierten GridDICOM-Befehl übertragen wurde.

DGIS-Lösung

Die Ergebnisse der DGIS-Lösung müssen mit Vorsicht interpretiert werden, da sie, genau wie in den vorherigen Tests, sehr stark von der Rechner-Hardware abhängen. Dennoch zeigt sich im direkten Vergleich, dass das DGIS-System in allen Szenarien deutlich längere Transferzeiten als alle anderen Verfahren erzielt. Dies liegt mitunter daran, dass das System nicht auf eine Fehlerkorrektur optimiert ist. So komprimiert es alle Bilder einer Serie zunächst zu einem Archiv, was, abhängig von der Zahl der Bilder und der genutzten Rechner, eine beträchtliche Zeit dauern kann, verglichen zu den schnellen Übertragungszeiten in dem lokalen Grid. Im Fehlerfall wird der gesamte Komprimierungsprozess wiederholt, was ein zweiter Grund für die relativ hohen Zeiten in den Ergebnissen ist. Dennoch überträgt auch die DGIS-Lösung in allen drei Szenarien die Bilder fehlerfrei.

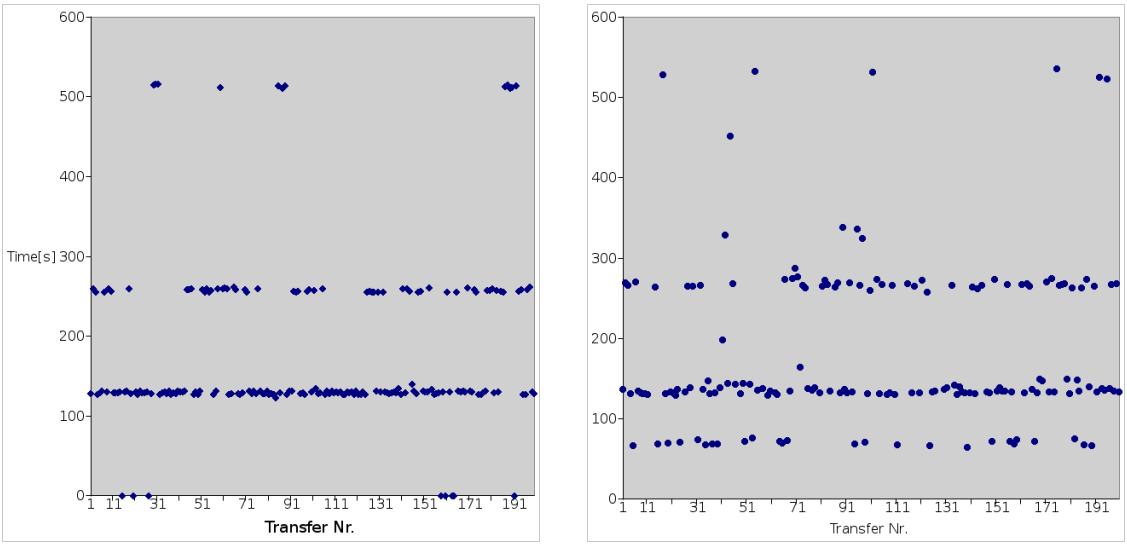


Abbildung 5.20: Ergebnisse der RDT-Tests in der MediGRID-Umgebung nach etwa acht Stunden simulierter Grid-Nutzung. Links die Dauer der einzelnen Übertragungen ohne, rechts mit Fehlerkorrektur. Ein Wert von Null entspricht einem fehlgeschlagenen Transfer.

Tests in der MediGRID-Umgebung

Nach den Vergleichstests wurde das Modell mit den besten Ergebnissen in die Produktivumgebung von MediGRID installiert. Dies ist das Serienbasierte Modell, da es für alle Szenarien die Bilder am effektivsten überträgt. Um die Fehlertoleranz zu evaluieren, wurden acht Stunden typischer Gridnutzung durch wiederholte Übertragung von der 100er CT-Bildserie in 0-4 Sekunden-Intervallen simuliert. Diese Tests wurden sowohl mit dem einfachen als auch mit dem fehlertoleranten Modell ausgeführt und im Anschluss die Fehlerraten verglichen.

Die Abbildung 5.20 zeigt die Transferzeiten von den Tests in der Produktivumgebung des MediGRIDs. Die linke Abbildung zeigt die Übertragungen basierend auf einem Modell ohne Fehlerkorrektur. Ein Wert von Null bedeutet ein fehlgeschlagener Transfer aufgrund eines Systemfehlers. In diesen Tests zeigten sich bei etwa 5-6% der Übertragungen Ausfälle, meistens durch kurzzeitige Überlastung der Dienste. Da alle Tests mit der gleichen Bildserie durchgeführt wurden, unterscheiden sich die Übertragungszeiten untereinander nur wenig. Es zeigt sich aber, dass sie deutlich ansteigen, sobald gleichzeitige Übertragungen von mehreren Bildserien stattfinden. Dies erklärt die fast diskreten „Sprünge“ bei bis zu vier verschiedenen gleichzeitigen Übertragungen. Die rechte Abbildung zeigt die Ergebnisse des gleichen Tests mit den fehlertoleranten Modellen. Im Durchschnitt brauchen einzelne Transfers länger, aber die Ergebnisse zeigen, dass keine Übertragungen mehr fehlgeschlagen sind. Allerdings haben vier Transfers effektiv länger als zehn Minuten gedauert durch einen längeren Ausfall des PACS. Diese sind aus Übersichtsgründen nicht in der Grafik enthalten. Die Ergebnisse verdeutlichen auch einen interessanten Kompensierungseffekt: Übertragungen, die fehlschlugen, enthalten Fehlerwarteschleifen, bevor sie den Transfer wiederholen. Durch diese länger

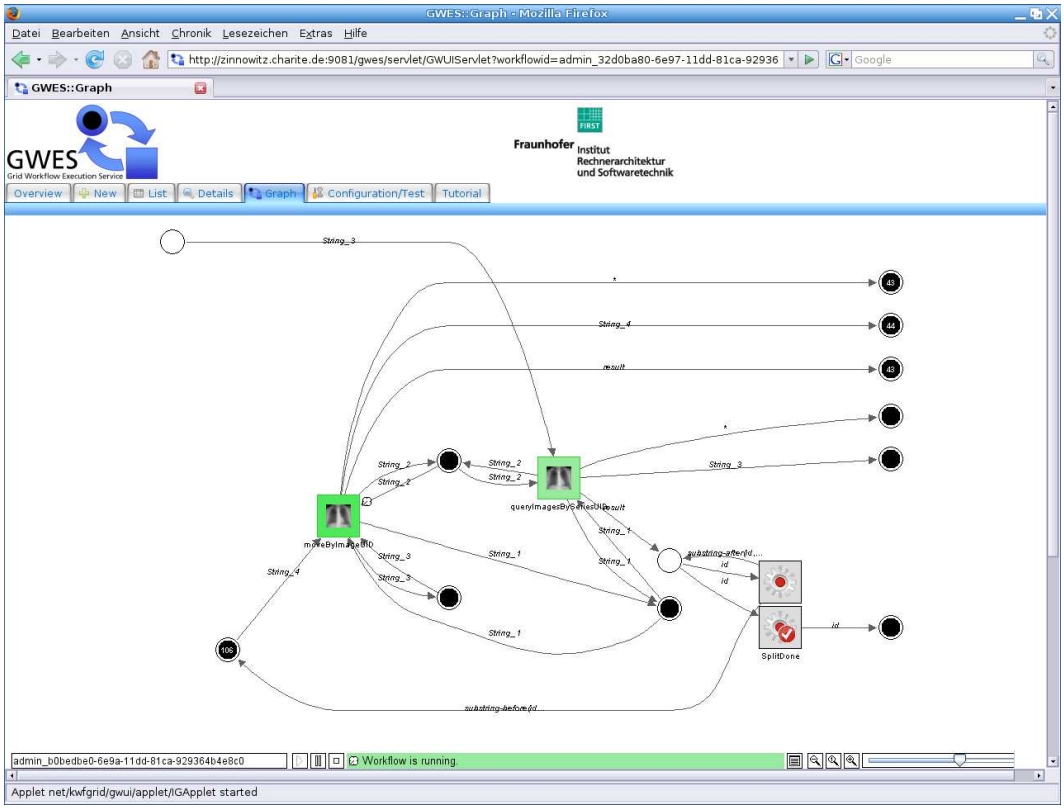


Abbildung 5.21: Bildschirmfoto der Echtzeit-Visualisierung einer Bildübertragung mit dem RDT in der webbasierten GWES-Benutzeroberfläche. Sofern gewollt, kann der Benutzer hier zu jeder Zeit den Status der Übertragungen verfolgen.

abwartenden Prozesse, reduziert sich teilweise die Gesamtlast auf das System, wodurch einzelne Übertragungen teilweise wiederum schneller durchliefen als in den nicht-fehlertoleranten Tests mit gleichmäßiger Verteilung.

Zusammenfassend kann man sagen, dass die Serien-basierten Modelle wesentlich effektiver übertragen für alle Szenarien. Die Verwendung der Modelle mit expliziter Fehlerkorrektur verlängert zwar die Transferzeit, überbrückt aber auch die Systemausfälle und ermöglicht eine zuverlässige Bildübertragung. Falls gewünscht, kann der Benutzer den Status und die Ergebnisse der Übertragung durch den Zustand des gekoppelten Petri-Netz-Modells durch die webbasierte Echtzeit-Visualisierung des GWES überprüfen. Abbildung 5.21 zeigt ein Bildschirmfoto für eine Beispielübertragung.

Kapitel 6

Diskussion

Das Ziel der vorliegenden Arbeit war ein effizientes und sicheres Verfahren zur DICOM-Bildübertragung in medizinischen Grid-Infrastrukturen. Die Grundlage dieses Verfahrens bildet dabei eine durchgängige DICOM-Kommunikation nach dem in Grids genutzten Sicherheitsstandard GSI. Darauf aufbauend ermöglichen Software-Router, die herkömmlichen, bereits verfügbaren DICOM-Geräte ohne weitere Änderungen an das Grid anzuschließen. Ein dritter, wesentlicher Bestandteil bilden zusätzliche Sicherheitsmaßnahmen zum Schutz patientenbezogener Daten auf den Gridrechnern sowie zur sicheren Anbindung klinikinterner Bildarchive an die öffentliche Infrastruktur. Schließlich werden die besonderen Vorteile dieser drei Methoden genutzt, um ein modell-basiertes System zu entwickeln, welches Bildserien im Grid automatisiert und übertragen kann. Dabei kann es auf Fehler und Systemausfälle im Grid selbständig reagieren und somit eine erfolgreiche und zuverlässige Bildübertragung garantieren. Das vorhergehende Kapitel beschreibt die entwickelten Verfahren und die Ergebnisse der jeweiligen Referenzimplementation zur Validierung. Im Folgenden werden diese Ergebnisse gewertet und mit ihren Vor- und Nachteilen diskutiert.

6.1 Durchgängige DICOM-Kommunikation

Die Ergebnisse der Referenzimplementation bestätigen die folgenden Vorteile der entwickelten, durchgehenden DICOM-Kommunikation über die bisher verfügbaren Verfahren:

- Schaffung einer transparenten, ununterbrochenen DICOM-Kommunikation zwischen den verschiedenen Anwendungen in einem Grid.
- Volle Integration der Grid-Sicherheits-Infrastruktur: Die Adaption an den GSI-Standard erlaubt die Verschlüsselung, Nachrichten-Integrität, gegenseitige Authentifizierung der

Benutzer und Systeme, die Autorisierung für lokale Zugriffsrechte und sogar die Weiterleitung autorisierter Benutzer zu weiteren Gridsystemen oder für Übertragungen im Drittauftrag.

- Kein Bilder-Export: DICOM-Objekte müssen nicht auf der Festplatte zwischengespeichert werden. Das Zwischenspeichern birgt ein mögliches Sicherheitsrisiko und mindert die Übertragungsleistung durch die involvierten Schreib- und Leseoperationen auf der Festplatte.

- Erhalt des asynchronen DICOM-Kommunikationsprotokolls: Komplexe Operationen, wie die Übertragung einer großen Anzahl von Bildern, können fehlschlagen oder unterbrochen werden, ohne dass der gesamte Übertragungsprozess fehlschlägt.

- Firewall-freundlich: die Systeme brauchen nur einen freigegebenen Zugang auf den Firewalls. Dies ist wesentlich einfacher zu administrieren als bei dem bisher verwendeten Protokoll „GridFTP“, dem eine ganze Bandbreite auf der Firewall freigeschaltet werden muss.

Im dem vorgestellten Vergleich zeigt sich eine klare Überlegenheit in den Transferraten der neuen Methoden gegenüber der bisher verfügbaren DGIS-Lösung. Allerdings muss man anmerken, dass die Übertragungsgeschwindigkeit des DGIS-Systems niedriger gemessen wurde als von Erberich et al. bei ihren eigenen Tests in [7] veröffentlicht. Der Unterschied liegt zum einen daran, dass die unterschiedliche Vernetzung der Gridrechner einen großen Einfluss auf die Übertragungsgeschwindigkeit hat. Zum anderen, komprimiert der DGIS die Bilder vor der Übertragung. Die Software-Kompression ist eine Operation, die sehr von der verwendeten Rechner-Hardware abhängt. In den Tests wurden, wie beschrieben, Standard-Arbeitsplatzrechner benutzt, was die Kompression deutlich verlangsamen und so zu niedrigeren Geschwindigkeiten führen kann.

Nachteilig bei der vorgestellten Lösung ist die Tatsache, dass für den eigentlichen Grid-Datentransport nicht auf bereits vorhandene, standardisierte Dienste zurückgegriffen werden kann, wie beispielsweise „GridFTP“ beim DGIS. Auch müssen die Anwendungen explizit das neue Sicherheitsprofil implementieren, um damit kommunizieren zu können. Eine Anpassung ist aber oft gerade auch bei älteren Systemen entweder nicht möglich oder zu teuer, weshalb es zusätzlicher Lösungen bedarf um diese Systeme zu integrieren.

6.2 Integration von vorhandenen DICOM-kompatiblen Systemen

Mit der entwickelten Methode der DICOM-Router können beliebige, auch ältere, DICOM-kompatible Systeme erfolgreich in das Grid integriert werden, ohne dass Änderungen an diesen Systemen vorgenommen werden müssen. Die Funktionstests der beiden Router zeigen, dass die geforderte Funktionalität mit beiden Systemarchitekturen gleichermaßen gut erreicht wird. Die Router übertragen alle DICOM-Nachrichten und -Bilder fehlerfrei vom Gerät zum Grid und umgekehrt.

Im Vergleich zu der direkten GridDICOM-Übertragung reduzieren beide Router die Transferrate allerdings deutlich. Dennoch bieten die Router eine ähnliche Übertragungsleistung wie die bereits existierende Lösung DGIS aus dem MEDICUS-Projekt. Zusätzlich bieten sie aber die folgenden Vorteile:

1. Datenzugriff: Da die Router die Daten nicht auf der Netzwerk- sondern auf der Anwendungsebene routen, bieten sie bei der Verarbeitung den vollen und detaillierten Zugriff auf die DICOM-Daten. Diese können dadurch beim Durchlauf verifiziert, auf Zugriffsrechte überprüft oder sogar verändert werden. Hackländer et al. [62] schlagen beispielsweise mit einem ähnlichen Konzept für herkömmliche Netzwerke eine transparente Verarbeitungskette von DICOM-Objekten vor, um diese zu Anonymisieren oder Korrekturmaßnahmen zu unterziehen.

2. Weitere Funktionen: Das bei der modularen Version verwendete J2EE-Kontrollsystem ermöglicht es, den Anwendungsbereich der Router flexibel zu erweitern. So wurden die Router zusätzlich mit einer Persistenzschicht ausgestattet, die alle durchlaufenden DICOM-Nachrichten in einer Datenbank persistent speichert. Dadurch kann bei späteren Sicherheitsaudits jeglicher Datenverkehr genau nachvollzogen werden.

Im Vergleich der beiden Architekturen zeigt sich, dass die klassische, monolithische Architektur etwas schneller arbeitet, jedoch bei stärkerer Belastung schlechter skaliert als die modulare. Damit ist sie für hohe Anforderungen einer Produktivumgebung nicht geeignet, weil nicht einschätzbar ist, wann sie überlastet ist. Die modulare Architektur dagegen kann jederzeit an wachsende Belastungen angepasst werden, weshalb sie im Sinne einer zuverlässigen und effizienten Bildübertragung vorzuziehen ist. Dabei können die Module sogar auf mehrere Rechner („Cluster“) verteilt werden, sodass die Kapazitäten im Leistungsbereich lediglich durch die verwendete Hardware eingeschränkt wird. Zwar wäre es theoretisch auch möglich, solch einen Cluster aus mehreren monolithischen Systemen zu bilden, jedoch könnten diese

Systeme im Unterschied zu den Modulen dann nicht untereinander kommunizieren. Dies verhindert wesentliche Leistungsmerkmale, wie beispielsweise die Weiterleitung der Zertifikate untereinander, die für die Gridnutzung notwendig ist.

Ein Nachteil der modularen Systeme ist, dass sie ein aufwändigeres Kontrollsystem benötigen. Diese sind aber durch die Verwendung der JMX- und J2EE-Technologien standardisiert, was die Administration im Allgemeinen erleichtert und die Verwendung für viele, verschiedene Anwendungen möglich macht. Die monolithischen Systeme sind weniger komplex, bedürfen dagegen aber immer einer eigenen, angepassten Installation und Administration.

Insgesamt lässt sich feststellen, dass die modulare Architektur basierend auf dem MBean- und J2EE-Standard für die Aufgabe eines hochperformanten GridDICOM-Routers, wie er in Grid-Infrastrukturen benötigt wird, wesentlich besser geeignet ist. Zu Testzwecken oder Grid-Strukturen, die weniger stark beansprucht werden, ist die herkömmliche Architektur ausreichend.

6.3 Zusätzliche Sicherheitsmaßnahmen

Bei der Umsetzung des Konzepts für die zusätzlichen Sicherheitsmaßnahmen ergibt sich ein deutlicher Vorteil des neuen Verfahrens „SecureDICOM“ gegenüber der bisher angewandten ALC. Die Auswertung der Bilder auf den Gridrechnern nach der Pseudonymisierung ergab, dass die personenbezogenen Daten entsprechend den Vorschriften pseudonymisiert und verschlüsselt wurden. Gleichzeitig konnten die Anwendungen auf den Gridrechnern einzelne Attribute nach wie vor referenzieren und in die neu erzeugten Bilder übertragen, ohne diese entschlüsseln zu müssen. Damit konnten die berechneten Bilder nach der Reidentifikation problemlos den Originalbildern im klinikinternen PACS wieder zugeordnet werden. Dies wäre nach den herkömmlichen Verfahren nicht möglich gewesen und bringt gerade im Bereich der Bearbeitung in Grid-Infrastrukturen einen deutlichen Vorteil.

Als nachteilig zeigt sich, dass das neue Verfahren durch das Anhängen der verschlüsselten Sequenz die Datenmenge im Vergleich zu ALC-Bildern leicht erhöht. Dieser Zuwachs ist aber, gerade bei größeren Bildern, im Vergleich mit der Größe der Pixeldaten, vernachlässigbar.

Die Anbindung des Klinik-internen PACS durch eine manuelle Übertragung der Bilder zu einem externen PACS bei gleichzeitiger Pseudonymisierung, erweist sich als eine praktikable Lösung. Zwar bedeutet dieser Zwischenschritt für den Benutzer einen erhöhten Aufwand bei der Arbeit mit der Grid-Infrastruktur, jedoch ist es aus Gründen der Sicherheit in den allermeisten Kliniken die einzig mögliche Anbindung des internen Bildarchivs. Durch die integrierte, webbasierte Benutzeroberfläche wird dem Benutzer zusätzlich eine einfache und intuitive

Möglichkeit geschaffen, sein Bildmaterial auszuwählen, zu pseudonymisieren und auf dem Grid zu bearbeiten.

6.4 Fehlertoleranz und Zuverlässigkeit

Die Ergebnisse zeigen, dass sich der Ansatz, die Kommunikation durch ein Petri-Netz zu modellieren, dieses an das reale Grid zu koppeln und dadurch einem automatischen System die Steuerung zu ermöglichen, als sehr erfolgreich erweist. Bei der Modellierung stellte sich der ursprüngliche Ansatz, die komplette Grid-Umgebung mit einem einzigen Petri-Netz abzubilden, durch die abzusehende hohe Komplexität der Netze als nicht praktikabel heraus. Jedoch boten die transferbasierten Modelle eine effektive Möglichkeit, selbst komplexe Fehlerstrategien flexibel umzusetzen. So können verschiedene Methoden der Fehlerkorrekturen für die unterschiedlichen Anforderungen durch einfache Änderungen an den zu Grunde liegenden Modellen umgesetzt werden. Ein Nachteil der transferbasierten Modelle ist, dass die Visualisierung des Gesamtgrids nicht mehr möglich ist.

Im Vergleich der unterschiedlichen Modelle zeigen sich deutliche Vorteile bei der Übertragung auf Serienbasis. Gerade bei einem Einsatz von den DICOM-Routern, die jede Nachricht noch einmal verarbeiten, zahlen sich Modelle mit möglichst geringer Nachrichtenanzahl aus. Als Nachteil verliert man dabei die feine Kontrolle über den Übertragungsstatus und benötigt zusätzliche Verifikationen der Bilder. Dies erhöht die Komplexität des Systems, auch wenn es sich in der Gesamtübertragung als schneller im Vergleich zu den Einzelbild-Modellen herausgestellt hat.

Im Vergleich zum direkten Transfer ohne Modell-Unterstützung braucht das RDT-System länger für die Übertragungen. Das Gesamtkonzept bietet jedoch gegenüber der manuellen Übertragung mehrere Vorteile:

- Automatisierung: Systeme, die prozess-orientierte Modelle als Basis nehmen, um die Kommunikation zu steuern, können selbständig und ohne Benutzerinteraktion auf Fehler reagieren und zuverlässig Bildserien übertragen.
- Flexibilität: Der Ansatz, die Petri-Netz-Modelle zur Steuerung zu verwenden, macht das System äußerst flexibel für die unterschiedlichen Anforderungen der medizinischen Anwendungen. Um unterschiedliche Übertragungsverfahren zu verwenden, müssen nur die Modell-Vorlagen ausgetauscht werden.
- Standardisierung: Das Verfahren setzt auf offene Standards wie Web-Services und Petri-Netze. Dadurch sind einzelne Komponenten, wie das GWES System, austauschbar ge-

gen andere, vergleichbare Systeme, die möglicherweise bereits installiert sind.

Als Nachteil dieses Verfahrens ist zu verzeichnen, dass das Gesamtsystem relativ aufwändig und komplex ist. In der Praxis gibt es Anwendungen, deren Ansprüche an eine fehlertolerante Bildübertragung diesen Aufwand eventuell nicht rechtfertigen. So macht es sicherlich keinen Sinn, eine einfache Bildübertragung ohne Fehlertoleranz für eine wissenschaftliche Anwendung mit diesem modellgestützten Verfahren umzusetzen. Wie in der Einleitung aber schon beschrieben, setzen viele klinische Anwendungen eine zuverlässige Datenübertragung voraus. Bei diesen Anwendungen ist der zusätzliche Aufwand für ein solches System gerechtfertigt.

6.5 Gesamtsystem

In abschließender Betrachtung der Ergebnisse lässt sich feststellen, dass die entwickelten Verfahren in der Kombination einen zuverlässigen und sicheren Datentransfer in medizinischen Healthgrids ermöglichen. Dieser Transfer ist in vielen Punkten den bisherigen Methoden überlegen:

- Er bietet mehr Anwendungsmöglichkeiten durch die direkte und durchgängige DICOM-Kommunikation zwischen allen DICOM-kompatiblen Geräten.
- Er ermöglicht das Arbeiten mit Bilddaten aus klinikinternen Archiven.
- Er ist sicherer, da grundsätzlich weniger Daten zwischengespeichert werden.
- Durch den Einsatz von Modellen ist er flexibel an die unterschiedlichen Anforderungen anpassbar, vom einfachen Transport bis zu ausfallsicheren Übertragungen.

Nachteilig wirkt sich aus, dass die Verfahren aufwändiger sind als die Nutzung bereits verfügbarer, standardisierter Methoden. Durch die konsequente Umsetzung offener Standards bei der Entwicklung der Verfahren und die Veröffentlichung der Referenzimplementationen wurde allerdings auf eine möglichst einfache, künftige Integrationsfähigkeit in die vorhandene Globus-Middleware geachtet. Mit der zuverlässigen Bildübertragung steigen die Möglichkeiten eines Einsatzes von Grid-Infrastrukturen in der Medizin in der Zukunft deutlich.

Kapitel 7

Zusammenfassung

Der gemeinsame Zugriff auf verteilte Datenbanken und die Möglichkeit zur Kooperation ist für die Verbundforschung in der Medizin von zunehmender Wichtigkeit. Auch spielen bildgebende Verfahren eine immer größere Rolle. Der Einsatz von 3D- und 4D-Techniken sowie die kontinuierliche Verbesserung der räumlichen und zeitlichen Auflösung stellen immer höhere Anforderungen an die digitale Bildverarbeitung, vor allem an Speicherplatz und Rechenleistung. Ein Lösungsansatz zur Erfüllung dieser Anforderungen ist der Einsatz von „Grid-Infrastrukturen“. Dies sind neuartige Strukturen bei der Vernetzung von Informationssystemen. Dabei werden viele räumlich verteilte Rechner zu einem virtuellen Großcomputer zusammengeschlossen. Im Unterschied zu anderen Forschungsbereichen, in denen diese Technologie bereits seit langem genutzt wird, erfordert der Einsatz in der Medizin zusätzliche Maßnahmen. Dies liegt unter anderem an den sensiblen Daten, die hohe Sicherheitsanforderungen an Datentransfer und Kommunikationswege stellen. Die Folge ist, dass der bisherige de facto Standard zur Bildübertragung, DICOM, allein nicht mehr ausreicht.

Das Ziel dieser Arbeit war es daher, ein möglichst effizientes und sicheres Verfahren zur DICOM-Bildübertragung in medizinischen Grid-Infrastrukturen zu entwickeln. Die Grundlage dieses Verfahrens bildet dabei die durchgängige DICOM-Kommunikation nach dem in Grids genutzten Sicherheitsstandard GSI. Gegenüber den bisherigen Verfahren hat dies den Vorteil, dass die grundlegenden Eigenschaften des DICOM-Protokolls erhalten bleiben. Dazu wurden die notwendigen Anpassungen an das bestehende DICOM-Protokoll definiert und im Rahmen eines zusätzlichen Profils Standard-konform festgehalten. Mit einer Referenzimplementation, die das neue Profil prototypisch umsetzt, ist das Verfahren erfolgreich in Zusammenhang mit dem Charité-Projekt „3D Ultraschall Prostatabiopsien“ in MediGRID, der Grid-Infrastruktur für die Medizin und Lebenswissenschaften in Deutschland, getestet worden.

Zusätzlich ermöglichen Software-Router, die herkömmlichen, bereits verfügbaren DICOM-

Geräte ohne weitere Änderungen an das Grid anzuschließen. Dazu wurden zwei verschiedene Architekturen, ein herkömmlicher, monolithischer und ein moderner, modularer Aufbau, für die Router-Systeme entwickelt und auf einen möglichst praxistauglichen Einsatz hin untersucht. Es zeigte sich, dass beide Lösungsansätze funktionell erfolgreich die DICOM-Geräte anbinden können, jedoch nur das System, mit einem modernen, modularen Aufbau, den Ansprüchen einer praxisnahen Belastung gewachsen ist.

Ein dritter, wesentlicher Bestandteil der Arbeit bilden zusätzliche Sicherheitsmaßnahmen zum Schutz patientenbezogener Daten auf den Gridrechnern sowie zur sicheren Anbindung klinikinterner Bildarchive an die öffentliche Infrastruktur. Dazu wurden erfolgreich der Einsatz einer neuen, noch nicht im DICOM-Standard verabschiedeten Pseudonymisierungstechnik untersucht, die den Zugriff auf einzelne Daten in den Bildern erlaubt, ohne diese auf den fremden Rechnern entschlüsseln zu müssen. Gleichzeitig wurde ein Konzept entwickelt und erfolgreich evaluiert, bei dem der Zugriff auf das klinikinterne PACS durch einen manuellen Bildtransfer in ein temporäres Grid-PACS unter gleichzeitiger Verschlüsselung ermöglicht wird.

Schließlich wurden die besonderen Vorteile dieser drei entwickelten Übertragungsverfahren genutzt, um ein modellbasiertes System zu entwickeln, welches Bildserien automatisiert im Grid übertragen kann. Dabei kann es auf Fehler und Systemausfälle im Grid selbständig reagieren und somit eine erfolgreiche und zuverlässige Bildübertragung garantieren. Verschiedene Modelle auf Einzelbild- und auf Serienbasis, jeweils mit und ohne Fehlerkorrektur, wurden entwickelt und mit einer Referenzimplementierung des Systems in ihrer Leistung verglichen. Die erfolgreichsten Modelle ergaben bessere Übertragungszeiten als bisher existierenden Lösungen und boten gleichzeitig die Möglichkeit einer erfolgreichen, flexiblen Fehlerkorrektur bei Systemausfällen.

Damit stellt die Arbeit neue Verfahren vor, die eine zuverlässigere, schnellere und sichere Bildübertragung in Grid-Infrastrukturen ermöglichen, als die bisher verfügbaren Methoden es boten. Mithilfe dieser Verfahren steigt die Zuverlässigkeit von Grid-Systemen in der medizinischen Bildverarbeitung deutlich und ermöglicht so einen Einsatz in der klinischen Routine.

Glossar

Attribute
Daten in einem DICOM-Bild, wie beispielsweise Patientenname.

Authentifikation
Feststellung der Identität gegenüber einem anderen Teilnehmer.

Autorisierung
Feststellung der Rechte eines Teilnehmers.

CERN
Conseil Européen pour la Recherche Nucléaire. Kernforschungszentrum in Genf mit dem weltgrößten Teilchenbeschleuniger.

Certificate Authority
Eine Organisation, die Zertifikate ausstellt und für sie bürgt.

Client
Bei einer Netzwerkverbindung ist ein Client derjenige Teilnehmer, der die Verbindungen mit einer Anfrage eröffnet.

Integrität
Sicherstellung, dass Daten nicht geändert wurden.

Nutzer-Zertifikat
Ein Zertifikat für eine natürliche Person.

Server
Ein Server bietet einen Dienst an und wartet auf Anfragen von Klienten.

Server-Zertifikat
Ein Zertifikat von einem Rechnersystem.

Single-Sign-On
Einmalige Identifikation gegenüber mehreren, verschiedenen Systemen.

Verschlüsselung

Sicherstellung, dass vertrauliche Daten nicht von Fremden gelesen werden können.

Webbrowser

Ein Programm zum Ansehen von Web-Inhalten, bzw. Webseiten, die von einem Webserver angeboten werden.

Webserver

Ein Webserver bietet Web-Inhalte zum Ansehen mit einem Webbrowser an.

Webservice

Synonym für einen standardisierten, Internet-basierten Informationsdienst, der automatisiert von Programmen aufgerufen werden kann.

X.509

Standard für Zertifikate.

Abkürzungsverzeichnis

AET	Application Entity Title
ALC	Attribute Level Confidentiality
caBIG	Cancer Biomedical Informatics Grid
CR	Computed Radiography
CT	Computed Tomography
DGIS	Dicom Globus Interface Service
DICOM	Digital Imaging and Communication in Medicine
DMZ	Demilitarized Zone
EGEE	Enabling Grids for E-Science
FIRST	Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik
GSI	Globus Security Interface
GSS	Generic Security Standard
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HLPN	High-Level Petri-Netz
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISCL	Integrated Secure Communication Layer
J2EE	Java2 Enterprise Edition

LCG	LHC Computing Grid
LHC	Large Hadron Collider
MDM	Medical Data Manger
MEDICUS	Medical Imaging and Computing for Unified Information Sharing
MRT	Magnetic Resonance Tomography
OFFIS	Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und -Systeme
OSI	Open Systems Interconnection
PACS	Picture Archiving and Communication System
PKI	Publik-Key-Infrastruktur
RFT	Reliable File Transfer
SAAS	Software as a Service
SOA	Service Oriented Architectur
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	Unique Identification
VOMRS	Virtual Organization Management Registration Service
WSRF	Webservice Resource Framework

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A

Das GridDICOM-Sicherheitsprofil

Sicherheitsrelevante Protokolle

Die Tabelle A.1 legt die nötigen Protokolle und Mechanismen fest, die derzeit für einen erfolgreichen Verbindungsaufbau nach dem GSI implementiert sein müssen [14]. Dabei müssen von einer Anwendung nicht notwendigerweise **alle** Funktionen unterstützen werden. Die Konformität einer Anwendung zu dem Profil muss in dem jede Anwendung begleitenden „DICOM Conformance Statement“ erläutert werden.

Erläuterungen

Die Teilnehmer-Authentifikation erfolgt über RSA-Zertifikate nach dem X.509-Standard. Dies erfordert eine gültige PKI-Infrastruktur aus Zertifikaten, anerkannter Organisationen („Certificate Authorities“) zur Ausstellung und Signierung der Zertifikate sowie täglich aktualisierte „Certificate Revocation Lists“ mit einer Auflistung ungültig gewordener Zertifikate. Im Unterschied zu bisherigen Verfahren wie beispielsweise TLS, erfolgt die Authentifikation immer für

Unterstützte GSI-Funktion	Minimaler Mechanismus
Teilnehmer Authentifikation	RSA Zertifikate nach X.509 Standard
Teilnehmer Autorisierung	„GridMap“-Datei
Weiterleitung (Delegation)	X.509 Proxy Zertifikatserweiterung, wie in [55] definiert
Verschlüsselung	Triple DES EDE, wie bei TLS 1.0
Austausch der Session-Schlüssel	RSA, wie bei TLS
Integrität	SHA, wie bei TLS

Tabelle A.1: Minimale Mechanismen zur Unterstützung des GSI-Profils

Status	Bedeutung
11	GSI-Authentifizierung fehlgeschlagen: Serverzertifikat entspricht nicht dem Hostnamen
12	GSI-Authentifizierung fehlgeschlagen: Allgemeiner Zertifikatsfehler des Proxy-Zertifikats
13	GSI-Autorisierung fehlgeschlagen: DN nicht in GridMap-Datei gefunden

Tabelle A.2: Status Codes für das „Reason“-Attribut in der ASSOCIATE-RJ Antwort.

beide Teilnehmer. Bei Zertifikaten für einen Rechner müssen die Namen in den Zertifikaten mit dem Hostnamen übereinstimmen. Zertifikate für Personen müssen in der “GridMap“-Datei eingetragen sein:

Die Teilnehmer-Autorisierung erfolgt serverseitig durch die systemweite „GridMap“-Datei. Diese bildet die Zertifikate auf lokale Benutzer des Systems mit entsprechenden Zugriffsrechten ab. Das Profil gibt keine Vorgaben, wie diese Zugriffsrechte von der Anwendung zu benutzen sind.

Die Weiterleitung (Delegation) ist eine wesentliche Eigenschaft der Gridnutzung zur Verteilung von Anfragen auf mehrere Systeme ohne erneute Authentifizierung. GSI nutzt dafür den Proxy-Mechanismus [55], eine Erweiterung zum X.509 Standard. Die Weiterleitung von authentifizierten Zertifikaten beim Verbindungsaufbau ist optional. Sofern sie nicht stattfindet, kann die Kommunikation allerdings nur mit dem einen Teilnehmer stattfinden.

Die Verschlüsselung und Sicherstellung der Datenintegrität erfolgt über den Einsatz des TLS 1.0 Protokolls, beschränkt sich aber im Gegensatz zum gesamten Protokoll auf den Verschlüsselungs-Algorithmus „Triple DES EDE“.

Ports

Die „IP Ports“, also Adressen, auf den denen ein Server Verbindungen akzeptiert, sind frei wählbar, sollen aber im „Conformance Statement“ festgelegt werden. Die festgelegten Ports sollen sich deutlich von anderen sicheren oder unsicheren Transport-Profilen unterscheiden. Bewährt hat sich als registrierter Standard-Port die „2105“ mit dem Dienste-Namen „dicom-gsi“.

Erfolg- und Fehlerbehandlung

Nachdem erfolgreich eine Verbindung nach dem GSI-Connection-Profil aufgebaut wurde, kann die übergeordnete Anwendung mit dem regulären Nachrichtenaustausch wie im Standard definiert, über den gesicherten Kanal fortfahren.

Bei Fehlern in der initialen Verbindungsphase des TLS-Handshake sollte die Verbindung abgebrochen werden. Bei grundsätzlich erfolgreichem Aufbau einer TLS-Verbindung aber Fehlern in der zusätzlichen GSI-Authentifizierungs oder -Autorisierung soll die Verbindung abgebrochen werden, aber die Anwendung sollte veranlassen einen „A-ABORT“-Status mit einem GSI-spezifischen Fehlercode anzugeben. Tabelle A.2 listet die vorgeschlagenen Status-Codes.

Literaturverzeichnis

[1] Ian Foster, Carl Kesselman, and Steven Tuecke. The anatomy of the grid: Enabling scalable virtual organizations. *Int. J. High Perform. Comput. Appl.*, 15(3):200–222, 2001.

[2] F. Berman, G.C. Fox, and A.J.G. Hey, editors. *Grid-Computing: Making the Global Infrastructure a Reality*. Wiley, 2003.

[3] I. Foster and C. Kesselman, editors. *The Grid 2: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann, California, 2003.

[4] Salvator Roberto Amendolia, Florida Estrella, C del Frate, J Galvez, Waseem Hassan, Tamas Hauer, David Manset, Richard McClatchey, M. Odeh, Dmitry Rogulin, Tony Solomonides, and R Warren. Deployment of a grid-based medical imaging application. In *Studies in Health Technology & Informatics*, pages 59–69, 2005.

[5] H.E. Krüger-Brand. World Community Grid unterstützt Aids-Forschung. *Dtsch Arztebl*, 102(50):A–3529 / B–2984, 2005.

[6] Andrew C. von Eschenbach and Kenneth Buetow. Cancer Informatics Vision: caBIG. *Cancer Informatics*, 2:24–26, Feb 2006. http://cabig.nci.nih.gov.

[7] S.G. Erberich, M. Bhandekar, A. Chervenak, and C. Kesselman. DICOM grid interface service for clinical and research PACS: a globus toolkit web service for medical data grids. *International Journal of Computer Assisted Radiology and Surgery*, 1(7):87–105, June 2006.

[8] Christophe Blanchet, Christophe Combet, and Gilbert Deléage. Integrating Bioinformatics Resources on the EGEE Grid Platform. In *Sixth IEEE International Symposium on Cluster Computing and the Grid Workshops (CCGRIDW'06)*, page 48, 2006. http://www.eu-egee.org.

[9] Wolfgang Gentzsch. D-Grid, an E-Science Framework for German Scientists. In *Proceedings of The Fifth International Symposium on Parallel and Distributed Computing (ISPDC'06)*, pages 12–13, July 2006. http://www.d-grid.de.

[10] Dagmar Krefting, Julian Bart, Kamen Beronov, Olga Dzhimova, Jürgen Falkner, Michael Hartung, Andreas Hoheisel, Tobias A. Knoch, Thomas Lingner, Yassene Mohammed, Kathrin Peter, Erhard Rahm, Ulrich Sax, Dietmar Sommerfeld, Thomas Steinke, Thomas Tolxdorff, Michal Vossberg, Fred Viezens, and Anette Weisbecker. MediGRID: Towards a user friendly secured grid infrastructure. *Future Generation Computer Systems*, 25(3):326–336, March 2009. http://dx.doi.org/10.1016/j.future.2008.05.005.

[11] R. Menday and B. Hagemeier. UNICORE/w3. In *Proceedings of 3rd UNICORE Summit 2007 in conjunction with EuroPar 2007, Rennes, France, LNCS 4854*, pages 72–81, 2007.

[12] E Laure, F Hemmer, F Prelz, S Beco, S Fisher, M Livny, L Guy, M Barroso, P Buncic, Peter Z Kunszt, A Di Meglio, A Aimar, A Edlund, D Groep, F Pacini, M Sgaravatto, and O Mulmo. Middleware for the next generation grid infrastructure. (EGEE-PUB-2004-002):4 p, 2004.

[13] Ian Foster. Globus toolkit version 4: Software for service-oriented systems. In *IFIP International Conference on Network and Parallel Computing*, pages 2–13. Springer-Verlag LNCS 3779, 2005.

[14] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A security architecture for computational grids. In *Proc. 5th ACM Conference on Computer and Communications Security Conference*, pages 83–92, 1998. http://www.globus.org.

[15] Johan Montagnat, Daniel Jouvenot, Christophe Pera, Ákos Frohner, Peter Kunszt, Birger Koblitz, Nuno Santos, and Charles Loomis. Bridging clinical information systems and grid middleware: a medical data manager. In *Proceedings of the HealthGrid conference (HealthGrid'06), Valencia, Spain*, pages 14–24. IOS Press, Jun 2006.

[16] W. D. Bidgood Jr., Steven C. Horii, Fred W. Prior, and Donald E. Van Syckle. Understanding and using DICOM, the data interchange standard for biomedical imaging. *J Am Med Inform Assoc*, 4(3):199–212, 1997.

[17] W. Allcock. GridFTP Protocol Specification (Global Grid Forum Recommendation GFD.20). Technical report, The Globus Alliance, 2003. http://www.globus.org/alliance/datagrid/deliverables/GridFTP-Overview-200201.pdf.

[18] Michael S Wolf and Charles L Bennett. Local perspective of the impact of the HIPAA privacy rule on research. *Cancer*, 106(2):474–479, 2006.

[19] T. Scavo and V.Welch. A grid authorization model for science gateways. *Concurrency and Computation: Practice and Experience*, to appear, 2008.

[20] Y.S. Dai, M. Xie, and K.L. Poh. Reliability analysis of gird computing systems. In *Proc. of the 2002 Pacific Rim Intl. Symp. on Dependable Computing (PRDC'02), Japan*, 2002.

[21] M. Schulz. Realisierung fehlertoleranter workflows in einer service-orientierten grid-architektur, 2007.

[22] T. Kosar, G. Kola, and M. Livny. Building reliable and efficient data transfer and processing pipelines. *Concurrency and Computation: Practice and Experience*, 18(6):609–620, 2006.

[23] W.E. Allcock, I. Foster, and R. Madduri. Reliable data transport: A critical service for the grid. Technical report, Building Service Based Grids Workshop, Global Grid Forum (GGF), June 2004.

[24] V. Breton, A.E. Solomonides, and R.H.McClatchey. A perspective on the Healthgrid initiative. In *4th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid 2004), Chicago, Illinois, USA*, pages 434–439. IEEE Computer Society, 2004.

[25] D. Krefting und B. Haupt und T. Tolxdorff. Segmentation of prostate biopsy needles in transrectal ultrasound images. In *Proc of the 2007 SPIE*, volume 6512, 2007.

[26] D. Krefting und B. Haupt und T. Tolxdorff. Segmentierung von biopsienadeln in transrektalen ultraschallaufnahmen der prostata. In *Bildverarbeitung für die Medizin*, Informatik aktuell, pages 131–135. Springer-Verlag, 2007.

[27] Network Working Group. RFC791 - Internet Protocol. Technical report, IEFT, 1981.

[28] Network Working Group. RFC793 - Transmisstion Control Protocol. Technical report, IEFT, 1981.

[29] Tim Dierks. The TLS Protocol Version 1.2. Technical report, The TLS IETF WG, 2006.

[30] Network Working Group. RFC2616 - Hypertext Transfer Protocol – HTTP/1.1. Technical report, IEFT, 1999.

[31] P. Mildenberger, M. Eichelberg, and E. Martin. Introduction to the DICOM standard. *Eur Radiol*, 12(4):920–927, April 2002.

[32] S. L. Fritz, S. Munjal, J. Connors, and D. Csipo. Implementing a DICOM-HL7 interface application. In R. G. Jost and S. J. Dwyer, editors, *Proc. SPIE Vol. 2435, p. 100-107, Medical Imaging 1995: PACS Design and Evaluation: Engineering and Clinical Issues, R. Gilbert Jost; Samuel J. Dwyer; Eds.*, pages 100–107, May 1995.

[33] K. Kita, T. Nohara, M. Hosoba, M. Yachida, M. Yamaguchi, and N. Ohyama. New secure communication-layer standard for medical image management (ISCL). In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, volume 3662, pages 120–129, July 1999.

[34] R. van Engelen. Pushing the SOAP Envelope with web services for scientific computing. In *Proceedings of the 1 st International Conference on Web-services, Las Vegas, USA*, Jun 2003.

[35] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, and S. Tuecke. Security for grid services. In *Twelfth International Symposium on High Performance Distributed Computing (HPDC-12)*, JUNE 2003.

[36] Network Working Group. RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Technical report, IEFT, 2008.

[37] Jörg Matthias Lenz und Christiane Schmidt. *Die elektronische Signatur*. Dt. Sparkassen-Verl., Stuttgart, 2004. ISBN 3-09-305705-1.

[38] Lukas Gundermann. Telematikinfrastruktur der elektronischen Gesundheitskarte: Basis für sichere Datenspeicherung. *Dt. Ärzteblatt*, 105(6):A268, 2008.

[39] Peter Gola und Rudolf Schomerus. *Bundesdatenschutzgesetz (BDSG) vom 20.12.1990; Kommentar*. C. H. Beck Verlag, München, 2005.

[40] Common Criteria Protection Profile BSI-PP-0018: Health Professional Card (HPC), Heilberufsausweis (HBA). Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2007. online http://www.bsi.bund.de/zertifiz/zert/reporte/PP0018.pdf.

[41] Carl-Michael Reng und Peter Debold und Klaus Adelhard und Klaus Pommerening. Vernetzte medizinische Forschung: Akzeptiertes Datenschutzkonzept. *Dt. Ärzteblatt*, 100(33):A2134–2137, 2003.

[42] A. Hermeler. *Rechtliche Rahmenbedingungen der Telemedizin*. C. H. Beck Verlag, München, 2000.

[43] B. Chen and R. Morris. Flexible control of parallelism in a multiprocessor PC router. In *Proc of the 2001 USENIX Annual Technical Conference (USENIX '01), Boston*, pages 333–346, June 2001.

[44] Jörg Fritsch und Jürgen Luksch. Schutzportale - SSL-Gateways als Volks-VPNs. *iX*, 1:110, 2004.

[45] Greg Barish, editor. *Building Scalable and High-Performance Java Web Applications Using J2EE Technology*. Addison-Wesley Professional, 2007.

[46] Andreas Thiel und Marco Eichelberg und Johannes Bernading. Adaptive security for medical image processing. *International Journal of Computer Assisted Radiology and Surgery*, 3:320–321, Juni 2008.

[47] Andreas Hoheisel and Martin Alt. Petri nets. In Ian J. Taylor, Dennis Gannon, Ewa Deelman, and Matthew S. Shields, editors, *Workflows for e-Science - Scientific Workflows for Grids*. Springer, 2006.

[48] ISO/IEC 15909-1. High-level Petri nets – Part 1: Concepts, definitions and graphical notation, 2004.

[49] Martin Alt, Andreas Hoheisel, Hans-Werner Pohl, and Sergei Gorlatch. A grid workflow language using High-Level Petri Nets. In R. Wyrzykowski et al., editor, *Proceedings of the 6-th Intl. Conf. on Parallel Processing and Applied Mathematics PPAM'2005, Poznan, Poland*, volume 3911 of *LNCS*, pages 715–722. Springer-Verlag Berlin Heidelberg, 2006.

[50] Andreas Hoheisel. Grid Workflow Execution Service – dynamic and interactive execution and visualization of distributed workflows. In *Proceedings of the Cracow Grid Workshop 2006, Cracow, Poland*, 2007.

[51] Andreas Hoheisel. User tools and languages for graph-based grid workflows. *Concurrency Computat.: Pract. Exper.*, 18:1101–1113, 2006.

[52] Falk Neubauer, Andreas Hoheisel, and Joachim Geiler. Workflow-based grid applications. In Peter Sloot, editor, *Future Generation Computer Systems*, volume 22, pages 6–15. Elsevier, 2006.

[53] J. Linn. RFC1508 - Generic Security Service Application Program Interface. Technical report, IEFT, 1993.

[54] R. Baker, D. Yu, and T. Wlodek. A Model for Grid User Management. *ArXiv Computer Science e-prints*, June 2003.

[55] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, and F. Siebenlist. X.509 proxy certificates for dynamic delegation. In *Proc. 3rd Annual PKI R&D Workshop*, 2004.

[56] G. Zeilinger. dcm4chee, a J2EE based PACS. http://www.dcm4che.org.

[57] Gregor von Laszewski, Ian Foster, Jarek Gawor, and Peter Lane. A Java Commodity Grid Kit. *Concurrency and Computation: Practice and Experience*, 13(8-9):643–662, 2001.

[58] Michal Vossberg, Thomas Tolxdorff, and Dagmar Krefting. DICOM Image Communication in Globus-Based Medical Grids. *IEEE Transactions on Information Technology in Biomedicine*, 12(2):145–153, March 2008.

[59] Marc Fleury and Francisco Reverbel. The JBoss extensible server. In Markus Endler and Douglas Schmidt, editors, *Middleware 2003 — ACM/IFIP/USENIX International*

Middleware Conference, volume 2672 of *LNCS*, pages 344–373. Springer-Verlag, 2003. citeseer.ist.psu.edu/fleury03jboss.html.

[60] Andreas Knopke. K-PACS, die kostenlose PACS-Workstation, 2008. online http://www.k-pacs.de.

[61] Wolfgang Meier. eXist: An Open Source Native XML Database. In *Revised Papers from the NODe 2002 Web and Database-Related Workshops on Web, Web-Services, and Database Systems*, pages 169–183, London, UK, 2003. Springer-Verlag.

[62] T. Hackländer, K. Kleber, J. Martin, and H. Mertens. DICOM router: An opensource toolbox for communication and correction of DICOM objects. *Acad Radiol*, 12:385–392, 2005.

Lebenslauf

Mein Lebenslauf wird aus datenschutzrechtlichen Gründen in der elektronischen Version meiner Arbeit nicht veröffentlicht.

Publikationsliste

2006

- D. Krefting, M. Vossberg und T. Tolxdorff „Medizinische Bildverarbeitung in MediGRID“ 20. Treffpunkt Medizintechnik, Juni 2006, Berlin
- U. Sax, F. Viezens, Y. Mohammed, T. Lingner, B. Morgenstern, M. Vossberg, D. Krefting, O. Rienhoff „MediGRID: Medical Grid Computing“ EGEE – Enabling Grids for E-Science, September 2006, Geneva, Switzerland

2007

- M. Vossberg, T. Tolxdorff und D. Krefting „Using DICOM in Medical Grids: Secure Image Communication and Integration of External DICOM Devices in Globus Grids“ Biomedical Engineering (BioMED) Feb. 2007, Innsbruck, Austria
- M. Vossberg, D. Krefting und T. Tolxdorff „Gridcomputing in der medizinischen Bildverarbeitung: das MediGRID Projekt" Bildverarbeitung für die Medizin, pp. 429-433, 2007, Springer-Verlag: Informatik aktuell
- S. Kottha, K. Peter, T. Steinke, J. Bart, J. Falkner, A. Weisbecker, F. Viezens, Y. Mohammed, U. Sax, A. Hoheisel, T. Ernst, D. Sommerfeld, D. Krefting, M. Vossberg "Medical Image Processing in MediGRID" German E-Science Conference 2007, Baden-Baden, Germany

2008

- M. Vossberg, A. Hoheisel, T. Tolxdorff und D. Krefting „A reliable DICOM transfer grid service based on Petri net workflows“ 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2008), 19-22 May 2008, Lyon, France, pp. 441-448
- M. Vossberg, T. Tolxdorff, D. Krefting „DICOM Image Communication in Globus-Based Medical Grids" IEEE Transactions on Information Technology in Biomedicine, vol. 12, no. 2, pp. 145-153, March 2008
- D. Krefting, M. Vossberg und T. Tolxdorff „Fortschritte Medizinische Bildverarbeitung in MediGRID“ 21. Treffpunkt Medizintechnik, Mai 2008, Berlin
- D. Krefting, M. Vossberg, T. Tolxdorff „Simplified Grid Implementation of Medical Image Processing Algorithms using a Workflow Management System“ 11th Int. Conf. on Medical Image Comp. and Computer Assisted Intervention, New York, Sept. 2008

- D. Krefting, M. Vossberg, K. Beronov, T. Tolxdorff, „Standortunabhängiger Zugang und interaktive Steuerung von gridbasierten Diensten zur medizinischen Bildverarbeitung über ein Gridportal, GMDS 2008
- K. Beronov, O. Dzhimova, A. Delgado, M. Vossberg, D. Krefting, T. Tolxdorff, " Virtual endovascular correction and hemodynamic analysis over the MediGRID-portal", eMBEC 2008
- D. Krefting, J. Bart, K. Beronov, O. Dzhimova, J. Falkner, M. Hartung, A. Hoheisel, T. A. Knoch, T. Lingner, Y. Mohammed, K. Peter, E. Rahm, U. Sax, D. Sommerfeld, T. Steinke, T. Tolxdorff, M. Vossberg, F. Viezens, A. Weisbecker "MediGRID: Towards a user friendly secured grid infrastructure" Future Generation Computer Systems, vol. 25, no. 3, pp. 326-336, March 2009
- M. Vossberg, A. Hoheisel, T. Tolxdorff, D. Krefting, "A Workflow-based Approach for Fault-tolerant Medical Image Transfer in Health Grids", eingereicht bei Future Generation Computer Systems, Sept. 2008
- D. Krefting, M. Vossberg, T. Tolxdorff, "Simplified Grid Implementation of Medical Image Processing Algorithms using a Workflow Management System", angenommen bei Future Generation Computer Systems, Juli 2009

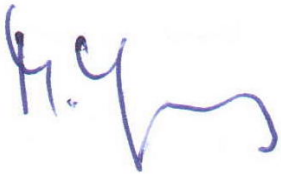
Erklärung

„Ich, Michal Vossberg, erkläre, dass ich die vorgelegte Dissertation mit dem Thema:

Sichere und fehlertolerante DICOM-Bildübertragung

in medizinischen Grid-Infrastrukturen

selbst verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, ohne die (unzulässige) Hilfe Dritter verfasst und auch in Teilen keine Kopien anderer Arbeiten dargestellt habe.“



13. Januar 2009