UNIVERSITÄT LEIPZIG

Fakultät für Mathematik und Informatik

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)

Referenzmodell für die Kommunikation eines Universitätsklinikums mit dem niedergelassenen Bereich

Diplomarbeit

Leipzig, Februar 2006

vorgelegt von:

Sebastian Stäubert

geb. am: 22.11.1978

Betreuer:

Dr.-Ing. Gert Funkat

Prof. Dr. Alfred Winter

Zusammenfassung

Das traditionell gewachsene System der deutschen Gesundheitsversorgung gliedert sich in den stationären und niedergelassenen Bereich. Stand der Technik ist es in beiden Bereichen die Vorteile der elektronischen Verarbeitung der Patientendaten zu nutzen. Defizite gibt es jedoch bei der elektronischen Kommunikation zwischen den beiden Teilbereichen.

Dies liegt zum einen an der komplexen Gesetzeslage, zum anderen an den vielfältigen Anforderungen einer technischen Umsetzung der sektorübergreifenden Kommunikation. Hier setzt die vorliegende Arbeit an, indem ein Katalog für die gesetzlichen, technischen und ökonomischen Anforderungen erstellt wird.

Für den elektronischen Datenaustausch gibt es zahlreiche etablierte Verfahren, wie z.B. die E-Mail-Kommunikation. Es werden einige weit verbreitete aber auch speziell auf die Gegebenheiten des deutschen Gesundheitswesens zugeschnittene Verfahren vorgestellt und den Anforderungen gegenübergestellt. Ziel der Untersuchung ist die Ermittlung eines anforderungskonformen Verfahrens.

Die auf diese Weise gewonnenen Erkenntnisse werden bei der Erstellung eines Referenzmodells für die Kommunikation zwischen stationären und ambulanten Bereich genutzt. Dabei wird ein schrittweises Vorgehen verfolgt. Zunächst werden mit UML Use Case Diagrammen Anwendungsfälle analysiert. Anschließend werden mit Hilfe von Sequenzdiagrammen die Kommunikationsprozessabläufe modelliert. Alle Erkenntnisse münden in der Erstellung eines Drei-Ebenen-Modells. Das $3LGM^2$-Referenzmodell soll dem Informationsmanager in einem Krankenhauses bei der Modellierung des Informationsflusses zwischen den Einrichtungen des Gesundheitswesens unterstützen.

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

3LGM²	Three-layer Graph-based Meta Model
ADT	Admission, Discharge, Transfer - Administrative Patientendaten
ANSI	American National Standards Institute
AöR	Anstalt öffentlichen Rechts
ASCII	American Standard Code for Information Interchange
BSDG	Bundesdatenschutzgesetz
bzw.	beziehungsweise
ca.	circa
CR/LF	Carriage Return/Line Feed - Wagenrücklauf/Zeilenumbruch
D2D	Docter-to-Docter
DGIV	Deutsche Gesellschaft für Integrierte Versorgung e.V
DICOM	Digital Imaging and Communications in Medicine
DIMDI	Deutschen Institut für medizinische Dokumentation und Information
DIN	Deutsches Institut für Normung e.V.
DMP	Desease Management Program
DOS	Disk Operating System
DRGs	Diagnosis Related Groups - Fallpauschalen mit Risikoadjustierung
EDV	elektronische Datenverarbeitung
eGK	elektronischen Gesundheitskarte
ggf.	gegebenenfalls
HBA	Heilberufeausweis
HL7	Health Level 7
HPC	Health Professionial Card - elektronischer Arztausweis
HPG	Health Profession Group
IBMT	Fraunhofer Institut für Biomedizinische Technik
ICD	International Statistical Classification of Diseases and Related Health Problems
IGV	integrierten Versorgungssystem
IMISE	Institut für medizinische Informatik, Statistik und Epidemiologie
ISDN	Integrated Services Digital Network
ISO	International Organisation for Standardization
IT	Informationstechnologie
IV	Integrierte Versorgung
KBV	Kassenärztlicher Bundesvereinigung

KIS	Krankenhaus Informationssystem
KVK	Krankenversichertenkarte
KVNo	Kassenärztlichen Vereinigung Nordrhein
MTA	Message Transfer Agent
OID	Object Identifier
OPS	Operationen- und Prozedurenschlüssel
OSI	Open Systems Interconnection Standard
P2P	Peer2Peer, Peer-to-Peer
PaDok	Patientenbegleitende Dokumentation
PDMS	Patienten Daten Management System
PrIS	Praxis Informationssystem
PC	Personal Computer
PVS	Patientenverwaltungssystem
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RFC	Requests for Comments
RIM	Referenz Information Modell
RPC	Remote Procedure Call
S/MIME	Secure / Multipurpose Internet Mail Extension
SCIPHOX	Standardized Communication of Information Systems in Physician Offices and Hospitals using XML
SGB	Sozialgesetzbuch
SSL	Secure Socket Layer
SSU	Small Semantic Unit
StGB	Strafgesetzbuch
UKL	Universitätsklinikum Leipzig Anstalt öffentlichen Rechts
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
uvm.	und vieles mehr
usw.	und so weiter
VCS	VDAP Communikation Standard
VDAP	Verband Deutscher ArztPraxis-Softwarehersteller e.V.
VHitG	Verband der Hersteller von IT-Lösungen für des Gesundheitswesen e. V.
WHO	World Health Organisation
VPN	Virtual Private Network
vs.	versus

XML	Extensible Markup Language
z.B.	zum Beispiel
ZI	Zentralinstitut für die kassenärztliche Versorgung

1 Einleitung

1.1 Gegenstand und Motivation

1.1.1 Gegenstand

Die vielfältigen Untersuchungs- und Therapiemöglichkeiten der modernen Medizin haben zu einer ebenso vielfältigen Landschaft von Krankenhäusern, niedergelassenen (Fach-) Ärzten und Therapeuten, Apotheken, Laboratorien und Pflegediensten geführt. Die medizinischen Einrichtungen sind Elemente des regionalen Systems der Gesundheitsversorgung. Die Kooperation der Einrichtungen stellt ein zentrales Thema für die Sicherstellung der Patientenversorgung einer Region dar. Im Zuge des Vorantreibens einer effizienten integrierten Versorgung der Patienten, ist eine noch engere Zusammenarbeit nötig. Vor allem die Kommunikation der Einrichtungen untereinander muss verbessert werden. Moderne digitale Kommunikationstechniken halten hier viele Vorteile und Chancen bereit [Paland2005]. Durch die integrative Kopplung der medizinischen Einrichtungen einer Region mit Hilfe moderner Kommunikationstechniken entsteht ein leistungsfähiges Health Information System [Winter2004].

Da es sich bei den zu transportierenden Informationen dieses Systems um sensible medizinische Daten handelt, werden hohe Anforderungen an die Kommunikation und insbesondere an den Datenschutz gestellt. Ähnlich komplex wie die gestellten Anforderungen haben sich diverse Produkte und Verfahren zur Herstellung sichere Kommunikation entwickelt.

Der Informationsmanager (z.B. eines Krankenhauses) hat die Aufgabe den Informationsfluss zu steuern, zu regeln und zu überwachen. Damit ist er herausgefordert, sichere Kommunikation zwischen den verschiedenen Einrichtungen unter Berücksichtigung der Anforderungen und Verwendung geeigneter Produkte und Verfahren zu ermöglichen [Winter2002].

Auch am Universitätsklinikum Leipzig AöR[1] (UKL) werden Vorbereitungen dahingehend getroffen, für den sicheren Austausch medizinischer Daten mit externen Einrichtungen und damit für eine bessere Integration in das Health Information System der Region zu sorgen.

1.1.2 Problematik

Die Anzahl und Komplexität der Anforderungen an die Kommunikation und Integration sind vom Informationsmanager nur noch sehr schwer zu erfassen und einzuhalten. Mindestens genau so schwer fällt bei der Planung im Rahmen des strategischen Informationsmanagements die Entscheidung, welche Produkte und Verfahren die Erfüllung einer Aufgabe optimal unterstützen und zum Einsatz kommen sollten.

Entscheidungshilfe für die Auswahl geeigneter Produkte und Verfahren bietet dem Informationsmanager der Einsatz von Werkzeugen. Am Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE) wurde aus diesem Grund das Three-layer Graph-based

1 Anstalt öffentlichen Rechts

Meta Model (3LGM²) entwickelt. Mit dem darauf basierenden 3LGM²-Baukasten lässt sich ein Health Information System zur besseren Übersicht grafisch darstellen [3LGM2HP], [Brigl2004]. Beim derzeitigen Stand der Entwicklung ist es jedoch nicht möglich, Unterstützung zu geben bei der Frage: „Mit welchen Produkten und Verfahren können welche Kommunikations- und Integrationsanforderungen erfüllt werden?“. Bei der Beantwortung dieser Frage könnten in den 3LGM²-Baukasten integrierte Musterlösungsansätze helfen. Derartige integrierte Musterlösungen, die z.B. ein auf PaDok®[2] basierendes System abbilden [PADOKHP], gibt es jedoch bisher nicht.

Das vom Fraunhofer Institut für Biomedizinische Technik entwickelte PaDok hat sichere Kommunikation zwischen Ärzten und damit einen wichtigen Teilaspekt der Integrierten Versorgung zum Ziel. Das Potential dieser Technologie wurde erkannt und soll auch am UKL nutzbar gemacht werden. Am UKL gibt es diesbezüglich jedoch noch keine Erfahrungen.

Der Vergleich und die Evaluation von Lösungsansätzen Dritter im Bereich der integrierten Versorgung wird durch das Fehlen von Standards bei der Art der Darstellung und der Definition der Schnittstellen erschwert. Deshalb ist es nur mit erheblichem Aufwand möglich, die an anderen Einrichtungen gemachten Erfahrungen zu nutzen und auf deren Lösungen aufzubauen.

Mit Problemen ist auch die Einführung der elektronischen Gesundheitskarte (eGK) bzw. des elektronischen Arztausweises (Health Professionial Card - HPC) zu rechnen [eGKHPC2005]. Der sehr enge Zeitplan für die Einführung lässt derzeit keine genaue Einschätzung zu, wann welche Fähigkeiten der Karten nutzbar sein werden. Dies hat Auswirkungen auf die eingesetzten Softwareprodukte und Arbeitsabläufe, da diese teilweise auf Funktion der eGK angewiesen sind.

1.1.3 Motivation

Musterlösungsansätze in einem geeigneten Werkzeug erleichtern dem Informationsmanager den Umgang mit der Vielzahl der Anforderungen und vereinfachen die Auswahl geeigneter Produkte und Verfahren. Die Entwicklung von Musterlösungen, um komplexe Zusammenhänge zu vereinfachen, ist keine neue Idee und in der Literatur unter der Erstellung von so genannten Referenzmodellen bekannt [Winter1995].

In einem komplexen Umfeld, wie dem Health Information System, bringt das Vorhandensein eines Referenzmodells für die Kommunikation viele Vorteile mit sich. Der Informationsmanager kann so relativ einfach die Voraussetzungen für den Austausch medizinischer Daten mit anderen Einrichtungen schaffen, indem er sich aus dem Referenzmodell eine passende anforderungskonforme Architektur zusammenstellt. Mit der aus dem Referenzmodell abgeleiteten Architektur werden automatisch kompatible Schnittstellen bereitgestellt und sowohl unterstützte Funktionen als auch Einschränkungen dargestellt.

Kommt das Referenzmodell einrichtungsübergreifend im Health Information System zum Einsatz, sind die auf diesem Wege entwickelten Kommunikationsarchitekturen aufgrund einheitlicher, klar definierter Schnittstellen untereinander vergleichbar. Mittels Modifikationen und Erweiterungen lassen sich die vorhandenen Architekturen an die spezifischen Gegebenheiten der jeweiligen Einrichtung anpassen. Informationsmanager von Krankenhäusern außerhalb des Health Information System können so von dem im Referenzmodell gespeicherten Wissen profitieren und es für die Lösung ihrer Kommunikationsprobleme benutzen oder darauf aufbauen.

---

2 Im Verlauf der Arbeit wird der Markenname PaDok® ohne das Markenzeichen verwendet.

Die Entwicklung eines Referenzmodells für die Kommunikation zwischen stationären und ambulanten Bereich bietet den Vorteil die Nutzung moderne Technologien voranzutreiben, in bestehende Informationstechnik (IT) zu integrieren und für das strategische Management darstellen zu können.

Für das strategische Management (z.B. eines Krankenhauses) ist ein derartiges um ein Kommunikationsreferenzmodell erweitertes Werkzeug mit seinen grafischen Darstellungsmöglichkeiten ein geeignetes Mittel, um sich über den Informationsfluss im Krankenhaus zu informieren und um gegebenenfalls steuernd Einfluss zu nehmen. Bei der Erstellung von Anträgen oder Rahmenkonzepten können die so aufbereiteten Informationen für das strategische Management eines Krankenhauses ebenfalls sehr nützlich sein.

Neue Chipkarten, wie die elektronische Gesundheitskarte und der elektronische Arztausweis bilden die Basis, der von der Bundesregierung geplanten Einführung elektronischer Kommunikationsvorgänge im Gesundheitswesen. Durch die auf diesen Chipkarten gespeicherten Parameter werden sichere elektronische Kommunikationsvorgänge ermöglicht. Deshalb sind sie bei der Planung neuer Kommunikationsinfrastrukturen ein Zentrales Element und werden sich deshalb auch im Kommunikationsreferenzmodell wiederfinden [Secaritas2004].

1.2 Problemstellung

Bei der einrichtungsübergreifenden Kommunikation im Health Information System bzw. bei der Umsetzung der integrierten Patientenversorgung treten folgende Probleme auf:

1. Es gibt eine Vielzahl von Anforderungen an die sektorübergreifende Kommunikation. Diese komplexen Anforderungen sind bisher noch nicht umfassend katalogisiert. Es fehlt eine Übersicht der Gesetzeslage und der Technologiesituation.
2. Es fehlt weiterhin ein Katalog von Produkten und Verfahren, die sich zur Erstellung der benötigten Kommunikationsarchitekturen eignen. In diesem Katalog müssten außerdem Verweise zu den jeweils zu beachtenden Anforderungen im Anforderungskatalog bzw. Hinweise, Funktionen und Einschränkungen verfügbar sein. Bei der Vorauswahl der Produkte und Verfahren widmet sich diese Arbeit der Frage, wie zwischen stationären und niedergelassener Bereich medizinische Daten ausgetauscht werden können, um dem Ziel Integrierte Versorgung näher zu kommen.
3. Es gibt keine Musterlösungen bzw. kein Referenzmodell für die einrichtungsübergreifende Kommunikation zwischen stationären und niedergelassen Bereich.

   Es fehlt ein auf einem Referenzmodell basierendes Werkzeug, welches den Informationsmanager bei der Erfüllung seiner Aufgaben unterstützt.

   Bisher entwickelte Methoden folgen keinem Standard und es ist nicht garantiert, dass sie untereinander vergleichbare Architekturen erzeugen. Ein Vergleich ist problematisch und sie sind aufgrund unterschiedlichster Konzepte nur schwer zu evaluieren.

1.3 Zielsetzung

Ziel Z1:Anforderungskatalog

Ziel Z2:Produkt- und Verfahrensbeschreibung

Ziel Z3:Referenzmodell für die Kommunikation

Zu Z1: Anforderungen gibt es in den unterschiedlichsten Bereichen. Unterschieden werden kann hauptsächlich zwischen gesetzlichen und technischen Anforderungen. Um den Umgang mit der Vielzahl und Komplexität der Anforderungen zu erleichtern, werden Kriterien herausgearbeitet, die als Entscheidungsbasis für ein zum Einsatz kommendes Verfahren dienen sollen. Ergebnis ist eine Übersicht der technischen Voraussetzungen und der Rechtssitutation.

Zu Z2: Durch Recherche vorhandener Lösungen und Lösungsansätze für die sektorübergreifende Kommunikation soll eine Übersicht in Frage kommender Produkte und Verfahren entstehen. Es soll dabei kein vollständiger Katalog mit dem sich auf dem Markt befindlichen Produkten erstellt werden, sondern vielmehr etablierte Ansätze vorgestellt und beschrieben werden und vertiefend auf speziell für den Datenaustausch im Gesundheitswesen entwickelte Verfahren eingegangen werden.

Zu Z3: Nachdem in Ziel Z1 und Ziel Z2 alle nötigen Informationen zusammengetragen und aufbereitet wurden, können diese nun als Entscheidungsgrundlage für ein Verfahren zur Unterstützung der Kommunikation zwischen stationären und ambulanten Bereich dienen. Auf Basis des ermittelten Verfahrens wird das Referenzmodell erstellt. Bei der Erstellung soll das 3LGM^2-Metamodell verwendet werden.

1.4 Vorgehensweise und Aufbau der Arbeit

Diese Arbeit gliedert sich in acht Kapitel. Neben den einleitenden Betrachtungen in Kapitel 1 werden in Kapitel 2 die Grundlagen für das weitere Verständnis der Arbeit vermittelt.

Kapitel 3 beschäftigt sich mit den gesetzlichen und technischen Rahmenbedingungen der Kommunikation im Gesundheitswesen. Dabei werden gesetzliche, technische und ökonomische Anforderungen berücksichtigt und in einer Übersicht zusammengefasst.

Kapitel 4 stellt Kommunikationstechniken vor. Zunächst wird dabei auf allgemeine und derzeit weit verbreitete Techniken eingegangen. Ausführlicher werden dann speziell an die Gegebenheiten im Gesundheitswesen angepasste Verfahren vorgestellt.

In Kapitel 5 werden Ist- und Soll-Zustand der beiden Kommunikationspartner behandelt. Desweiteren werden Kriterien für eine Entscheidungsgrundlage aus den Anforderungen aus Kapitel 3 erstellt und auf die vorgestellten Verfahren aus Kapitel 4 angewendet. Das Ergebnis

dieser Analyse ist ein anforderungskonformes Verfahren für die Modellierung des Referenzmodells, die in Kapitel 6 vorgestellt wird. Bei der Modellierung werden mit Hilfe der semiformalen Sprache UML (Unified Modeling Language) Anwendungsfälle und Abläufe von Kommunikationsbeziehungen abgebildet. Das 3LGM^2-Referenzmodell ist schließlich das Ergebnis der Modellierung.

In Kapitel 7 werden die Ergebnisse der vorliegenden Arbeit diskutiert und die Erfüllung der gestellten Ziele überprüft. Abschließende Betrachtungen geben eine Ausblick auf zukünftige Entwicklungen bzw. geben Empfehlungen für weiterführende Studien.

Im darauf folgendem Anhang sind zahlreiche Abbildungen und Beispiele untergebracht, auf die im Text verwiesen wird. Teil des Anhangs ist zusätzlich eine CD-Rom, welche die verwendeten Softwarewerkzeuge und die damit erstellten Modellen enthält.

2 Grundlagen

In diesem Kapitel werden für die folgenden vertiefenden Kapitel Grundlagen vermittelt, die dem späteren Verständnis dienen.

Zuerst werden die zu untersuchenden Bereiche im Gesundheitswesen vorgestellt, um die es in dieser Arbeit geht. Anschließend folgt eine Übersicht über die Kommunikation im Gesundheitswesen in Bezug auf das betreffende Umfeld. Der Schwerpunkt liegt dabei auf den Protokollen und Formaten, die computergestützte Kommunikation unterstützen oder unterstützen sollen. Danach wird die Verwendung von Chipkarten im Gesundheitswesen behandelt und in die Thematik „integrierte Versorgung“ eingeführt. Abschließend wird der Begriff Referenzmodell definiert und auf die 3LGM^2-Modellierung eingegangen.

2.1 Der zu untersuchende Bereich

Als Teilnehmer am Gesundheitswesen lassen sich Patienten, Leistungserbringer sowie Abrechnungs- und Kostenstellen identifizieren. Die Leistungserbringer medizinischer Versorgung unterteilen sich in Deutschland in den stationären und ambulanten Bereich (Abbildung 2-1). Die beiden Bereiche sind getrennt voneinander organisiert, was sich zum Teil auch in der unterschiedlichen Finanzierung niederschlägt [Stock2002]. Durch den wachsenden Kostendruck und mit dem Ziel die Behandlungsqualität weiter zu erhöhen, sollen nun die traditionell getrennten Bereiche enger vernetzt werden. Bei der Zusammenarbeit und insbesondere bei der Kommunikation dieser beiden Bereiche gibt es im Hinblick auf die Möglichkeiten elektronischer Kommunikation Optimierungspotential.

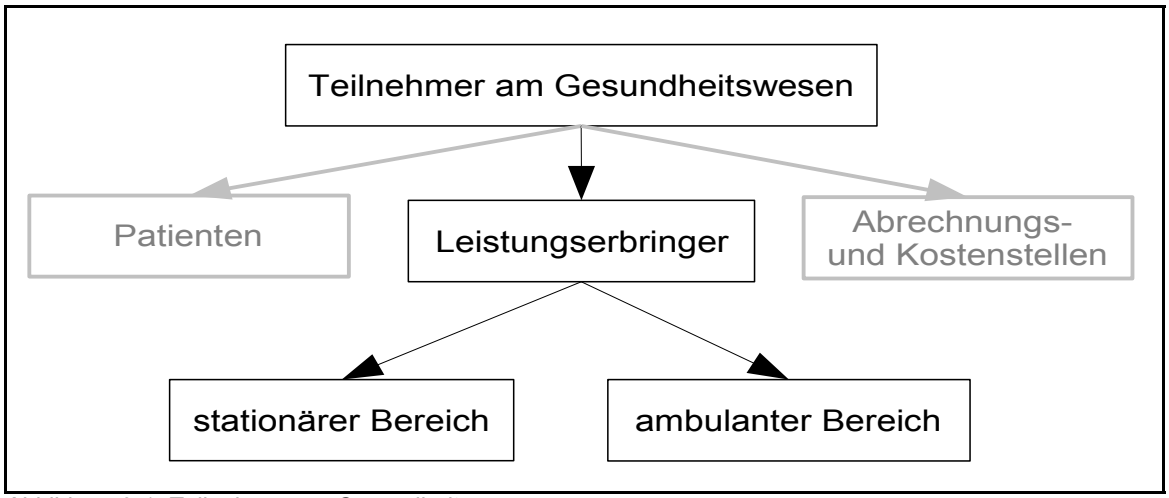

Abbildung 2-1: Teilnehmer am Gesundheitswesen

Diese Arbeit konzentriert sich für die weiteren Untersuchungen auf die Kommunikation zwischen dem Universitätsklinikum Leipzig (UKL) Anstalt öffentlichen Rechts (AöR) als Vertreter des

stationären Bereichs und niedergelassenen Arztpraxen (z.B. eines praktizierenden Hautarztes) stellvertretend für den ambulanten Bereich.

Vorbereitend auf die geforderte Kooperation zwischen den Leistungserbringern werden im folgenden die Informationssysteme beider (zukünftiger) Kooperationspartner vorgestellt, um einen Eindruck vom Umfang des Vorhabens zu bekommen.

2.1.1 Krankenhausinformationssysteme

Für den Begriff Krankenhausinformationssystem (KIS) lassen sich in der Literatur unterschiedliche Definitionen finden.

Ein Krankenhaus ist eine öffentliche oder private Einrichtung nach den Vorgaben des Krankenhausfinanzierungsgesetzes [KHG] und des fünften Bundessozialgesetzbuches [SGBV] zur zeitweiligen Aufnahme von Kranken zwecks stationärer Pflege und vollständiger ärztlicher Behandlung. Es können Teileinrichtungen für die ambulante Versorgung, zur ärztlicher Beratung sowie zur Prophylaxe vorhanden sein. Darüber hinaus kann ein Krankenhaus auch Ausbildungs- und Forschungseinrichtungen besitzen [Roche03].

Die Teileinrichtungen stellen Funktionsbereiche dar, welche die Erfüllung verschiedener Aufgaben zum Ziel haben. Diese Aufgaben können in modernen Krankenhausern durch den Einsatz spezieller Softwareprodukte effizienter und kostensparender unterstützt werden. Die größte Herausforderung ist jedoch das Zusammenarbeiten dieser Softwareprodukte, die einen Teil des Informationssystems eines Krankenhauses bilden.

Ein Informationssystem ist ein soziotechnisches System, welches aus Teilsystemen für optimale Bereitstellung von Information und Kommunikation dient [Krcmar2003]. Krcmar weist darauf hin, dass technische Systeme allein nicht informieren können. Sie sind nur Mittler von Informationsanbietern und Informationsabnehmern.

Ausgehend von diesen beiden Definitionen entsteht schnell der Eindruck, bei einem KIS handle es sich um ein Konglomerat von technischen Geräten, welches zur Aufgabe hat, bestimmten Zielgruppen Informationen bereitzustellen.

Hersteller von Softwareanwendungen zur Unterstützung einzelner Aufgaben eines Krankenhauses vermarkten ihre Produkte ebenfalls als KIS. Dabei erwächst der Eindruck, dass es sich bei einem KIS um eine Ansammlung von Programmen zur Bearbeitung medizinischer und administrativer Daten im Krankenhaus handelt. Den Funktionsbereichen des Krankenhauses wird jeweils ein Softwareprodukt zugeordnet. Personen, materielle Informationsträger wie z.B. Akten oder Rezepte und sogar die zugrundeliegende technische Infrastruktur bleiben bei dieser Sichtweise außen vor.

Am Institut für medizinische Informatik, Statistik und Epidemiologie (IMISE) in Leipzig wird ein KIS in seiner Gesamtheit definiert. Im weiteren Verlauf der Arbeit soll die am IMISE erstellte Definition für ein KIS verwendet werden:

Definition KIS nach Winter:

> *„Ein Krankenhausinformationssystem (KIS) ist das Teilsystem eines Krankenhauses, das alle informationsverarbeitenden (und -speichernden) Prozesse und die an ihnen beteiligten menschlichen und maschinellen Handlungsträger in ihrer informationsverarbeitenden Rolle umfasst. Das KIS dient dazu, die Mitarbeiter des Krankenhauses zu unterstützen. Es umfasst daher*
>
> - *alle Bereiche des Krankenhauses,*

- *alle Gebäude des Krankenhauses und*
- *alle Personengruppen, die im Krankenhaus tätig sind.“*

Nach dieser Definition ist ein Produkt einer Softwarefirma, welches z.B. die Patientenaufnahme oder die Netzwerkstruktur des Krankenhauses abdeckt noch kein KIS. Diese beiden Komponenten sind lediglich wichtige Bestandteile des Informationssystems eines Krankenhauses [Winter2002].

Da diese Arbeit sich vorrangig mit der elektronischen Kommunikation von Informationen des Gesundheitswesens befasst, wird der Fokus eher auf dem technischen Aspekt der Definition liegen. Wird der KIS-Begriff derartig eingeschränkt, findet der Terminus „rechnerbasierter Teil des KIS“ Verwendung. Menschliche Komponenten oder papierbasierte Dokumente werden aber trotzdem weiterhin als essentieller Bestandteil des KIS eines Krankenhauses angesehen.

2.1.2 Praxisinformationssysteme

Analog zur Definition eines KIS wird in dieser Arbeit der Begriff Praxisinformationssystem folgendermaßen definiert:

> *Ein Praxisinformationssystem ist ein Teilsystem einer niedergelassenen Arztpraxis, dass die informationsverarbeitenden (und -speichernden) Prozesse und die an ihm beteiligten menschlichen und maschinellen Handlungsträger in ihrer informationsverarbeitenden Rolle umfasst.*

Eine Kombination aus Hard- und Software ist nach dieser Definition bspw. wiederum noch kein Praxisinformationssystem (PrIS). Menschliche und papierbasierte Komponenten spielen auch in diesem Bereich weiterhin eine große Rolle. Im weiteren Verlauf dieser Arbeit steht auch hier der „rechnerbasierte Teil des Praxisinformationssystems“ im Vordergrund.

Da es sich im Gegensatz zum KIS bei dieser Art von Informationssystemen nicht um einen Verbund von mehreren fachspezifischen Subsystemen handelt, sondern um ein in sich geschlossenes Informationssystem, kommen meist integriertes Softwareprodukte zum Einsatz. In der Regel gibt es keine Softwaremodule für die Unterstützung von Einzelaufgaben und daher wird auch kein großer Wert auf die Kommunikation über standardisierte Protokolle innerhalb des PrIS gelegt. Die integrierten Softwareprodukte für den Einsatz in einer Arztpraxis, sind auch unter dem Namen Praxisverwaltungssysteme bekannt.

In Deutschland sind bisher circa 235 Softwarelösungen für Praxisinformationssysteme von den Kassenärztlichen Vereinigungen (KVen) zugelassenen. Die am häufigsten eingesetzte Softwarelösung Medistar der Compugroup Holding AG hat einen Marktanteil von circa 14%. Es gibt aber auch eine große Auswahl an Individuallösungen mit jeweils nur einer Einzelplatzinstallation [Keading2005].

Softwarelösungen für Praxisinformationssysteme werden vornehmlich in Arzt- oder Facharztpraxen im niedergelassenen Bereich eingesetzt. Laut Kassenärztlicher Bundesvereinigung (KBV) nutzen 70% der an der vertragsärztlichen Versorgung teilnehmenden Ärzte rechnerbasierte Praxisinformationssysteme. Es gibt allerdings auch Fälle, in denen Softwarelösungen für Praxisinformationssysteme im ambulanten Bereich eines Klinikums eingesetzt werden. In diesen Bereichen dienen sie der schnellen Dokumentation von Diagnosen,

Befunden und Therapien, einhergehend mit der integrierten Terminverwaltung zur Planung von Kontrolluntersuchungen und Weiterbehandlung.

Die Dokumentation kann dabei strukturiert in Form von anzukreuzenden Checklisten oder völlig unstrukturiert mit karteikartenähnlichen Freitextfeldern erfolgen. Softwarelösungen für Praxisinformationssysteme unterstützen in der Regel die alltäglichen Prozesse im ambulanten bzw. niedergelassenen Bereich und dienen vor allem der Arbeitserleichterung z.B. durch die Unterstützung von:

- Arztbriefschreibung
- Terminverwaltung
- Abrechnung
- Zielmonitoring
- leitliniengestützer Betreuung
- Behandlungsplanung
- Case- und Deseasemanagement
- indikatorbezogener Auswertung von Laborwerten
- Therapievergleichen (Benchmarking).

Gemeinsam haben alle zugelassenen Softwarelösungen, dass sie die Grundlage für Vergütungsvereinbarungen stellen. Die in der Arztpraxis erbrachten Leistungen werden dazu nach einem von den KVen vorgegebenen Verfahren kodiert, exportiert und zu Abrechnungszwecken quartalsweise an die KVen übermittelt.

Ein Datenaustausch zwischen den Praxisinformationssystemen ist aufgrund der unterschiedlichen Ansätze der Softwarelösungen problematisch. Unstrukturiert dokumentierte können nicht oder nur mit erheblichem Aufwand in eine strukturierte Dokumentation überführt werden. Außerdem fehlen direkte Export- und Kommunikationsschnittstellen. Es gibt dennoch die Möglichkeit mit Hilfe der so genannten xDT-Protokolle (Abrechnungsdatenträger - ADT, Behandlungsdatenträger – BDT usw. zusammengefasst unter der Abkürzung xDT, siehe Kapitel 2.2) und entsprechender Datenträger (in der Regel Disketten) Daten auszutauschen. Neuere Ansätze nutzen Datennetze und tauschen die Behandlungsdaten über den VDAP Communication Standard (VCS) oder mit Hilfe des PaDok-Verfahrens aus. Beide Verfahren werden ausführlicher in Kapitel 4 und 5 diskutiert.

2.2 Kommunikationsstandards im Gesundheitswesen

Für ein effektives Zusammenarbeiten der Leistungserbringer ist beim derzeitigen Stand der Technik der Austausch von Patientendaten auf elektronischen Wege naheliegend. Nur so können die Herausforderungen des entstehenden Health Information System [Winter2004] bei wachsenden Kostendruck erfüllt werden.

Für die elektronische Kommunikation haben sich im Laufe der EDV-Entwicklung im Gesundheitswesen eine Vielzahl von Datenformaten entwickelt. In diesem Zusammenhang ist vielfach die Rede von Standards und Normen.

> *Eine Norm ist eine planmäßig durchgeführte Festlegung von Begriffen und Eigenschaften durch autorisierte Normungsinstitute, wie zum Beispiel dem Deutschen Institut für Normung e.V. (DIN), des American National Standards Institute (ANSI) oder der International Organisation for Standardization (ISO).* [Winter2002]
>
> *Standards sind De-facto-Normen und legen Begriffe und Eigenschaften von Systemen durch allgemeine Akzeptanz fest. Sie liefern so eine allgemeine Richtschnur und entstehen in der Regel ohne vorgegebenen Plan.* [Winter2002]

Den technischen Standards sind auch die Requests for Comments (RFC) der Internet Engineering Task Force (IETF, [IETFHP]) zuzurechnen. Einige Netzwerkprotokolle, welche in den Betrachtungen in Kapitel 4 eine Rolle spielen werden, haben dort ihren Ursprung.

Wie im vorangegangenen Kapitel schon angedeutet, entwickelten sich austauschbare Datenformate im ambulanten und stationären Bereich getrennt von einander. So entstand im niedergelassenen Bereich die xDT-Protokollfamilie. Im stationär-/klinischen Bereich kommt dagegen überwiegend das HL7-Protokoll zum Einsatz [Lenz2005]. Die Clinical Document Architecture (CDA) ist im Vergleich dazu ein relativ neuer Standard, der nun versucht die entstandene Lücke zu schließen. In beiden Bereichen kommen noch weitere Formate zum Einsatz. Es handelt sich dabei teilweise um proprietäre Lösungen einzelner Softwarehersteller oder um ergänzende Standards, wie z.B. das zum Austausch von medizinischen Bilddaten entwickelte DICOM. Auf diese Formate wird im dieser Arbeit nicht weiter eingegangen.

Die folgende Abbildung 2-2 zeigt die verbreitetsten Kommunikationsstandards im Gesundheitswesen und ordnet sie ihrem Aufgabenbereich (medizinisch, administrativ) bzw. dem eingesetzten Bereich (stationär, ambulant) zu. Die in der Arbeit in diesem Kapitel weiter betrachteten Standards HL7, BDT und CDA sind rot umrandet. CDA nimmt dabei eine Sonderstellung ein. Wie sich zeigen wird, bietet der CDA-Standard die Möglichkeit, einrichtungsübergreifend eingesetzt zu werden.

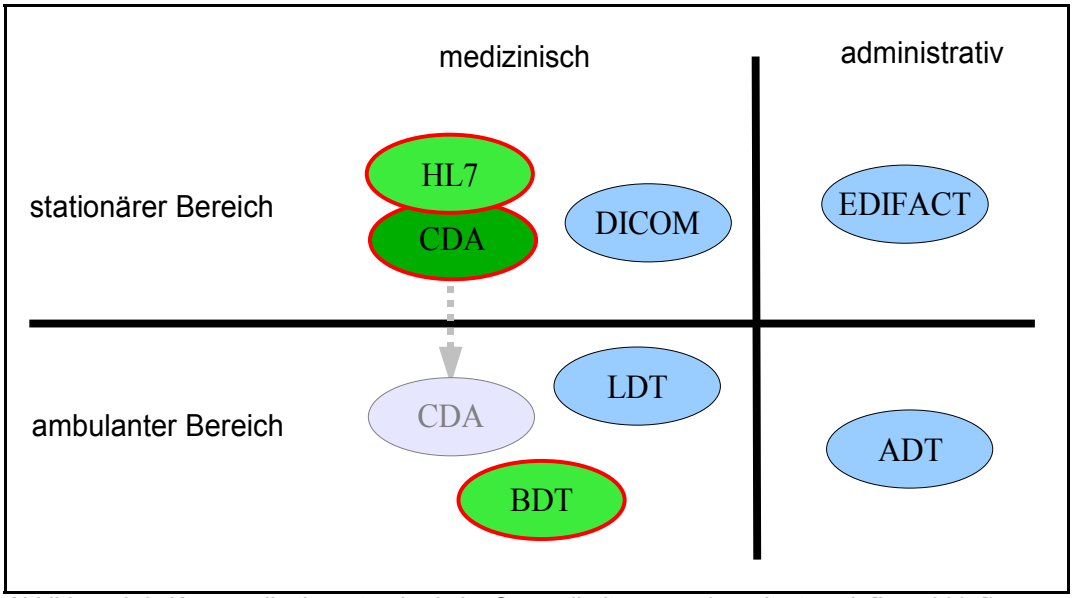

Abbildung 2-2: Kommunikationsstandards im Gesundheitswesen (erweitert nach [Lenz2005])

Neben diesen technischen Standards gibt es die inhaltlichen Standards. Sowohl im niedergelassenen als auch im stationären Bereich herrscht Konsens über die Verwendung dieser Standards. Dies ist damit zu begründen, dass der Gesetzgeber hier eindeutige Vorgaben

macht. In Sozialgesetzbuch V §295 Absatz 1 ist für Vertragsärzte und in §301 Absatz 2 für Krankenhäuser festgelegt, dass Diagnosen und Prozeduren nach den Vorgaben des Deutschen Instituts für medizinische Dokumentation und Information (DIMDI) zu verschlüsseln sind. Das DIMDI gibt zu diesem Zweck die deutschen Fassungen des International Classification of Diseases and Related Health Problems (ICD) zur Verschlüsselung von Diagnosen und die Operationen- und Prozedurenschlüssel (OPS) zur Verschlüsselung der Prozeduren heraus.

Aufgrund der zentralen Bedeutung der Kommunikationsstandards werden im Folgenden die relevanten technischen Standards xDT, HL7 und CDA genauer eingeführt. Eine Bewertung dieser Standards wird im Rahmen der Analyse im Kapitel 5 erfolgen.

2.2.1 xDT-Protokollfamilie

Die xDT-Protokollfamilie findet vor allem im niedergelassenen Bereich Verwendung und ist ein vom Zentralinstitut für die kassenärztliche Versorgung (ZI) entwickelter Standard. „DT“ steht für Datenträger und ist kennzeichnend für die Herkunft dieses Standards. In neueren Versionen steht das „DT“ auch für Datentransfer. 1987 wurde mit dem Abrechnungsdatenträger (ADT) die erste bundesweit gültige DTA-Datenschnittstelle (DTA = Datenträgeraustausch, Wortschatz KBV) vorgestellt. Wichtiger als die Tatsache, dass die Übermittlung der Daten elektronisch per Datenträger (Diskette) erfolgte, war damals, dass erstmals ein bundesweit einheitliches Format zur Anwendung kam [KBV_SS]. Mit der Version ADT 03/89 wurde die so genannte ADT-Zulassung der Softwareprodukte für Vertragsärzte eingeführt. Seitdem ist das dafür vergebene Zertifikat Voraussetzung für Praxissoftwareprodukte, die Abrechnung mit den Kassenärztlichen Vereinigungen auf dem elektronische Wege abzuwickeln.

Die guten Erfahrungen, die mit der einheitlichen Schnittstelle für die damals rund 200 Praxisverwaltungssysteme gemacht wurden, führte dazu, dass Forderungen nach weiteren Schnittstellen nach dem Muster ADT laut wurden. So kam es kurze Zeit später zur Entwicklung des Behandlungsdatenträger-Standards (BDT), welcher vor allem die Abbildung der Karteikarteninformationen zum Ziel hatte [BDT1994]. Damit konnten nun Behandlungsdaten, die auf einem Praxisverwalungssystem erzeugt wurden, exportiert und in ein anderes Praxisverwaltungssystem importiert werden. Ein Datenaustausch zwischen Arztpraxen bzw. die Migration auf andere Praxisverwaltungssysteme wurde damit möglich.

Folgende der xDT-Protokollfamilie hinzuzurechnende Standards wurden entwickelt und sind weit verbreitet:

- ADT (Abrechnungsdatenträger): Austausch von Abrechnungsdaten zwischen KV und Praxis
- KVDT (KV Datentransfer): Ablösung des ADT (seit 1.7.2000 Pflicht)
- BDT (Behandlungsdatenträger): Austausch von Behandlungsdaten
- LDT (Labordatenträger): Austausch von Labordaten
- GDT (Gerätedatenträger): Austausch zwischen Praxisverwaltungssystemen und Meßgeräten
- SDKT (Stammdaten-Kostenträger): quartalsweiser Austausch der Stammdaten der Krankenkassen und sonstiger Kostenträger
- SDGO/SDRW (Stammdatei Gebührenordnung/Regelwerk): quartalsweiser Austausch der (KVspezifischen) Gebührenordnungen/Regelwerke

Der BDT-Standard stellt derzeit den kleinsten gemeinsamen Nenner in Punkto Datenaustausch zwischen den Praxisverwaltungssystemen dar und ist daher das wichtigste Austauschformat in diesem Bereich.

2.2.2 HL7

Im stationären Bereich kommt vor allem HL7 (Health Level Seven) als Kommunikationsprotokoll zum Einsatz. Die Sieben in HL7 spielt dabei auf die Einordnung von HL7 in Schicht 7 des OSI Referenzmodells (ISO7498-1), dem „Application Layer“, an. Sinn und Zweck des HL7 Protokoll ist es, Interoperabilität zwischen den Einrichtungen im Gesundheitswesen zu schaffen. Dies soll durch die Definition von Standards zum Austausch von klinischen und administrativen Daten erreicht werden.

Die erste Version von HL7 wurde 1987 am Universitätsklinikum in Palo Alto in den USA entwickelt. Noch im selben Jahr wurde Health Level Seven, Inc. [HL7USA] als non-profit Organisation gegründet. Diese Dachorganisation koordiniert die Aktivitäten der weltweit verbreiteten HL7-Nutzergruppen und treibt die Entwicklung des HL7-Standards voran.

Für die Übersetzung der HL7 ANSI-Standards und die Anpassung an die deutschen Verhältnisse ist die HL7-Benutzergruppe Deutschland e.V. (gegründet 1992) [HL7DE] verantwortlich. Sie gliedert sich in technische Komitees, die unterschiedliche Schwerpunkte haben. So gibt es z.B. die technische Komitees „Konformität“, „XML“ und „Version 3“. Weitere wichtige Aufgaben der HL7-Benutzergruppe Deutschland sind das Abhalten von Workshops, die jährlich stattfindenden Tutorials und Beratungsleistungen bei Implementierungsfragen.

HL7-Version 2

Derzeit ist in Deutschland die HL7-Version 2 am weitesten verbreitet. Sie deckt die Bereiche Patientenverwaltung (Aufnahme, Verlegung, Entlassung), Auftrags- und Befundübermittlung sowie finanzielle Transaktionen ab. Der Datenaustausch beruht bei HL7-Version 2 auf dem Nachrichten-Paradigma. Die zwischen den Informationssystemen ausgetauschten Nachrichten haben unterschiedliche Nachrichtentypen. Je nach Einsatzzweck beinhaltet eine HL7-Nachricht Administrative Patientendaten (ADT), Befunde (ORF) oder Bestellungen (ORM). HL7 ist ein internationaler Standard und erlaubt innerhalb der vorgegebenen Nachrichtenstruktur die Definition so genanter z-Segmente zur Anpassung an nationale Gegebenheiten. Die Definition der z-Segmente ist Aufgabe der nationalen Nutzergruppen. Die für Deutschland angepasste HL7-Version 2 beinhaltet bspw. Informationen zur Pflegestufe, zu Bankverbindungsdaten oder auch Zusatzinformationen für Bundeswehrangehörige. In Anhang B können weitere Details zu Aufbau und Struktur von HL7-Nachrichten in der Version 2 eingesehen werden.

HL7-Version 3

Bereits seit 1996 laufen die Entwicklungen an der HL7-Version 3. Version 3 setzt bei den HL7-Nachrichten konsequent auf eine Kodierung in der Extensible Markup Language (XML). Zusätzlich zu dem bereits seit Version 2 verwendeten Nachrichten-Paradigma, verwendet Version 3 ein objektorientiertes, modellbasiertes Paradigma. Das mit Version 3 verfügbare HL7 Message Development Framework basiert auf der Meta-Modell Spezifikation des Referenz Model Repository (RMR) und dem Referenz Information Modell (RIM) [HL7M15], [HL7RIM].

Die Kodierung von Nachrichten und Dokumenten in XML spielt eine zentrale Rolle. Es geht weiterhin darum über den modellbasierten Ansatz die Entwicklung in Richtung strukturierte Dokumente und Electronic Health Record (EHR) voranzutreiben.

2.2.3 CDA - SCIPHOX

Bei dem im vorangegangenen Abschnitt erwähnten Paradigmenwechsel von HL7 Nachrichten hin zu strukturierten Dokumenten, ist XML die Technologie der Wahl. Die XML-basierte Clinical Document Architecture (CDA) wird Ende 2000 zum ANSI-Standard für Strukturierung, Inhalt und Austausch klinischer Dokumente im Gesundheitswesen. Aufgrund des Dokumenten-Paradigmas und der Nähe zur gewohnten Art und Weise der Dokumentation, beschränkt sich CDA nicht auf den Einsatz in Krankenhäusern, sondern findet auch Akzeptanz im ambulanten Umfeld.

Bereits Ende der 1990er Jahre gab es Bemühungen, Protokolle und Dokumente auf XML-basis zu entwickeln. Diese Entwicklungen beruhten auf einer Umsetzung der bestehenden xDT-Protokolle und fanden aufgrund fehlender Verbesserungen keine Akzeptanz unter Herstellern und Nutzern von Arztpraxissoftware [Noelle2001].

HL7 Deutschland e.V. und der Qualitätsring medizinischer Software (QMS) sind die beiden Gründungs- und Trägervereine der SCIPHOX Gbr mbH [SCIPHOXHP]. SCIPHOX steht für „Standardized Communication of Information Systems in Physician Offices and Hospitals using XML“. Seine Wurzeln hat SCIPHOX im technischen Komitee „XML“ des HL7 Deutschland e.V.. Anfang 2000 formierte sich die SCIPHOX-Gruppe mit dem Ziel, die Clinical Document Architecture (CDA) in Deutschland zu etablieren. Seitdem gibt SCIPHOX die an die deutschen Gegebenheiten angepasste Fassung des CDA Standards heraus.

Definition CDA-Dokument nach Heitmann [Heitmann2001], [SCIPHOXP1]:

> *„Ein CDA-Dokument ist ein klinisches Dokument, dass Beobachtungen und Maßnahmen enthält und folgende Eigenschaften aufweist:*
>
> - *Persistenz*
> - *geregelte Verwaltung*
> - *Möglichkeit zur Authentifizierung*
> - *Ganzheit der Authentifizierung*
> - *Lesbarkeit für das menschliche Auge (kein Binärformat)*
>
> *Ein CDA-Dokument ist ein definiertes und komplettes Informationsobjekt, das Texte, Bilder, Klänge und andere multimediale Objekte enthalten kann. CDA-Dokumente sind in der Extensible Markup Language XML kodiert.“*

Die in der Definition verwendeten Eigenschaften bedeuten dabei im Einzelnen [HL7CDA], [SCIPHOXP1]:

Persistenz: Der "medizinische Kontext" bleibt bestehen. Ein einmal zusammengestelltes CDA-Dokument als Folge einer ärztlichen Untersuchung bleibt als Ganzes im Zusammenhang bestehen.

Geregelte Verwaltung: Das medizinische Dokument wird von der Person oder Organisation verwaltet, die auch für seiner Pflege zuständig ist.

Möglichkeit zur Authentifizierung: Das medizinische Dokument ist mit einer Zusammenstellung von Informationen ausgestattet, welche gesetzlich authentifiziert werden können. Es kann also in jedem Fall eine für das vorliegende Dokument verantwortliche Person oder Organisation eindeutig bestimmt werden.

Ganzheit der Authentifizierung: Das medizinische Dokument wird als Ganzes authentifiziert und nicht in Teilen ohne Zusammenhang des vollständigen Dokuments.

Lesbarkeit für das menschliche Auge: Das medizinische Dokument soll nicht im Binärformat vorliegen und menschenlesbar sein. Diese Forderung schließt nicht aus, dass zur Darstellung weitere Hilfsmittel wie Stylesheets oder XML/HTML-Browser etc. verwendet werden.

Aufbau und Struktur eines CDA-Dokuments

Das „komplette Informationsobjekt“ (vergleiche Definition CDA-Dokument) ist vollständig in XML kodiert. XML ist ein menschen- und maschinenlesbarer Standard [W3XML], der Regeln zum Aufbau von Dokumenten mit Hilfe einer Baumstruktur definiert. Diese Regeln zur Erstellung von Dokumenten für die Anwendungsfälle in der Medizin, spezifiziert der CDA-Standard.

Die CDA-Spezifikation [HL7CDA] bzw. [SCIPHOXP1] unterteilt ein CDA-Dokument in zwei Teile: Header und Body. Die kodierten Informationen basieren auf den im HL7-Version 3 definierten Datentypen [HL7DT] und dem Referenz Information Model [HL7RIM]. Diese Datentypen werden auch in den HL7-Version 3 Nachrichten verwendet, sodass eine semantische Kompatibilität gegeben ist und bspw. Namen, Adressen etc. direkt verarbeitet werden können.

Header

Aufgabe des Headers ist, die Metainformationen zum Dokument zu speichern und damit das Management und den Austausch der Dokumente zu unterstützen. Eine weitere Funktion liegt in der Speicherung von Verweisen von weiteren einem Patienten zugehörigen Dokumenten im Sinne einer lebensbegleitenden Patientenakte [Heitmann2001], [CEN13606]. Der Header wird in einer separaten XML-Schemadatei definiert und gliedert sich in vier Teile:

1. Dokumentinformationen: Identifikation des Dokuments, Vertraulichkeit, Beziehung zu anderen Dokumenten
2. Ereignisinformationen: Zeit, Ort und Umstände unter denen das Dokument entstand
3. Aktoren: Personen, die das Dokument authentifiziert haben, Urheber, Verfasser, Empfänger einer Kopie, alle an der dokumentierten medizinischen Maßnahme beteiligten Leistungserbringer
4. Empfänger: Personen, die die dokumentierte Leistung erhalten haben (z.B. Patienten oder auch Angehörige von Patienten)

Eine Besonderheit ist die Identifikation eines Dokuments. Dazu können eindeutige Dokumenten-IDs benutzt werden. SCIPHOX hat zu diesem Zweck von HL7 einen ISO Object Identifier (OID) zugewiesen bekommen. Die SCIPHOX Wurzel-OID lautet: 2.16.840.1.113883.3.7.2 . Unterhalb dieser OID können eigenständig OIDs vergeben werden [OID2005], z.B. für die an SCIPHOX teilnehmenden Institutionen. Diese Instituts-OID ermöglicht im Zusammenhang mit einer vom Patientenverwaltungssystem erzeugten Kennung eine weltweit eindeutige Identifizierung eines

Dokuments. Über die OIDs können Patientenverwaltungssysteme eigene Dokumente erkennen und einem Fall oder Patienten zuordnen z.B. wenn Dokumente beantwortet zurückgeschickt wurden. Mittels OIDs wird außerdem auf die verschiedenen Codesysteme wie HL7, LOINC, ICD10, SNOMED usw. verwiesen. Die eindeutige Zuordnung von Objekten und Konzepten ist für den Austausch der Dokumente essenziell, da ein gemeinsames Bezugssystem für die kommunizierten Dokumente in den unterschiedlichen Einrichtungen genutzt werden kann. Das gemeinsame Bezugssystem definiert Syntax und Semantik und stellt sicher, dass im CDA-Dokument beschriebene Objekte auch einrichtungsübergreifend „verstanden“ werden.

In Deutschland wurde im März 2005 entschieden die Verwaltung der deutschen OIDs durch die „OID Registratur DE GW“ zentral zu regeln [OID2005]. Technisch und organisatorisch verantwortlich für die Registratur ist das DIMDI. Hier können bspw. Institutionen des Gesundheitswesen eine OID beantragen.

Body

Im Body wird der eigentliche Inhalt des medizinischen Dokumentes untergebracht. Das können im Einzelnen Diagnosen, Therapien, Prozeduren, Medikation, Befunde, weiteres Vorgehen usw. sein.

Für den Body sieht der CDA-Standard drei Spezialisierungsebenen vor. Diesen so genannten Levels werden unterschiedlichen Spezialsierungsgrade klinischer Dokumente zugeordnet. Die Level des CDA-Body werden in separaten XML-Schemadateien definiert. Einmal erstellte CDA-Dokumente lassen sich nach den von ihnen eingebundenen Schemata validieren und auf CDA-Konformität prüfen.

Level 1 (levelone) stellt einen generischen Ansatz dar, der lediglich eine Strukturierung in Überschriften, Paragrafen, Tabellen und Listen etc. vorgibt. Mit levelone-Dokumenten wird Phase 1 des SCIPHOX Projektes [SCIPHOXP1] realisiert. SCIPHOX Phase 1 konzentriert sich dabei auf den standardisierten, elektronischen Kurzbericht (Entlassungsbrief, Überweisung, Einweisung). Ein Beispiel für ein levelone-CDA-Dokument befindet sich in Anhang B.

Level 2 und 3 fügen dem Dokument Schritt für Schritt mehr „Markup“ (=Auszeichnung von Text durch Tags) hinzu und führen so zu Dokumenten mit immer größerer Strukturierung. Diese Art der Einteilung in Level nach Strukturierungsgrad stellt einen Migrationspfad vom Freitext hin zu strukturierten Dokumenten zur Verfügung und erlaubt einen flexiblen Umgang mit klinischen Dokumenten. Abbildung 2-3 (Seite 16) zeigt den strukturellen Aufbau eines CDA-Dokumentes.

Small Semantic Units - SSUs

Um eine Anpassung an die deutschen Gegebenheiten vorzunehmen, hat die SCIPHOX Arbeitsgruppe den CDA-Standard um die Small Semantic Units (SSUs) erweitert. Diese landesspezifischen Informationscontainer werden so markiert, dass eine Validierung des gesamten Dokuments gegen den HL7 Standard im Ergebnis zu einem validen CDA-Dokument führt (Namespace Definition *sciphox:sciphox-ssu*, *local_header* Tag mit dem Attribut *ignore=„all“* versehen). Dieses Konzept wird „shared sematics“ genannt und sorgt für eine optimale Anpassung an lokale Bedürfnisse ohne den internationalen Standard zu verletzen. Es ist ferner möglich, dass nationale Anpassungen in den internationalen Standard aufgenommen werden.

Die lokalen Anpassungen für Deutschland (SSUs) sind erforderlich, um die durch SCIPHOX Phase 1 angestrebte Kommunikation des standardisierten elektronischen Kurzberichts, zu unterstützen.

Folgende SSUs wurden daher definiert [SCIPHOXP1]:

- insurance: Versicherungsinformationen
- labresult: Laborwerte
- diagnoses: Diagnosen
- medication: Medikationen
- procedures: Prozeduren
- referral: Einweisung/Überweisung

Bis auf insurance sind alle SSUs im Body angesiedelt und dienen im wesentlichen der Kennzeichnung medizinischer Informationen.

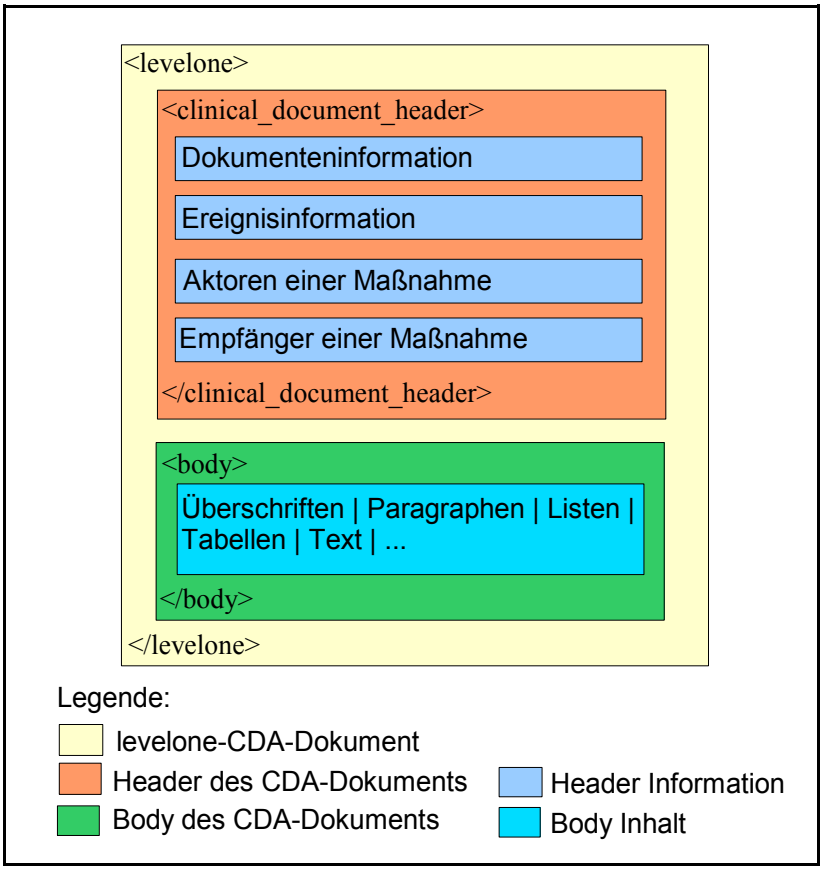

Abbildung 2-3: Aufbau eines levelone-CDA-Dokuments

2.3 Chipkarten im Gesundheitswesen

Chipkarten in der Medizin sind durch die bevorstehende schrittweise Einführung der elektronischen Gesundheitskarte ab dem 1.1.2006 ein derzeit viel diskutiertes Thema. Dies belegen nicht nur zahlreiche Pressemitteilungen in Rundfunk und Printmedien, sondern auch die Vielzahl an wissenschaftlichen Publikationen zu diesem Thema (siehe bspw. Sonderausgaben des „Telemedizinführer Deutschland“ [TMFS2005] und [TMF2006]).

Für diese Arbeit sind die neuen Möglichkeiten des elektronischen Heilberufeausweises und der elektronischen Gesundheitskarte von Bedeutung. Die elektronische Identifikation von Ärzten und Patienten, Verschlüsselungs- sowie Signaturfunktionen und nicht zuletzt die Möglichkeit Zugriffsinformationen oder Behandlungsdaten zu speichern sind wichtige Elemente für die sichere Vernetzung im Gesundheitswesen.

Dieser Abschnitt soll einen Überblick über den aktuellen Stand der Einführung der elektronischen Gesundheitskarte vermitteln und den Funktionsumfang der verschiedenen Chipkarten aufzeigen.

2.3.1 Krankenversichertenkarte

Mit der Krankenversichertenkarte (KVK) wurde in Deutschland 1994/95 erstmals flächendeckend eine Chipkarte für das Gesundheitswesen eingeführt. Diese Chipkarte hatte zur Funktion, die Berechtigung des Leistungsempfangs nachzuweisen und eine eindeutige Zuordnung zur zahlungspflichtigen Institution zu gewährleisten. Seine rechtliche Grundlage hat die Krankenversichertenkarte im Sozialgesetzbuch 5 und in Verträgen zwischen den gesetzlichen Krankenkassen und den Kassenärztlichen Vereinigungen (SGB V, § 291, Absatz 3).

Die einfache Speicherkarte fasst circa 300 Byte und beinhaltet:

- Name und Nummer der Krankenkasse,
- Titel, Name, Anschrift, Geschlecht und Geburtsdatum des Versicherten,
- Versicherungstatus und -nummer, Zuzahlungsstatus,
- Ablaufdatum der Gültigkeit der Karte. (SGB V, § 291, Absatz 2)

Die Krankenversicherungskarte ist eine rein administrativ genutzte Chipkarte und beinhaltete keine medizinischen Informationen [Koehler2002].

2.3.2 Elektronischer Heilberufeausweis - HBA

Der elektronische Heilberufeausweis (HBA, international: Health Professional Card – HPC) nach der Spezifikation Version 2.0 [SPEZHPC], geht über die Funktionalität eines Sichtausweises mit administrativen Daten hinaus. Der HBA dient als Zugriffsberechtigungskarte (Schlüsselkarte) zur Telematikinfrastruktur der elektronischen Gesundheitskarte (siehe folgenden Abschnitt 2.3.3 elektronische Gesundheitskarte) für Ärzte und Angehörige eines Heilberufs[3]. Aus diesem Grund ist auf der HBA ein Zertifikat zur Erzeugung einer qualifizierten elektronische Signatur nach dem

3 Angehörige eines Heilberufs sind nach [Goetz2005] bzw. SGB V § 291a Absatz 4: Ärzte, Zahnärzte, Apotheker, Psychotherapeuten sowie teilweise deren Gehilfen.

Signaturgesetz (SIG, [SIG]) untergebracht, die es dem Besitzer ermöglicht, Patientendaten elektronisch zu unterschreiben sowie zu ver- und entschlüsseln.

Insgesamt hat der bis zu 64 Kilobyte speichernde und mit einem Prozessor für Kryptografieanwendungen ausgestattete HBA folgenden Funktionsumfang:

- optischer Sichtausweis mit Foto des Inhabers
- Authentifikation – elektronische Identitätsprüfung und Zugriff auf Patientendaten der elektronischen Gesundheitskarte
- digitale Signatur – zum rechtsgültigen Signieren elektronischer Dokumente
- Verschlüsselung – zum sicheren Versand über Datenleitungen.

Herausgegeben wird der elektronische Heilberufeausweis von der Bundesärztekammer, welche in diesem Zusammenhang auch als Zertifizierungsdiensteanbieter[4] fungiert.

2.3.3 Elektronische Gesundheitskarte - eGK

Wie der elektronische Heilberufeausweis hat die elektronische Gesundheitskarte (eGK) ihre rechtlichen Grundlagen im GKV-Modernisierungsgesetz (GMG, [GMG]) und im § 291a, SGB V. Die elektronische Gesundheitskarte löst ab 1.1.2006 schrittweise die Krankenversichertenkarte ab und stellt zusammen mit dem HBA den Schlüssel für die Versicherten zur Teilnahme an der zukünftigen Telematikinfrastruktur des deutschen Gesundheiswesens dar [SPEZLA]. Die Telematikinfrastruktur vernetzt dabei über HBA und eGK ca. 80 Millionen Versicherte, ca. 22.000 Apotheken, ca. 123.000 niedergelassene Ärzte, ca. 2.200 Krankenhäuser sowie die rund 300 Krankenkassen und ist Grundlage für zahlreiche Telematikanwendungen. Dazu zählen: das elektronische Rezept, die elektronische Arzneimitteldokumentation, der elektronische Notfallausweis oder der elektronischen Arztbrief.

Zum Funktionsumfang der eGK gehört:

- elektronische Speicherung administrativer Daten (entsprechend den administrativen Daten der KVK)
- europäische Krankenversichertenkarte als Sichtausweis auf der Rückseite
- elektronisches Rezept - löst das bisherige Rezept in Papierform ab
- Sicherheitsfunktionen - Authentifizierung, Verschlüsselung, elektronische Signatur und Protokollierung der letzten 50 Zugriffe
- Speicherung von Gesundheitsdaten wie Notfalldatensatz, Arzneimitteldokumentation, Patientenquittungen, Patientenakte, Arztbrief.

Zu den Pflichtbestandteilen gehören die administrativen Daten, die nun auch über ein Online-Verfahren abgeglichen werden können, der europäische Krankenversicherungsausweis und das elektronische Rezept. Die Speicherung der persönlichen Gesundheitsdaten ist freiwillig und hat eine qualitative Verbesserung der Gesundheitsversorgung zum Ziel. Die Sicherheitsfunktionen sind für den Schutz der auf der eGK gespeicherten Gesundheitsdaten zuständig. Mit ihnen lassen sich Daten verschlüsselt und signiert speichern, sodass ein Missbrauch nach gegenwärtigem Kenntnisstand der Betreiber ausgeschlossen wird. Als Folge der gewünschten Sicherheitsfunktionen ist die eGK analog zum HBA als Prozessorkarte ausgelegt.

4 Ein Zertifizierungsdiensteanbieter ist ein Aussteller qualifizierter Zertifikate nach §§ 4 – 13 SIG.

Mit der Einführung der eGK gehen weitere Ziele wie die Steigerung der Wirtschaftlichkeit [Lux2005] und die Stärkung der Eigenverantwortung der Patienten (Patiententen-Empowerment, [Graetz2005]) einher.

Die zu Grunde liegenden Telematikinfrastruktur befindet sich seit März 2004 in der Entwicklung. Anfang 2004 wurde die erste Version der Rahmenarchitektur von der damaligen Projektgesellschaft protego.net vorgestellt. Die Weiterentwicklung wurde durch das biT4health Projekt fortgesetzt und führte zur Spezifikation der Lösungsarchitektur durch das FuE-Projekt “eGK“ (FuE - Forschung und Entwicklung) der Fraunhofer Gesellschaft [SPEZLA]. Aktuell ist die Anfang 2005 per Gesetzesbeschluss gegründete Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik, § 291b, SGB V) für die Weiterentwicklung der Spezifikation sowie für Einführung und Betrieb verantwortlich.

Bei der Realisierung der Telematikinfrastruktur sind bisher zwei Ansätze für die Speicherung der Gesundheitsdaten sowie des elektronischen Rezepts in der Diskussion. Das Servermodell geht davon aus, dass Gesundheitsdaten und elektronisches Rezept verschlüsselt und signiert auf zentralen Servern gespeichert werden. Mit Hilfe von eGK und HBA kann dabei auf die gespeicherten Daten zugegriffen werden. Beim Kartenmodell werden die Daten dagegen auf der eGK selbst gespeichert. Die am 15.12.2005 gestartete Testphase sieht eine Erprobung beider Ansätze vor. Die Ergebnisse der Testphase sollen dazu genutzt werden, die Spezifikation der Lösungsarchitektur für den Produktiveinsatz weiter zu verbessern. Die Ausgabe der eGK an die Versicherten wird nach Angaben des Bundesministerium für Gesundheit nach Abschluss der Testphase schrittweise noch in 2006 erfolgen [BMGeGK2006].

Die zeitnahe Einführung der eGK ist für die in Kapitel 4 vorgestellten Verfahren zur Unterstützung der Kommunikation von großer Bedeutung. Durch die Möglichkeit der Speicherung von Gesundheitsdaten lassen sich Zugriffsinformationen bequem auf der Chipkarte transportieren, ohne den Umweg über Ausweichtechnologien, wie der Speicherung auf externen Datenträgern oder gar dem Ausdruck der Tickets, zu gehen.

2.4 Integrierte Versorgung

Als Bestandteil der Gesundheitsreform aus dem Jahre 2000 definiert das Sozialgesetzbuch V den Begriff der integrierten Versorgung (§ 140a ff SGB V) als sektorübergreifende Versorgung durch die Kooperation von Leistungerbringern und Kostenstellen im Gesundheitswesen. Mit den Regelungen zur integrierter Versorgung werden die Rahmenbedingungen für eine Kooperation der Leistungserbringer untereinander und ihrer Abrechnungs- und Kostenstellen geschaffen. Dies soll den gesetzlich Versicherten eine über verschiedene medizinische Bereiche übergreifende Versorgung ermöglichen.

Integrierte Versorgung soll eine interdisziplinäre und sektorübergreifende Versorgung von Patienten nach abgestimmten Behandlungsprogrammen bieten. Durch das Zusammenlaufen von Informationen über Behandlungsfälle, die in verschiedenen Einrichtungen gewonnen wurden, sollen

- Doppeluntersuchungen vermieden,
- die Behandlungsdauer verkürzt,
- koordinierte Dienstleistungen bereitgestellt,

- regelmäßige Nachsorgeuntersuchungen (Monitoring) ermöglicht und
- die Versorgungsqualität durch enge Kooperation von ambulanten und stationären Bereich verbessert

werden [LIV2005]. Diese Ziele haben sowohl finanzielle als auch gesundheitliche Aspekte. Kürzere Liegezeiten und die Vermeidung von Doppeluntersuchungen führen zu Kosteneinsparungen. Die Vermeidung von gesundheitsbelastenden Doppeluntersuchungen, wie z.B. mehrfache radiologische Untersuchen eines Patienten, führt zudem zu einer Verbesserung der Behandlungsqualität. Abbildung 2-4 zeigt den anvisierten medizinischen Versorgungskreislauf und veranschaulicht Kommunikationsbeziehungen zwischen den Teilnehmern des integrierten Versorgungssystem (IGV-System).

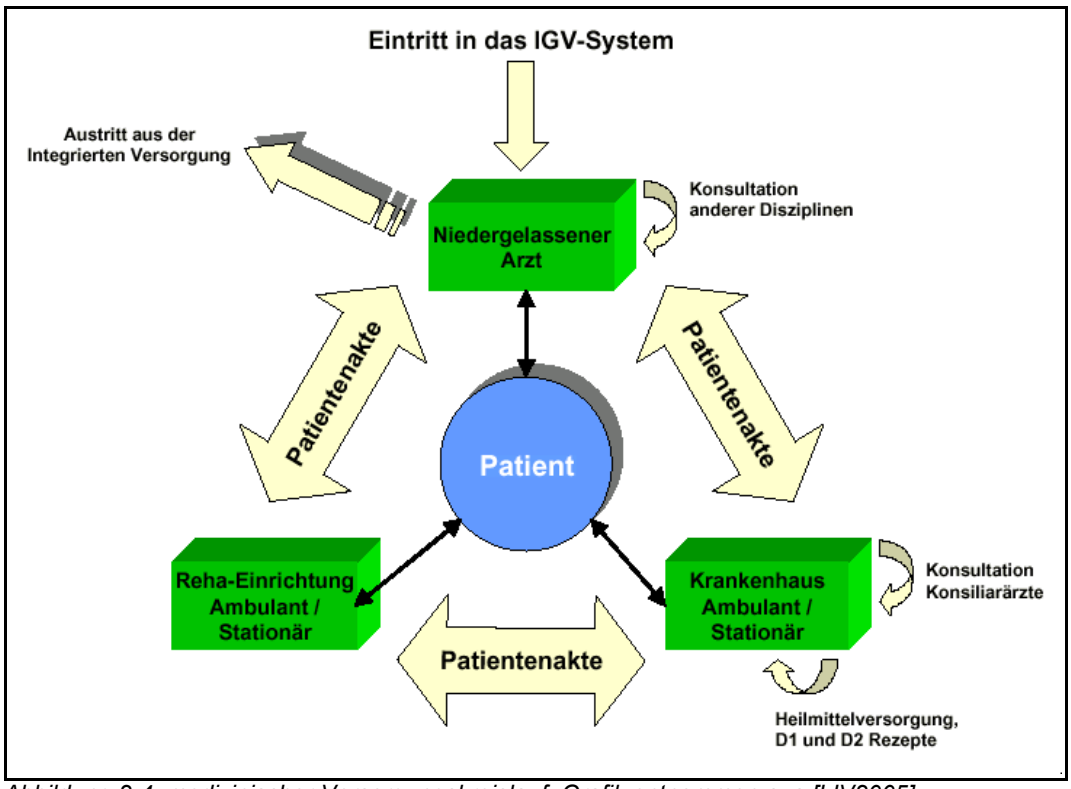

Abbildung 2-4: medizinischer Versorgungskreislauf, Grafik entnommen aus [LIV2005]

Ihren Ursprung hat Integrierte Versorgung in den USA. Dort ist in diesem Zusammenhang von 'managed competition' die Rede. Unter 'managed competition' (in Deutschland unter dem Namen 'Managed Care' bekannter) sind verschiedene Techniken zusammengefasst. Ein Instrument von Managed Care ist z.B. das 'Gatekeeping', welches sein Gegenstück im Hausarztmodell einiger Krankenkassen [IVB2004] wiederfindet. Bei Hausarztmodell sollen Kosteneinsparungen eintreten durch den initialen Besuch des Patienten bei einem von ihm gewählten Hausarzt. Der Hausarzt trifft anschließend geeignete Maßnahmen zur Weiterbehandlung, wie die Überweisung an einen Facharzt oder ein Krankenhaus. Diese Vorgehensweise wird als 'Gatekeeping' oder eben Hausarztmodell bezeichnet und soll helfen standardisierte Behandlungspfade zu etablieren sowie teure Facharztbesuche zu reduzieren. Die Patienten profitieren vom Hausarztmodell durch die Schaffung von Anreizen, wie Bonussystemen oder Rabatten und natürlich durch die Verbesserung der Behandlungsqualität.

Ähnlich verhält es sich mit Case- und Desease Management sowie Diagnosis Related Groups (Fallpauschalen, DRGs) und Kopfpauschalen. Auch hier wird durch die Einführung standardisierter Behandlungsmuster und Pauschalbeträgen versucht Kosten zu senken und die Qualität der Behandlung zu erhöhen.

Die gesetzliche Grundlage zur Integrierte Versorgung in Deutschland wurde im Jahr 2000 mit §140a ff Sozialgesetzbuch 5 (SGB V) geschaffen. Davor waren lediglich Modellprojekte und Verträge zwischen Krankenkassenverbänden, Kassenärztlichen Vereinigungen und Krankenhausgesellschaften ("dreiseitige Verträge") möglich. Die Umsetzung dieser Vorhaben blieb jedoch sehr begrenzt und beschränkte sich auf die Bildung von lokalen Praxisnetzen, siehe auch Kapitel 3.1.7 „Datennetze“.

Mit dem Inkrafttreten der Gesundheitsreform am 1.1.2004 wurden die Möglichkeiten der Integrierten Versorgung erweitert. Es wurden rechtliche Hemmnisse abgebaut und finanzielle Anreize geschaffen, um den Ausbau der Integrierten Versorgung voranzutreiben. Im Zeitraum vom 1.1.2004 bis zum 31.12.2006 stehen dabei jährlich bis zu 1 Prozent der jeweiligen Gesamtvergütung der Kassenärztlichen Vereinigungen und der Krankenhausvergütungen als Anschubfinanzierung zur Verfügung [Schmidt2004], SGB V § 140d Absatz 1. Das entspricht ca. 680 Millionen Euro pro Jahr. Integrierte Versorgungsverträge dürfen auch dann von den Krankenkassen geschlossen werden, wenn dafür Beitragserhöhungen nötig sind, SGB V § 140 d Absatz 4.

Diese Anreize zeigen ihre Wirkung. So meldete die Deutsche Gesellschaft für Integrierte Versorgung e.V. (DGIV), dass bisher 1859 Verträge (Stand 31.12.2005) mit einem Finanzierungsvolumen von ca. 450 Millionen Euro zum Abschluss gekommen sind [DGIV2005]. Die DGIV stellt die gemeinsame Registrierungsstelle zur Unterstützung der Umsetzung des § 140d SGB V dar. Bei ihr laufen die Informationen über die Verträge zur Integrierten Versorgung nach Versorgungsregionen zusammen. Diese Informationen werden in regelmäßigen Stellungnahmen zur aktuellen Situation veröffentlicht. Die DGIV hat weiterhin beratende Funktionen für Entscheider in der Politik, Verwaltung und bei den Leistungsträgern. Dazu veranstaltet und organisiert sie Foren für Wissenschaft und Praxis, Informationsveranstaltungen sowie Fort- und Weiterbildungsmaßnahmen und trägt somit zum Erfahrungs- und Informationsaustausch bei [DGIVHP].

Am Universitätsklinikum Leipzig AöR sind bisher noch keine Erfahrungen mit Verträgen nach dem SGB V §140a gemacht worden. Es gibt jedoch Vorbereitungen entsprechende Verträge in einigen Kliniken (Dermatologie, Onkologie) zu etablieren.

Im Zusammenhang mit dem Begriff „Integrierte Versorgung“ werden oft Projekte vorgestellt, die eine verbesserte Kommunikation zwischen den Leistungserbringern zum Ziel haben. Vor allem Projekte aus dem Bereich Gesundheitstelematik eignen sich dazu die Integrierte Versorgung zu unterstützen. Telematik[5] ist oft das Mittel zum Zweck der besseren Zusammenarbeit zwischen Ärzten und der Einführung neuer Behandlungs- und Therapiemöglichkeiten von Patienten [Krueger2005].

Ein Beispiel für ein derartiges Telematikprojekt ist der vom Verband Deutscher Artzinformationssystemhersteller und Provider e.V. (VDAP) entwickelte VDAP Communication Standard (VCS). VCS konzentriert sich vorwiegend auf die Kommunikation zwischen niedergelassenen Ärzten [VDAPHP].

Ein weiteres Forschungsprojekt hat den Datenaustausch zwischen den Leistungserbringern bzw. zwischen Leistungsträgern und Krankenkassen zum Ziel. Dies soll das am Fraunhofer Institut für Biomedizinische Technik entwickelte PaDok leisten, welches in einer Umsetzung unter dem Namen Doctor2Doctor (D2D) in NRW bereits seit 2002 im Einsatz ist [D2DHP].

Der Grund für das geweckte Interesse an Telematikprojekten im Gesundheitswesen ist in der geforderten engen Kooperation zwischen der Leistungserbringern bei gleichzeitiger

5 Der Begriff Telematik ist eine Wortzusammensetzung aus Telekommunikation und Informatik.

Kostenreduzierung zu sehen. Die positiven Erfahrungen in lokalen Praxisnetzen und die Existenz von auf die Bedürfnisse im Gesundheitswesen angepassten Kommunikationslösungen sind ein weiterer Grund. Der Einsatz der computergestützten Vernetzung soll den Informationsfluss beschleunigen, Medienbrüche vermeiden und den bisher auftretenden, kostenverursachenden Informationsverlust verhindern. Durch den Einsatz von Telematik werden Kosten vermieden, die bspw. entstehen durch qualitative Einbußen bei Medienbrüchen oder wenn behandlungsrelevante Informationen nicht rechtzeitig verfügbar oder verlorengegangen sind [Haensch2005]. Durch die Anschubfinanzierung für Infrastrukturprojekte im Rahmen der integrierten Versorgung wird ein zusätzlicher Anreiz für Investitionen in diesem Bereich geschaffen.

Das Konzept der integrierten Patientenversorgung hat viele positive Ziele. Dennoch haben vor allem niedergelassene Ärzte bedenken, wenn es um die Einführung neuer Telematikanwendungen geht. Die Finanzierung der „Kommunikationsendpunkte“ im niedergelassenen Bereich sehen sie kritisch, denn die Kosten für Software, Schulungen und Arbeitsausfall sind nicht Gegenstand der Verträge nach §140d SGB V (IV-Verträge) und müssen vielfach von den niedergelassenen Ärzten getragen werden. Unmut schafft dies besonders deshalb, da die Kostenreduzierung auf Seiten der Kostenstellen und Leistungsträger ensteht aber nicht zurückfließt. Das heißt, es gibt in der Regel keinen Ausgleich für die Kosten, die durch die Verwendung von Telematikanwendungen entstehen.

Weitere Kritikpunkte sind, dass durch Bürokratisierung und Technisierung immer mehr Gelder in medizinfremde Bereiche fließen, die letztlich nicht mehr für die eigentliche Behandlung des Patienten zur Verfügung stehen.

Für den Patienten sind die IV-Verträge und deren Auswirkungen teilweise zu komplex und schränken bestimmte Freiheiten ein, wie z.B. der Hausarztvertrag der Barmer [IVB2004].

Viele IV-Verträge erwecken den Eindruck primär auf Kostenreduzierung ausgelegt zu sein. Sie werden außerdem nur bei bestimmten Krankheiten (vergleiche auch Case-/Deseasemanagement) abgeschlossen. Bei wenig verbreiteten Krankheiten, die ein geringeres Einsparpotential erwarten lassen, sind dem Autor keine Bestrebungen bekannt, IV-Verträge mit dem Ziel der Verbesserung der Behandlungsqualität aufzusetzen.

2.5 Referenzmodelle

Hauptziel der Arbeit ist es, ein Referenzmodell für die Kommunikation zwischen stationären und niedergelassenen Bereich zu erstellen. Der folgende Abschnitt soll in die Thematik Referenzmodelle einführen.

Krankenhausinformationssysteme bestehen in der Regel aus vielen Subsystemen und können sehr komplex sein. Zur Beschreibung dieser Informationssysteme werden Modelle eingesetzt.

> *Ein Modell ist die Beschreibung eines Sachverhaltes mit einem für das Modellierungsproblem geeigneten Beschreibungsmittel.* [Winter2002]

Modelle erlauben dem Modellbenutzer, z.B. einem Informationsmanager im Krankenhaus, einen übersichtlichen Zugriff auf relevante Informationen in komprimierter Form.

2.5.1 Definition Referenzmodell

Die Erstellung von Modellen kann dadurch unterstützt werden, dass für eine Klasse von Sachverhalten Modellmuster herangezogen werden. Ein Modellmuster wird auch Referenzmodell genannt.

Definition Referenzmodell nach Winter [WinterAF1999]:

> *„Sei eine Klasse S von Sachverhalten gegeben. Ein Modell R ist Referenz für S oder R ist ein Referenzmodell für S, genau dann wenn gilt:*
>
> *1: R ist ein Modell AND*
>
> *2a: R ist Grundlage spezieller Modelle für Sachverhalte der Klasse S OR*
>
> *2b: R ist Vergleichsobjekt für Modelle von Sachverhalten der Klasse S“*
>
> *„In einem Referenzmodell sollte beschrieben sein,*
>
> - *in welcher Weise spezielle Modelle auf der Grundlage des Referenzmodells konstruiert werden können und/oder*
> - *wie das Referenzmodell als Vergleichsobjekt benutzt werden kann.“*

Referenzmodelle bieten den Vorteil, dass durch Modifikationen, Einschränkungen oder Ergänzungen konkrete Modelle abgeleitet werden können. Die so durch Konkretisierung oder durch Festlegen diskriminierender Eigenschaften aus einem Referenzmodell entstandenen Modelle, werden als spezielle Modelle bezeichnet. Spezielle Modelle beschreiben einzelne, konkrete Sachverhalte aus eine Klasse von Sachverhalten genauer und können wiederum als Referenzmodell dienen, um den Detailgrad weiter zu verfeinern. Aus einem Referenzmodell abgeleitete spezielle Modelle sind untereinander vergleichbar und können z.B. hinsichtlich ihrer Vollständigkeit gegenüber dem Referenzmodell untersucht werden. Aus der Vergleichbarkeit der speziellen Modelle mit dem Referenzmodell ergibt sich die Vergleichbarkeit der speziellen Modelle untereinander. Aus dem Vergleich der speziellen Modelle können so weitere Rückschlüsse bezüglich Gleichheit, Ähnlichkeit bzw. Unterschiedlichkeit der modellierten Sachverhalte getroffen werden.

Teil zwei der Definition empfiehlt, dass eine Anleitung zur Konstruktion spezieller Modelle dem Referenzmodell zu entnehmen sein sollte, bzw. sollten Hinweise vorhanden sein, wie sich das Referenzmodell als Vergleichsobjekt nutzen lässt.

Im Kapitel 2.2 wurden unter anderem die Begriffe Standards und Normen erläutert. Standards und Normen können in gewisser Weise auch als Referenzmodelle aufgefasst werden, jedoch mit höheren Verbindlichkeitsgrad. Umgekehrt sind Referenzmodelle aber keine Normen. Referenzmodelle können ungeachtet dessen durch praktische Bewährung im Unternehmen oder durch Empfehlung einer anerkannten Organisation von großer Bedeutung sein.

2.5.2 Typen von Referenzmodellen

Abhängig von der Klasse der Sachverhalte, die es zu modellieren gilt, können eine Vielzahl von Referenzmodellen zum Einsatz kommen. Für diese Arbeit sind Referenzmodelle folgenden Typs von Bedeutung:

Organisations-Referenzmodell:

Aus Organisations-Referenzmodellen lassen sich Modelle der Aufgaben, (Produktions-) Abläufe sowie der Daten- und Organisationsstrukturen einer Klasse von Organisationen ableiten.

Ein Organisations-Referenzmodell ist demnach z.B. das Referenzmodell „Arztpraxis im niedergelassenen Bereich“ oder auch das Referenzmodell „Klinik im Universitätsklinikum“. In diesen Referenzmodellen könnten Aufgaben, Abläufe, Daten- und Organisationsstrukturen für die Klasse der niedergelassenen Arztpraxen bzw. der Klasse der Kliniken im Universitätsklinikumsverbund empfohlen werden. Daraus abgeleitete spezielle Modelle könnten das Modell einer niedergelassenen Hautarztpraxis sein bzw. das Modell einer Fachklinik im Universitätsklinikum.

Informationssystem-Referenzmodell:

Bei einem Informationssystem-Referenzmodell liegt der Fokus der Modellierung auf der Informationsverarbeitung einer Klasse von Organisationen. Es handelt sich daher bei einem Informationssystem-Referenzmodell um eine Spezialform des Organisations-Referenzmodells. Informationssystem-Referenzmodelle können verschiedene Sichten beinhalten, wie z.B. eine Sicht auf den konventionellen, papierbasierten Teil oder auf den rechnerbasierten Teil eines Informationssystem. Der rechnerbasierte Teil eines Informationssystem kann wiederum weitere Sichten beinhalten, wie die Sicht auf den physischen Teil des rechnerbasierten Informationssubsystems die Servercomputer, Arbeitsplatzcomputer oder Netzwerkhardware.

Um ein Organisations- und Informationssystem-Referenzmodell geht es in dieser Arbeit. In Kapitel 6 wird ein Referenzmodell vorgestellt, das sowohl Aufgaben, als auch die Sicht auf das Informationssystem in sich vereint. Diese vielschichtige Beschreibung wird durch den Modellierungsansatz 3LGM^2-Metamodell bestimmt.

2.5.3 Architekturen und Architekturstile

Abhängig vom betrachteten Kontext gibt es unterschiedliche Auffassungen über den Architekturbegriff. Für diese Arbeit ist die Architektur von Informationssystemen von Interesse.

> *Die Architektur von Informationssystemen beschreibt die Komponenten des Informationssystems und die Beziehungen zwischen den Komponenten (vergleiche [Wendt2005], [Winter2002]).*

Die Zerlegung eines Informationssystems in klar abgegrenzte Bausteine, die Komponenten, kann z.B. aus einem Referenzmodell für Informations- oder Softwaresysteme abgeleitet werden. Die Komponenten können verschiedenen Sichten unterworfen werden, je nach Ziel der Architekturbetrachtung.

Charakteristische Architekturen von Informationssystem lassen sich bestimmten Architekturstilen zuordnen, wenn sie für eine Klasse von Informationssysteme zutreffend sind. Es wird an dieser Stelle auch von Entwurfsstilen, Entwurfsmustern bzw. von Architektur-Referenzmodellen gesprochen.

Architekturbetrachtungen werden in Kapitel 4 eine Rolle spielen und sind für die Identifizierung der Modellkomponenten aus der logischen und physischen Sicht auf das Informationssystem von Bedeutung.

2.6 3LGM²-Modellierung

Um die komplexen Sachverhalte der zu betrachtenden Informationssysteme in geeigneter Weise beschreiben zu können, wird auf das am Institut für medizinische Informatik, Statistik und Epidemiologie (IMISE) entwickelte Three-layer Graph-based Meta Modell (3LGM²) zurückgegriffen, [3LGM2HP], [Winter2002], [Winter2003]. Im folgenden Abschnitt wird das 3LGM²-Metamodell vorgestellt.

2.6.1 3LGM²-Metamodell

In Bezug auf die Definitionen für KIS und PrIS in Kapitel 2.1 als soziotechnische Subsysteme, müssen bei der Modellierung dieser Informationssysteme verschiedene Sichten berücksichtigt werden. Das 3LGM²-Metamodell wurde mit der Zielsetzung entwickelt, komplexe Informationssysteme unter Berücksichtigung von drei Sichtweisen zu modellieren. Diese Sichten spiegeln sich in den Modellebenen wieder und umfassen im 3LGM²-Metamodell die fachliche Ebene, die logische Werkzeugebene und die physische Ebene. Die Ebenen beinhalten charakteristische Elemente, die zudem zu einander in Beziehung stehen. Sie beschreiben die Informationssystemstrukturen in einer Ebene bzw. die zur Ebene korrespondierende Sicht auf das Informationssystem. Desweiteren können zahlreiche Beziehungen zwischen den Ebenen abgebildet werden, die so genannten Interebenenbeziehungen.

Für die Beschreibung der Informationssystemstrukturen auf den Ebenen sowie für die Beschreibung der Interebenenbeziehungen kommen beim 3LGM²-Metamodell Klassendiagramme der semiformalen Sprache UML (Unified Modeling Language, [UMLV2], [Oestereich1997]) zum Einsatz. Klassen fassen gleichartige Objekte zusammen und stehen über Assoziation und Generalisierung in Beziehung. Den Beziehung können Multiplizitäten und Rollen zugewiesen werden. Eine Beziehung zwischen zwei Klassen kann weiterhin durch Attribute und Operationen beeinflusst werden. Eine derartig definierte Beziehung wird Assoziationsklasse genannt.

Fachliche Ebene

Auf der fachlichen Ebene sind die Aufgaben einer Organisation verankert. Mit Organisation ist im Folgenden stehts ein Krankenhaus oder eine Praxis gemeint. Weiterhin sind die durch die Aufgaben zu bearbeitenden und zu interpretierenden Objekttypen Bestandteil der fachlichen Ebene.

Die Aufgaben ergeben sich aus den Unternehmenszielen und haben daher keinen definierten Anfang und kein definiertes Ende. Sie lassen sich in Teilaufgaben zerlegen. Auf diesem Wege lässt sich der gewünschten Detailgrad erreichen. Typische Aufgaben sind Patientenaufnahme, Labordiagnostik oder Archivverwaltung.

Objekte können real existierende oder virtuelle Elemente einer Organisation sein. Diese Objekte besitzen bestimmte Eigenschaften. Objekte mit denselben Eigenschaften werden zu Objekttypen zusammengefasst. Die Objekttypen repräsentieren die bei der Erledigung einer Aufgabe anfallenden bzw. benötigten Informationen. Beispiele für Objekttypen sind der Behandlungsfall oder die Patientenstamminformationen. Abbildung 2-5 zeigt die fachliche Ebene in UML Notation.

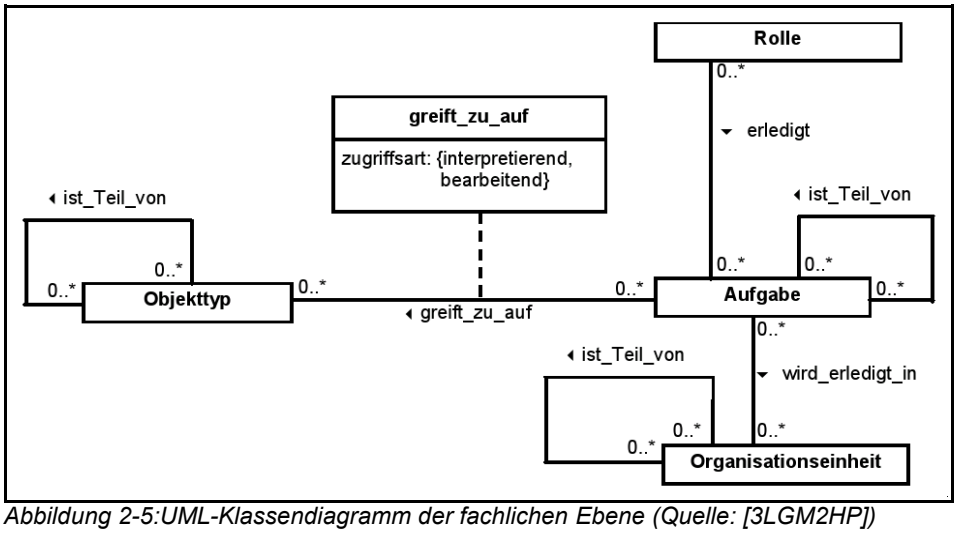

Abbildung 2-5:UML-Klassendiagramm der fachlichen Ebene (Quelle: [3LGM2HP])

Logische Werkzeugebene

Bei der Erledigung der Aufgaben werden die Mitarbeiter einer Organisation von informationsverarbeitenden Werkzeugen unterstützt. Diese Werkzeuge werde auf der logischen Ebene als Anwendungsbausteine dargestellt. Es lassen sich zwei Typen von Anwendungsbausteinen unterscheiden: rechnergestützte z.B. ein Softwareprodukt oder Programm und konventionelle z.B. ein Organisationsplan oder ein papierbasiertes Verfahren zur Erledigung einer Aufgabe. Die Anwendungsbausteine können Daten verarbeiten, speichern und über Schnittstellen austauschen. Auf diese Weise kann ein Anwendungsbaustein auf Informationen, die im Datenbanksystem eines weiteren Anwendungsbausteins gespeichert sind, zugreifen. Datensatztypen korrespondieren mit den Objekttypen der fachlichen Ebene. Das komplexe Zusammenspiel zwischen den Anwendungsbausteinen und die Beziehungen zu weiteren Komponenten der logischen Werkzeugebene ist im UML-Klassendiagramm in Abbildung D-1 (Anhang C) dargestellt.

Physische Werkzeugebene

Die Anwendungsbausteine auf der logischen Werkzeugebene basieren auf physischen Datenverarbeitungsbausteinen. Diese sind auf der physischen Werkzeugebene angesiedelt und können in konventionelle z.B. Regale oder Schreibmaschinen und rechnerbasierte Bausteintypen z.B. Servercomputer oder physische Netzwerkkomponenten unterschieden

werden. Über Datenübertragungsverbindungen können die physischen Datenverarbeitungsbausteine kommunizieren. Das UML-Klassendiagramm in Abbildung C-2 (Anhang C) beschreibt die Klassen und Beziehung der physischen Werkzeugebene.

Interebenenbeziehungen

Die drei Ebenen existieren nicht unabhängig voneinander, sondern stehen über Interebenenbeziehungen in Verbindung (siehe [Brigl2003]). Es gibt Beziehungen zwischen fachlicher Ebene und logischer Werkzeugebene sowie zwischen logischer und physischer Werkzeugebene. In den UML-Klassendiagrammen in Abbildung D-1 und Abbildung C-2 sind die Interebenenbeziehungen durch gepunktete Linien und Rechtecke gekennzeichnet.

Die Aufgaben auf der fachlichen Ebene und die Anwendungsbausteine auf der logischen Werkzeugebene stehen über Anwendungsbausteinkonfigurationen in Beziehung. Eine Aufgabe kann über eine Anwendungsbausteinkonfigurationen durch ein oder mehrere Anwendungsbausteine gemeinsam unterstützt werden (erste Möglichkeit). Es ist auch möglich, dass eine Aufgabe durch mehrere Anwendungsbausteinkonfigurationen unterstützt wird (zweite Möglichkeit). Fällt bei Möglichkeit zwei eine Anwendungsbausteinkonfigurationen aus, kann eine andere die Aufgabe dennoch erfüllen. Bei Möglichkeit eins ist im Gegensatz dazu jeder Anwendungsbaustein essentiell für die Unterstützung der Aufgabe notwendig. Fällt ein Anwendungsbaustein aus, kann die Aufgabe nicht mehr unterstützt werden.

Eine ähnliche Beziehung besteht zwischen Aufgaben und Softwareprodukten. Anwendungsbausteine können durch Parametrierung eines zugewiesenen Softwareproduktes jedoch einen eingeschränkten Funktionsumfang aufweisen, sodass nicht mehr sämtliche Aufgaben, die das Basis-Softwareprodukt unterstützt, vom parametrierten Anwendungsbaustein erledigt werden können. Weitere Interebenenbeziehungen legen fest, in welchen Datenbanksystemen Objekttypen gespeichert werden und wie diese auf der logischen Werkzeugebene repräsentiert werden.

Aufgaben können Ereignisse eines Ereignistyps auslösen und somit das Versenden von Nachrichten eines festgelegten Nachrichtentyps steuern. Mit dieser Interebenenbeziehung zwischen Aufgabe und Ereignis wird die Darstellung nachrichtenbasierte Kommunikation ermöglicht.

Zwischen logischer und physischer Werkzeugebene werden Interebenenbeziehungen als Datenverarbeitungskonfigurationen bezeichnet. Ein Anwendungsbaustein kann dabei auf mehreren physischen Datenverarbeitungsbausteinen verteilt installiert sein. Es ist auch möglich, dass auf einem physischen Datenverarbeitungsbaustein mehrere Anwendungsbausteine laufen.

Kommunikationsprozessmodellierung mit dem 3LGM²-Metamodell

Kommunikationsprozesse können auf der logischen Ebene als Folge von Kommunikationsverbindungen zwischen Anwendungsbausteinen realisiert werden. Voraussetzung dafür ist allerdings eine Folge von Aufgaben auf der fachlichen Ebene. Jede Aufgabe mit Ausnahme der letzten in der Folge bearbeitet dabei mindestens einen Objekttyp, der von einer nachfolgenden Aufgabe interpretiert werden muss. Den Aufgaben über Interebenenbeziehungen zugewiesene Anwendungsbausteine können daraufhin über Bausteinschnittstellen und Kommunikationsverbindungen Nachrichtentypen austauschen. Der Informationsaustausch wird über Ereignisse von den Aufgaben gesteuert. Für die Zuordnung von

Ereignissen und Nachrichten sind so genannte Ereignistyp-Nachrichtentypkombinationen (ETNT-Kombination) verantwortlich. Diese ETNT-Kombinationen können den Kommunikationsverbindungen zugewiesen werden. Sind alle Bausteinschnittstellen mit den passenden Kommunikationsstandards konfiguriert und ist allen beteiligten Aufgaben und Anwendungsbausteinen eine entsprechende Anwendungsbausteinkonfiguration zugewiesen, können Kommunikationsprozesse dargestellt werden (siehe auch UML-Klassendiagramm logische Werkzeugebene Abbildung D-1, Anhang C). Ein Beispiel für einen mit dem 3LGM²-Baukasten modellierten Kommunikationsprozess befindet sich in .

2.6.2 3LGM²-Baukasten

Eine Implementierung des 3LGM²-Metamodells stellt der 3LGM²-Baukasten dar. Der in Java geschriebene 3LGM²-Baukasten ist plattformunabhängig einsetzbar und über 3LGM²-Homepage [3LGM2HP] verfügbar. Eine Einführung und Beschreibung des Funktionsumfangs dieses Werkzeugs bietet z.B. [Wendt2004].

Abbildung 2-6 zeigt ein mit dem 3LGM²-Baukasten erstelltes 3LGM²-Modell eines Informationssystems. Es sind die drei Ebenen mit ihren in Beziehung stehenden Elementen dargestellt. Desweiteren sind zusätzlich die farblich markierten Interebenenbeziehungen visualisiert.

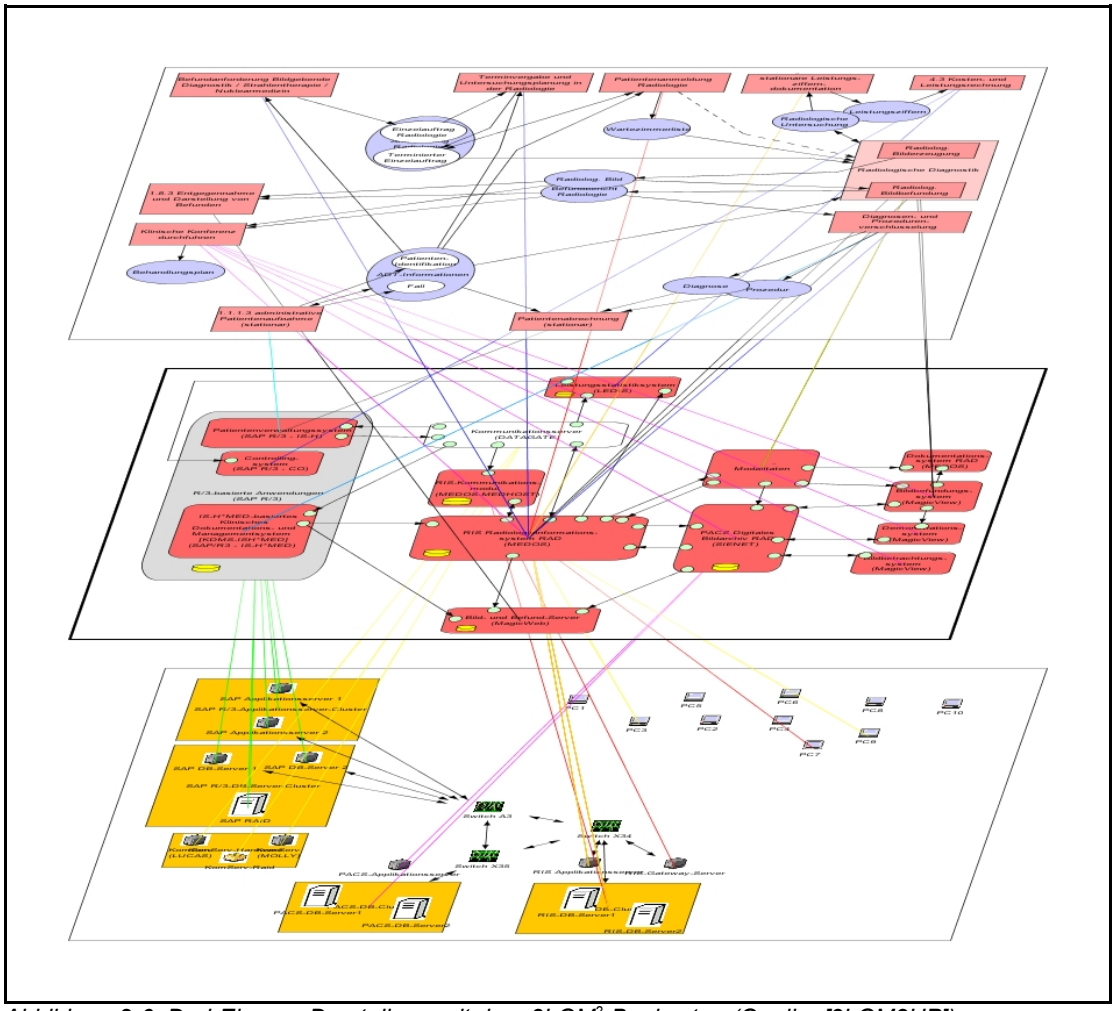

Abbildung 2-6: Drei-Ebenen Darstellung mit dem 3LGM²-Baukasten (Quelle: [3LGM2HP])

3 Gesetzliche und technische Rahmenbedingungen

In diesem Kapitel werden Anforderungen an die elektronische Übertragung medizinischer Daten herausgearbeitet. Der zu untersuchende Bereich ist die rechnergestützte Kommunikation zwischen einem Klinikum, als Vertreter des stationären Bereichs, und einer Arztpraxis, als Vertreter des niedergelassen Bereichs.

Unterschieden wird zwischen gesetzlichen, technischen und ökonomischen Anforderungen. Die gesetzlichen Anforderungen werden in hohem Maße durch datenschutzrechtliche Regelungen bestimmt. Bei den technischen Anforderungen wird zwischen Anforderungen an physische Datenverarbeitungsbausteine und an die Software unterschieden. Aufgrund der Komplexität der Informationssysteme und unter Berücksichtigung der eingespielten Arbeitsabläufe in beiden Bereichen, werden bei den technischen Anforderungen zusätzlich Integrationsanforderungen in die Betrachtungen einfließen. Die ökonomischen Anforderungen zielen darauf ab, zu prüfen, in wie weit bereits vorhandene Ressourcen und Technologien einbezogen werden können.

Am Ende dieses Kapitel steht ein Anforderungskatalog bereit.

3.1 Gesetzliche Anforderungen

Die gesetzlichen Anforderungen an die elektronische Verarbeitung medizinischer Daten setzen sich aus den in Deutschland geltenden Gesetzen und Verordnungen zusammen. Die hier zusammengetragenen gesetzlichen Anforderungen stellen einen komprimierten Auszug aus der vorherrschenden gesetzlichen Vielfalt dar. Sie sollen die rechtliche Situation bei der Kommunikation von Personendaten in Deutschland umreißen und vor allem für den Schutz der Patientendaten sensibilisieren. Es besteht kein Anspruch auf Vollständigkeit und keine rechtliche Verbindlichkeit. Als Quellen fanden Gesetzbücher, Verordnungen, Berufsordnungen sowie Datenschutzberichte und wissenschaftliche Papiere zum Thema Verwendung.

Bei den auf elektronischem Wege zu verarbeitenden medizinischen Patientendaten handelt es sich um personenbezogene Daten nach § 3 Satz 1 und 9 Bundesdatenschutzgesetz. Das Verarbeiten von Patientendaten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten, siehe § 3 Satz 4 Bundesdatenschutzgesetz [BDSG].

Die bei der Verarbeitung personenbezogener Patientendaten geltenden allgemein rechtlichen Bestimmungen, gelten auch bei der elektronischen Verarbeitung der Patientendaten. Dieser Grundsatz verhindert das Beschneiden von Patientenrechten durch den Einsatz elektronischer Datenverarbeitung. Die veränderten technischen Bedingungen erfordern jedoch eine Anpassung bzw. neue datenschutzrechtliche Konzepte [Bultmann2002].

Im niedergelassenen Bereich gilt für die Verarbeitung von Patientendaten das Bundesdatenschutzgesetz (BDSG). Bei Krankenhäusern kann es für die Verarbeitung von Patientendaten bereichsspezifische Regelungen wie Landeskrankenhausgesetze oder Gesundheitsdatenschutzgesetze etc. geben. Gibt es keine derartigen Regelungen, kommen die

allgemeinen datenschutzrechtlichen Vorschriften, das Bundesdatenschutzgesetz, zur Anwendung. Weiterhin sind Regelungen der Berufsordnung, des Strafgesetzbuches, der Strafprozessordnung sowie Sonderregelungen von Religionsgemeinschaften zu beachten.

3.1.1 Behandlungsvertrag

In Deutschland gilt der Grundsatz der freien Arztwahl. Dieser Grundsatz ist im Sozialgesetzbuch V §76 (SGB V, [SGBV]) festgelegt. Hat sich der Patient für einen Arzt seiner Wahl entschieden, haben beide den ersten Kontakt, rechtlich gesehen, indem sie einen so genannten Behandlungsvertrag miteinander abschließen. Ein Behandlungsvertrag muss nicht in Schriftform bestehen und ist ein Sonderfall eines allgemeinen Dienstvertrages nach §611ff Bürgerliches Gesetzbuch (BGB). Die Einordnung als Dienstvertrag hat zur Folge, dass mit Vertragsabschluß keine Erfolgsgarantie seitens des Arztes gegeben werden muss.

Der Behandlungsvertrag ermächtigt den Arzt, die zur Behandlung notwendigen Daten zu erheben und zu verarbeiten. Sind die erhobenen Daten nicht unbedingt für den Behandlungsfall erforderlich, ist eine zusätzliche Einwilligung des Patienten notwendig. Dies trifft z.B. auf zusätzliche Daten für eine Forschungsstudie zu. Im Bundesdatenschutzgesetz ist dieser Grundsatz in § 3a unter dem Begriff der Datensparsamkeit verankert.

Weiterhin verpflichtet der Behandlungsvertrag den behandelnden Arzt zur Dokumentation der im Laufe des Behandlungsprozesses gemachten Feststellungen und der getroffenen Maßnahmen. Diese Dokumentationspflicht kann auch in weiteren Regelwerken verankert sein, wie z.B. in der Berufsordnung (§ 10 Musterberufsordnung, MuBO) [Dierks2005].

Für alle dokumentierten objektiven Daten hat der Patient ein Recht auf Auskunft und Einsicht. Ausnahmen des Auskunfts- und Einsichtsrechts gelten in der Psychatrie. Regelungen diesbezüglich finden sich im Landeskrankenhausgesetz z.B. Sächsisches Krankenhausgesetz [SaechsKHG], im Gesundheitsdatenschutzgesetz und im Bundesdatenschutzgesetz. Ein Gesundheitsdatenschutzgesetz ist nicht in allen Bundesländern vorhanden. Gesundheitsdatenschutzgesetz gibt es bspw. In Nordrhein-Westfalen [GDSGNRW]. In Bundesländern in denen es kein Gesundheitsdatenschutzgesetz gibt, finden sich Regelungen diesbezüglich jedoch im Landesdatenschutzgesetz wieder.

3.1.2 Ärztliche Schweigepflicht

Eine durch § 6 Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (SächsGDG, [SaechsGDG]) und durch § 203 Strafgesetzbuch bzw. § 9 Musterberufsordnung normierte Pflicht des behandelnden Arztes ist die ärztliche Schweigepflicht. Sie ist neben den datenschutzrechtlichen Vorschriften zu beachten. Bei der ärztlichen Schweigepflicht handelt es sich um ein Datengeheimnis nach § 5 Bundesdatenschutzgesetz [Bultmann2002]. Auch in § 6 Landesdatenschutzgesetz des Freistaates Sachsen (SächsDSG, [SaechsDSG]) ist sie verankert. Es ist zu beachten, dass auch die Gehilfen des Arztes der ärztlichen Schweigepflicht unterliegen, siehe § 53 Strafprozessordnung bzw. Kapitel 3.1.6 „Beschlagnahmeverbot“.

Eine Übermittlung und Weitergabe von Patientendaten ist nur im Rahmen der datenschutzrechtlichen Regelungen und nach den Vorgaben von § 203 Strafgesetzbuch gestattet.

Folgende Ausnahmen können dabei zur Anwendung kommen:

1. eine gesetzliche Regelung, die ein übergeordnetes Wohl der Allgemeinheit zum Ziel hat z.B. das Krebsregistergesetz, das Infektionsschutzgesetz sowie Ausnahmen im Sozialgesetzbuch 5.
2. durch diesbezügliche Klauseln im Behandlungsvertrag, wobei dann eine schriftliche Einwilligung nötig ist.
3. durch eine explizite Einwilligung des Patienten.

Diese Vorschriften gelten auch bei einem Datenaustausch zwischen Ärzten.

3.1.3 Einwilligung

Mit der Einwilligung wird dem Patienten die Möglichkeit gegeben, sein nach Artikel 2 Absatz 1 Grundgesetz (allgemeine Handlungsfreiheit) und Artikel 1 Absatz 1 Grundgesetz (Menschenwürde) verankertes Recht auf informationelle Selbstbestimmung wahrzunehmen. Dies gilt insbesondere für die elektronische Verarbeitung von Personendaten, da die dauerhaft elektronisch gespeicherten Informationen automatisch ausgewertet werden können, sodass die betroffene Person nicht mehr sicher sein kann, was wem über sie bekannt ist.

Damit die Einwilligung des Patienten rechtswirksam wird, müssen nach § 4a Absatz 1 Bundesdatenschutzgesetz folgende Anforderungen erfüllt sein:

1. Freiwilligkeit: Die Einwilligung muss freiwillig erfolgen.
2. Der Patient muss informiert werden über:
   – den Umfang und Zweck der geplanten Verarbeitung der Daten
   – die Freiwilligkeit der Einwilligung
   – die Möglichkeit des Widerrufs der Einwilligung.
3. Pauschale Einwilligungen in denen Zweck und Umfang unklar sind, sind unzulässig.
4. Die Einwilligung muss in Schriftform erfolgen. Nur falls die Schriftform nicht möglich ist, darf eine andere angemessene Form gewählt werden (§ 4a Absatz 1 Satz 3 und Absatz 2 Bundesdatenschutzgesetz).

Bei der Einwilligung zur telemedizinischen Verarbeitung, kommt hinzu, dass der Patient in allen Phasen des Verfahrens ausreichend über die Verarbeitung seiner personenbezogenen Daten informiert sein muss. Dies setzt voraus, dass das ihn informierende Personal ebenfalls diesbezüglich ausgebildet ist. Mit der Einwilligung zur telemedizinischen Verarbeitung muss dem Patienten Umfang, Zweck und die Rechtsgrundlage der Verarbeitung der Daten sowie Grundprinzipien des technischen Verfahrens bekannt gegeben werden [Mueller2005]. Ferner muss auch über mögliche Alternativen informiert werden.

Das Vorzeigen der Versichertenkarte reicht aus den oben genannten Gründen nicht als Einwilligung aus. Außerdem dient die Versichertenkarte als Nachweis der Leistungsberechtigung und muss schon aus diesem Grunde vorgelegt werden. Hat der Patient der Speicherung von persönlichen und medizinischen Daten z.B. auf einer Chipkarte zugestimmt, die bei jedem Arztbesuch vorgelegt werden muss, sind die rechtlichen Anforderungen an die Einwilligung ebenfalls nicht erfüllt.

§ 4 und §4a Bundesdatenschutzgesetz gehen konform mit der europäischen Datenschutzrichtlinie, die bereits 1995 herausgegeben wurde und einen verbindlichen Rahmen für die Mitgliedsstaaten schafft.

Auch in Verträgen zur integrierten Versorgung findet sich eine Regelung für die Einwilligung wieder. Ärzte die über derartige Verträge vernetzt sind, müssen daher ebenfalls die Einwilligung des Patienten einholen (vergleiche IV-Hausarztvertrag der Barmer, [IVB2004]).

3.1.4 Spezielle Regelungen

Bezüglich der Datenübermittlung an vor-, mit- und nachbehandelnde Ärzte kann es abweichende Regelungen im jeweiligen Landesdatenschutzgesetz geben. So kann z.B. das Widerspruchsrecht des Patienten nach Informationen über die geplanten Datenübertragungen im Landesrecht abweichen, siehe § 22 Datenschutzgesetz des Freistaates Sachsen.

Als weitere Spezialregelungen gelten unter anderem die erst in den letzten Jahren beschlossenen oder geänderten folgenden Paragraphen im Sozialgesetzbuch 5:

- § 63a Absatz 3a Modellvorhaben zur Einführung der elektronischen Gesundheitskarte
- § 68 finanzielle Unterstützung bei Nutzung elektronischer Datenverarbeitungsverfahren
- § 73a hausarztzentrierte Versorgung
- §137f,g Desease Management Programme
- § 140a integrierte Versorgung
- § 291a elektronischen Gesundheitskarte

Diese Paragrafen behandeln die Zusammenarbeit von Leistungserbringern im Gesundheitswesen und setzen dabei auch auf die Möglichkeiten elektronischer Datenverarbeitung. Alle diese Paragrafen haben gemein, dass personenbezogene Daten erst nach der Einwilligung des Patienten verarbeitet oder kommuniziert werden dürfen.

3.1.5 Externe Dritte

Im Auftrag des Arztes können Patientendaten zu Datenverarbeitungsaufgaben, wie z.B. Schreibarbeiten, Archivierung oder Rechnungslegung für Leistungen, die nicht von den gesetzlichen Krankenkassen übernommen werden, an externe Dritte weitergeben werden. Es handelt sich hierbei datenschutzrechtlich nicht um eine Datenübertragung, da der Arzt als Auftraggeber datenverarbeitende Stelle bleibt. Die Weitergabe von Patientendaten ist jedoch eine Durchbrechung der ärztlichen Schweigepflicht und bedarf daher der Einwilligung des Patienten (§ 203 Strafgesetzbuch), falls keine weitere Regelung, z.B. im Landeskrankenhausgesetz, existiert. Wird hingegen sichergestellt, dass externe Dritte die übergebenen Daten nicht zur Kenntnis nehmen können, z.B. durch eine Verschlüsselung der Daten, sodass sie zu keinem Zeitpunkt der Verarbeitung im Klartext vorliegen, handelt es sich nicht um eine Durchbrechung der ärztlichen Schweigepflicht [Bultmann2002].

Liegt schließlich die Einwilligung des Patienten zur externen Auftragsdatenverarbeitung durch Dritte vor, muss die Datensicherheit an den datenverarbeitenden Stellen trotzdem gewährleistet sein. Dass heißt, es müssen technische und organisatorische Maßnahmen zur Sicherstellung der Datensicherheit (§ 9 BDSG) getroffen werden. Zusätzlich ist der Personenkreis, der Kenntnis

der Patientendaten nehmen könnte, soweit wie möglich einzuschränken. Idealer Weise sollte eine Kenntnisnahme der Patientendaten durch Dritte ausgeschlossen werden.

3.1.6 Beschlagnahmeverbot

Nach § 97 Absatz 1 Strafprozessordnung unterliegen alle Gegenstände im Gewahrsam des behandelnden Arztes dem Beschlagnahmeverbot. Der behandelnde Arzt ist nach § 53 Absatz 1 Satz 3 Strafprozessordnung berechtigt und nach den Regelungen der ärztlichen Schweigepflicht verpflichtet, Zeugnis zu verweigern. Es ist zu beachten, dass Gegenstände und dazu zählen auch auf Datenträgern gespeicherte Daten, die sich im Gewahrsam des Arztes bzw. einer Krankenanstalt befinden, diesem Schutz des Vertrauensverhältnisses zwischen Arzt und Patienten unterliegen. Auf Gegenstände, die Angehörigen eines Heilberufes oder EDV-Dienstleistern anvertraut wurden, trifft § 97 Strafprozessordnung seit dem Inkrafttreten des Gesundheitsmodernisierungsgesetztes am 1. Januar 2004 ebenfalls zu. § 97 Absatz 2 Satz 1 StPO wurde dafür entsprechend geändert. Das heißt, sensible Daten dürfen bei externen Dritten nicht beschlagnahmt werden, wenn sie dem Zeugnisverweigerungsrecht unterliegen [Schneider2005]. Somit verschlechtert sich der Schutz der Patientenrechte diesbezüglich nicht, falls Patientendaten zu einer Auftragsdatenverarbeitung an externe Dritte weitergegeben werden.

3.1.7 Datennetze

Die elektronische Bereitstellung von Patientendaten ist in § 10 Bundesdatenschutzgesetz bzw. in § 8 Sächsisches Datenschutzgesetz unter der Überschrift *„automatische Abrufverfahren“* geregelt. Die Einrichtung eines derartigen Verfahrens ist nur *„unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen“* zulässig und wenn es nach den Aufgaben der beteiligten Stellen angemessen ist. Das Sächsisches Datenschutzgesetz fordert außerdem die Führung eines Verzeichnisses, welches den Zweck sowie Angaben zum Verfahren dokumentiert.

In [Bultmann2002] wird § 10 Bundesdatenschutzgesetz allerdings so interpretiert, dass ein *„Bereitstellen von Patientendaten durch einen Arzt über ein Datennetz“ „nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig“* ist. Sollte es hierbei zu einem Abruf durch nicht berechtigte Dritte kommen, liegt eine Straftat nach § 203 Strafgesetzbuch vor. Die Freigabe von Patientendaten durch Einwilligung des Patienten für den Zugriff eines Berechtigten ist außerdem nur im Einzelfall zulässig. Der behandelnde Arzt ist verpflichtet vor der Freigabe der Patientendaten zu prüfen, ob eine Befugnis zur Offenbarung der Patientendaten an den Empfänger für den konkreten Fall vorliegt. Sollte dem behandelnden Arzt nachgewiesen werden, dass er durch unterlassene technische oder organisatorische Maßnahmen nach § 9 Bundesdatenschutzgesetz den Abruf von Patientendaten nicht verhindert hat, handelt es sich hierbei wiederum um eine Verletzung von Privatgeheimnissen nach § 203 Strafgesetzbuch.

Neben den datenschutzrechtlichen Regelungen gibt es Gesetze, die sich mit der Infrastruktur von Datennetzen beschäftigen. In § 73a Sozialgesetzbuch 5 finden sich Regelungen zu so genannten Strukturverträgen. Diese Verträge können zwischen den Kassenärztlichen Vereinigungen und den Landesverbänden der Krankenkassen bzw. dem Ersatzkassen nach § 83 Sozialgesetzbuch V geschlossen werden und beinhalten Versorgungs- und Vergütungsstrukturen. Dies hat die Bildung von Praxisnetzen ermöglicht. Dabei handelt es sich um regional begrenzte Verbünde von niedergelassenen Ärzten. Weitgehend unklar ist die

Finanzierung derartiger Netze. Vor allem wenn zusätzlich der stationäre Bereich an der Vernetzung teilnehmen soll. Die unklare Finanzsituation verhinderte bisher eine sektorübergreifende Vernetzung. Abhilfe und Anreize gibt es erst seit dem inkrafttreten des Gesundheitsmodernisierungsgesetztes und dem damit verbundenen § 140 a ff Sozialgesetzbuch V, siehe Kapitel 2.4 „Integrierte Versorgung“.

Eine weitere rechtlich abgesicherte Möglichkeit der vertraglichen und elektronischen Vernetzung von Arztpraxen zu einem Praxisverbund bieten so genannte Modellvorhaben. Durch die*„Weiterentwicklung der Verfahrens-, Organisations-, Finanzierungs- und Vergütungsformen der Leistungserbringung“* müssen die Modellvorhaben eine Verbesserung von Qualität und Wirtschaftlichkeit zum Ziel haben, siehe § 63 Absatz 1 Sozialgesetzbuch 5. Desweiteren kann ein Modellvorhaben mit der Verhütung und Früherkennung von Krankheiten (§ 63 Absatz 2 Sozialgesetzbuch V) oder der Vermeidung von *„unkoordinierten Mehrfachinanspruchnahme von Vertragsärzten durch die Versicherten“* (§ 64 Absatz 4 Sozialgesetzbuch V) begründet werden. Modellvorhaben sind beschränkt auf eine Laufzeit von 8 Jahren und können nur von Vertragsärzten mit der Kassenärztlichen Vereinigung oder der Kassenärztlichen Bundesvereinigung geschlossen werden [Dierks1999].

3.1.8 Die zehn Gebote des Datenschutzes

Zu den grundlegenden Sicherheitsanforderungen zählen die in der Anlage zu § 9 Bundesdatenschutzgesetz definierten allgemeinen technischen und organisatorischen Maßnahmen zur Umsetzung des Bundesdatenschutzgesetzes. Die ehemals 10 Anforderungspunkte - daher der Name - sind mittlerweile in der Neufassung des Bundesdatenschutzgesetzes auf 8 Punkte komprimiert worden. Die Maßnahmen zum Schutz personenbezogener Daten lauten im Einzelnen:

1. Zutrittskontrolle – Nur Befugten ist der Zutritt zu Datenverarbeitungsanlagen zu gewähren.
2. Zugangskontrolle – Nur Befugte dürfen Datenverarbeitungssysteme benutzen können.
3. Zugriffskontrolle – Befugte dürfen nur die Daten verarbeiten können, zu denen sie nach ihren Zugriffsberechtigungen ermächtigt sind.
4. Weitergabekontrolle – Personenbezogene Daten dürfen bei der elektronischen Übertragung oder beim Speichern auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfrent werden können. Es muss weiterhin überprüfbar und feststellbar sein, welche Stellen Ziel der Übertragung sind.
5. Eingabekontrolle – Es muss nachträglich überprüft und festgestellt werden können, welche Daten von wem in ein Datenverarbeitungssystem eingegeben, verarbeitet oder entfernt wurden.
6. Auftragskontrolle – Im Auftrag verarbeitete personenbezogene Daten dürfen nur nach den Weisungen des Auftraggebers verarbeitet werden können.
7. Verfügbarkeitskontrolle – Personenbezogene Daten müssen gegen zufällige Zerstörung geschützt sein.
8. Daten die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden können.

Diese Sicherheitsmaßnahmen sind im Wesentlichen technischer Natur und anpassungs- bzw. erläuterungsbedürftig. Der Datenschutzbeauftragte des Bundes und die Datenschutzbeauftragten der Länder empfehlen daher, sich an der Verwendung von *„an den*

Daten ausgerichteten Sicherheitszielen“ zu orientieren [Bultmann2002], [Mueller2005]. Derartig angepasste Sicherheitsziele finden sich auch in den Neufassungen einiger Landesdatenschutzgesetze, siehe § 9 SächsDSG. Die grundlegenden Sicherheitsziele, die zur Verarbeitung medizinischer Daten gewährleistet sein müssen, sind:

1. Verfügbarkeit – Personenbezogene Daten müssen zeitgerecht in der benötigten Form zur Verfügung stehen. Dies setzt auch die Verfügbarkeit der zur Verarbeitung benötigten Komponenten des Informationssystems voraus.
2. Integrität – Personenbezogene Daten müssen während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben. Die Echtheit, Korrektheit und Vollständigkeit der Daten muss gewährleistet sein.
3. Vertraulichkeit – Durch die ärztliche Schweigepflicht geschützte Daten dürfen nur von Befugten zur Kenntnis genommen oder verarbeitet werden können.
4. Authentizität (Zurechenbarkeit der Daten) – Der Urheber bzw. Verantwortliche von personenbezogenen Daten sowie der Auslöser bzw. der Verantwortliche für einen Verarbeitungsvorgang muss jederzeit eindeutig feststellbar sein.
5. Nicht-Abstreitbarkeit von Datenübermittlungen – Der Sender eines patientenbezogenen Dokuments muss sicher sein können, dass der bestimmte Empfänger das Dokument erhalten hat und darf den Versand nicht abstreiten können. Der Empfänger muss sicher sein, dass genau dieses Dokument von angegebenen Absender stammt und darf seinerseits den Erhalt des Dokuments nicht abstreiten können.
6. Nutzungsfestlegung (Zugriffskontrolle) – Für jedes elektronisch zu verarbeitende personenbezogene Dokument müssen ein Benutzerkreis sowie abgestufte Nutzungsrechte und Nutzungsausschlüsse definierbar sein.
7. Revisionsfähigkeit von Kommunikationsprozessen – Alle Verarbeitungsprozesse müssen lückenlos nachvollziehbar sein. Es muss jederzeit festgestellt werden können, wer wann welche personenbezogenen Daten auf welche Weise verarbeitet hat. Siehe auch Kapitel 3.1.1 „Behandlungsvertrag“ und die sich daraus ableitende Dokumentationspflicht.
8. Rechtssicherheit von Kommunikationsprozessen – Für jeden Verarbeitungsvorgang sowie für die daraus resultierenden Ergebnisse ist der Verursachende beweiskräftig nachweispflichtig.

Neben den in § 9 BDSG aufgestellten Anforderungen und den angepassten Schutzzielen lässt die Neufassung des BDSG vom 23.5.2001 (Neubekanntmachung 14.1.2004) in § 9a die Prüfung und Bewertung des Datenschutzkonzeptes sowie der technischen Einrichtungen durch unabhängige Gutachter im Rahmen eines Datenschutzaudits zu. Diese Maßnahmen hat eine weitere Verbesserung des Datenschutzes und der Datensicherheit zum Ziel.

3.1.9 Weitere Aspekte

In diesem Abschnitt werden weitere Gesetzen und Verordnungen tabellarisch aufgelistet, die den Themenbereich der computergestützten Kommunikation im Gesundheitswesen tangieren. Ob diese rechtlichen Bestimmungen bei der praktischen Umsetzung eines Projektes zu beachten sind, sollte in der Phase der Projektplanung geprüft werden.

Gesetz, Verordnung	Themenbereich
Berufsordnung	Werbeproblematik; Fernbehandlung per Website, E-Mail
Informations- und Kommunikations-dienstegesetz (Multimediagesetz)	Bereitstellung von Telediensten (Provider)
Medizinproduktegesetz	Betreiber- und Anwendervorschriften für Medizinprodukte
Signaturgesetz, Signaturverordnung	Rahmenbedingungen für elektronische Signaturen
Strahlenschutzverordnung	Mobilfunktechniken (GPRS, UMTS), Funktechniken (WLAN); elektronische Geräte allgemein

Tabelle 3-1: Überblick weitere Gesetze

Zur Werbeproblematik zählt z.B. Werbung einer Praxis: „Mitglied in Ärztenetz ...“. In Deutschland herrscht Werbeverbot für Ärzte, d.h.: Werbung für die Teilnahme an Ärztenetzen ist untersagt. Dies betrifft auch die Anfertigung von Stempeln, Aufdrucken, Schildern, Briefbögen o.ä. mit einer Werbebotschaft. Lediglich durch das Ärztenetz in der Gesamtheit ist eine dreimalige Erwähnung drei Monate nach Gründung möglich. Siehe auch [Dierks1999].

3.1.10 Tabellarischer Überblick: Gesetze

In Tabelle 3-2 (Seite 37) sind die in den Abschnitten 3.1.1 – 3.1.8 erörterten gesetzlichen Anforderungen zusammengefasst.

Abschnitt	Was ist geregelt?	Gesetze	Bemerkungen
3.1.1 Behandlungsvertrag	Freie Arztwahl	SGB V	Innerhalb der vertragsärztlichen Versorgung, sonst nur im Notfall
	Erhebung der Patientendaten	BGB, BDSG	Datensparsamkeit; Einwilligung bei zusätzlich Daten
	Medizinische Dokumentation	MuBO	
	Auskunft und Einsicht	SaechsKHG, BDSG	Einschränkung bei psychischer Instabilität
3.1.2 Ärztliche Schweigepflicht	Schweigepflicht	SächsGDG, StGB, StPO, MuBO	Zusatzbedingung zu BDSG, SaechsDSG; trifft auch für Gehilfen des Arztes zu; Ausnahmen: übergeordnetes Wohl der Allgemeinheit, schriftlicher Behandlungsvertrag, Einwilligung durch den Patienten
3.1.3 Einwilligung	Informationelle Selbstbestimmung	GG, BDSG	Freiwilligkeit, Aufklärung, keine pauschale Einwilligung, Schriftform; IV Verträge bilden keine Ausnahme
3.1.4 Spezielle Regelungen bei der Arzt-zu-Arzt Kommunikation	Widerspruchsrecht bei geplante Datenübertragungen	SaechsDSG	
	Modellvorhaben, DMP, IV, eGK, Hausarztmodell	SGB V	Einwilligung des Patienten ist in allen Fällen nötig
3.1.5 Externe Dritte	Beauftragung zu Datenverarbeitungszwecken	BDSG	Erlaubt mit Einwilligung; Unbedenklich bei Einsatz geeigneter Maßnahmen (Verschlüsselung)
3.1.6 Beschlagnahmeverbot	Beschlagnahmeverbot, Zeugnisverweigerungsrecht	StPO	Gilt für Datenträger im Gewahrsam des Arztes oder beauftragter Dritte
3.1.7 Datennetze	Automatische Abrufverfahren	BDSG, SaechsDSG	Nur unter Berücksichtigung der Patienteninteressen; Verzeichnis
	Strukturverträge	SGB V	Unklare Finanzierung
	Modellvorhaben	SGB V	Dienen der Optimierung; zeitlich beschränkt
3.1.8 Datenschutz	Schutzziele	BDSG, SaechsDSG	Überprüfung durch Datenschutzbeauftragte und Audits

Tabelle 3-2: Übersicht Gesetze

3.2 Technische Anforderungen

Bei den technischen Anforderungen computergestützter, sektorübergreifender Kommunikation im Gesundheitswesen wird eine Unterteilung in zwei Abschnitte vorgenommen. Der erste Abschnitt beschäftigt sich mit den funktionalen Anforderungen an die Technik und zeigt auf, welche Eigenschaften beim Einsatz technischer Lösungen aus Sicht der Benutzer von Bedeutung sind. Der zweite Abschnitt setzt sich mit den technischen Rahmenbedingungen auseinander, die beim Einsatz technischer Lösungen zu beachten sind.

3.2.1 Funktionale Anforderungen an die Technik

Funktionale Anforderungen spiegeln die Erwartungen der späteren Anwender wider und beeinflussen die technischen Eckdaten der zum Einsatz kommenden Lösung für die computergestützter Kommunikation im Gesundheitswesen. Sind Anforderungen verletzt, sinkt die Akzeptanz der Anwender und negative Effekte können auftreten, wie z.B. Verzögerungen durch zu komplexe Arbeitsabläufe [Beyer2004], [Mueller2005].

Einige funktionale Anforderungen ergeben sich bereits aus den gesetzlichen Rahmenbedingungen. An erster Stelle wird dort die Verfügbarkeit medizinischer Daten gefordert. Dass heißt, medizinische Daten müssen zur richtigen Zeit, am richtigen Ort, im richtigen Format und vollständig vorliegen. Die an dieser Stelle geforderte Präzision, ist eine Stärke technischer Verfahren. Voraussetzung dafür ist jedoch die Verfügbarkeit der Informationstechnik, die an der technischen Umsetzung beteiligt ist. Hier müssen die technischen Rahmenbedingungen aus Abschnitt 3.2.2 so gewählt werden, dass die Verfügbarkeit zu jeder Zeit gewährleistet ist. Maßnahmen sind bsw. die redundante Auslegung wichtiger Komponenten sowie die Berücksichtigung von Ausfallkonzepten.

Eine zentrale Anforderung bei der Verarbeitung von Patientendaten ist die Sicherstellung des Datenschutzes. Eine technische Lösung im medizinischen Sektor muss die gesetzlich geforderten Sicherheitsmaßnahmen berücksichtigen. Dazu gehören Integrität, Vertraulichkeit, Authentizität und Nutzungsfeststellung. Diese Anforderungen sind bereits in Kapitel 3.1.8 behandelt. Es gilt technischen Rahmenbedingungen zu schaffen, die die funktionalen Anforderungen unterstützen. Die Sicherheit der Patientendaten kann bspw. nur durch den ordnungsgemäßen Einsatz sicherer Verfahren, wie der digitalen Signatur, Public-Key Infrastrukturen oder darauf basierende Methoden, erreicht werden. Die Einführung zusätzlicher Arbeitsschritte führt in der Regel zu einer ablehnenden Grundhaltung gegenüber technischen Neuerungen bei den Nutzern. Dem kann begegnet werden, indem die Nutzer für den verantwortungsvollen Umgang mit diesen Verfahren geschult werden. Auf diese Weise wird das Verständnis für die technischen Abläufe und deren Nutzen vermittelt. Mit diesem Wissen lässt sich eine weitere wichtige funktionale Anforderung positiv beeinflussen: die Forderung der Nutzer nach einer möglichst einfachen Bedienung einer technischen Lösung.

Praktikabilität und Gebrauchstauglichkeit, auch unter dem Begriff Usability (ISO 9241-11 [ISOHP]) bekannt, sind entscheidende Kriterien für die Beherrschbarkeit eines technischen Systems [Mueller2005]. Die technischen Rahmenbedingungen sind diesbezüglich so zu gestalten, dass die Beteiligten optimal bei der Erfüllung ihrer Aufgaben unterstützt werden.

Die Entwicklungen in Medizin und Technik schreiten zügig voran, sodass Flexibilität und Erweiterbarkeit technischer Lösungen zusätzliche Anforderungen darstellen. Einmal etablierte Lösungen sollen mit geringem Aufwand einer veränderten Situation angepasst werden können, [Beyer2004].

Weitere gesetzlich verankerte funktionale Anforderungen sind die Nicht-Abstreitbarkeit, Revisionsfähigkeit und Rechtssicherheit von Kommunikationsprozessen. Diesen Anforderungen kann technisch durch Quittungsbetrieb und Protokollierung Rechnung getragen werden.

Bei der Einführung einer technischen Lösung gibt es gerade bei komplexen System, wie den Informationssystemen im Gesundheitswesen, die Forderung nach Integration. Auf diesem Gebiet gibt es viele Facetten und Herausforderungen, weshalb hier gesondert auf dieses Thema eingegangen werden soll.

Integration

Der Begriff Integration hat unterschiedliche Bedeutungen in den verschiedenen Bereichen von Mathematik bis Soziologie. In Bezug auf den Themenbereich dieser Arbeit wird Integration aus Sicht der Informatik, im speziellen der Softwareentwicklung, als die Verknüpfung von Anwendungssystemen verstanden. Integration dient dabei primär der Vermeidung von Schnittstellen.

Integration kann grob in Funktionsintegration, Datenintegration und Geschäftsprozessintegration unterschieden werden.

Funktionsintegration ist die Zusammenfassung mehrerer eigenständiger Anwendungen mit unterschiedlichen Funktionsbereichen zur gemeinsamen Bearbeitung einer Aufgabe zu einer komplexen Anwendung. Durch die Zusammenfassung werden Mehrfachimplementierungen von Funktionen und Schnittstellen zum Datenautausch zwischen den Anwendungen vermieden.

Bei der Datenintegration liegt mehreren Anwendungen ein gemeinsames Datenmodell zu Grunde. Die Anwendungen greifen auf einen Datenbestand zu und vermeiden so Redundanzen [Wendt2005].

Geschäftsprozessintegration nutzt eine Integrationsplattform, um verschiedene Funktionen der Geschäftsprozesse zu vereinen. Dies hat den Vorteil, dass die Anwendungen unberührt bleiben und bspw. auf Standardanwendungen zurückgegriffen werden kann. Für die Integration ist allein die Integrationsplattform zuständig. Mit Hilfe eines komplexen Regelwerkes werden Daten in der richtigen Reihenfolge übergeben und die Ergebnisse weitergeleitet. Im Gegensatz zur Funktions- und Datenintegration entstehen so leichter wartbare Systeme, da sämtliche Integrationsaspekte in der Integrationsplattform konzentriert sind [quelle][EAI].

Durch zusätzliche Sichten auf die Integrationsproblematik können noch weitere Integrationsarten unterschieden werden [Wendt2005].

Von semantischer Integration ist die Rede, wenn unterschiedliche Anwendungen Daten in gleicher Weise interpretieren. Dies ist z.B. bei der Benutzung eines gemeinsamen Begriffsystems der Fall.

Physische Integration besteht, wenn die für die Bearbeitung der Daten nötige physische Infrastruktur vorhanden ist. Ein Beispiel dafür ist die Installation verschiedener Anwendungen auf einem Rechner.

Muss ein bestimmter Kontext nur einmal hergestellt werden und steht dieser dann verschiedenen Anwendungen automatisch zur Verfügung, wird dies als Kontextintegration bezeichnet. Bei der

Auswahl eines Patienten im Patientenverwaltungssystem wird bei Kontextintegration bspw. automatisch der entsprechende Patient im OP-Planungssystem selektiert.

3.2.2 Technische Rahmenbedingungen

In diesem Abschnitt werden die technischen Rahmenbedingungen untersucht. Dazu zählen bspw. Leistungsparameter von Hard- und Softwarebausteinen aber auch Eckdaten von Supportverträgen wichtiger Komponenten.

Hard- und Softwarekomponenten werden getrennt voneinander betrachtet. Unter dem Begriff Hardware sind alle physischen Datenverarbeitungskomponenten zusammengefasst. Wobei diese weiter in Computern, dazu zählen z.B. Arbeitsplatz-PCs und Server, und Kommunikationsinfrastruktur strukturiert und daher separat betrachtet werden.

Im nachfolgenden Abschnitt werden folgende Bezeichnungen benutzt:

Abkürzung	Vollständige Benennung der Anforderung
Protokoll	Nicht-Abstreitbarkeit, Revisionsfähigkeit und Rechtssicherheit von Kommunikationsprozessen
Usability	Praktikabilität und Gebrauchstauglichkeit
Erweiterbarkeit	Flexibilität und Erweiterbarkeit technischer Lösungen
Sicherheit	Sicherheit (Integrität, Vertraulichkeit, Authentizität und Nutzungsfeststellung)

Tabelle 3-3: Abkürzungen für Anforderungen

Betrachtungen zur Computer-Hardware

Generell lassen sich Computer in Arbeitsplatz-PCs, in der Regel die Clients, und Server unterscheiden. An dieser Stelle wird auf die unterschiedliche Bedeutung von Arbeitsplatz-PCs und Servern eingegangen. Der Ausfall eines Arbeitsplatz-PCs hat bspw. die vorübergehenden Beeinträchtigung eines einzelnen Mitarbeiters zur Folge. Im Gegensatz dazu stellen Server in der Regel für viele Anwendungssysteme bzw. Benutzer Anwendungen, Dienste oder Daten bereit. Deshalb nehmen sie eine zentralen Rolle im Informationssystem ein. Diese Rolle muss bei der Umsetzung der Anforderungen berücksichtigt werden. So sind Leistungsparameter anhand des geplanten Einsatzzweckes und der zu erwartenden Nutzerzahl angemessen zu dimensionieren. Besonders ist auf Verfügbarkeit und Sicherheit zu achten. Die Verfügbarkeit und Sicherheit kann durch zusätzliche Maßnahmen wie:

- Schaffung von Redundanzen: doppelte Netzteile, Einsatz von Festplattenarrays (RAID)
- Einsatz von Komponenten für eine unterbrechungsfreien Stromversorgung (USV)
- Unterbringung in einem Rechenzentrum (Zugangskontrolle, Betriebssicherheit, Klimatisierung)
- Bedienung durch geschultes Personal (Administrator)

erhöht werden. Generell kann eine hohe Verfügbarkeit durch die Vermeidung von Single-Point-of-Failures erreicht werden. Punkt eins der aufgeführten Maßnahmen geht bereits in diese Richtung. Zusammenfassend kann zur Ausfallproblematik einzelner Bauteile oder gar ganzer

Rechner die folgende Empfehlung formuliert werden: Für wichtige Komponenten müssen Ausfallkonzepte bereitstehen, um den Produktivbetrieb im Havariefall nicht oder nur so kurz wie möglich zu beeinträchtigen.

Beachtung finden sollten außerdem Garantiezeiten und Ausfallquoten einzelner Bauteile. Auch in Bezug auf Wartungsverträge und Support müssen bei Servern strengere Auflagen gemacht werden.

In der folgenden Tabelle 3-4 sind die wichtigsten Eckdaten für die Computer-Hardware zusammengefasst. Die Tabelle gliedert sich in die Spalte 'Kategorie', in der die Anforderungen aufgeführt sind. Die Spalte 'Parameter, Maßnahmen und Hinweise' liefert jeweils die dazu passenden Erläuterungen.

Kategorie	Parameter, Maßnahmen und Hinweise
Leistung	Parameter: CPU, Speicher, Grafik, Festplatte, Schnittstellen
Verfügbarkeit	Parameter: Lebensdauer, Ausfallquoten Maßnahmen: Redundanz, USV, Auswahl qualitativ hochwertiger Komponenten Hinweis: bei Servern von zentraler Bedeutung
Sicherheit	Maßnahmen: Zugangskontrolle, Betriebssicherheit (Dokumentation und Schulung), Einsatz von Spezialhardware (Chipkartenleser, Geräte die Biometrische Verfahren unterstützen, Kryptographiechips)
Protokoll	Hinweis: wird in der Regel nicht unterstützt
Usability	Maßnahmen: Ergonomie beachten z.B. bei Tastaturen und Bildschirmen
Erweiterbarkeit	Maßnahmen: angemessene Hardware einsetzen mit Blick auf sich abzeichnende Entwicklungen Hinweis: Leistungsreserven einplanen
Integration	Maßnahmen: Auswahl von Hardware-Komponenten, die sich in die vorhandene Hardwarelandschaft integrieren. Bspw. durch die Auswahl von vergleichbaren Geräten einer Firma oder Bauart -> auch Sinnvoll bei Supportverträgen
Support	Parameter: Garantiezeiten, Reaktionszeiten Maßnahmen: Wartungsverträge und festgelegte Reaktionszeiten im Fehlerfall Hinweis: Garantie- und Reaktionszeiten müssen für Server höher als für Arbeitsplatz-PCs bewertet werden.

Tabelle 3-4: Anforderungen an Computer-Hardware (Arbeitsplatz-PCs, Server)

Vergleichbar mit den Anforderungen für Server sind die Anforderungen und technischen Rahmenbedingungen für wichtige Komponenten der Kommunikationsinfrastruktur.

Anforderungen an die Komponenten der Kommunikationsinfrastruktur (Netzwerkkomponenten)

Zu diesen physischen Datenverarbeitungbausteinen zählen unter anderem Router, Gateways, Modems, Firewalls und Accesspoints. Für diese Geräte ist es charakteristisch, dass sie zum einen aus einem physischen Baustein und zum anderen aus einer speziellen Software, der Firmware, bestehen. Durch einen immer komplexer werdenden Funktionsumfang und umfangreichere Konfigurationsmöglichkeiten erhöht sich zunehmend die Bedeutung der Firmware derartiger Geräte. Mit Blick auf die Datenblätter aktueller Netzwerkkomponenten, ist ein Trend hin zu Geräten zu verzeichnen, die viele der genannten Funktionen integrieren. Ein Beleg dafür sind bspw. die von Providern angebotenen Router, die neben Einwahl, Routing, WLAN-, Ethernet- und USB-Schnittstellen auch VPN-Clients uvm. im Funktionsumfang haben.

Typische Leistungsparameter von Kommunikationstechniken sind Bandbreite, Latenz und Quality-of-Service (QoS). Die Bandbreite beschreibt, welche Datenmenge in einer bestimmten Zeit maximal übertragen werden kann. Die Latenz gibt die Zeitverzögerung bei der Übertragung an und Quality-of-Service ermöglicht eine Priorisierung von Diensten. Diese Parameter sind abhängig von der zu unterstützenden Aufgabe festzulegen. Anhand eines Vergleichs mit den Parametern der tatsächlich zur Verfügung stehenden Kommunikationstechniken, können dann Aussagen bezüglich der Durchführbarkeit, der zu erledigenden Aufgabe, getroffen werden. Mit anderen Worten: die Erfüllung welcher Aufgaben in welcher Qualität möglich ist, ist Abhängig von der am Standort zur Verfügung stehenden Netzwerkanbindung. Steht bspw. nur ein ISDN-Zugang zur Verfügung, muss bei der Übertragung großer Datenmengen, wie z.B. bei medizinischen Bilddaten, eine entsprechende Übertragungszeit berücksichtigt werden.

Um eine höhere Verfügbarkeit der Netzwerkkomponenten zu erreichen, lässt sich ebenfalls das Aufbauen von Redundanzen nutzen. So können Komponenten parallel über Load-Balancing betrieben werden um Lastspitzen abzufangen sowie im Fall einer Störung den problemlosen Austausch zu ermöglichen. Eine Erhöhung der Verfügbarkeit durch Redundanz wird auch durch die Verwendung von Geräten gewährleistet, die einen Zugang zu Netzen über mehrere Einwahlmöglichkeiten bereitstellen. Mit dieser integrierten Redundanz kann ein Router, der primär einen Breitbandzugang bietet, bei Ausfall seines Primärzugangs dennoch eine Netzwerkverbindung über einen Sekundärzugang herstellen. Dies kann z.B. eine Schmalbandverbindung (ISDN, Modem) oder eine Funkverbindung (UMTS) sein.

Router, Gateways und Accesspoints stellen Schnittstellen zu anderen Netzen dar und bedürfen deshalb verstärkter Sicherheitsmaßnahmen. An dieser Stelle ist der Einsatz kryptographischer Verfahren notwendig, welche die Sicherheitsanforderungen erfüllen. Diese Verfahren finden bei der Authentifizierung der Kommunikationsendpunkte (z.B. eines Routers) bzw. bei der Transportsicherung Verwendung. Eine Kombination aus Authentifizierung und Transportsicherung bieten bsw. Virtual-Private-Networks (VPN), die eine sichere Verbindung zwischen zwei oder mehreren Kommunikationsteilnehmern oder ganzen Netzten herstellen können. Sie sind in der Lage sichere Tunnel durch unsichere Netzte, wie dem Internet, herzustellen.

Ein möglicher Angriffspunkt bei der Verbindung zum Internet ist der Router. Einen weiteren Angriffspunkt stellen Angriffe „von innen“ dar, welche durch unachtsam geöffnete Webseiten oder E-Mails mit schadhaften Anhängen ausgelöst werden können. Daher fordern Datenschützer die strickte physische Trennung von Internet und Intranet [D2D2005]. Die Kommunikation

medizinischer Daten kann daher durch die Einwahl über Provider von speziellen Netzen für das Gesundheitswesen [DGNHP], [TelemedHP], [IMOTIONHP] vorgenommen werden.

Eine Protokollierung zur Sicherstellung von Nicht-Abstreitbarkeit und Revisionsfähigkeit wird auf Ebene der Kommunikationsinfrastrukur nur im Rahmen der Aufzeichnung von Einwahlvorgängen vorgenommen. Diese Protokolle können aber bestenfalls als Indiz für eine Datenübertragung dienen.

Integrationsbemühungen müssen bei der Kommunikationsinfrastruktur kritisch betrachtet werden. Der Zugang über die sicheren Netze für das Gesundheitswesen sind die Voraussetzung für Datenübertragungen von medizinischen Dokumenten. Eine Integration in Richtung Internet gilt es aufgrund der oben beschriebenen Anfgriffsmöglichkeiten zu vermeiden. Als Optimal wird eine physische Trennung von medizinischem Intranet und Internet angesehen, um möglichen Angreifern und Angriffsszenarien [Wozak2004] aus dem Weg zu gehen.

Support- und Wartungsverträgen sollte ebenfalls ein hoher Stellenwert eingerechnet werden, um Verfügbarkeit und Sicherheit dauerhaft zu gewährleisten.

Die folgende Tabelle fasst die wichtigsten Rahmenbedingung für die Komponenten von Kommunikationsinfrastrukturen zusammen.

Kategorie	Parameter, Maßnahmen und Hinweise
Leistung	Parameter: Bandbreite, Latenz, QoS, Schnittstellen
Verfügbarkeit	Maßnahmen: Redundanz, Load-Balancing
Sicherheit	Maßnahmen: Zugangskontrolle, Betriebssicherheit (Dokumentation und Schulung), Integrität (fehlertolerante Protokolle), Authentifizierung und Verschlüsselung der Kommunikation (Einsatz kryptographischer Verfahren: Zertifikate, Transportverschlüsselung)
Protokoll	Hinweis: teilweise Unterstützt (Protokollierung von Einwahlzeiten)
Usability	Unterschiedlich je nach Personengruppe: → Komplizierte Sicht zur Administration für geschultes Personal (Administrator) → Einfache Sicht (Ein/Aus/Reset) für Benutzer Erklärung: Netzwerkkomponenten sollen auf Grund meist komplexer Netzwerkstrukturen von Administratoren konfiguriert und gewartet werden.
Erweiterbarkeit	Hinweis: Ist gegeben, da dies Sinn und Zweck eines Netzwerkes ist.
Integration	Maßnahmen: Auswahl neuer Komponenten, die sich in vorhandene Infrastruktur (Netzwerktopographie) einpassen.
Support	Parameter und Maßnahmen: Siehe Hardware Hinweis: Garantie- und Reaktionszeiten zentraler Netzwerkkomponenten höher bewerten.

Tabelle 3-5: Anforderungen an die Komponenten der Kommunikationsinfrastruktur

Anforderungen an die Software

Software umfasst die logischen Datenverarbeitungsbausteine, also Betriebssysteme und Anwendungsprogramme [Winter2002].

Anforderungen an die Leistungsfähigkeit von Softwareprodukten ist vor allem der Funktionsumfang. Beim Stichwort Leistung muss geprüft werden, in wie weit sich mit dem Funktionsumfang einer Softwarelösung die zu unterstützende Aufgabe erledigen lässt.

Die Verfügbarkeit von Softwareprodukten ist von der Verfügbarkeit der involvierten physischen Datenverarbeitungsbausteine abhängig. Maßnahmen zur Steigerung der Stabilität liegen in der Regel beim Hersteller und entziehen sich dem Einfluß der Anwender. Einmal bekannt gewordene Sicherheitslöcher werden in der Regel von Seiten der Hersteller durch das Bereitstellen von Updates und Patches behoben. Auch Softwareprodukte unterliegen einer regelmäßigen Wartung, bei der diese Softwareaktualisierungen eingespielt werden.

Software ist in entscheidendem Maße für die Sicherheit verantwortlich. Die gesetzlich geforderten Maßnahmen zielen deshalb vor allem auf die Sicherheit von und durch Software. Zur Wahrung der Integrität muss Software die Echtheit, Korrektheit und Vollständigkeit der Daten garantieren. Vertraulichkeit, Authentizität und Nutzungsfeststellung sind in Software umzusetzende gesetzliche Anforderungen zum Schutz der Patientendaten und damit des Vertrauensverhältnisses zwischen Arzt und Patient. Maßnahmen zur Erfüllung dieser Sicherheitsanforderungen sind der Einsatz von sicheren Methoden, wie kryptographischen Verfahren, im Zusammenhang mit der Regelung der Zugriffsrechte. Mit Hilfe von Rollenkonzepten, Zertifikaten, digitalen Signaturen und Public-Key Infrastrukturen werden die Anforderungen erfüllt.

Nicht-Abstreitbarkeit, Revisionsfähigkeit und Rechtssicherheit von Datenverarbeitungsprozessen muss durch Softwareprodukte ebenfalls unterstützt werden. Maßnahmen hierfür sind bspw. der Quittungsbetrieb und die manipulationssichere Protokollierung der Datenverarbeitungsprozesse bspw. durch das Signieren der Protokolle.

Trotz der komplexen Anforderungen an Software muss die Praktikabilität und Gebrauchstauglichkeit für die Anwender gewahrt werden. Hierbei helfen softwareergonomische Ansätze, Komplexität und Usability optimal zu verknüpfen, um die Akzeptanz der Nutzer zu erlangen.

Erweiterbarkeit und Flexibilität kann bspw. durch die gezielte Verwendung von Software, die im Source-Code vorliegt (Open Source), die Bevorzugung offener Schnittstellen und durch Modularisierte Software erreicht werden. Der fortschreitenden Entwicklungen von Medizin und Technik kann so Rechnung getragen werden.

Bei der Integration neue Softwareprodukte in ein bestehendes Informationssystem gibt es viele Aspekte zu beachten [Wendt2005], [Lehmann2002]. Eine zusätzliche Verschärfung verfährt die Integrationsproblematik, wenn Software die heterogenen Informationssysteme in stationären und ambulanten Bereich im Gesundheitswesen verknüpfen soll [Lenz2005]. Als Parameter für diese Fragen können die Integrationsarten dienen. Zielorientiert kann zusammen mit allen Beteiligten eine individuelle Lösung gefunden werden.

Bei produktiv eingesetzter Software ist darauf zu achten, dass Wartungsverträge Bedingungen enthalten, die die zeitnahe Korrektur von Fehlern und das Einpflegen neuer Funktionen bei geänderten Rahmenbedingungen regeln.

Anforderungen an die Software fasst die folgende Tabelle zusammen.

Kategorie	Parameter, Maßnahmen und Hinweise
Leistung	Parameter: Funktionsumfang
Verfügbarkeit	Parameter: Stabilität Maßnahmen: Fehlerbehandlung
Sicherheit	Parameter: Integrität, Vertraulichkeit, Authentizität, Nutzungsfeststellung Maßnahmen: Einsatz sicherer Methoden, wie kryptographischer Verfahren (Zertifikate, digitale Signaturen, Public-Key Infrastrukturen)
Protokoll	Parameter: Nicht-Abstreitbarkeit, Revisionsfähigkeit und Rechtssicherheit Maßnahmen: Protokollierung der Verarbeitung insbesondere der Kommunikationsvorgänge (Wer hat Wann, Welche Daten verarbeitet), manipulationssiches speichern der Protokolle
Usability	Hinweis: Software Ergonomie beachten (Farben, Menustrukturen, uvm.)
Erweiterbarkeit	Maßnahmen: Modularisierung, Schnittstellen, Plugins Hinweis: Plattformunabhängigkeit ist ein Flexibiltätsmerkmal
Integration	Parameter: Integrationsarten (Funktions-, Daten- , Geschäftsprozess-Kontextintegration, Physische und Semantische Integration) Maßnahmen: sehr Vielfältig und Individuell
Support	Parameter: Reaktionszeiten Maßnahmen: Verpflichtung der Hersteller zur Bereitstellung von Updates und Bugfixes. Abschließen von Wartungsverträgen und festlegen von Reaktionszeiten im Fehlerfall.

Tabelle 3-6: Anforderungen an die Software

3.2.3 Übersicht technische Anforderungen

Die folgende Tabelle umfasst die technischen Anforderungen und stellt sie den Technikbereichen gegenüber. Die durch ein 'x' gekennzeichneten Felder, weisen darauf hin, welche Anforderung von welchem Bereich hauptsächlich abgedeckt wird bzw. eine große Rolle spielt.

Anforderung\Bereich	Computer	Netzwerk	Software
Leistung	x	x	x
Verfügbarkeit	x	x	x
Sicherheit		x	x
Protokoll			x
Usability	x		x
Erweiterbarkeit	x	x	x
Integration			x
Support	x	x	x

Tabelle 3-7: Übersicht technische Anforderungen

Aus dieser Tabelle ersichtlich ist, dass Software eine enorme Bedeutung hat. Alle Anforderungen müssen von ihr bedient werden. Dies ist nicht verwunderlich, da Software die Schnittstelle zum Nutzer und der unterstützenden Hardware darstellt.

3.3 Ökonomische Anforderungen

Ohne die Festlegung ökonomischer Rahmenbedingungen ließen sich die meisten Anforderungen in optimaler Weise erfüllen. Finanzielle Ressourcen sind jedoch begrenzt und sogar Motivation für die Einführung computerbasierte Kommunikation im Gesundheitswesen.

Das Einsparpotential, das computerbasierte Kommunikation im Gesundheitswesen bietet, ist beachtlich. Modellrechnungen für das elektronische Rezept oder die elektronische Arzneimitteldokumentation belegen dies [Lux2005]. Im Gegensatz zur rechnerbasierten Kommunikation von Behandlungsdaten oder der elektronischen Patientenakte lassen sich für diese Anwendungsfälle mit ihren gut strukturierten Daten Berechnungen auf einer soliden empirischen Basis anstellen.

Für das Einsparpotential bei der computerbasierten Kommunikation von Arztbriefen liegen bislang keine Angaben vor. Einsparungen kann es jedoch schon durch die Vermeidung von Medienbrüchen und die Verbesserung der Qualität bei der Kommunikation, was die Rechtzeitigkeit, Vollständigkeit und Fehleranfälligkeit betrifft, geben. Wie hoch diese Einspareffekte sind, und ob sie zur Finanzierung der Einführung computerbasierte Kommunikationsformen zwischen stationären und niedergelassenen Bereich ausreichen werden, ist nicht geklärt und sollte in Pilotprojekten untersucht werden.

Nicht für jede Krankheit und jeden Bereich werden sofort integrierte Versorgungsverträge geschlossen. Damit steht nicht automatisch jedem Vorhaben die durch die Verträge nach § 140a-d SGB V zugesicherte Anschubfinanzierung zur Verfügung.

Um mit den finanziellen Ressourcen schonend umzugehen, lohnt sich das Aufstellen ökonomischer Anforderungen. Diese Anforderungen beziehen sich weitest gehend auf die Nutzung der vorhandenen Ressourcen und die Nutzung bereits vorhandener Technologien. Oft sind bereits die Voraussetzungen für die Umsetzung einer Anforderung erfüllt und es kann auf die Anschaffung neuer Systeme verzichtet werden. Ähnlich verhält es sich bei der Entscheidung eine neue Technologie zu entwickeln oder auf ein bereits verfügbares Verfahren zurückzugreifen. Da eine Neuentwicklung in der Regel um ein vielfaches teurer ist, sollten die Einsatz- und Anpassungmöglichkeiten etablierter Verfahren geprüft werden.

Die folgende Tabelle zeigt eine Übersicht der ökonomischer Anforderungen.

Anforderung	**Bemerkungen und Hinweise**
Keine Eigenentwicklung	Vorteil Eigenentwicklung: alle Anforderungen können erfüllt werden Nachteil: teuer, zeitaufwändig
Nutzung vorhandener Ressourcen	Dies können vorhandene Computer, Netzwerkkomponenten oder Softwareprodukte sein
Outsourcing	Konzentration auf die Kernkompetenzen und Nutzung von unternehmensfremden Know-How, wo dies ökonomisch sinnvoll ist. z.B. Nutzung von Providern von Medizin Netzen, statt des Aufbaus eigener Infrastrukturen.
Vermeidung proprietärer Lösungen	Nachteil proprietärer Lösungen: Schränkt die Modularisierung ein und erschwert oder verhindert die Integration. Starke Herstellerbindung.
Betriebs- und Wartungskosten, Supportverträge, Lizenzkosten	Müssen den Prioritäten der einzelnen Komponenten angepasst werden, wo dies möglich ist. Auf transparente Lizenzverträge ist zu achten.
Investitionsschutz	Die Entscheidung für eine Lösung sollte auf Zukunfssicherheit untersucht werden (Firmenumfeld, sich abzeichnende zukünftige Lösungen).

Tabelle 3-8: Übersicht der ökonomische Anforderungen

3.4 Anforderungskatalog

Mit diesem Abschnitt werden abschließend alle Anforderungen zusammengefasst.

Gesetzliche Anforderungen	Resultierende Maßnahmen
Schutzziele	
Verfügbarkeit	Dokumentationspflicht, (Hoch-) Verfügbarkeit der Daten und IT-Systeme sicherstellen
Integrität	Digitale Signatur verwenden
Vertraulichkeit	Verschlüsselung mit Public-Key Verfahren verwenden
Authentizität	Digitale Signatur, Protokoll verwenden
Nicht-Abstreitbarkeit	Quittung, Protokoll
Nutzungsfeststellung	Zugangskontrolle, Chipkarten
Revisionssicherheit	Protokoll, Dokumentationspflicht
Rechtssicherheit	Protokoll, digitale Signatur
Weitere Anforderungen	
Freie Arztwahl	Technische Verfahren müssen dies gewährleisten
Aufklärung	Erklärung/Schulung Personal und Patienten
Patienteneinwilligung	Schriftliche Einwilligung, digitale Signatur
Datensparsamkeit	Auswahlmöglichkeiten der zu kommunizierenden Dokumente

Tabelle 3-9: gesetzliche Anforderungen

Technische Anforderungen	Resultierende Maßnahmen
Kernanforderungen	
Verfügbarkeit	Redundanz, Load-Balancing, Fehlerbehandlung, Ausfallkonzepte
Sicherheit	Zugangskontrolle, Schulung, Einsatz sicherer Methoden, kryptographische Verfahren (Zertifikate, digitale Signaturen, Public-Key Infrastrukturen)
Nachvollziehbarkeit	Quittungsbetrieb, manipulationssichere Protokollierung der Datenverarbeitungsprozesse
Usability	Beachtung der Ergonomie
Erweiterbarkeit und Flexibilität	Produkte mit Blick auf sich abzeichnende Entwicklungen auswählen, Leistungsreserven einplanen, Modularisierung, (offene) Schnittstellen bevorzugen, Plugins
Integration	Vorauswahl neuer Komponenten, die sich in vorhandene Infrastruktur einpassen. Individuelle Lösung finden. Hinweise bieten Integrationsarten.
Weitere Anforderungen	
Leistung	Angemessene Dimensionierung der Bauteile und Teilsysteme.
Support	Abschließen von Wartungs- und Supportverträge.

Tabelle 3-10: technische Anforderungen

ökonomische Anforderungen	Resultierende Maßnahmen
Keine Eigenentwicklung	Auf vorhandene Techniken und Verfahren zurückgreifen.
Nutzung vorhandener Ressourcen	Prüfen, wo dies sinnvoll ist oder wo Neuanschaffungen besser geeignet sind.
Konzentration auf Kerngeschäft	Outsourcing, nutzen von Dienstleistern.
Vermeidung proprietärer Lösungen	Prüfen, ob sich vergleichbare offene Lösungen finden lassen.
Betriebs- und Wartungskosten, Supportverträge, Lizenzkosten	Staffelung der Verträge nach Prioritäten. Verhandlungen über angepasste Lizenzkosten mit den Herstellern.
Investitionsschutz	Anvisierte Lösung auf Zukunftsfähigkeit prüfen.

Tabelle 3-11: ökonomische Anforderungen

4 Verfahren zur Unterstützung der Kommunikation

Nach dem im vorangegangenen Kapitel die vielfältigen Anforderungen erfasst wurden, widmet sich dieses Kapitel den Verfahren, die für die computerbasierte Kommunikation zwischen den zu untersuchenden Bereichen zur Verfügung stehen. Der Begriff 'Verfahren' wird dabei als Art und Weise der Durchführung z.B. eines Kommunikationsvorganges verstanden.

Computerbasierte Kommunikation findet in der Regel mit Hilfe eines Netzwerkes statt. Die über das Netzwerk verbundenen Rechner kommunizieren nach festen Regeln, den Netzwerkprotokollen, siehe OSI-Referenzmodell (ISO 7498-1, DIN ISO 7498, ITU-T X.200). Die Rechner nehmen dabei unterschiedliche Rollen ein. Server-Computer bieten Dienste an, während Client-Computer diese Dienste nutzen. Dienste sind in sich geschlossene Anwendungsprogramme, die eine bestimmte Funktionalität oder Informationen bereitstellen [Tanenbaum2000]. Welche Rechner welche Rolle einnehmen beschreibt die Architektur eines Netzwerks. Zunächst werden deshalb drei verbreitete Netzwerkarchitekturen vorgestellt und der so genannte Kommunikationsmodus erläutert. Dann werden allgemeine computerbasierte Kommunikationsverfahren besprochen, die in den unterschiedlichsten Bereichen Verwendung finden, von der Wirtschaft bis hin zum Privatgebrauch. Anschließend werden zwei Verfahren vorgestellt, die speziell für die Bedürfnisse des Gesundheitswesens entwickelt wurden. Zum Abschluss dieses Kapitels werden alle Kommunikationsverfahren in einer Übersicht zusammengefasst.

4.1 Vorbetrachtungen

4.1.1 Architekturen

Im dieser Arbeit werden die in Abbildung 4-1 dargestellten drei Architekturen unterschieden.

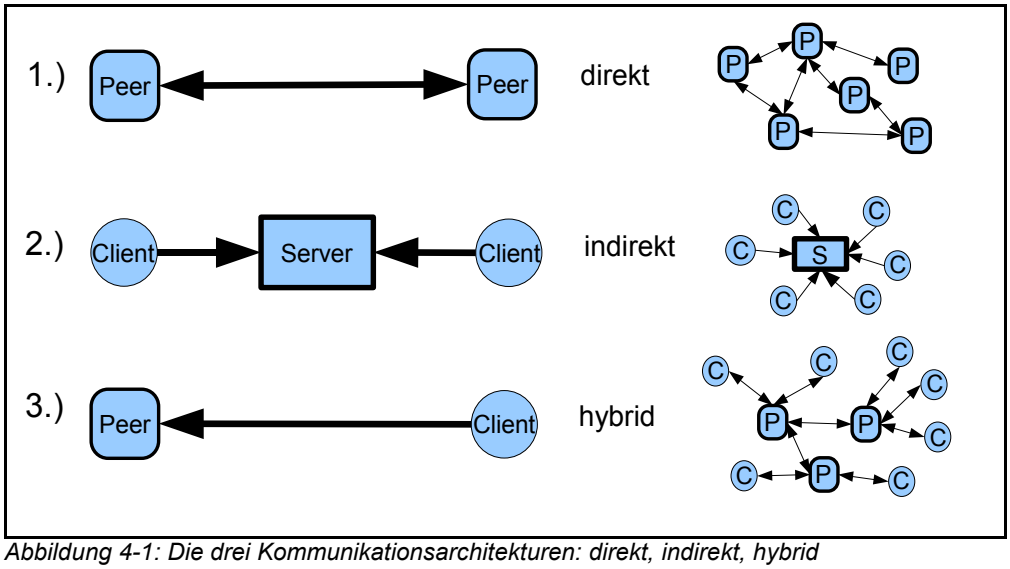

Abbildung 4-1: Die drei Kommunikationsarchitekturen: direkt, indirekt, hybrid

Die Übersicht in Abbildung 4-1 fasst Kommunikationsarchitekturen zusammen und nimmt dabei keine Unterscheidung zwischen Hard- und Softwarekomponenten vor. Es werden vielmehr prinzipielle elektronische Kommunikationsmöglichkeiten beschrieben.

Die in Abbildung 4-1 dargestellten Elemente haben folgende Bedeutung: Client - Kreis, Server – Rechteck, Peer - Rechteck mit abgerundeten Ecken. Mit Peer ist ein Rechner gemeint, der sowohl die Rolle eines Servers als auch die eines Client einnimmt. Die Pfeile können als Anfragen an ein Element verstanden werden. Voraussetzung ist, dass die Elemente auf die die Pfeile zeigen Dienste anbieten. Da Clients keine Dienste anbieten, sind die Pfeile stehts von ihnen weg gerichtet. Sie können also lediglich Anfragen stellen und Antworten entgegen nehmen. Bei Servern ist das Gegenteil der Fall. Sie stellen Dienste bereit und warten auf Anfragen, die sie beantworten können. Peers können beide Rollen einnehmen.

Bei Abbildung 4-1 1.) handelt es sich daher um eine Peer-zu-Peer-Architektur (Peer-to-Peer, Peer2Peer, P2P). Bei der P2P-Architektur gibt es keine zentralen Elemente. Alle Rechner sind gleichberechtigt und kommunizieren als Folge davon direkt miteinander. Dies führt zu einem robusten, jedoch komplexen Netzwerk.

Architektur 2.) hat mit dem Server eine zentrales Element. Alle Anfragen in diesem Netzwerk gehen an den Server, der die Ergebnisse zwischenspeichert oder beantwortet. Soll eine Nachricht zwischen zwei Clients ausgetauscht werden, dann geht dies nur indirekt über den Server. Diese Architektur wird als Client-Server-Architektur bezeichnet. Handelt es sich bei den Anfragen um Nachrichten, die vom Server vorerst zwischengespeichert und zu einem späteren Zeitpunkt auf Anfrage ausgeliefert werden, ist vom Store-and-Forward-Prinzip die rede.

Architektur 3.) ist eine Mischform, daher die Bezeichnung 'hybrid'. Bei dieser Architektur schlüpfen die Peers in die Rolle eines Servers, können gleichzeitig aber auch als Clients die Dienste weiterer Peers nutzen. Jeder Peer stellt außerdem einer Reihe von Clients lokal verfügbare Dienste bereit. Die Kommunikation zwischen zwei Clients erfolgt immer indirekt über den lokalen Peer. Aus Sicht der Clients handelt es sich also beim Peer um einen Server. Im Unterschied zur Client-Server-Architektur muss ein Peer nun nicht die Anfragen aller Clients verarbeiten, sondern nur einer lokalen Gruppe. Die Peers sind in der Lage sich untereinander zu synchronisieren, sodass sie logisch wie ein einziger Server erscheinen.

Bei den im Folgenden vorgestellten Verfahren und bei der Analyse in Kapitel 5.3 wird auf die Architekturen Bezug genommen.

4.1.2 Kommunikationsmodus

Neben der Architektur ist auch der Kommunikationsmodus von Bedeutung. Der Kommunikationsmodus charakterisiert den zeitlichen Ablauf eines Kommunikationsvorganges zu. Es wird zwischen synchroner und asynchroner Kommunikation unterschieden.

Tauschen zwei Kommunikationspartner Informationen synchron aus, so blockieren beide während der Übertragung. Das heißt, sie sind nicht in der Lage, weitere Anfragen während einer Übertragung zu senden oder zu empfangen. Ist die Übertragung vollständig abgeschlossen, können die Kommunikationspartner mit der nächsten Aktion fortfahren.

Im Gegensatz dazu blockieren die Kommunikationspartner bei der asynchronen Kommunikation nicht, sondern sind in der Lage das Senden und Empfangen zeitlich versetzt durchzuführen. Pufferbausteine sorgen dafür, dass Nachrichten oder Nachrichtenteile zwischengespeichert werden können, bis die Übertragung vollständig abgeschlossen ist.

Die in diesem Kapitel vorgestellten Kommunikationsverfahren machen von der asynchronen Kommunikation Gebrauch, da das Blockieren der von einander entfernten Kommunikationspartner vermieden werden soll. Typisch synchrone Kommunikationsbeziehungen, wie z.B. eine Videokonferenz, können und sollen über diese Verfahren nicht abgedeckt werden und bedürfen anderer Techniken. Für den in dieser Arbeit betrachteten Austausch von Patientendaten zwischen stationärem und niedergelassenem Bereich eignet sich die asynchrone Kommunikation insbesondere, da nicht von einer ständigen Verfügbarkeit der verteilten und unabhängigen Kommunikationspartner ausgegangen werden kann[6].

4.2 Allgemeine Kommunikationsverfahren

In diesem Abschnitt werden Kommunikationsverfahren vorgestellt, die generell weit verbreitet sind und sich nicht auf das Gesundheitswesens beschränken. Bei der späteren Analyse und Bewertung werden sie den speziell auf die Kommunikation medizinischer Daten zugeschnittenen Verfahren gegenübergestellt. Durch ihre weite Verbreitung und die ausgereiften Implementierungen dienen diese Standardverfahren als Diskussionsgrundlage und Vergleichsobjekt. Auf ihre Eignung für einen Einsatz im Gesundheitswesen wird in Kapitel 5 eingegangen.

4.2.1 E-Mail

Elektronic Mail oder kurz E-Mail gibt es etwa seit einem viertel Jahrhundert. Das weit verbreitete Verfahren zum Versenden von Nachrichten [RFC2821], [RFC2822] besteht aus zwei Subsystemen: User Agents und Message Transfer Agents [Tanenbaum2000].

Die User Agents sind die Schnittstelle zum Benutzer. Sie sind lokal installierte Programme, die mittels Befehlen oder grafischer Oberflächen das Lesen, Verfassen, Versenden und Abholen von Nachrichten unterstützen. Sie bieten speziell bei der Adressierung, beim Umgang mit den zahlreichen Header-Feldern[7] und bei der Verwaltung der Nachrichten Unterstützung.

Die Message Transfer Agents (MTA) sind für den Transport der Nachrichten verantwortlich. Sie sind im Hintergrund laufende Systemdienste, die E-Mails entgegennehmen, anhand ihrer Adressinformationen weiterleiten oder für den Abruf zwischenspeichern.

E-Mail ermöglicht das übertragen von Nachrichten in zwei Formaten: im ASCII-Text Format nach [RFC2822] und im MIME-Format nach [RFC2045]. Während bei ersteren eine Nachricht aus im ASCII-Format kodierten Header und Body besteht, führt das MIME-Format weitere Kodierregeln für ASCII-fremde Nachrichten sowie weitere Header-Felder ein. Zusätzlich ermöglicht es eine Strukturierung des Bodies und das Übertragen von nicht-ASCII-kodierten Nachrichtenteilen sowie Binärformaten, wie z.B. Multimedia Dateien.

Die auf diese Weise übertragenen Nachrichten genügen datenschutzrechtlichen Anforderungen nicht. Vertraulichkeit, Authentizität und Integrität sind nicht garantiert. E-Mail Nachrichten werden

---

6 Dies liegt unter anderem an der Verwendung von Wählverbindungen und deren Tarifenbedingungen auf Seiten der niedergelassenen Ärzte.

7 Header-Felder beinhalten Adressinformationen, Informationen zur Kodierung des Inhaltes einer E-Mail, den Betreff der Nachricht und viele weitere Meta-Informationen [RFC2822].

bspw. im Klartext übertragen und sind nicht vor einer Sichtung Dritter geschützt. Desweiteren lassen sich die Adressinformationen fälschen und der Nachrichteninhalt manipulieren. Es gibt jedoch Möglichkeiten, wie Pretty Good Privacy (PGP) [RFC2440] und S/MIME [RFC2633], die Datensicherheit zu gewährleisten.

PGP basiert auf dem Public-Key Verfahren [Schneier1996]. Benutzer erstellen sich dabei ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel ist geheim und dient zum Signieren und Entschlüsseln. Der öffentliche Schlüssel wird zu einem Key-Server übertragen und damit anderen Benutzern zur Verfügung gestellt. Sie können jetzt mit diesem öffentlichen Schlüssel Nachrichten für den zugehörigen Nutzer verschlüsseln. Außerdem können sie die Echtheit des Schlüssels bestätigen, indem sie ihn mit ihrem privaten Schlüssel signieren. Dies sollte allerdings ausschließlich dann erfolgen, wenn der zu signierende Schlüssel zweifelsfrei einer Person oder Organisation zugeordnet werden kann, d.h. wenn er authentisch ist. Auf diese Weise wird die Authentizität der öffentlichen Schlüssel sichergestellt. Das gegenseitige Signieren der öffentlichen Schlüssel lässt ein so genanntes Web-of-Trust entstehen.

S/MIME (Secure / Multipurpose Internet Mail Extension) geht hier sogar noch einen Schritt weiter. Es basiert ebenfalls auf einem kryptographischen Verfahren mit öffentlichen und privaten Schlüsseln. Jedoch kommen jetzt durch Zertifikate beglaubigte Schlüssel zum Einsatz [RFC2633]. Die Zertifikate werden durch einen vertrauenswürdigen Dritten, einer Zertifizierungsstelle ausgestellt. Beispiele für diese sogenannten Trust-Center sind die Bundesnetzagentur, Verisign oder Provider eines medizinischen Intranets. Ein Zertifikat garantiert die Echtheit eines Schlüssels. Echtheit bedeutet, dass ein Schlüssel auch zu demjenigen gehört, der vorgibt, Inhaber des Schlüssels zu sein. Um die Echtheit des Zertifikates zu garantieren, ist dieses mit einer digitalen Signatur der Zertifizierungsstelle versehen. Mit Hilfe des zertifizierten öffentlichen Schlüssels der Zertifizierungsstelle kann nun die digitale Signatur der Zertifizierungsstelle geprüft werden. Das Zertifikat des öffentlichen Schlüssels der Zertifizierungsstelle ist wiederum digital signiert. Am Ende dieses Zertifizierungspfades steht das Wurzelzertifikat der obersten Zertifizierungsstelle (Root Certificate Authority, Root CA). In Deutschland übernimmt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen diese Aufgabe [BNAHP]. Ist die Hierarchie der Zertifikate bis zu diesem Wurzelzertifikat überprüfbar, ist garantiert, dass das Zertifikat und der zugehöriger Schlüssel echt ist und nicht etwa der Schlüssel eines Angreifers ist.

4.2.2 FTP

Sollen große Datenmengen ausgetauscht werden, ist das E-Mail System durch die ineffiziente Kodierung der Nachrichten ungeeignet. Hier bietet sich die Verwendung von FTP (File Transfer Protokoll) an [RFC959]. Ein FTP Server ist ein Systemdienst, der es dem FTP Client ermöglicht angebotene Dateien herunterzuladen oder eigene Dateien auf dem Server abzulegen. Zum Datenaustausch legt bspw. Nutzer A eine Datei auf dem FTP Server ab, Nutzer B kann sich diese Datei anschließend vom Server herunterladen.

Abgesehen von der Authentifizierung mittels Nutzernamen und Passwort gibt es keine Sicherheitsmaßnamen. Auch der Transfer wird nicht verschlüsselt, sodass ein Angreifer alle übertragenen Informationen im Klartext mitlesen kann. Auch bei FTP gibt es Bemühungen die Sicherheit zu erhöhen. Bei SFTP (Secure FTP) wird die FTP-Verbindung teilweise über einen sicheren SSH-Tunnel (Secure Shell Tunnel) aufgebaut. Zur Sicherung des Übertragung ist auch die Benutzung eines FTP Servers über ein Virtuelles Privates Netz (VPN) möglich.

Weitere Verfahren, wie Secure Copy Protokoll (SCP), FTP-over-SSL (FTPS) und WebDAV-over-SSL (WebDAV, [RFC2518]) ermöglichen ebenfalls den (transport-)gesicherten Datenaustausch und haben einen ähnlichen Funktionsumfang wie FTP.

4.2.3 Datenaustausch via P2P

Peer2Peer-Netzwerke kommen derzeit zum Einsatz, wenn große Datenmengen (>100MByte)unter vielen Nutzern verteilt werden sollen. Ein Beispiel ist das BitTorrent Netzwerk [BITTHP], welches sich großer Beliebtheit in der Open Source Szene bei der Verbreitung von Linux-Distributionen erfreut und von Softwareherstellern sowie von Multimedia Anbietern zur dezentralen und damit ressourcensparenden Verbreitung ihrer Produkte im Internet genutzt wird. Jeder Peer im Netzwerk kann Teile einer angeforderten Datei von mehreren Peers herunterladen. Gleichzeitig stellt er die Teile der Datei, die schon bei ihm verfügbar sind, selbst wieder anderen Peers zur Verfügung. So lässt sich die Last gleichmäßig auf das Netz verteilen.

Auch medizinische Daten können verteilt auf mehreren Rechnern liegen. In der Schweiz gibt es Überlegungen ein Peer2Peer Netzwerk im Gesundheitswesen zu etablieren [Geissbuhler2004]. Die Idee des so genannten e-toile Network ist, keinen zentralen Server zu benutzen, um Daten auszutauschen, sondern sich die Informationen zu einem Behandlungsfall dort abzuholen, wo sie gespeichert sind (siehe Abbildung 4-2). Gesichert wird die Kommunikation durch kryptographische Verfahren unter Verwendung von Zertifikaten. Ganz ohne zentrale Elemente kommt auch dieses Verfahren nicht aus. Zentrale Server stellen einen Index der verfügbaren Peers und eine zentrale Zertifizierungsstelle bereit. Einen Master Patient Index gibt es dagegen nicht. Patienten werden bei e-toile über einen „hardware token“ auf einer Chipkarte identifiziert.

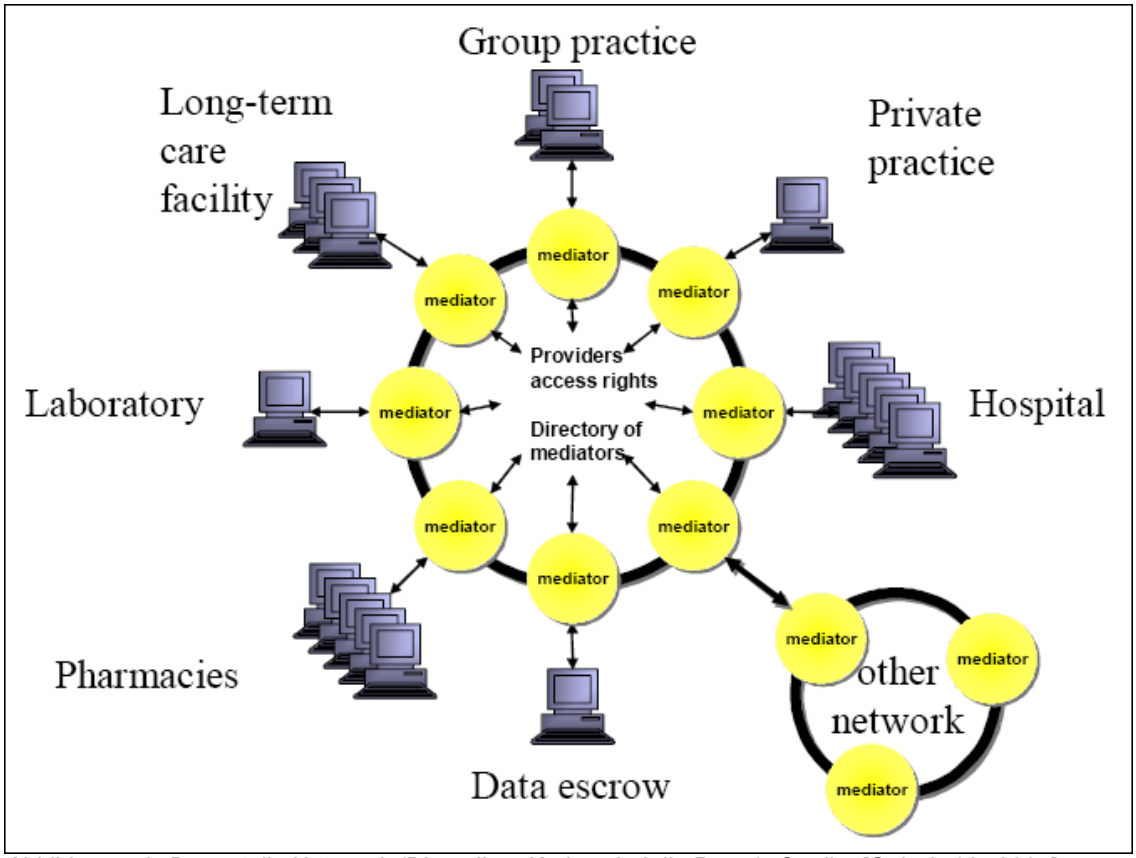

Abbildung 4-2: Das e-toile Netzwerk (Die gelben Kreise sind die Peers), Quelle: [Geissbuhler2004]

In den weiteren Untersuchungen wird die Peer2Peer-Technik aufgrund fehlender Diskussion und Implementierungen in Deutschland nicht weiter verfolgt. Bezüglich des e-toile Netzwerkes bleibt abzuwarten, wie die Ergebnisse beim derzeit laufenden Pilotprojekt in der Region Genf ausfallen.

4.3 VDAP Communication Standard – VCS

Der VDAP Communication Standard (VCS) ist eine vom Verband Deutscher Arztinformationssysteme und Provider e.V.[8] (VDAP, [VDAPHP]) entwickeltes Verfahren zur sicheren Kommunikation zwischen Arztpraxen. Der VCS wurde 2001 als PAS 1011 (Publicly Available Specification) beim DIN veröffentlicht [PAS1011].

Das VCS-Verfahren geht von einer kleinsten Einheit elektronischer Kommunikation aus, einem Sender und einem Empfänger und basiert auf dem E-Mail Verfahren. Die kleinste Nachrichteneinheit besteht aus einer patientenbezogenen Zusammenstellung von Daten, die um einen Steuerblock erweitert wird. Zur Sicherung der Kommunikation werden folgende Maßnahmen ergriffen:

- Signieren der Daten
- Signieren der Nachricht
- Verschlüsseln der Nachricht mit Public-Key Verfahren (mit Trust-Center)
- Protokollierung aller Transaktionen
- Versenden von Empfangsbestätigungen (Quittungsbetrieb)

Mit VCS lassen sich nach [PAS1011] folgende Kommunikationsszenarien abdecken:

Szenario	Erläuterung
Direkte oder gerichtete Kommunikation	Versand einer Nachricht vom Sender zu einem bekannten Empfänger
Mehrere Adressaten	Versand einer Nachricht vom Sender zu mehreren bekannten Empfängern
Initial ungerichtete Kommunikation	Bereitstellen einer Nachricht für einen später zu bestimmenden Empfänger

Tabelle 4-1: Kommunikationsszenarien VCS

Als Datenaustauschformat ist für den Nachrichteninhalt der VCS-Arztbrief definiert. Dieser kann aus Arztbriefen im BDT-Format, LDT-Format und in der Spezifikation nicht näher bestimmten Bild-Formaten sowie weiteren Formaten bestehen. Für zukünftige VCS-Arztbriefe ist eine Kodierung in XML angekündigt.

Realisiert ist der VCS durch das Kommunikations- und Prozessmodul (KPM). Dieses enthält verschiedene Teilmodule zur Ermittlung der Empfängeradressen, zur Signierung, zur Signaturprüfung, zum Ver- und Entschlüsseln sowie zum Versenden und Empfangen von Nachrichten, für Einsicht in Protokolle und zur Administration. Das KPM ist dabei stets in ein bestimmtes Anwendungsprogramm eingebunden und existiert nicht als eigenständiges Softwareprodukt.

8 Ehemals Verband Deutscher ArztPraxis-Softwarehersteller e.V.

Im Folgenden wird beschrieben, wie die Kommunikationsvorgänge für die aufgeführten Szenarien ablaufen.

Die direkte oder gerichtete Kommunikation ist in Abbildung 4-3 dargestellt.

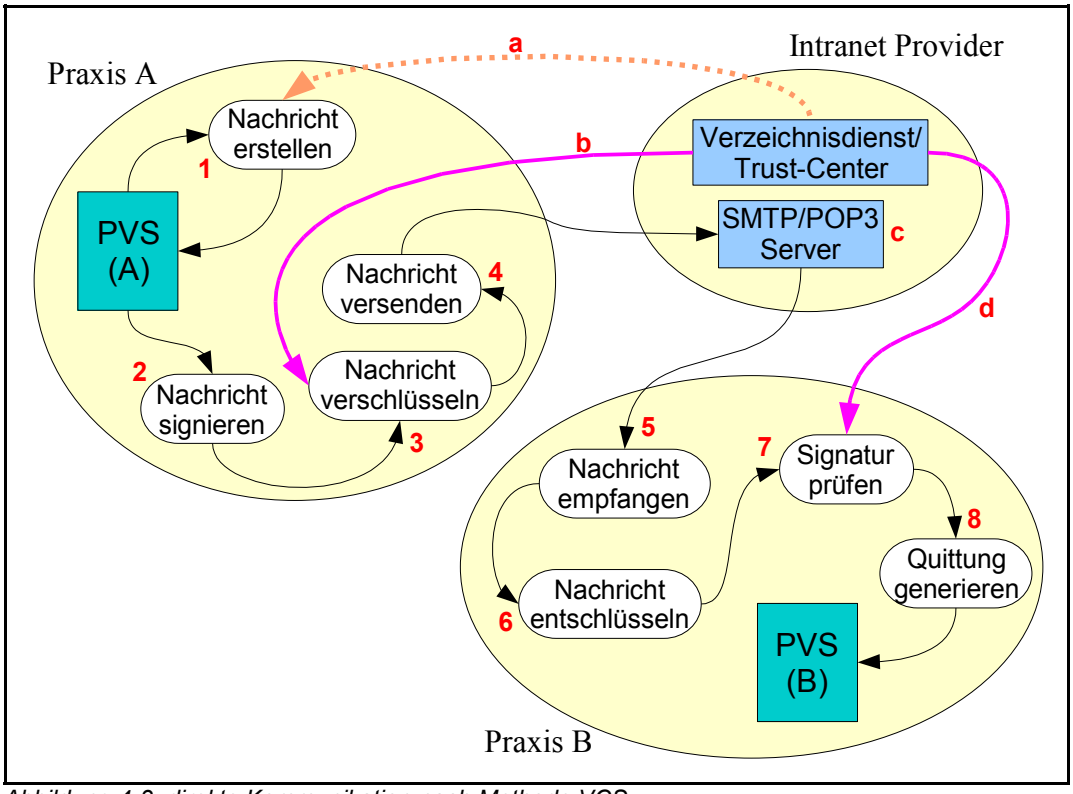

Abbildung 4-3: direkte Kommunikation nach Methode VCS

Der in Abbildung 4-3 dargestellte Kommunikationsvorgang geht von zwei miteinander kommunizierenden Arztpraxen aus: Paxis A und Praxis B. Bestandteil des Praxisinformationssystems der beiden Arztpraxen ist ein Patientenverwaltungssystem (PVS).

Zu Beginn wird aus den im PVS von Praxis A gespeicherten Patientendaten eine Nachricht erstellt (1). Diese Nachricht besteht aus dem VCS-Arztbrief und einem Steuerblock, in dem unter anderem Sender- und Empfängeradresse hinterlegt sind. Im nächsten Schritt werden alle im VCS-Arztbrief enthaltenen Dokumente signiert. Anschließend wird die komplette Nachricht signiert (2). Das Signieren erfolgt jeweils anhand der im Steuerblock hinterlegten Senderadresse und dem zugehörigen, auf einer Chipkarte gespeicherten privaten Schlüssel. Die Schlüsselpaare und die zugehörigen Zertifikate werden von einem Trust-Center beim Intranet Provider erstellt. VCS-Zertifiziert sind z.B. die Provider DGN - Deutsches Gesundheitsnetz, I-motion und Telemed. Die Zertifikate und öffentliche Schlüssel sowie Adressinformationen werden durch einen ITU X.500 (LDAP, [RFC2251]) Verzeichnisdienst allen Intranet Teilnehmern vom Provider zur Verfügung gestellt. Aus dem Steuerblock der signierten Nachricht wird anschließend die Empfängeradresse ausgelesen. Mit dieser Adresse wird eine Anfrage an den Verzeichnisdienst des Intranet Providers gestellt. Als Ergebnis der Anfrage wird der öffentliche Schlüssel des Empfängers übermittelt (b). Mit diesem Schlüssel wird die Nachricht nun verschlüsselt (3). Die signierte und verschlüsselte Nachricht wird per SMTP [RFC2821] an den E-Mail Server des Intranet Providers gesendet (4).

Der E-Mail Server (MTA) erstellt bei erfolgreicher Übertragung eine Quittung für den Absender, generiert einen Protokolleintrag und speichert die Nachricht in der Mailbox des Empfängers (c).

In Praxis B wird in regelmäßigen Abständen per POP3 [RFC1939] die Mailbox abgerufen. Liegen neue Nachrichten vor, werden diese sofort empfangen (5). Anschließend erfolgt die Entschlüsselung der Nachricht mit Hilfe des, auf einer Chipkarte gespeicherten, privaten Schlüssels des Empfängers (6). Die Signatur der entschlüsselten Nachricht wird nun mit Hilfe des öffentlichen Schlüssels des Senders überprüft (7). Dieser öffentliche Schüssel wird dazu vom Verzeichnisdienst erfragt (d). War die Prüfung der Signatur erfolgreich, wird eine positive Quittung erstellt. Diese Quittung wird signiert und an den Absender geschickt (8). Der Empfang der Nachricht sowie das Ergebnis der Signaturprüfung werden protokolliert. Die entschlüsselte und geprüfte Nachricht steht nun PVS B zur Verfügung.

Eine zentrale Rolle nehmen Verzeichnisdienst und E-Mail Server des Intranet Providers ein. Die Datensicherheit auf dem E-Mail Server ist garantiert, da E-Mails auf ihm nur in verschlüsselter Form zwischengespeichert werden. Das Protokoll des Servers, wie auch das der Kommunikationsmodule in der Praxissoftware ist gegen Manipulation geschützt, da alle Protokolleinträge eine fortlaufende Nummer bekommen und signiert werden. Der Verzeichnisdienst übernimmt zwei Aufgaben. Er dient als gemeinsames Adressbuch zur Ermittlung der Empfängeradresse (a) und stellt die öffentlichen Schlüssel sowie Zertifikate zur Überprüfung der Schlüssel und Signaturen bereit.

Das zweite Szenario, die Übermittlung einer Nachricht an mehrere Adressaten, wird über das mehrmalige Versenden der gleichen Nachricht an die verschiedenen Adressaten abgebildet.

Bei Szenario drei, der Initial ungerichteten Kommunikation, ist die Empfängeradresse des Arztes zunächst nicht bekannt. Ist jedoch die Adresse der behandelnden Zielpraxis bekannt, kann der beim Verzeichnisdienst hinterlegte Praxisschlüssel genutzt werden. Im Fall, dass weder Empfängeradresse eines Arztes noch einer Zielpraxis bekannt oder festgelegt ist, wird der Patient zum Überbringer von Zugriffsinformationen. Dazu werden auf einem Datenträger, einer Chipkarte oder einem Ausdruck eine Transaktionsnummer und die Adresse des Absenders hinterlegt. Beim Absender wird außerdem der VCS-Arztbrief erstellt, signiert und mit den Zusatzinformationen Transaktionsnummer, Patientenstammdaten und der zum Abruf berechtigten Arztgruppe versehen. Da keine Empfängeradresse vorhanden ist, wird der so vorbereitete VCS-Arztbrief in einem lokalen Zwischenspeicher des KPM abgelegt. Der Patient geht nun mit Absenderadresse und Zugriffsinformationen zu einem VCS-fähigen Arzt seiner Wahl und übergibt die Informationen. Der Empfängerarzt erstellt mit diesen Informationen eine signierte Anfrage und versendet sie an den Absender. Beim Absender wird diese Anfrage vom Kommunikationsmodul geprüft. Empfäger, Arztgruppe und Transaktionsnummer sowie Patientenstammdaten müssen stimmen. Ist das der Fall, steht ein Empfänger fest und der direkte Kommunikationsvorgang wird eingeleitet (in Abbildung 4-3 ab Schritt (3)). Entsprechende Quittungen und Protokolleinträge werden bei diesem Szenario ebenfalls berücksichtigt.

4.4 Patientenbegleitende Dokumentation – PaDok, D2D

Patientenbegleitende Dokumentation oder kurz PaDok [PADOKHP] ist eine vom Fraunhofer Institut für Biomedizinische Technik (IBMT) [IBMTHP] entwickelte rechnergestützte Verfahren zur sicheren Kommunikation im Gesundheitswesen. Implementierungen des PaDok-Verfahrens gibt es seit 1998. Mit anfänglich kleineren Anwendungsprojekten und den dabei gemachten Erfahrungen wurde schrittweise die derzeitige Version des PaDok-Verfahrens entwickelt. Die Anwenderversion von PaDok ist die D2D-Kommunikationsplattform der Kassenärztlichen

Vereinigung Nordrhein (KVNo) in Zusammenarbeit mit dem IBMT. D2D steht in Analogie zu B2B für Docter-to-Docter.

Im Gegensatz zur E-Mail-basierten Kommunikation beim VCS kommt beim PaDok-Verfahren eine vom IBMT entwickelte Serverlösung zu Einsatz. Der PaDok-Server kommuniziert über eine RPC-Schnittstelle (Remote Procedure Call) mit dem in der Praxis installierten PaDok-Client.

PaDok setzt ebenfalls auf anerkannt sichere Methoden wie dem Signieren von Nachrichten, dem Verschlüsseln mit Public-Key Verfahren, der Protokollierung der Aktivitäten und der Bestätigung erfolgreicher Transfers. PaDok deckt dabei die folgenden Szenarien ab [D2D2005]:

Szenario	Erläuterung
Adressierter Versand	Versand einer oder mehrerer Nachrichten an bekannte Empfänger
Gerichteter Versand	Versand an einen unbestimmten Empfänger einer Arztgruppe
Ungerichteter Versand	Fall bezogene temporäre Netz-Patientenakte

Tabelle 4-2: Kommunikationsszenarien PaDok

Beim Vergleich dieser Szenarien mit den beim VCS abgedeckten Szenarien lässt sich feststellen, dass dem Terminus „gerichtet“ bei beiden Verfahren eine unterschiedliche Bedeutung zukommt. 'Gerichtete Kommunikation' im VCS ist gleichzusetzen mit dem 'adressierten Versand' bei PaDok, während 'gerichteter Versand' bei PaDok in etwa mit der 'initial ungerichteten Kommunikation' des VCS zu vergleichen ist (siehe Tabelle 4-1 „Kommunikationsszenarien VCS“).

Als Datenaustauschformat setzt PaDok konsequent auf XML. Zum Einsatz kommen strukturierte Dokumente nach dem HL7 CDA-Standard, in der angepassten deutschen Fassung nach SCIPHOX [SCIPHOXP1]. Wie in Kapitel 2.2.3 beschrieben, können CDA-Dokumente auf weitere Dateien in beliebigen Formaten verweisen bzw. diese in kodierter Form enthalten. SCIPHOX CDA ist aufgrund der XML-Basis ein flexibles und gut an lokale Gegebenheiten anpassbares Austauschformat. PaDok stellt in seiner Referenzimplementierung D2D bereits vorgefertigte XML-Formulare zur Verfügung. Dazu gehören unter anderem ein elektronischer Arztbrief, die elektronische Überweisung, die elektronische Krankenhauseinweisung und der elektronische EU-Notfallausweis. Mit Hilfe des auf der SCIPHOX-Homepage [SCIPHOXHP] veröffentlichten Working Drafts [SCIPHOXP1] und der verfügbaren XML-Schema-Dateien lassen sich für weitere Anwendungen entsprechende Formulare erstellen.

Die gesamte Kommunikation wird beim PaDok-Verfahren auf Seiten des Praxis- oder Krankenhausinformationssystems über eine Schnittstelle abgewickelt. Diese ist ein eigenständige Softwareprodukt und wird als PaDok-Client oder D2D-Client bezeichnet. Der PaDok-Client ist für die Kommunikation mit dem PaDok-Server über die RPC-Schnittstelle zuständig und stellt eine Schnittstelle auf Basis von Kommandodateien zur Steuerung zur Verfügung. Die Kommunikationsvorgänge, das Signieren, Signaturprüfen sowie das Ver- und Entschlüsseln laufen weitestgehend automatisch im Hintergrund und damit ohne Mehraufwandt für den Nutzer ab.

Im Folgenden wird beschrieben, wie die vom PaDok-Verfahren abgedeckten Kommunikationsvorgänge für die aufgeführten Szenarien ablaufen. In Abbildung 4-4 ist das erste Szenario dargestellt, der adressierte Versand.

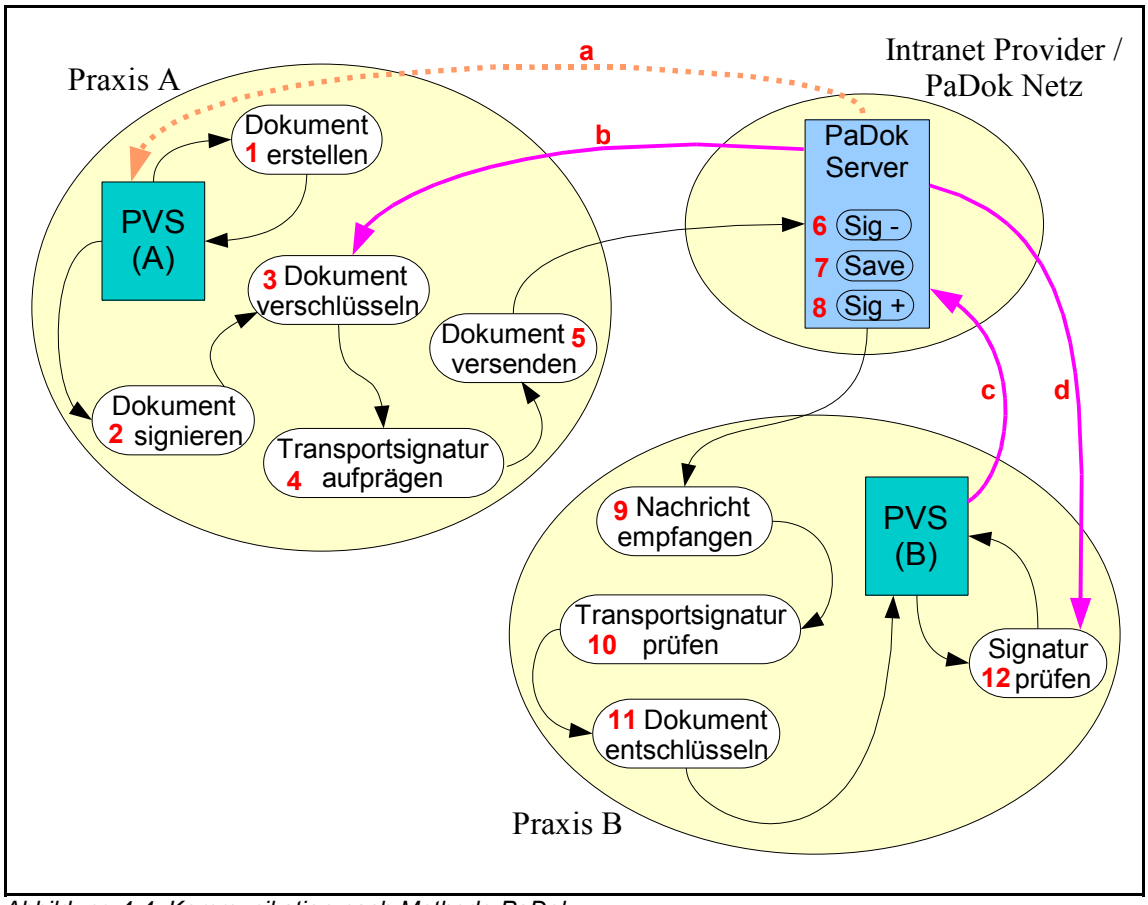

Abbildung 4-4: Kommunikation nach Methode PaDok

Nachdem ein Dokument erstellt ist (1), wird es mit dem sich auf einer Chipkarte befindlichen privaten Schlüssel des Absenderarztes in Praxis A digital signiert (2). Bis zur Einführung des elektronischen Arztausweises werden vorübergehend Musterchipkarten oder ein Verfahren unter Benutzung eines Softwareschlüssels verwendet. Beim hier vorgestellten Szenario 'adressierter Versand' ist der Empfängerarzt bekannt. Die Adresse des Empfängerarztes kann mit Hilfe einer integrierten Suchfunktion ermittelt werden (a). Ist die gewünschte Adresse ausgewählt, wird der öffentliche Schlüssel des Adressaten angefordert (b) und das signierte Dokument verschlüsselt (3). Um Übertragungsfehler zu erkennen und einen fehlerfreien Transfer zu gewährleisten, wird dem verschlüsselten Dokument eine Transportsignatur hinzugefügt (4). Anschließend wird das Dokument über eine gesicherte Verbindung zum PaDok-Server per RPC übertragen (5). Die Verwendung einer gesicherten Verbindung ist eine weitere Sicherheitsmaßnahme, die durch eine ISDN Call-Back Verbindung zum PaDok-Server oder über die VPN-Einwahl bei einem zertifizierten Medizinnetz Provider ('Intranet Provider') realisiert wird. Der PaDok-Server prüft nun die Transportsignatur. Liefert die Prüfung ein positives Ergebnis, wird die Signatur entfernt (6) und das Dokument im Postfach des Empfängers abgelegt (7). In regelmäßigen Abständen prüft PVS B sein Postfach auf dem PaDok-Server (c). Liegt eine Nachricht vor, wird diese zum Versand vom PaDok-Server vorbereitet, indem eine neue Transtortsignatur angebracht wird (8). Anschließend kann PVS B die Nachricht über eine gesicherte Verbindung empfangen (9). Die Transportsignatur wird geprüft und nach bestandener Prüfung entfernt (10). Das Dokument wird nun mit dem privaten Schlüssel des Empfängers entschlüsselt (11) und PVS B zur Verfügung gestellt. Das übertragene Dokument wird dabei stets mit seiner vom Absender angebrachten Signatur gespeichert. So kann jederzeit die Echtheit des Dokuments überprüft werden (12),(d).

Sämtliche Aktionen sind bei PaDok mit positiven oder negativen Rückgabewerten (Fehlercodes) quittiert und werden protokolliert. Der PaDok-Server ist das zentrale Element für den Austausch

der Dokumente. Jedwede Kommunikation läuft über ihn. Der PaDok-Server ist nicht nur Datenspeicher für die verschlüsselten Dokumente, sondern übernimmt auch die typischen Funktionen eines Verzeichnisdienstes, wie das Bereitstellen des zentralen Adressbuches und der Verwaltung der Schlüssel und Zertifikate.

Szenario zwei, der gerichtete Versand, ermöglicht das Versenden eines Dokuments an einen zum Zeitpunkt des Abschickens unbekannten Empfänger. Dieses Szenario läuft in mehreren Phasen ab. Zunächst wird das zu versendende Dokument erstellt und signiert. Daraufhin wird ein zufälliger Vorgangsschlüssel erzeugt und das digital signierte Dokument damit verschlüsselt. Der Vorgangsschlüssel und eine Vorgangs-ID, die zur Identifikation des Vorgangs dient, werden auf einem so genannten Ticket gespeichert und dem Patienten übergeben. Dies kann in herkömmlicher Form durch einen Barcodeausdruck oder elektronisch per Datenträger oder Chipkarte geschehen. Das mit dem Vorgangsschlüssel verschlüsselte Dokument wird nun ein zweites mal mit dem öffentlichen Schlüssel des PaDok-Servers verschlüsselt, mit einer Transportsignatur versehen und so „verpackt“ zum PaDok-Server gesendet. Dort erfolgt die Prüfung der Transportsignatur. Falls erfolgreich wird das verschlüsselte Dokument im Vorgangspuffer abgelegt. Kommt der Patient nun zu einem Arzt seiner Wahl, übergibt er das Ticket. Aus dem Ticket lassen sich anschließend Vorgangs-ID und Vorgangsschlüssel ermitteln. Der Empfänger fordert nun beim PaDok-Server das Dokument mit der im Ticket enthaltenen Vorgangs-ID an. Der PaDok-Server überprüft die Identität des Empfängers - dabei wird auch die Fachgruppe des Arztes[9] berücksichtigt - und ermittelt das gewünschte Dokument über die Vorangs-ID. Das sich im Vorgangspuffer befindliche Dokument ist allerdings noch verschlüsselt. Daher entschlüsselt der PaDok-Server zunächst das Dokument mit seinem privaten Schlüssel und verschlüsselt es anschließend mit dem öffentlichen Schlüssel des designierten Empfängers. Wiederum mit einer Transportsignatur versehen, wird das Dokument von der vom Patienten gewählten Praxis empfangen. Nachdem die Transportsignatur erfolgreich geprüft wurde, wird das doppelt verschlüsselte Dokument zunächst mit dem privaten Schlüssel des Empfängers entschlüsselt. Zur entgültigen Entschlüsselung wird der im Ticket transportierte Vorgangsschlüssel benötigt. Das vollständig entschlüsselte Dokument kann jetzt der Signaturprüfung unterzogen werden.

Von entscheidender Bedeutung beim gerichteten Versand ist die doppelte Verschlüsselung des Dokuments und der Transport des Tickets durch den Patienten. So wird sichergestellt, dass nur der berechtigte Empfänger das Dokument entschlüsseln kann.

Szenario drei ‚ungerichteter Versand' läuft im wesentlichen wie Szenario zwei ab. Im Unterschied zum gerichteten Versand wird bei der ungerichteten Kommunikation jedoch die Nachricht nicht in einem Vorgangspuffer vom PaDok-Server gespeichert, sondern es wird eine temporäre Fallakte auf dem PaDok-Server angelegt. In einer derartigen Akte können mehrere Ärzte Behandlungsdaten eines Patienten zu einem Fall zusammenstellen. Die mitbehandelnden Ärzte haben damit Zugang zu einer gemeinsamen Fallakte. Der Patient erhält ein Ticket mit Vorgangs-ID und Vorgangsschlüssel für den Zugriff auf die Fallakte. Er kann dieses Ticket nun mehreren mitbehandelnden Ärzten übergeben. Diese sind damit in der Lage lesend auf für sie freigegebene Teile der Netzakte zugreifen und können in eigenen Unterordnern weitere behandlungsrelevante Dokumente beisteuern. Durch die stehts zum Einsatz kommende Transportsignierung, Doppelverschlüsselung und Prüfung der Signaturen, wird der sichere Datenaustausch zwischen den behandelnden Ärzten gewährleistet. Nach Abschluß des Behandlungsfalles oder Ablauf eines Zeitlimits wird die Akte vom Moderator[10] bzw. durch den PaDok-Server geschlossen. Da die auf dem PaDok-Server zur gemeinsamen Behandlung

9 Auch bekannt als Health Profession Group (HPG).

10 Moderator ist automatisch der Arzt, der die Fallakte angelegt hat.

herangezogenen Dokumente der einzelnen Ärzte nur Kopien der lokalen Dokumentation sind, ist im Falle eines Serverausfalls eine Rekonstruktion der Fallakte möglich.

4.5 Übersicht

In der folgenden Übersicht werden die behandelten Verfahren zur Kommunikation im Gesundheitswesen zusammengefasst.

Merkmal / Verfahren	E-Mail[11]	FTP[12]	VCS	PaDok
Adressierter Versand	x	o	x	x
Versand an Gruppen von Empfängern	x	o	x	x
Versand bei nicht bekannten Empfänger	o	-	x	x
Temporäre Netzakte	-	o	-	x
Gesicherter Netzzugang	o	o	x (VPN)	x (VPN, CB)
Zertifizierte Netze (Provider)	o	-	med. Prov.	med. Prov.
Sicherheit	PKI, TC, WoT	-	PKI, TC	PKI, TC
Standardisierung	RFC	RFC	RFC/PAS	PaDok/RPC
Kommunikationsmodus	asynchron	asynchron	asynchron	asynchron

Tabelle 4-3: Übersicht Kommunikationsverfahren

Legende zu Tabelle 4-3:

x: unterstützt

o: geringe Unterstützung oder mit erheblichen Aufwand umsetzbar

-: nicht unterstützt, nicht vorhanden oder nicht bekannt

CB: ISDN Call Back, Rückrufverfahren mit Überprüfung der ISDN-Nummer

Med. Prov.: Provider für Medizin-Netze: D/G/N Service GmbH, i-motion, telemed GmbH

TC: Trust Center

WoT: Web-of-Trust

Bereits bei der Gegenüberstellung lassen sich bei E-Mail und FTP diverse Schwachpunkte in Punkto Sicherheit und Funktionsumfang feststellen. VCS und PaDok sind gegenüber diesen Gesichtspunkten besser aufgestellt. Im folgenden Kapitel werden weitere Untersuchungen durchgeführt, bei denen die vorgestellten Verfahren den in Kapitel 3 erarbeiteten Anforderungen gegenüber gestellt werden.

11 E-Mail in sicherer S/MIME Variante

12 FTP und weitere Fileserverdienste, wie SFTP, FTPS und SCP

5 Analyse und Bewertung der Verfahren für die elektronische Kommunikation

In diesem Kapitel werden die im vorhergehenden Kapitel vorgestellten Verfahren für den computerbasierten sektorübergreifenden Datenaustausch im Gesundheitswesen detaillierter untersucht. Um eine Empfehlung für ein Verfahren geben zu können und in Vorbereitung der Erstellung des Referenzmodells, wird der Ist-Zustand der Informationssysteme in den betreffenden Bereichen analysiert und modelliert. Desweiteren wird der Soll-Zustand definiert. In der anschließenden Diskussion werden die in Kapitel 3 erarbeiteten Anforderungen den Verfahren aus Kapitel 4 gegenübergestellt.

Das Ergebnis der Analyse des Ist-Zustandes und das Ergebnis der Diskussion der Verfahren bezüglich der Erfüllung der Anforderungen ist die Empfehlung eines anforderungskonformen Verfahrens als Basis für das zu erstellende Referenzmodell.

5.1 Ist-Zustand

Die Analyse des Ist-Zustandes für den niedergelassenen Bereich fußt auf einem internen IT-Konzeptpapier zur Integrierten Versorgung des Universitätsklinikums Leipzig AöR in Zusammenarbeit mit dem Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE) [MuellerU20051], [MuellerU2005]. Die Analyse des stationären Bereichs basiert auf Gesprächen mit den Informationsmanagern des UKL sowie auf Auswertungen bereits bestehender 3LGM^2-Modelle des UKL.

Aufbauend auf den in diesen Materialien ermittelten Eckdaten wird ein verallgemeinertes Ist-Modell der Informationssysteme im stationären und niedergelassenen Bereich erstellt. Dieses Modell wird im 3LGM^2-Baukasten erstellt und dient zur Veranschaulichung der Ist-Situation in Bezug auf die Kommunikation. Spezielle Ist-Modelle einer konkreten Institution sind weitaus komplexer. Diese Arbeit hat nicht zum Ziel, möglichst vollständige 3LGM^2-Modelle eines Bereiches zu erstellen, sondern es wird sich auf wesentliche Elemente der beiden Sektoren konzentriert, mit dem Ziel die computerbasierte sektorübergreifende Kommunikation zu modellieren.

5.1.1 Stationärer Bereich

Bereits in den Grundlagen wurde festgestellt, dass ein Krankenhaus in der Regel aus mehreren Abteilungen verschiedener Fachrichtungen aufgebaut ist. Beteiligte Personengruppen sind die Patienten, Pflegepersonal und Krankenhausärzte.

Aufgaben des stationären Bereichs

Die Aufgabenseite eines Krankenhauses kann in Administration und Behandlung der Patienten unterteilt werden.

Unter Administration sind alle Aufgaben zusammengefasst, die mit der Verarbeitung verwaltungsrelevanter Daten eines Patienten (Administrative Patientendaten) z.B. Patientenstammdaten sowie der Zuordnung eindeutiger Patienten- und Fallidentifikatoren[13] zu tun haben. Darunter fallen bspw. die Aufnahme, die Überweisung und Entlassung von Patienten[14].

Die Behandlung ist die Durchführung der medizinischen Maßnahmen zur Heilung des Patienten. Darin enthalten ist die Dokumentation der Patientengeschichte. Diese umfasst die bei der Behandlung dokumentierten Maßnahmen, Diagnosen, Befunde, Anamnesen, Epikrisen und vieles mehr (siehe Abbildung D-1, Anhang D: Objekttypen der Patientengeschichte für eine detailierte Auflistung [UMIT2005]). Sollen ausgewählte Dokumente ausgetauscht werden, werden zu diesem Zweck die angeforderten Auszüge der Patientengeschichte erstellt.

Logische Sicht auf das Informationssystem

Die logische Sicht auf das Informationssystem dient zur Darstellung der zur Erfüllung der Aufgaben bereitgestellten Anwendungssysteme. Zur Unterstützung der Aufgabe 'Administration' wird im stationären Bereich ein Patientenverwaltungssystem verwendet. Es handelt sich dabei im Wesentlichen um einen rechnerbasierten Anwendungsbaustein zur Verwaltung der Patientenstammdaten und zur Koordination der Patientenbewegungen, wie Aufnahme, Verlegung und Entlassung. Zur Unterstützung der Aufgabe 'Patientenbehandlung' findet in der Regel ein separater rechnerbasierter Anwendungsbaustein Verwendung: das Dokumentations- und Managementsystem. Im Idealfall werden hier alle dokumentierten Diagnosen, Maßnahmen, Befunde und Arztbriefe verwaltet. Dadurch besteht Zugriff auf alle behandlungsrelevanten Patientendaten im Krankenhaus. Die Speicherung dieser Informationen übernimmt ein Datenbanksystem.

Die verschiedenen Fachbereiche eines Krankenhauses können über weitere fachspezifische Anwendungssysteme verfügen. Die in diesen Anwendungssystemen erhobenen Daten werden vielfach in separaten Datenbanken abgelegt. Die Integration der vollständigen Patientengeschichte über alle Teilsysteme verschiedener Hersteller ist eine besondere Herausforderung. Bei der weiteren Modellierung wird verallgemeinernd davon ausgegangen, dass alle Patientendaten über das Dokumentations- und Managementsystem erreichbar sind.

Neben den rechnerbasierten Anwendungsbausteinen zur Unterstützung der Aufgaben, gibt es weitere Komponenten, welche bspw. für die Kommunikation der Teilsysteme untereinander zuständig sind. Jeder Anwendungsbaustein besitzt zu diesem Zweck eine oder mehrere Schnittstellen, über die der Informationsaustausch ermöglicht wird. Sollen viele Teilsysteme untereinander kommunizieren, ist die direkte Kommunikation der Teilsysteme problematisch. Die Ursachen sind vielfältig und reichen von fehlenden Schnittstellen bis unterschiedlichen Implementierungen von Standards durch verschiedene Hersteller. Ein Beispiel sind die HL7-Dialekte verschiedener Hersteller. Aus diesen Gründen kommt vielfach ein Kommunikationsserver im stationären Bereich zum Einsatz. Der Kommunikationsserver ist in der Lage, Nachrichten entgegen zu nehmen, sie gegebenenfalls zu transformieren, zwischenzuspeichern und an einen Anwendungsbaustein angepasst zu versenden.

---

13 Patienten-ID = PID bzw. Fall-ID = FID

14 Die sogenannten ADT-Daten (ADT = Admission, Discharge, Transfer).

Der Datenaustausch mit niedergelassenen Ärzten wird bisher ausschließlich papierbasiert unterstützt. Dazu werden auszutauschende Dokumente ausgedruckt und stehen anschließend als papierbasierte Auszüge der Patientengeschichte für den Austausch bereit.

Physische Sicht auf das Informationssystem

Ebenso vielfältig wie die logische Sicht gestaltet sich der Blick auf die physische Ebene. Die Anwendungssysteme werden auf diversen Rechnern installiert, die über ein lokales Netzwerk miteinander in Verbindung stehen. Prinzipiell sollen alle physischen Datenverarbeitungsbausteine erfasst werden. Unterschieden werden kann zwischen Servern, Clients, Peripherie und Netzwerkkomponenten.

Server können unterschiedliche Dienste anbieten. Auf ihnen können Datenbanken, zentrale Teile von Anwendungsbausteinen (Applikationsserver), Datenbanken, Datei- oder Kommunikationsserver installiert sein.

Die Clients greifen in der Regel auf die von den Servern bereitgestellten Dienste zu und beinhalten die nötigen Frontends und Interfaces für die Benutzer. Im Vergleich zu den Servern sind die Clients zahlenmäßig viel stärker vertreten und werden daher als Gruppen von Arbeitsplatz-PCs modelliert.

Zu den Peripheriegeräten gehören Drucker, Scanner und vieles mehr. Peripheriegeräte sind aufgrund ihrer geringen Bedeutung für die Kommunikationsvorgänge im Modell nur in Form von Chipkartenlesern vertreten.

Zur besseren Übersichtlichkeit können den physischen Datenverarbeitungsbausteinen Subnetz und Standort zugewiesen werden.

Als Kommunikationsmöglichkeit mit externen Einrichtungen stehen konventionelle Dienste, wie Post, Fax und Bote zur Verfügung. Auf diesem Weg wird bspw. der papierbasierte Datenaustausch realisiert.

5.1.2 Niedergelassener Bereich

Der niedergelassenen Bereich beherbergt in der Regel nicht verschiedenen Fachrichtungen in einer Praxis sondern ist spezialisiert auf einen Bereich z.B. die fachärztliche Versorgung oder die hausärztliche Versorgung. Beteiligte Personen sind die Patienten, niedergelassene Haus- oder Fachärzte sowie deren unterstützendes Personal z.B. Schwestern oder Sprechstundenhilfen).

Aufgaben

Wie im stationären Bereich lassen sich die Aufgaben Administration und Behandlung der Patienten identifizieren. Die Administration beinhaltet Aufnahme, Überweisung und Entlassung von Patienten.

Die Behandlung der Patienten unterscheidet sich zwar im Umfang der Leistungen, die in einer Praxis erbracht werden können, die Bandbreite der zu erstellenden Dokumentation ist aber nahezu gleich der im stationären Umfeld. Über die niedergelassenen Praxen verteilt, finden sich alle Objekttypen der Patientengeschichte auch bei den niedergelassenen Leistungserbringern wieder. Daher sind die Aufgabenebenen nahezu identisch.

Logische Sicht auf das Informationssystem

Die Aufgaben Administration und Behandlung werden im niedergelassenen Bereich im Allgemeinen durch einen integrierten Anwendungsbaustein unterstützt. Aufnahme, Überweisung, Entlassung werden ebenso unterstützt wie Arztbriefschreibung, Terminverwaltung, Verwaltung von Diagnosen und Befunden sowie die Dokumentation der medizinischen Maßnahmen. Es handelt sich um integrierte Werkzeuge zur Verwaltung der Patientengeschichte sowie zur Unterstützung von Administration und Behandlung der Patienten. Die Patientendaten werden zentral in einer Datenbank gespeichert, sodass Schnittstellen nur zum Datenaustausch mit externen Einrichtungen nötig sind.

Bei den untersuchten Praxen werden Softwareprodukte unterschiedlicher Hersteller eingesetzt. Dabei wurden in den 14 untersuchten Praxen sieben verschiedene Produkte ermittelt.

Müssen Daten mit externen Einrichtungen ausgetauscht werden, werden diese ausgedruckt und auf konventionellem Wege per Post, Fax oder Boten übermittelt.

Physische Sicht auf das Informationssystem

Auch auf der physischen Werkzeugebene ist eine deutlich einfachere Strukturierung als im stationären Bereich zu verzeichnen. Es ist theoretisch sogar möglich, dass der rechnergestützte Teil des Informationssystem einer Praxis aus lediglich einem physischen Datenverarbeitungsbaustein besteht. Praktisch kommen aus organisatorischen Gründen allerdings mindestens zwei Rechner zum Einsatz, da Aufnahme und Behandlung in der Regel von unterschiedlichen Personen (Schwester, Arzt) an verschiedenen Orten durchgeführt werden. Die Rolle des Servers kann dabei von einem der beiden Rechner übernommen werden. Es bietet sich jedoch an für diese Aufgabe einen separaten Computer zu verwenden. Leistungsengpässe werden so vermieden, Zugriffsrechte lassen sich besser kontrollieren, Erweiterbarkeit und Backup sind leichter zu realisieren. Eine Entscheidung bezüglich der Verwendung eines separaten Server Computers ist individuell nach den vorherrschenden Gegebenheiten zu treffen. Für die Modellierung wird die Variante dedizierter Server Computer verfolgt.

Als einzige Peripheriegeräte kommen die Chipkartenleser im Modell vor. Drucker und weitere Geräte werden nicht modelliert. Abgesehen von der Variante „Einzelplatzinstallation“ ist eine Vernetzung der Rechner über ein lokales Netzwerk nötig. Wie im Abschlussbericht der Systemanalyse [MuellerU20051] festgestellt, verfügten 50% der niedergelassenen Ärzte über einen Internetzugang und erfüllen damit bereits eine wichtige Voraussetzung für den elektronischen Datenaustausch.

5.1.3 Unterschiede und Gemeinsamkeiten der Informationssysteme

Durch die relativ grobe Sicht auf die Aufgaben der beiden Informationssysteme, finden sich im Modell nur geringe Unterschiede. Auf der logischen Ebene gibt es den gesetzlich verordneten Konsens bezüglich der Kodierung der Prozeduren (OPS301) und Diagnosen (ICD10). Der Austausch von Patientendaten zwischen beiden Bereichen ist papierbasiert. Das heißt, beide Informationssysteme ermöglichen das Ausdrucken von Dokumenten, die einen für den Behandlungsfall relevanten Auszug der Patientengeschichte darstellen. Auf der physischen

Ebene stehen dann konventionelle Transportmechanismen wie der Postweg, die Übermittlung per Fax oder Boten zur Verfügung. Für die Vernetzung der lokalen Rechner in den Bereichen kommt Ethernet nach IEEE 802.3 zum Einsatz. Für den Zugang zum Internet bzw. zu den medizinischen Netzen stehen in beiden Sektoren Techniken, wie ISDN oder DSL zur Verfügung, wenngleich für den stationären Bereich die Leistungsparameter aufgrund des höheren Datenaufkommens großzügiger dimensioniert sind. Bisher wird der Zugang zu den medizinischen Netzen von keinem der im Rahmen der Systemanalyse befragten Einrichtungen genutzt.

Unterschiede sind vor allem auf der logischen und physischen Ebene zu verzeichnen. Aufgrund der schon mehrfach erwähnten organisatorischen Unterschiede zwischen stationären und niedergelassenen Bereich ergibt sich eine unterschiedliche Struktur der Anwendungsbausteine. Stationär kommen für die Aufgaben 'Administration' und 'Behandlung' bei den untersuchten Einrichtungen SAP basierte Softwareprodukte wie IS-H und IS-H*med [SAPHP] zum Einsatz. Die interne Kommunikation wird über einen Kommunikationsserver abgewickelt. Für den niedergelassenen Bereich gibt es eine Vielzahl von zugelassen Herstellern integrierter Softwarelösungen. Ein gravierender Unterschied besteht bei den eingesetzten Datenformaten. Das ist zum einen HL7 im stationären Bereich und xDT im niedergelassenen Bereich (siehe Kapitel 2.2.). Auf der Ebene der physischen Datenverarbeitungsbausteine setzen sich die Unterschiede fort. Die komplexeren und zahlreicheren Anwendungsbausteine im stationären Bereich erfordern eine entsprechende physische Struktur. In der Regel werden zentrale Elemente wie Server in einem Rechenzentrum konzentriert, was die Verfügbarkeit erhöht. Die darauf zugreifenden Arbeitsplatz-PCs verteilen sich auf die vorhandenen Abteilungen. Verbunden werden die physischen Datenverarbeitungsbausteine über eine lokale Netzwerkinfrastruktur. Vielfach ist eine eigene IT-Abteilung für Wartung von Soft- und Hardware sowie für die Betreuung des Routinebetriebs (Help Desk) verantwortlich. Deutlich einfacher ist die physische Ebene dagegen im niedergelassenen Bereich strukturiert. In der Regel gibt es einen Server und einige Arbeitsplatz-PCs, welche über ein lokales Netzwerk verbunden sind. Wartungsarbeiten übernimmt der Arzt selbst oder beauftragt einen externen Dienstleister für diese Aufgabe.

Weitere Unterschiede lassen sich beim Datenschutz feststellen. Krankenhäuser haben in der Regel einen Mitarbeiter, der die Aufgabe des Datenschutzbeauftragten einnimmt. Niedergelassene Artzpraxen sind aufgrund ihrer geringen Mitarbeiterzahl nicht verpflichtet einen eigenen Datenschutzbeauftragten zu stellen und müssen sich allein auf Herstellerangaben verlassen. Daher kann davon ausgegangen werden, dass im stationären Bereich datenschutzrechtliche Aspekte, wie das Erstellen und Durchsetzten von Datenschutzkonzepten, konsequenter verfolgt wird.

Auch im Budget der beiden Systeme finden sich Unterschiede. Praxisinformationssysteme werden in der Regel vom Praxisarzt angeschafft. Laut dem Verband der Hersteller von IT-Lösungen für des Gesundheitswesen e.V. (VHitG) ist das Hauptentscheidungskriterium für ein Praxisinformationssystem der Preis [VHitG2005]. Bei den Krankenhausinformationssystemen wird eher auf die Integration in die bestehende IT-Landschaft Wert gelegt.

Der folgende tabellarische Vergleich zeigt, wo beide Systeme Schnittpunkte haben bzw. sich unterscheiden.

Sicht \ IS	PrIS	KIS
Fachliche Ebene		
Aufgaben	Patientenadministration und Patientenbehandlung	
Weitere Aufgaben	Terminverwaltung, xDT-Abrechnung mit den KVen	Stationsmanagement, Abrechnung mit Kostenträgern
Logische Ebene		
Logische Struktur	Einzelner integrierter Anwendungsbaustein	Mehrere spezialisierte Anwendungssysteme
Anzahl der verfügbaren Softwarelösungen	ca. 235 zugelassen	ca. 30 verfügbar
Kommunikation systemintern	Prozedur- und Funktionsaufrufe, in der Regel proprietär bzw. keine Kommunikation, da integrierte Anwendung. BDT	Anwendungssysteme tauschen Nachrichten über festgelegte Kommunikationsstandards aus. z.B. HL7, DICOM. Kommunikationsserver kommen zum Einsatz.
Kommunikation extern	Papierbasiert, xDT-Protokolle (Abrechnung)	Papierbasiert, HL7 (Austausch zwischen Krankenhäusern), EDIFACT (zur Abrechnung)
Prozedur- und Diagnosen-verschlüsselung	ICD10, OPS301	
Physische Ebene		
Physische Struktur	Ein Server, einige Arbeitsplatz-PCs	Mehrere Server, viele Arbeitsplätze
Netzwerk intern	Ethernet	
Netzwerkstruktur	Einfach	Komplex
Internetzugang	ISDN, DSL, weitere nach Verfügbarkeit	
Sektorübergreifende Kommunikation	Postweg, Fax, Bote	
Weitere Unterschiede		
Datenschutz	Kein Datenschutzbeauftragter	Datenschutzbeauftragter vorhanden
Budget	Vom Arzt allein finanziert	Von Trägern finanziert (Privat, Stadt, Land und weitere kommen in Frage)

Tabelle 5-1: Vergleich Praxisinformationssystem / Krankenhausinformationssystem

5.1.4 3LGM² Ist-Modell

Nach den Ergebnissen der vorangegangenen Abschnitte, lässt sich das nun folgende Ist-Modell mit dem 3LGM²-Baukasten erstellen. Das Modell umfasst die fachliche, logische und physische Ebene und beinhaltet Zusammenhänge zwischen diesen Ebenen.

Fachliche Ebene

Die fachliche Ebene beinhaltet die Aufgaben und Objekttypen. Aufgaben sind durch rot gefärbte Rechtecke, Objekttypen durch gelb gefärbte Ellipsen gekennzeichnet. Pfeile stellen die Beziehungen zwischen den Komponenten dar. Abbildung 5-1 ist so zu verstehen: Die

'Patientenadministration Krankenhaus' interpretiert die 'Patientenstamminformationen' und bearbeitet den 'Fall Krankenhaus'.

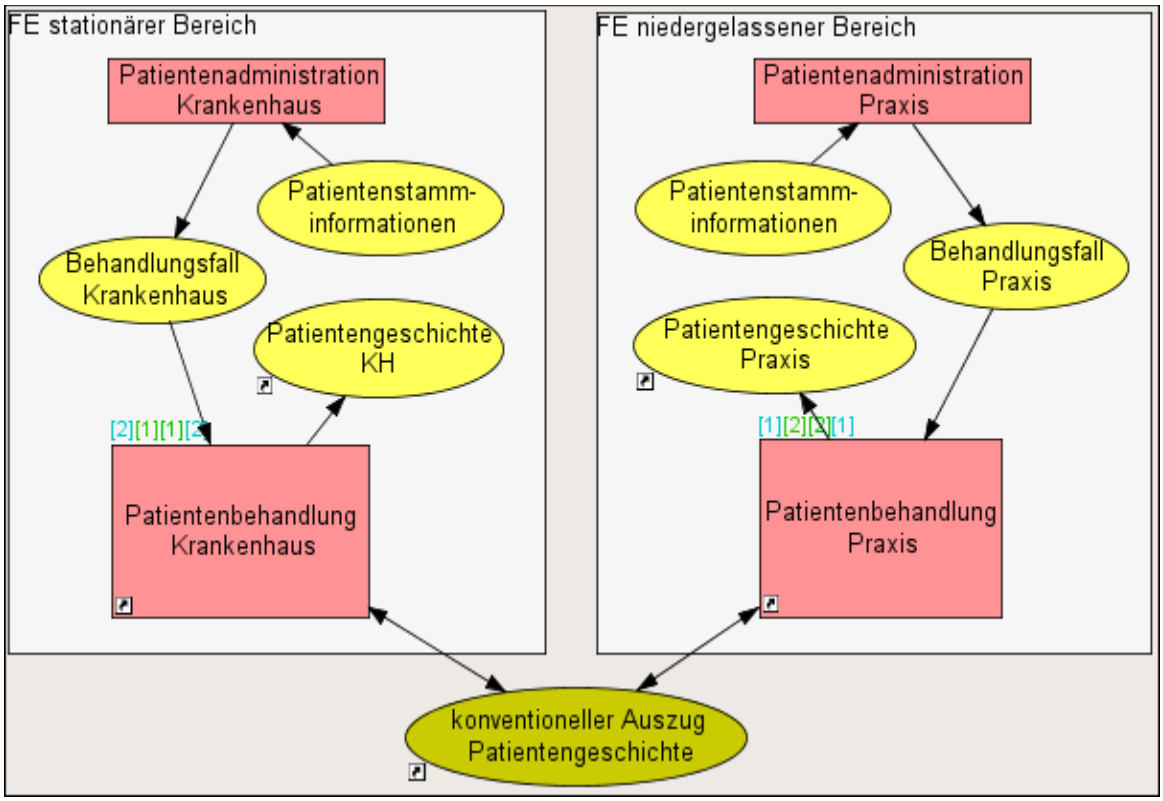

Abbildung 5-1: Ist-Modell der fachlichen Ebene

Zur Modellierung des Datenaustausches zwischen beiden Bereichen wurde der Objekttyp 'konventioneller Auszug der Patientengeschichte' eingeführt, welcher wechselseitig von stationären und niedergelassenem Bereich benötigt (interpretiert) bzw. erstellt (bearbeitet) wird.

Logische Werkzeugebene

In der logischen Werkzeugebene ist die Struktur der Anwendungsbausteine dargestellt. Anwendungsbausteine sind durch rot bzw. orange gefärbte, abgerundete Rechtecke, computerbasierte Bausteinschnittstellen durch grüne Kreise, papierbasierte Bausteinschnittstellen durch dunkelrote Kreise, Datenbanken durch gelbe Zylinder und Beziehungen zwischen den Elementen durch Pfeile gekennzeichnet. Papierbasierte Anwendungsbausteine und die zugehörige Dokumentensammlung sind blau bzw. weiß markiert.

Abbildung 5-2 zeigt die Kommunikationsserver-Architektur des stationären Bereichs und den im niedergelassenen Bereich zum Einsatz kommenden integrierten Anwendungsbaustein 'Patientenverwaltungssystem Praxis' mit seiner Datenbank und der BDT-Schnittstelle. Beide Systeme sind in der Lage, papierbasierte Dokumente zu erstellen und auf diesem Wege Patientendaten zu versenden. Eingehende Dokumente können konventionell verwaltet werden, dass heißt in einer papierbasierten Patientenakte, oder sie werden elektronisch erfasst z.B. durch einen Scanner und in einem Dokumentenmanagementsystem gespeichert.

Der Umgang mit diesen als problematisch und teuer anzusehenden Medienbrüchen wird durch die paarweise angeordneten und rotbraun gefärbten Schnittstellen zwischen rechnerbasierten

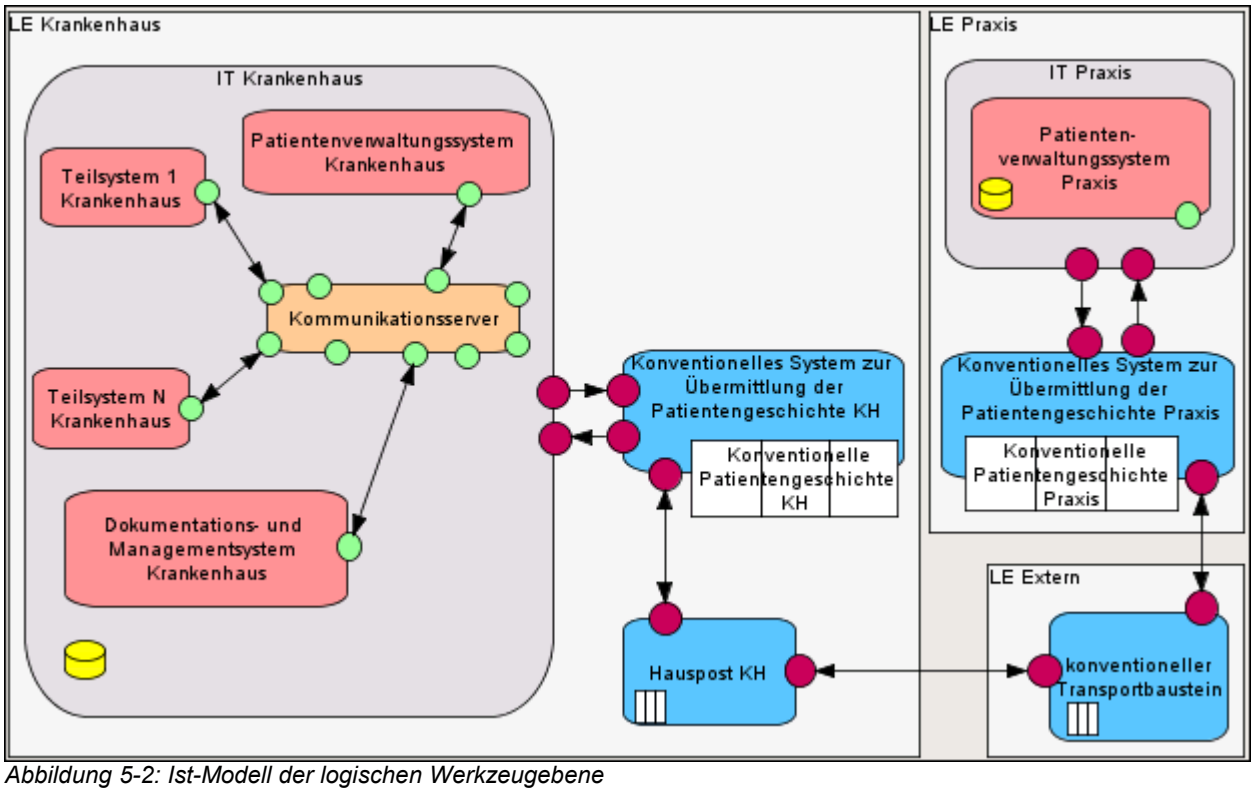

Abbildung 5-2: Ist-Modell der logischen Werkzeugebene

und papierbasierten Anwendungsbausteinen modelliert. Diese Schnittstellen sind als „Erzeugen“ bzw. als „Verwalten“ der papierbasierten Dokumente zu interpretieren. Die Schnittstellen zwischen den konventionellen Anwendungsbausteinen sind ebenfalls rotbraun gefärbt und symbolisieren die Übergänge auf dem papierbasierten Transportweg der angeforderten Patientendaten. So werden Dokumente im Krankenhaus zunächst von der Hauspost entgegengenommen und dann gegebenenfalls intern ausgeliefert oder extern über den hier modellierten 'konventionellen Transportbaustein'[15] weitergeleitet.

Physische Werkzeugebene

Die physische Werkzeugebene zeigt die Strukturen der Hardwarekomponenten. Server, Arbeitsplatz-PCs, Peripheriegeräte und Netzwerkkomponenten sind durch verschiedenfarbige Rechtecke dargestellt. Die Pfeile stellen Kommunikationsbeziehungen dar.

Post, Fax und Bote werden durch menschliche Handlungsträger zur sektorübergreifenden Kommunikation benutzt und sind mit Hilfe entsprechender Symbole dargestellt. Durch menschliche Handlungsträger ausgeführte Kommunikationsbeziehungen sind nicht modelliert.

Der stationäre Bereich ist zur besseren Übersicht in Abbildung 5-3 durch grün gefärbte Rechtecke in Bereiche ('Klinik 1' bis 'Klinik N' und 'Rechenzentrum') unterteilt. Die Netze der beiden Bereiche sind ebenfalls gekennzeichnet.

15 Darunter sind Postweg, Faxdienst und Botendienste zusammengefasst.

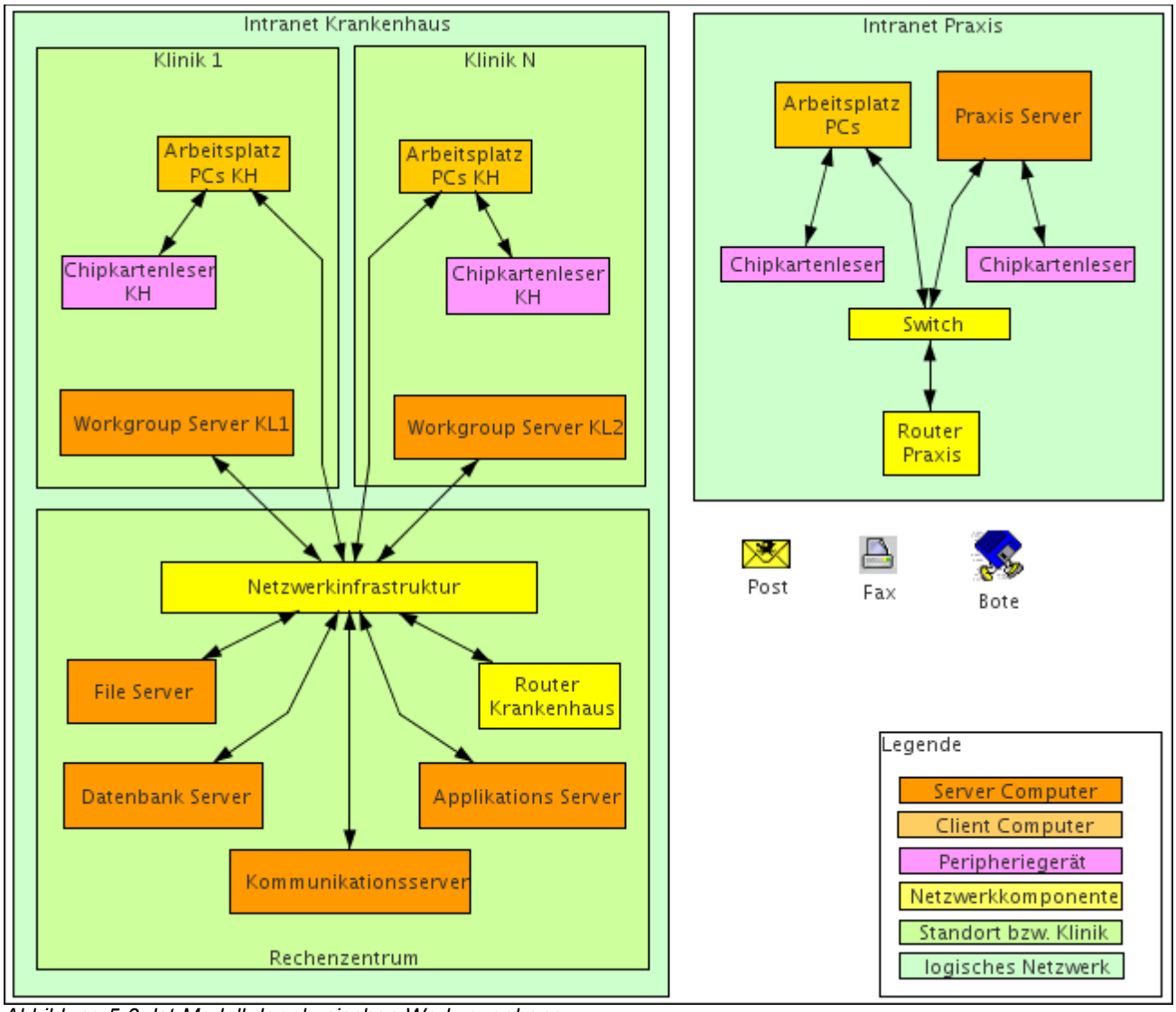

Abbildung 5-3: Ist-Modell der physischen Werkzeugebene

Interebenenbeziehungen

Zwischen Aufgaben- und logischer Ebene sowie zwischen logischer und physischer Ebene bestehen so genannte Interebenenbeziehungen. Mit ihnen lassen sich Aufgaben den Anwendungsbausteinen, Objekttypen den Datenbanken und Anwendungsbausteine den physischen Datenverarbeitungsbausteinen zuordnen.

Abbildung 5-4 zeigt bspw., dass die Aufgaben 'Patientenadministration Praxis' (1) und 'Patientenbehandlung Praxis' (2) durch den Anwendungsbaustein 'Praxisverwaltungssystem' (3) auf Seiten des niedergelassenen Bereichs durchgeführt werden. Dieser steht wiederum in Beziehung mit den Datenverarbeitungsbausteinen auf der physischen Ebene (4). Tatsächlich ist nur ein Teil der modellierten Interebenenbeziehungen in Abbildung 5-4 dargestellt. Je nach Fragestellung bietet der 3LGM^2-Baukasten zur besseren Übersicht die Möglichkeit, die Darstellung bestimmter Interebenenbeziehungen an und ab zuschalten. Weitere Interebenenbeziehungen sind im Modell vorhanden und können in eingesehen werden.

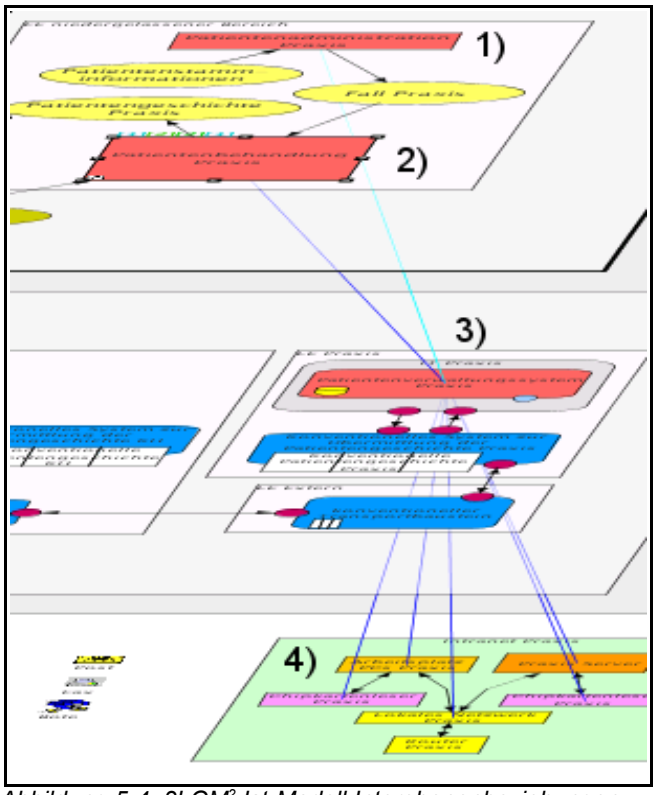

Abbildung 5-4: 3LGM² Ist-Modell Interebenenbeziehungen

Modellierung des konventionellen Kommunikationsprozesses

Mit den Möglichkeiten der Kommunikationsprozessmodellierung in 3LGM² (siehe Kapitel 2.6.1) lässt sich der papierbasierte Datenaustausch wie in Abbildung 5-5 dargestellt abbilden. Ausgehend von der Aufgabe 'Patientenbehandlung Krankenhaus' (1) werden auf der logischen Werkzeugebene die beteiligten Anwendungsbausteine (2, 8) und Bausteinschnittstellen (zwischen 3 bis 7, fett dargestellte Verbindungen) durchlaufen, um schließlich der Aufgabe 'Patientenbehandlung Praxis' den Objekttyp 'konventioneller Auszug der Patientengeschichte' zur Verfügung zu stellen. Besonders kritisch sind die Übergänge 3 und 7, da es sich hierbei um Medienbrüche zwischen den rechnerbasierten (rot) und papierbasierten (blau) Anwendungsbausteinen der logischen Ebene handelt.

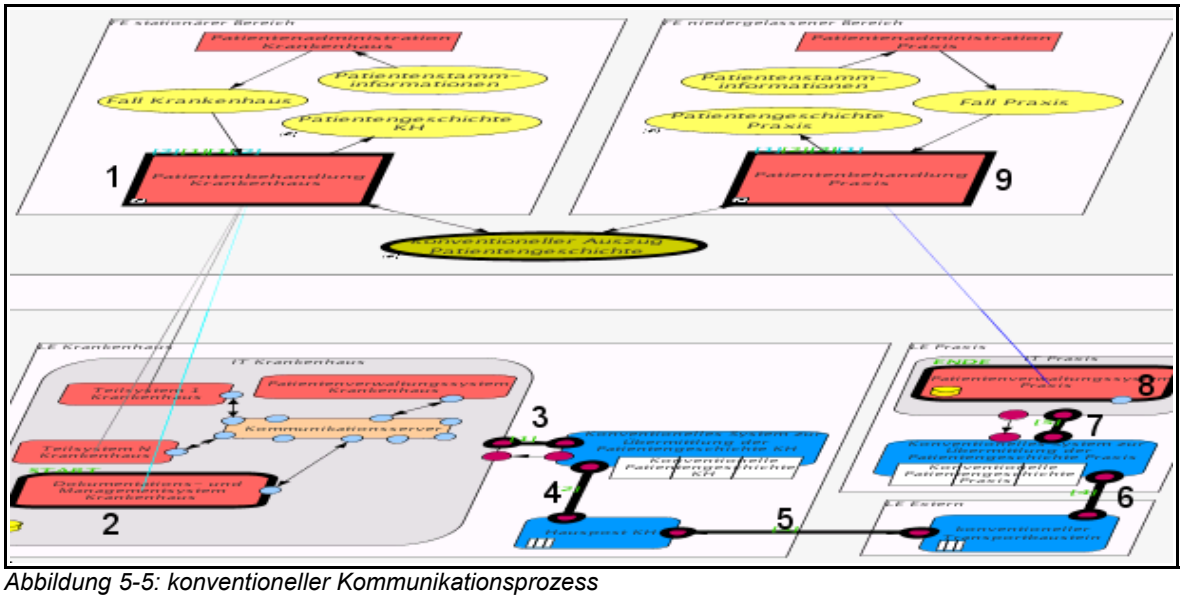

Abbildung 5-5: konventioneller Kommunikationsprozess

5.2 Soll-Zustand

Der Soll-Zustand beschreibt einen Ideal-Zustand eines Bereichs in Bezug auf eine festgelegte Zielsetzung [Haux1998]. Daher wird zunächst die Zielsetzung formuliert und anschließend Kriterien für einen Ideal-Zustand aufgestellt.

5.2.1 Zielsetzung

Im konkreten Fall ist die Zielsetzung die computerbasierte, sektorübergreifende Kommunikation zwischen stationären und niedergelassenen Bereich. Beide Sektoren sollen in der Lage sein, medizinische Daten, wie die Patientengeschichte in Form eines elektronischen Arztbriefes, auf elektronischem Wege auszutauschen. Um eingespielte Arbeitsabläufe nicht zu stören und doppelte Dokumentation zu vermeiden, soll sich die Kommunikationslösung in vorhandene Anwendungssysteme integrieren lassen.

Dieser computerunterstützte Informationsaustausch zieht weitere Vorteile nach sich:

- Medienbrüche werden vermieden. Dies zieht direkt eine Kostenreduzierung nach sich und sorgt für eine bessere Integration der auszutauschenden Dokumente in die Zielsysteme.
- Multimediale Inhalte können übertragen werden,
- schnellerer, vollständigerer und sicherer Transport wird ermöglicht.

Die aufgeführten Punkte reihen sich in die in [Horsch2002] beschriebenen Ziele durch den Einsatz von Telemedizin ein. Insbesondere die folgenden Ziele werden dadurch verfolgt:

- Vollständige Patientendatenverfügbarkeit
- Verbesserung der Dienstleistungsqualität
- effizientere Dienstleistungserbringung
- garantierte Vertraulichkeit.

Ziel ist es nicht, die konventionellen papierbasierten Kommunikationsmethoden vollständig zu ersetzen, da diese als Ausfallkonzept bzw. als Übergangs- oder Ersatzlösungen in Frage kommen. Weiterhin muß bei Nicht-Zustimmung des Patienten zur elektronischen Kommunikation eine konventionelle Alternative angeboten werden.

5.2.2 Kriterien

Die Erfüllung der Zielstellung ist an Bedingungen gebunden. Diese Bedingungen stellen die Bewertungskriterien für die verfügbaren Lösungsansätze aus Kapitel 4 dar. Dabei können den Kriterien Prioritäten zugeordnet werden. Kriterien, die in jedem Fall erfüllt werden müssen, werden als K.O.-Kriterien bezeichnet.

Die in Kapitel 3 erarbeiteten Anforderungen an die computergestützte Kommunikation sind die Rahmenbedingungen, die bei der Erfüllung der Zielstellung gelten. Dabei sind die gesetzlichen Anforderungen als K.O.-Kriterien anzusehen. Technische und ökonomische Anforderungen sind variable Anforderungen. Wobei auch hier in einer konkreten Umsetzung Mindest- oder Maximalwerte mit K.O.-Charakter für einzelne Unterpunkte oder Bereiche definiert werden können.

5.3 Analyse und Bewertung

Die in Kapitel 4 vorgestellten Verfahren bieten die Möglichkeit die Zielsetzung in Bezug auf die computerbasierte Kommunikation zwischen stationären und niedergelassenen Bereich zu erfüllen. Es gilt nun diese Verfahren hinsichtlich ihrer Konformität zu den in Kapitel 3 erarbeiteten Anforderungen zu bewerten und eine Auswahl zu treffen.

5.3.1 Anwendung der K.O.-Kriterien

Zunächst sollen die Verfahren auf die Erfüllung der gesetzlichen Anforderungen überprüft werden. Die gesetzlichen Anforderungen aus Kapitel 3.1 sind die K.O.-Kriterien für die Verfahren.

Die gesetzlichen Anforderungen verlangen ein hohes Maß an Sicherheit für die zu übertragenden personenbezogenen Informationen. Da bei FTP, bis auf die Erweiterungen hinsichtlich der Transportsicherheit, keine Sicherheitsmaßnahmen getroffen werden, scheidet dieses Verfahren an dieser Stelle aus.

Bei E-Mail Verfahren mit S/MIME Erweiterung, bei VCS und PaDok kommen sichere kryptographische Methoden zum Einsatz und sorgen so für das geforderte Maß an Sicherheit. Die drei Verfahren nutzen auf Zertifikaten basierende Public-Key Verfahren. Dadurch wird Integrität, Vertraulichkeit, Authentizität und Rechtssicherheit garantiert.

Beim E-Mail Verfahren unter Verwendung von PGP fehlen Zertifikate zur Überprüfung der zum Einsatz kommenden Schlüssel. Die Echtheit der Schlüssel wird von den Nutzern selbst durch das Web-of-Trust authentifiziert. Für den Einsatz im medizinischen Umfeld ist der Web-of-Trust Ansatz mangels technischen Verständnis der Nutzer, hohen Aufwandes und fehlender Rechtssicherheit ungeeignet.

Bei den Verfahren VCS und PaDok übernehmen zertifizierte Provider die Aufgaben des Trust Centers, welches zentral die Echtheit der Zertifikate garantiert. Beim S/MIME E-Mail Verfahren ist eine derartige offizielle Instanz nicht explizit vorgeschrieben und kann prinzipiell auch von unseriösen Parteien betrieben werden. Beim Einsatz dieses Verfahrens im medizinischen Umfeld ist daher darauf zu achten, die Wahl des Trust Centers mit den Datenschützern abzustimmen und nur auf vertrauenswürdigen Anbieter, wie z.B. Provider von medizinischen Netzen oder die Bundesnetzagentur, zurückzugreifen. Die gesetzlich geforderte Nicht-Abstreitbarkeit und Revisionssicherheit kann beim S/MIME E-Mail Verfahren erreicht werden. Dazu sind jedoch angepasste E-Mail Anwendungen oder entsprechende Vorschriften zur Einhaltung dieser Forderungen zu befolgen. Da die Einhaltung der Vorschriften praktisch nicht überprüft werden kann, ist die Rechtssicherheit dieser Herangehensweise fraglich. Aufgrund

dieser und der vorangegangenen Abstriche des S/MIME E-Mail Verfahrens, kommt es in den weiteren Betrachtungen nicht mehr vor und scheidet aus. VCS und PaDok erfüllen die Anforderungen Nicht-Abstreitbarkeit und Revisionssicherheit durch Quittungsbetrieb und die Verwendung signierter Protokolle.

Die gesetzlich festgeschriebene freie Arztwahl wird bei VCS durch die Initial ungerichtete Kommunikation und bei PaDok durch den gerichteten Versand unterstützt. Bei der Initial ungerichtete Kommunikation des VCS Verfahrens handelt es sich gesetzlich um ein automatisches Abrufverfahren nach §10 Bundesdatenschutzgesetz, welches weitere Bedingungen und Maßnahmen nach sich zieht (§10 Absatz 2,3,4 BDSG). Bei PaDok müssen zu diesem Zweck keine weiteren Vorkehrungen getroffen werden, da eine Realisierung der freien Arztwahl über eine doppelte Verschlüsselung gelöst ist (siehe Kapitel 4.3).

Aufklärung, Patienteneinwilligung und Datensparsamkeit sind gesetzliche Anforderungen, die derzeit überwiegend von den menschlichen Handlungsträgern zu leisten und zu überwachen sind.

Nach Anwendung der K.O.-Kriterien kommen noch VCS und PaDok in Betracht. Wobei das PaDok-Verfahren bei der Umsetzung der freien Arztwahl Vorteile bietet.

5.3.2 Anwendung technischer und ökonomischer Kriterien

Die technische Anforderungen Verfügbarkeit, Leistungsfähigkeit, Flexibilität und Erweiterbarkeit in Bezug auf die physischen Datenverarbeitungsbausteine sind weitgehend unabhängig vom eingesetzten Verfahren. Diese Kriterien richten sich an die darunter liegende Hardware.

Bei den Kriterien Leistungsfähigkeit, Flexibilität und Erweiterbarkeit lassen sich Unterschiede zwischen VCS und PaDok feststellen.

Die folgende Tabelle 5-2 stellt den Funktionsumfang der beiden Verfahren gegenüber. Daraus ist zu entnehmen, dass das PaDok-Verfahren zusätzlich das Anlegen einer temporären Fallakte unterstützt.

Bedeutung, Funktion	VCS	PaDok
Kommunikation mit vorher bekanntem Empfänger	Direkte oder gerichtete Kommunikation	Adressierter Versand
Unspezifizierter Empfänger	Initial ungerichtete Kommunikation	Gerichteter Versand
Temporäre Netz-Fallakte	-	Ungerichtete Kommunikation

Tabelle 5-2: Funktionsumfang VCS, PaDok

Ein weiterer Vorteil von PaDok gegenüber VCS ist das verwendete Datenaustauschformat. Bei VCS kommt der VCS-Arztbrief zum Einsatz, ein durch die xDT-Protokollfamilie festgelegtes Format. Dagegen kommt bei PaDok ein Austauschformat auf Basis von XML Dokumenten zum Einsatz. Diese sind flexibel erweiterbar und für verschiedene Anwendungen (eArztbrief, eÜberweisung, Mamma Akte NRW, DMP-Diabetes) standardisiert.

Die Kriterien Sicherheit und Protokollierbarkeit sind bereits durch die gesetzlichen Anforderungen abgedeckt. Bleiben Support und Integration auf der technischen Seite zu bewerten.

Beim vom VDAP entwickelten VCS stellt das Kommunikations- und Prozessmodul (KPM) die Implementierung der Spezifikation dar. Die Hersteller von Praxis-Softwareprodukten können das KPM integrieren, um dessen Funktionalität zu nutzen. Supportpflichtige Ansprechpartner sind beim VCS die Hersteller der integrierten Softwarelösungen.

Die KVNo als Herausgeber der PaDok Referenzimplementierung D2D stellt den Nutzern den D2D-Client bereit und übernimmt auch den Support. Ist der D2D-Client in die Praxissoftware integriert, übernimmt der Hersteller den Support. Beim Einsatz des kostenlosen D2D-Client ist in der Regel der Einsatz zusätzlicher Software zur Integration in das bestehende Praxisverwaltungssystem nötig. Die Hersteller derartiger Softwarelösungen übernehmen in der Regel auch Wartung und Support der D2D Schnittstelle. In beiden Fällen sind im Ergebnis eindeutig technische Ansprechpartner zu identifizieren.

Da beim VCS keine separate Implementierung des KPM verfügbar ist, sind die Software Hersteller für die Integration dieses Moduls verantwortlich. Durch die herstellerseitige Integration des KPM kann auf Seiten der Praxisinformationssysteme bei den Softwareprodukten mit VCS Funktionalität von einer optimalen Integration gesprochen werden. Konkrete Implementierungen im stationären Bereich sind jedoch nicht bekannt. Der als Datenaustauschformat zum Einsatz kommende VCS-Arztbrief liegt im xDT-Format vor. Damit eignet sich VCS besonders für den Austausch von Patientendaten innerhalb des niedergelassenen Bereichs. Für einen sektorenübergreifenden Datenaustausch ist beim VCS in seiner derzeitigen Form im stationären Bereich Anpassungsarbeit zu leisten. Fehlende Schnittstellen sind ein Problem aber auch die semantischen Inkompatibilitäten zwischen den xDT-Protokollen und den im klinischen Sektor vorherrschenden HL7 Standard.

Die PaDok-Funktionalität lässt sich bei bestehenden Informationssystemen aufgrund des frei verfügbaren D2D-Client nachrüsten. Optimale Funktionsintegration bieten, wie schon beim VCS, die Softwareprodukte, die den D2D-Client von Haus aus vollständig integrieren. Im Gegensatz zu VCS ist jedoch beim Einsatz des D2D-Client in Verbindung mit einer Integrationssoftware eine Integration in bestehende Informationssysteme möglich, die vorher keine Untersützung geboten haben. Ein weiterer Vorteil von PaDok liegt in der konsequenten Verwendung von CDA XML-Dokumenten (SCIPHOX). Es stehen derzeit SCIPHOX-standardisierte CDA-Dokumente für den elektronischen Kurzbericht, elektronische Überweisung und Entlassung sowie viele weitere Anwendungen zur Verfügung [XMLD2D]. XML Dokumente bieten wesentliche Vorteile bei sektorübergreifender Kommunikation in Bezug auf die semantische Integration. Auch das im CDA-Standard verwendete Phasenmodell (siehe Kapitel 2.2.3) hilft bei der schrittweisen Anpassung.

Eine ökonomische Anforderung ist bereits durch die Auswahl existierender Kommunikationsverfahren erfüllt. Die Nutzung von vorhandenen Ressourcen, Betriebs-, Support- und Lizenzkosten sind für eine konkrete Lösung im Detail zu Untersuchen.

Wie die Systemanalyse gezeigt hat, waren die in den Praxen eingesetzten Computer im Durchschnitt nicht älter als drei Jahre. Bei den darauf laufenden Betriebssysteme handelte es sich vorwiegend um Microsoft Windows in den Versionen Windows 2000 und Windows XP. Diese technischen Eckdaten gehen konform mit den Systemvoraussetzungen beider Verfahren und es müssen für deren Betrieb keine Computer oder Betriebssysteme neu angeschafft werden. Nachgebessert werden muss im niedergelassenen Bereich bei der Kommunikationstechnik. Nur 50% der Befragten nutzten einen Internetzugang. Der Zugang zu

einem Medizin-Netz Provider war bei keinem der untersuchten Arztpraxen vorhanden. An dieser Stelle müssen laufende Kosten für die Nutzung derartiger Netze eingeplant werden.

Beide Verfahren können über zertifizierte Provider genutzt werden und müssen nicht vor Ort implementiert und betreut werden. Dabei ist der Serverstandort durch die Nutzung des Internets/Medizin-Netz von untergeordneter Bedeutung.

Die Verwendung offener Standards ist ebenfalls gegeben. Beim Kriterium Investitionsschutz gibt es wiederum Vorteile bei der Fraunhofer-Lösung PaDok. Zum einen gibt es eine derzeit ständig anwachsende Zahl an Anwendungen, die auf D2D basieren, einzusehen auf der D2D-Homepage [D2DHP]. Zum anderen findet beim Entwickler des VCS, VDAP e.V., eine Umstrukturierung mit derzeit unklarem Ausgang statt. Zudem haben namhafte Hersteller, zum Teil Gründungsmitglieder, den Verband verlassen und das Scheitern der Etablierung des VCS verkündet [MCSDEG2004].

5.3.3 Ergebnis und Zusammenfassung

Aufgrund des Ausscheidens der Kommunikationsverfahren FTP und E-Mail durch K.O.-Kriterien, wird bei der Zusammenfassung der Ergebnisse nicht weiter auf diese beiden Verfahren eingegangen.

Die beiden Verfahren VCS und PaDok erfüllen die K.O.-Kriterien und haben hinsichtlich der zu Grunde liegenden Informationssystemarchitektur viele Gemeinsamkeiten. Beide Verfahren setzen auf starke Kryptographie und eine Public-Key Infrastruktur. In beiden Verfahren wird eine Client/Server Architektur zum Versenden asynchroner Nachrichten nach dem Store-and-Forward Prinzip verwendet. Diese Eigenschaften sind rechtlichen Grundlagen und dem aktuell technisch Machbaren geschuldet.

Bei den Kriterien Integration sowie Flexibilität und Erweiterbarkeit gibt es deutliche Vorteile beim PaDok-Verfahren. Es ist es von entscheidender Bedeutung, dass die auszutauschenden Informationen von allen beteiligten Anwendungen in gleicher Weise interpretiert werden. Da in stationären und niedergelassenen Bereich unterschiedliche Kommunikationsstandards etabliert sind, empfiehlt es sich ein offenes, flexibles und leicht zu transformierendes Format zu wählen. Die SCIPHOX-Arbeitsgruppe hat mit diesem Ziel den SCIPHOX CDA Standard entwickelt, welcher beim PaDok-Verfahren eingesetzt wird. Dies ist ein entscheidender Schritt der bestehenden syntaktischen wie semantischen Heterogenität zu begegnen.

In Hinblick auf die unklare Zukunft des VDAP und den Trend in Richtung PaDok/D2D erleichtert außerdem die Empfehlung des PaDok-Verfahrens zur sektorübergreifenden Kommunikation.

Abschließend stellt die folgende Tabelle die beiden Verfahren VCS und PaDok anhand der verwendeten Kriterien gegenüber.

Kriterien / Verfahren	VCS	PaDok
Gesetzliche Anforderungen	+	+
Funktionsumfang, Leistung	+	+
Erweiterbarkeit und Flexibilität	o	+
Support	+	+
Integration in bestehende PrIS	+	+
Integration in bestehende KIS	-	+
Integration Austauschformat	-	+
Outsourcing der Serverkomponente	+	+
Offene Standards	+	+
Investitionsschutz	-	+

Tabelle 5-3: Kriterien vs. Verfahren

Legende:

'+'erfüllt, 'o' mäßig erfüllt, '-' schlecht erfüllt

6 Das Referenzmodell

In diesem Kapitel laufen die Betrachtungen und Erkenntnisse der vorangegangenen Kapitel zusammen. In Kapitel 5 wurden die gesetzlichen, technischen und ökonomischen Anforderungen aus Kapitel 3 auf die ermittelten Verfahren zur Unterstützung der Kommunikation aus Kapitel 4 unter Berücksichtigung des Ist-Zustandes angewendet. Darauf aufbauend wird nun schrittweise ein Referenzmodell für den rechnergestützten Austausch von Patientendaten zwischen stationären und niedergelassenen Bereich entwickelt.

Mit Fokus auf den Aufgaben sowie der Sicht auf die logische und physische Ebene, kommt für die Modellierung des Referenzmodells das 3LGM²-Metamodell zum Einsatz. Um die Identifizierung der Modellkomponenten zu erklären, wird auf Beschreibungen mit Elementen der semiformalen Sprache UML (Unified Modeling Language, [UMLV2]) zurückgegriffen. Außerdem ermöglicht die Modellierung in UML mit ihrer Vielfalt an Darstellungsmöglichkeiten in Form von Diagrammen zusätzlich prozessorientierte Sichten auf das Modell.

6.1 Vorgehensweise der Modellierung

Wie zu Beginn dieses Kapitels erwähnt, wurde ein schrittweises Vorgehen bei der Modellierung verfolgt. Die einzelnen Schritte auf dem Weg zum Referenzmodell sind der Inhalt dieses Abschnittes.

Zu Beginn der Modellierung besteht das Problem, die in den vorangegangenen Kapiteln ermittelten Fakten in einen ganzheitlichen Zusammenhang zu betrachten. In einen ersten Versuch, Klarheit zu schaffen, stellen sich folgende Fragen: Was soll modelliert werden? Was sind die Aufgaben, die es zu erfüllen gilt? Für derartige Fragestellungen eignen sich UML Use Case Diagramme. Diese Diagramme bieten die Möglichkeit Beziehungen zwischen den Aufgaben darzustellen und zu verfeinern.

Sind die Aufgaben identifiziert, sind folgende Fragen zu beantworten: Wie können die Aufgaben erfüllt werden? Was wird benötigt, um die Aufgaben zu erledigen? Um sich diesen Fragestellungen zu nähern, wird auf die Ergebnisse aus Kapitel 5 zurückgegriffen. Die in Kapitel 3 ermittelten Anforderungen liefern die Entscheidungsgrundlage für die in Kapitel 4 untersuchten Kommunikationsmethoden. Aus dem anforderungskonformen PaDok-Verfahren wird auf die im Modell zu verwendende Architektur geschlossen. Zusammen mit dem Ist-Modell kommen UML Sequenzdiagramme zur Veranschaulichung von Kommunikationsprozessabläufen zum Einsatz. Die Untersuchung der Prozessabläufe unter Berücksichtigung der Anforderungen führt zur Identifizierung weiterer Modellkomponenten.

Die auf diesem Wege identifizierten Komponenten werden anschließend in das Ist-Modell integriert. Das so erweiterte Modell wird weiter konfiguriert und mit den Analysemöglichkeiten des 3LGM²-Baukasten auf seine Funktionstüchtigkeit in Bezug auf die Kommunikation zwischen stationären und niedergelassenen Bereich überprüft. Das Ergebnis dieser Vorgehensweise ist das im 3LGM²-Baukasten modellierte Referenzmodell.

Abbildung 6-1 illustriert die Vorgehensweise bei der Modellierung.

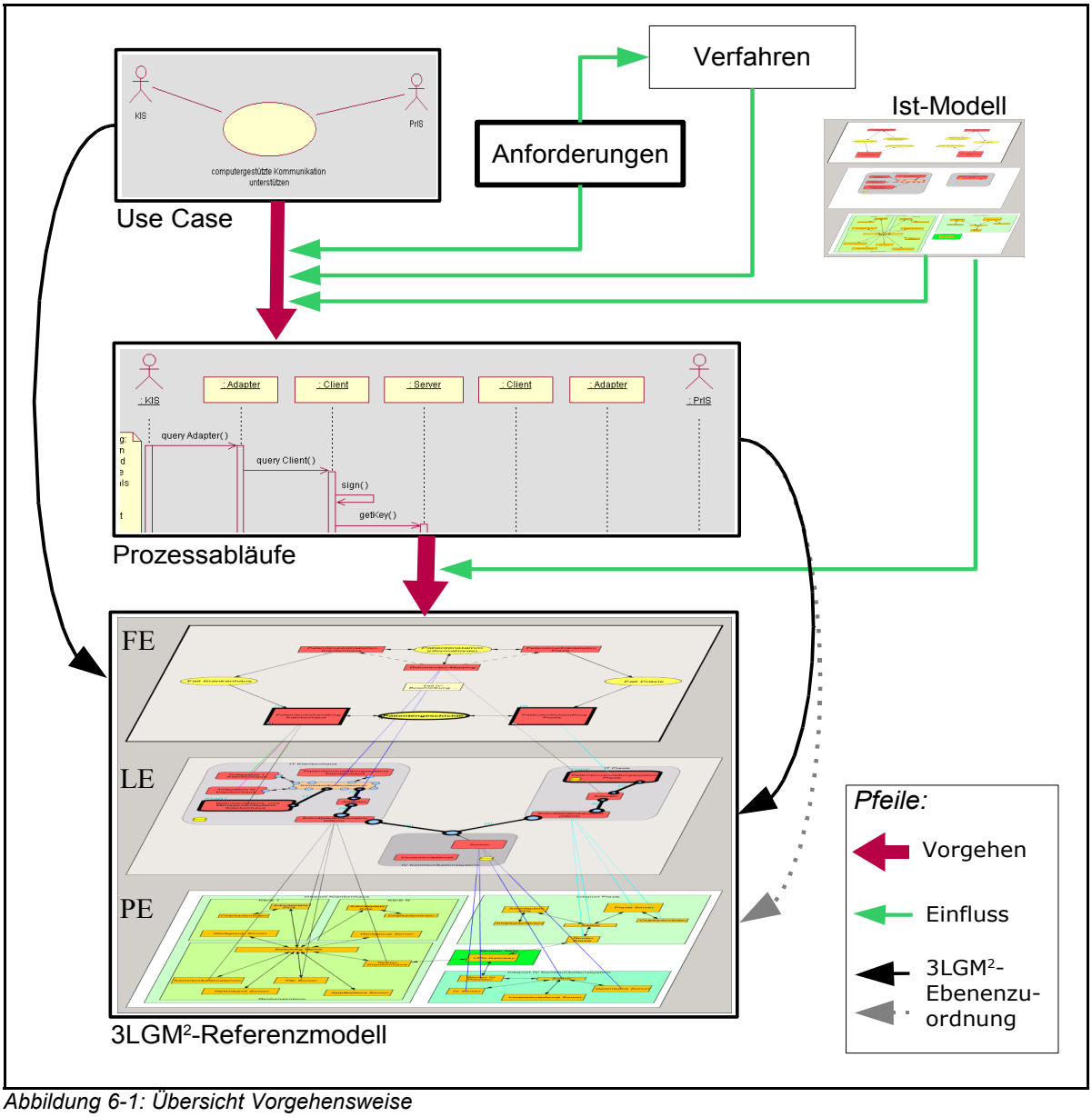

Abbildung 6-1: Übersicht Vorgehensweise

6.2 Use Case Modellierung

Use Case Diagramme eignen sich besonders gut dazu einen Überblick über die zu unterstützenden Aufgaben zu erhalten. Mit dieser, auf die Anwendungsfälle bezogenen Sicht, lässt sich der zu untersuchende Bereich in eine auf die Unternehmensaufgaben fokussierte Sicht einordnen.

Wie schon die deutsche Übersetzung des Begriffs andeutet, behandeln Use Case Diagramme Anwendungsfälle. Ein Anwendungsfall beschreibt einen Geschäftsprozess. Dabei wird nur das WAS und nicht das WIE des Geschäftsprozesses beschrieben.

Use Case Diagramme unterscheiden im wesentlichen drei Sprachelemente: Akteure, Anwendungsfälle und Assoziationen. Ein Akteur kann ein Nutzer oder ein System sein, welches eine bestimmte Rolle in Bezug auf das System einnimmt. Ein Anwendungsfall beschreibt eine Aktion zur Erledigung einer Aufgabe [WinterM2005]. Assoziationen sind Beziehungen zwischen den Anwendungsfällen. Ein Use Case Diagramm zeigt die Beziehungen zwischen Akteuren und Anwendungsfällen. Dabei wird das Systemverhalten aus Sicht eines externen Beobachters beschrieben. Use Case Diagramme können zwar verfeinert werden, stellen aber keinen Designansatz, im Sinne wie eine Aufgabe zu erfüllen ist, dar und beschreiben auch nicht das interne Verhalten des zukünftigen Systems [Oestereich1997], [Fowler1998].

Die wichtigsten Beziehungen zwischen Anwendungsfällen sind <<include>> und <<extend>>. Dabei drückt A <<include>> B aus, dass A eine Unteraufgabe B hat, die bei der Abarbeitung von Aufgabe A mindestens einmal durchlaufen wird. A <<extends>> B hingegen bedeutet, dass A eine Aufgabe des selben Typs ist wie B, nur das A spezialisierter ist als B.

Nach diesen Regeln lässt sich nun das folgende Use Case Diagramm erstellen.

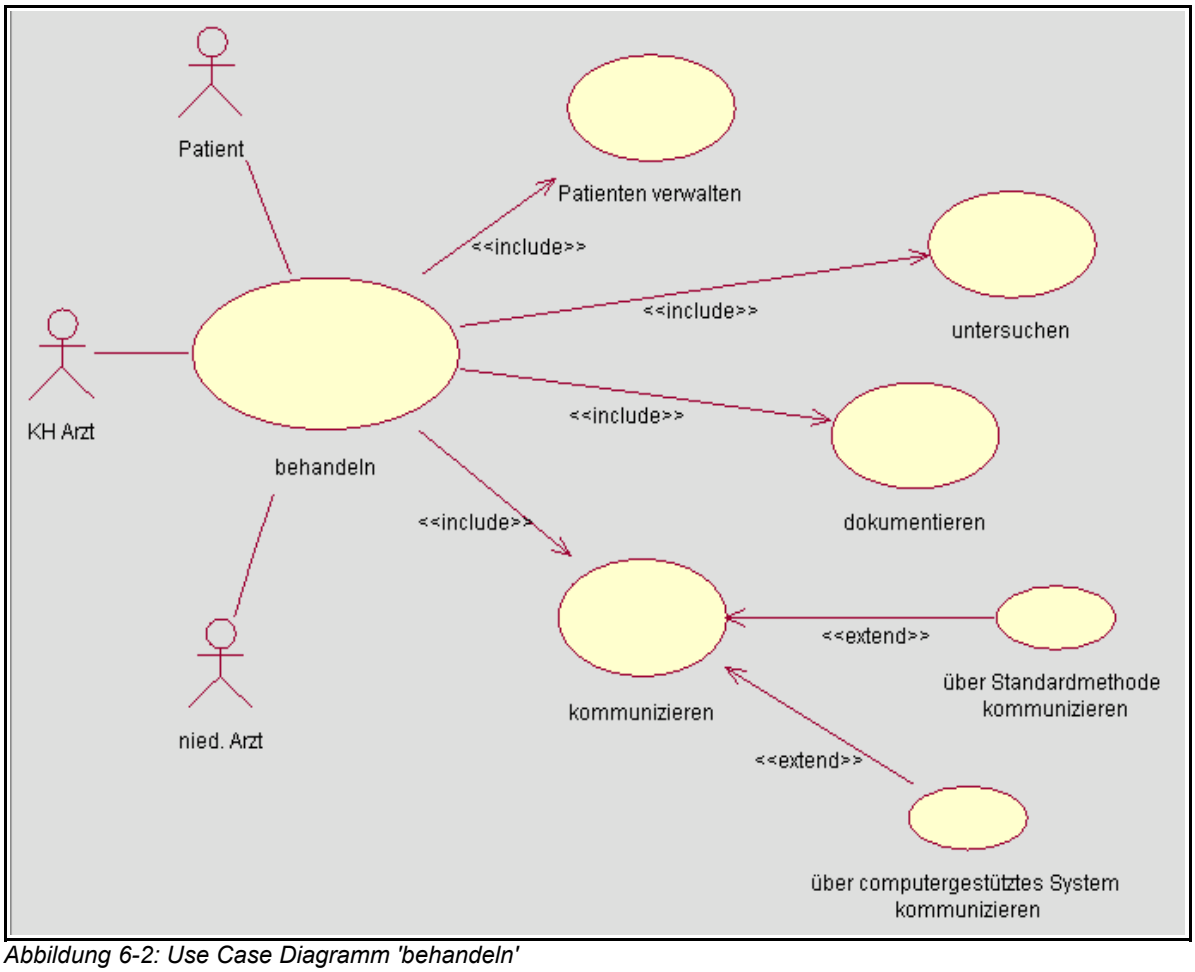

Abbildung 6-2: Use Case Diagramm 'behandeln'

Nach UML Syntax sind die Akteure als Strichmännchen abgebildet, die Anwendungsfälle als Ellipsen. Die Pfeile kennzeichnen die Beziehungen zwischen den Anwendungsfällen. Abbildung 6-2 zeigt den Anwendungsfall 'behandeln', welcher sich aus der Unternehmensaufgabe „Patientenbehandlung“ ableitet. Die Aufgabe „Patientenbehandlung“ ist dabei wie folgt definiert:

> *Unterstützung der Versorgung des Patienten im ambulanten bzw. stationären Bereich von der Aufnahme bis zur Entlassung und gegebenenfalls der Weiterleitung an andere Einrichtungen einschließlich von Tätigkeiten wie Dokumentation und Abrechnung.* [UMIT2005], [Lehmann2002]

Am Anwendungsfall 'behandeln' sind in Abbildung 6-2 die Akteure Patient, Krankenhausarzt (KH Arzt) und niedergelassener Arzt beteiligt. Der Anwendungsfall 'behandeln' lässt sich bspw. in durch die mit der <<include>> Beziehung assoziierten Anwendungsfälle 'Patienten verwalten', 'untersuchen', 'dokumentieren' und 'kommunizieren' unterteilen. Die Unterteilung in diese (Teil-) Anwendungsfälle leitet sich aus der Definition der „Patientenbehandlung“ ab. Die *„Unterstützung der Versorgung des Patienten im ambulanten bzw. stationären Bereich“* ist mit Anwendungsfall 'untersuchen' abgedeckt. Er steht für die Durchführung der medizinischen Maßnahmen und wurde in das Diagramm aufgenommen, um auf die Kernaufgabe der Patientenbehandlung hinzuweisen. Der Teil der Definition, der *„von der Aufnahme bis zur Entlassung und gegebenenfalls der Weiterleitung an andere Einrichtungen“* handelt, findet sich im Use Case Diagramm als (Teil-)Anwendungsfall 'Patienten verwalten' wieder. Darin ist z.B. auch die Erhebung der Patientenstamm- und Versicherungsdaten sowie die Prüfung auf Wiederkehr enthalten. Der Teilanwendungsfall 'dokumentieren' korrespondiert zu *„Tätigkeiten wie Dokumentation und Abrechnung“*. Nicht ganz so eindeutig ist die Zuordnung des Teilanwendungsfalls 'kommunizieren'. Wie auch die Dokumentation wird die Kommunikation nicht als eigene Aufgabe modelliert. Vielmehr werden 'dokumentieren' und 'kommunizieren' als inhärente Aufgaben der Patientenbehandlung verstanden. Einen Hinweis findet sich aber dennoch in der *„Weiterleitung an andere Einrichtungen“*, welche ohne eine Weiterleitung von Informationen (Kommunikation) nicht umsetzbar ist. Für die Modellierung der sektorübergreifenden Kommunikation ist es deshalb sinnvoll, diese inhärenten Aufgaben als eigenständigen Anwendungsfall zu betrachten, um sie weiter untersuchen zu können.

6.2.1 Verfeinerung: 'kommunizieren'

Der (Teil-)Anwendungsfall 'kommunizieren' kann nun in zwei spezialisierte Anwendungsfälle unterteilt werden: 'über Standardmethode kommunizieren' und 'über computergestütztes System kommunizieren'. Mit der Standardmethode ist die Kommunikation auf herkömmliche Weise per Fax, Telefon oder Post mit all ihren Vor- und Nachteilen gemeint. Die computergestützte Variante ist Gegenstand der Modellierung und soll weiter untersucht werden.

Aus den vorangegangenen Kapiteln ist bekannt, dass Informationssysteme Möglichkeiten bieten, die Aufgabe „Patientenbehandelung“ und ihre Teilaufgaben zu unterstützen. Werden diese Überlegungen auf den Anwendungsfall 'kommunizieren' angewendet, ergibt sich folgendes Use Case Diagramm:

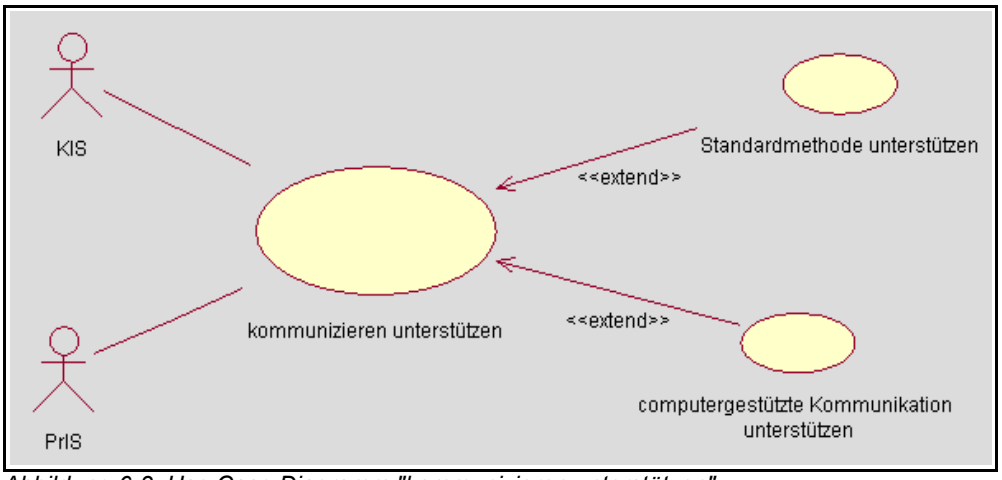

Abbildung 6-3: Use Case Diagramm "kommunizieren unterstützen"

Akteure sind diesmal die beiden Informationssysteme KIS und PrIS. Sie haben die Aufgabe, die Kommunikation als Teilaufgabe der Patientenbehandlung zu unterstützen und sind daher am Anwendungsfall 'kommunizieren unterstützen' beteiligt. Dieser kann analog zum Anwendungsfall 'kommunizieren' in Abbildung 6-2 in 'Standardmethode unterstützen' z.B. durch das Ausdrucken entsprechender Faxvorlagen, Formulare oder Arztbriefe und 'computergestützte Kommunikation unterstützen' unterschieden werden. In Abbildung E-1, Anhang E ist zusätzlich zu sehen, wie sich das Use Case Diagramm aus Abbildung 6-3 in jenes aus Abbildung 6-2 einfügt.

Durch die Eigenschaft der <<extend>> Beziehung, Spezialisierung zu modellieren, lässt sich ein weiteres Use Case Diagramm erstellen.

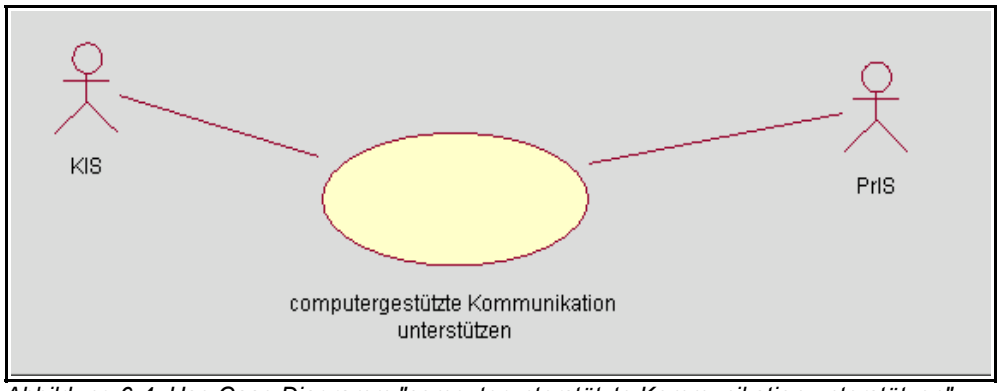

Abbildung 6-4: Use Case Diagramm "computerunterstützte Kommunikation unterstützen"

In dem in Abbildung 6-4 dargestellten Use Case Diagramm ist nun klar herausgearbeitet worden, was Gegenstand der Modellierung ist. Die beiden Hauptakteure KIS und PrIS sind identifiziert.

An dieser Stelle wird die Use Case Modellierung beendet. Eine weitere Verfeinerung des in Abbildung 6-4 dargestellten Use Case Diagramms ist möglich und kann Ausgangspunkt für detailiertere Untersuchungen der Prozesse sein. Für die weiteren Betrachtungen ist der Detailgrad in Abbildung 6-4 jedoch gut geeignet.

6.3 Anforderungen, Architektur und Ist-Modell - Prozessabläufe

Nachdem das WAS im vorangegangenen Abschnitt durch die Untersuchung der Anwendungsfälle erörtert wurde, beschäftigt sich dieser Abschnitt mit der Frage nach dem WIE. Konkret geht es um die Beantwortung folgender Fragen: Wie kann „computergestützte Kommunikation unterstützen“ modelliert werden? Welche Komponenten sind für eine anforderungskonforme Realisierung nötig?

Um zu verdeutlichen, wie Objekte zusammenarbeiten, kommen UML-Sequenzdiagramme zum Einsatz.

6.3.1 Sequenzdiagramme

Sequenzdiagramme gehören zu den Aktivitätsdiagrammen und beschreiben mit welchem Verhalten Gruppen von Objekten zusammenarbeiten. Dabei wird das Verhalten eines einzelnen Anwendungsfalls fokussiert. Im vorliegenden Fall sind die Objekte gleichzusetzen mit den Akteuren und Komponenten.

Die Elemente des Sequenzdiagramms sehen nun wie folgt aus: Akteure werden aus dem Use Case Diagramm übernommen und durch Strichmännchen symbolisiert. Die Komponenten werden in Form von Rechtecken dargestellt. Die Objekte (Akteure und Komponenten) verfügen über eine gestrichelte, nach unten gerichtete, vertikale Linie. Diese Linie ist die Lebenslinie des Objekts und verdeutlicht die Existenz des Objektes während der Interaktion.

Die Objekte interagieren, indem sie Nachrichten austauschen, welche im Diagramm durch benannte Pfeile zwischen den Lebenslinien repräsentiert werden. Ein Objekt kann dabei auch Nachrichten mit sich selbst austauschen (Selbstdelegation). Gestrichelte Pfeile sind Rückgabewerte eines zugehörigen Nachrichtenpfeils. Die Reihenfolge der Nachrichten ist durch die Anordnung anhand der vertikal verlaufenden Zeitachse festgelegt.

6.3.2 Anwendungsfall 'behandeln'

Bevor die eigentlichen Kommunikationsprozesse detailierter betrachtet werden, wird der Anwendungsfall 'behandeln' beispielhaft in einem Sequenzdiagramm in Abbildung 6-5 modelliert. In diesem Sequenzdiagramm wird der Ablauf eines typischen sektorübergreifenden Behandlungsfalls gezeigt. Im gezeigten Szenario wird der Patient krank und geht zur Behandlung zunächst zu einem niedergelassenen Arzt (z.B. seinem Hausarzt, (a)). Dort durchläuft er die schon im Use Case Diagramm in Abbildung 6-2 identifizierten Stationen:

- 'Patienten verwalten' – Der Patient wird Aufgenommen, Patientenstamm- und Versicherungsdaten werden erfasst,
- 'untersuchen' - es werden medizinische Maßnahmen zur Heilung durchgeführt,
- 'dokumentieren' - es wird sowohl die Leistungsdokumentation zur Abrechnung als auch Anamnese und ggf. ein Arztbrief erstellt,
- 'kommunizieren' - sollte sich bei der Untersuchung herausstellen, dass eine Behandlung bei einem weiteren Arzt nötig ist, werden Arztbrief und eventuell weitere Dokumente, die für die Weiterbehandlung notwendig sind, kommuniziert.

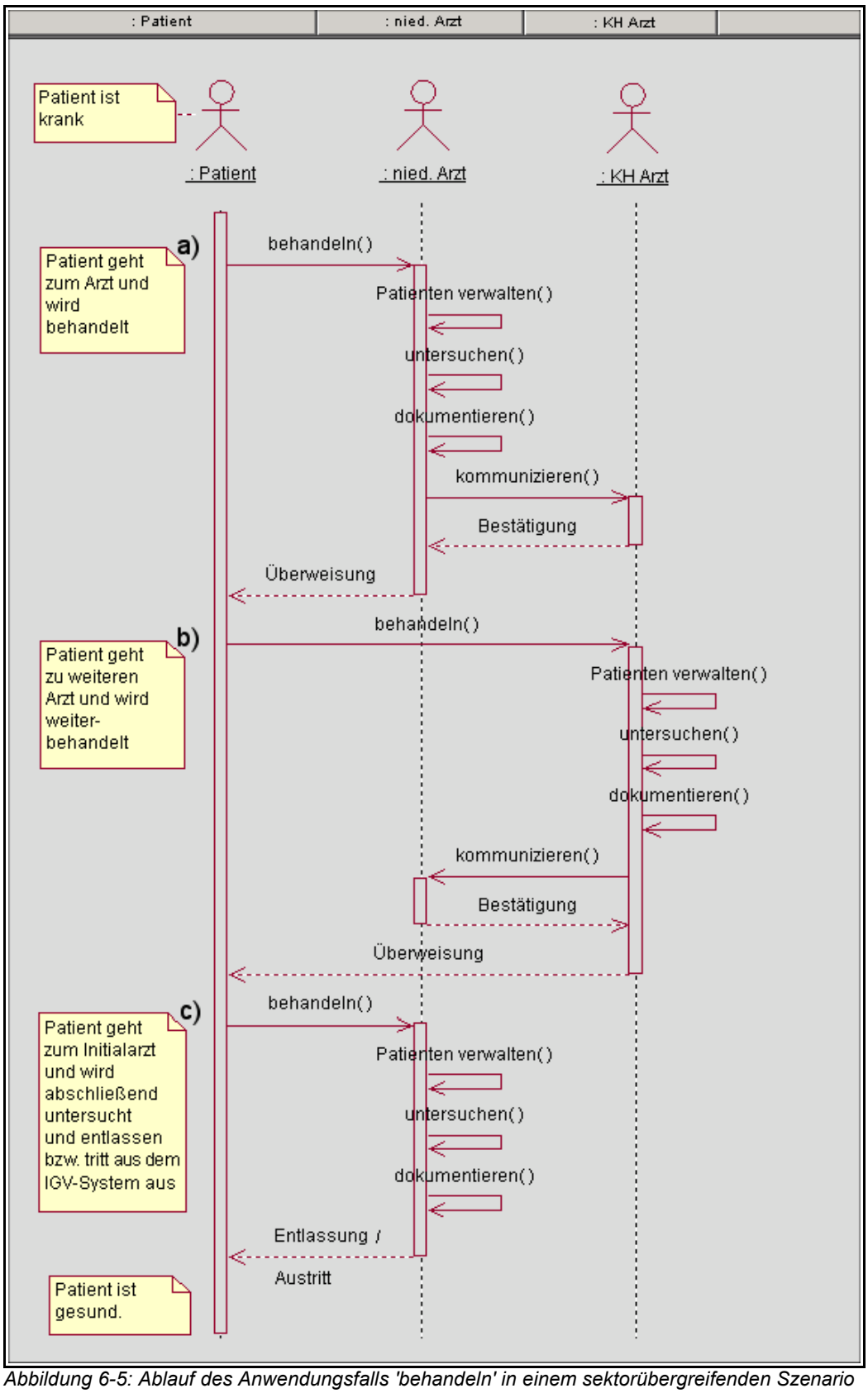

Abbildung 6-5: Ablauf des Anwendungsfalls 'behandeln' in einem sektorübergreifenden Szenario

Abschließend zum ersten Behandlungsschritt bekommt der Patient die Überweisung zum weiterbehandelnden Arzt. Im betrachteten Beispiel ist dies ein Arzt im Krankenhaus, z.B. für die Durchführung einer stationär-medizinischen Maßnahme (b). Mit der Überweisung geht der Patient zum weiterbehandelnden Arzt ins Krankenhaus und durchläuft die Stationen der Patientenbehandlung erneut. 'kommunizieren' ist in diesem Sequenzdiagramm noch

unspezifiziert und schließt sowohl die Standardmethode per Fax, Post und dergleichen als auch die computergestützte Kommunikation ein. Das hier beschriebene Szenario arbeitet mit Hilfe asynchroner Kommunikation. Das bedeutet, dass 'kommunizieren' auch ausgeführt werden kann, nachdem der Patient auf dem Weg zum weiterbehandelnden Arzt ist aber bevor er bei diesem ankommt. Der Patient kann natürlich die Unterlagen, soweit zu diesem Zeitpunkt schon vorhanden, auch persönlich zum weiterbehandelnden Arzt übertragen, was auch zur Standardmethode zählt und ebenfalls Nachteile, wie Medienbrüche, nach sich zieht.

Das in Abbildung 6-5 dargestellte Sequenzdiagramm modelliert den sektorübergreifenden Behandlungsfall in der Form, dass zunächst eine Behandlung in einer niedergelassenen Arztpraxis erfolgt, dann zur weiteren Behandlung an einen Arzt im Krankenhaus überwiesen wird. Abschließend erfolgt die Nachsorge beim Hausarzt (c). Dieser Behandlungspfad ist bei Hausarztmodellen der bevorzugte Weg. Weitere Sequenzdiagramme ließen sich anhand Abbildung 2-4 (medizinischer Versorgungskreislauf, Kapitel 2.4) konstruieren. Die einzelnen Stationen des Versorgungskreislaufes können dabei auch mehrfach durchlaufen werden, bis der Patient als gesund entlassen werden kann.

6.3.3 Kommunikationsprozess und neue Komponenten

Um die gesuchten Komponenten für die computergestützte Kommunikation zu identifizieren, wird nun auf Ergebnisse aus den Kapiteln 3 und 4 zurückgegriffen.

Durch die acht Schutzziele aus den gesetzlichen Anforderungen und die Diskussion der technischen Anforderungen, wurde für die sichere computergestützte Kommunikation das PaDok-Verfahren ermittelt. Weitere Punkte für diese Entscheidung gingen aus den ökonomischen Anforderungen hervor.

Das anforderungskonforme Kommunikationsverfahren PaDok basiert auf dem Client/Server Architekturstil. Dieser Architekturstil bietet die in Kapitel 4 vorgestellten Vorteile, wie z.B. die asynchrone Kommunikation, die sich positiv auf die laufenden Kosten für niedergelassene Ärzte auswirkt oder das Outsourcing der Serverkomponente. Diese Tatsachen wirken sich positiv auf die Betriebskosten aus, was besonders auf Seiten der niedergelassenen Ärzte zum Tragen kommt.

Mit der Analyse des Ist-Modells findet eine Berücksichtigung der vorhandenen Informationssysteme in beiden Bereichen statt. Im Ist-Modell sind die wesentlichen Informationssystemkomponenten aus stationären und niedergelassenen Bereich in einem 3LGM^2-Modell modelliert.

Aus den Anforderungen, den Verfahren und dem Ist-Modell lassen sich zwei weitere Komponenten identifizieren: Client und Server. Um zu verdeutlichen, wie KIS, PrIS, Client und Server zusammenarbeiten, kommt ein weiteres Sequenzdiagramm zum Einsatz.

Das zu beschreibende Verhalten zwischen KIS und PrIS, ist der Anwendungsfall aus Abbildung 6-4 'die computergestütze Kommunikation unterstützen'. Die dabei verwendeten Komponenten wurden durch den Architekturstil und die Kommunikationsverfahren bestimmt.

Während in Abbildung 6-5 der Ablauf eines sektorübergreifenden Behandlungsfalls gezeigt wird, ist in Abbildung 6-6 der Kommunikationsprozess „Senden einer Nachricht“ als Teilvorgang von 'kommunizieren' in Form eines Sequenzdiagramms dargestellt. Die Auswahl, Benennung und Abfolge der Nachrichtenpfeile erlaubt eine erste Vorstellung von der Interaktion der Komponenten.

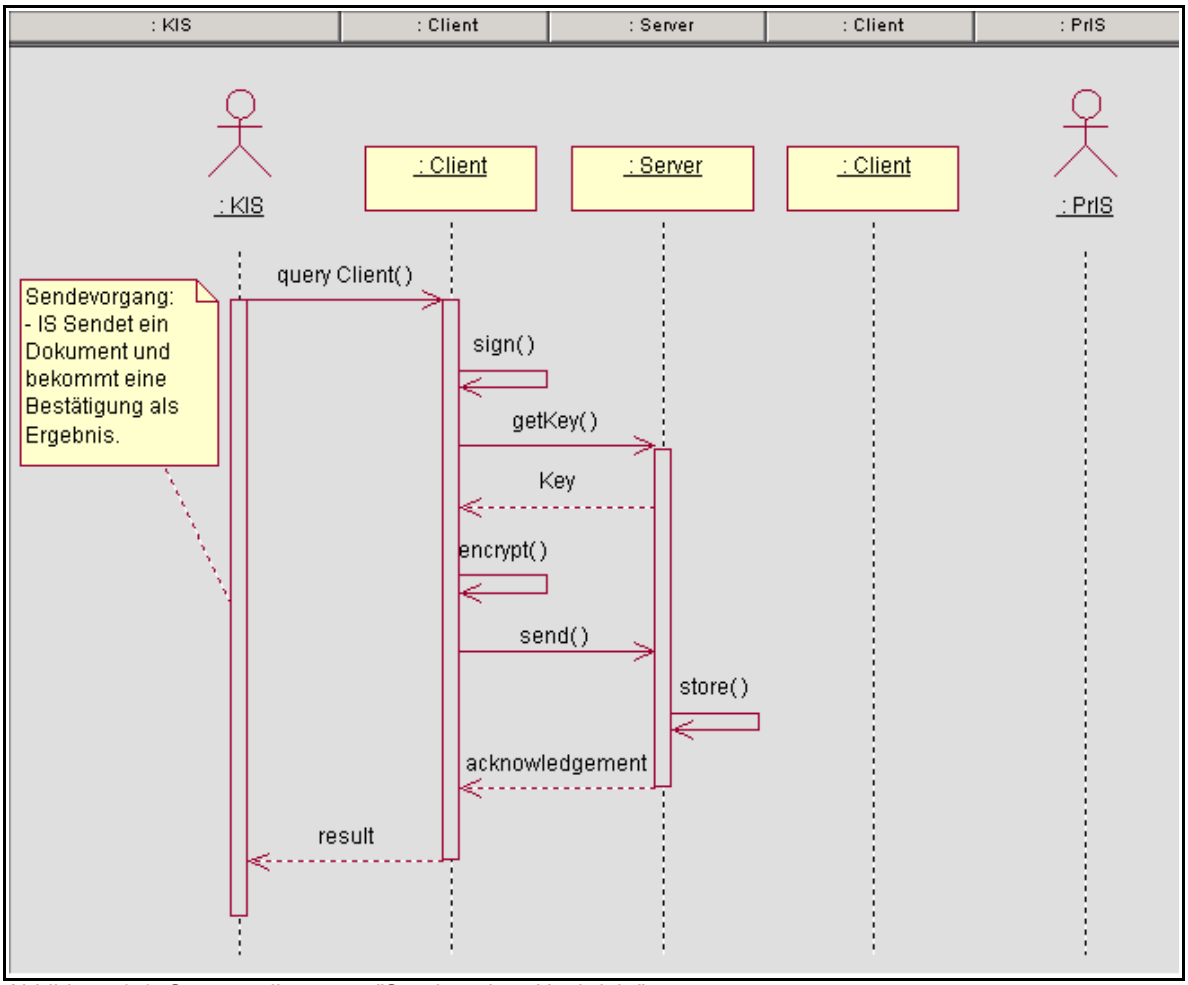

Abbildung 6-6: Sequenzdiagramm "Senden einer Nachricht"

Die hier dargestellte Sendevorgang geht in diesem Fall vom KIS aus. Die gleiche Abfolge an der Serverkomponente gespiegelt, kann jedoch auch vom PrIS ausgehen. Der Server fungiert nach dem Store-and-Forward-Prinzip als Speicher für die Nachrichten. Im Unterschied zum einfachen Nachrichtenspeicher gibt es hier jedoch weitere Funktionen, die durch die UML-Nachrichten *sign()*, *getKey()* und *encrypt()* repräsentiert sind und auf die beim verwendeten Verfahren getroffenen Sicherheitsmaßnahmen hindeuten. So werden alle Nachrichtenpakete an den Server signiert und für den oder die Empfänger verschlüsselt, sodass zu keinem Zeitpunkt Nachrichtenpakete im Klartext auf dem Server gespeichert sind. Die Kommunikation wird zusätzlich durch eine Transportverschlüsselung gesichert und jede Interaktion mit dem Server wird Protokolliert. Die in Abbildung 6-6 verwendeten Nachrichten sind nur grob skizziert und können mit Hilfe der Spezifikation [D2D2005] weiter verfeinert werden. Der verwendete Detailgrad soll lediglich zur Illustration der wesentlichen Ablaufschritte dienen.

In Abbildung 6-7 ist das Sequenzdiagramm vom Abruf einer bereitgestellten Nachricht zu sehen. Beim Abruf wird über den Client eine Anfrage an den Server (*queryClient()*, *queryServer()*) gestellt. Dieser liefert als Ergebnis das gewünschte Dokument (*result*). Der Client entschlüsselt die Nachricht (d*ecrypt()*), prüft die aufgeprägte Signatur (*checkSignature()*) und übergibt das Ergebnis dem PrIS.

Auch für dieses Sequenzdiagramm gilt, dass die UML-Nachrichten nur wesentliche Funktionen abbilden und der Nachrichtenabruf ebenfalls von der Gegenseite (KIS) ausgehen kann.

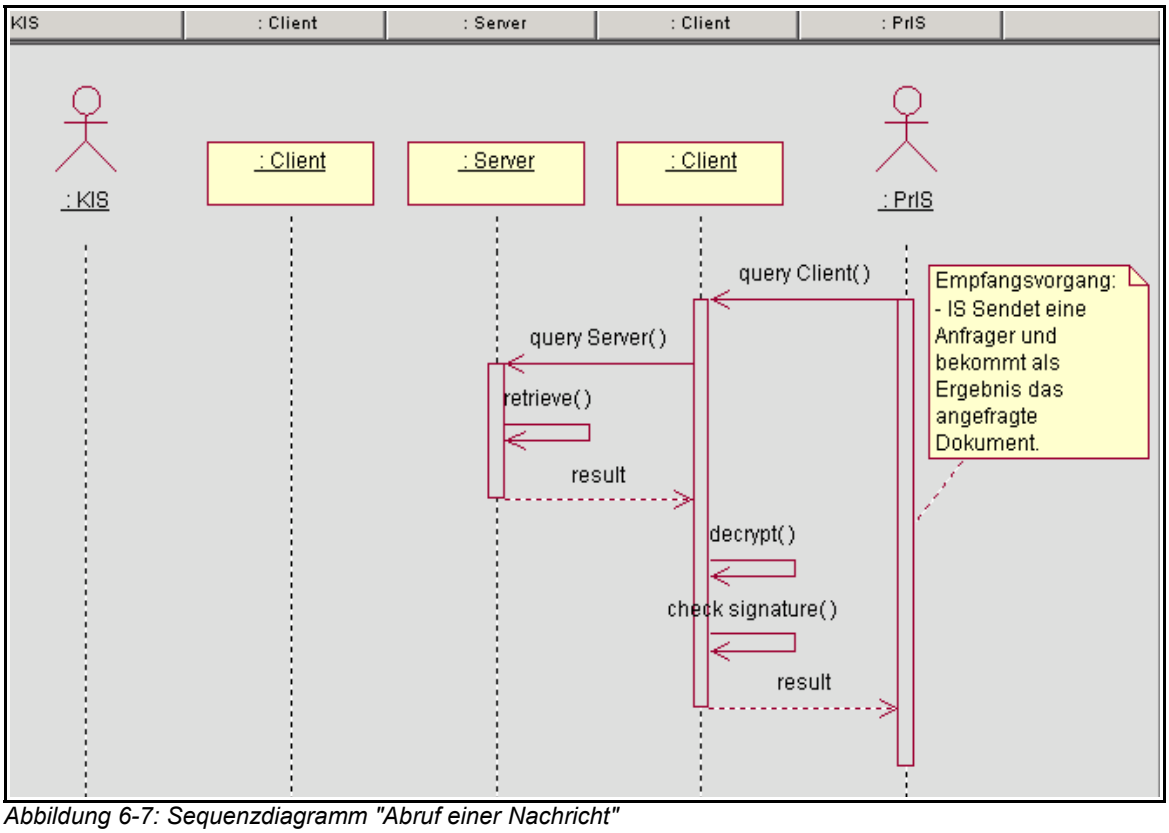

Abbildung 6-7: Sequenzdiagramm "Abruf einer Nachricht"

6.4 Integrationskomponente Adapter

Der Nachrichtenaustausch zwischen Client und Server ist in der Spezifikation des PaDok-Verfahrens definiert. Der Client stellt die Schnittstelle zum Server dar. Um sinnvoll mit dem Verfahren arbeiten zu können, ist eine Integration dieser Schnittstelle in das vorhandene Informationssystem notwendig. Abbildung 6-8 verdeutlicht das Problem der Integration des Clients in die vorhandenen Informationssyteme. Das Problem besteht auf sowohl auf Seiten des KIS als auch auf Seiten des PrIS.

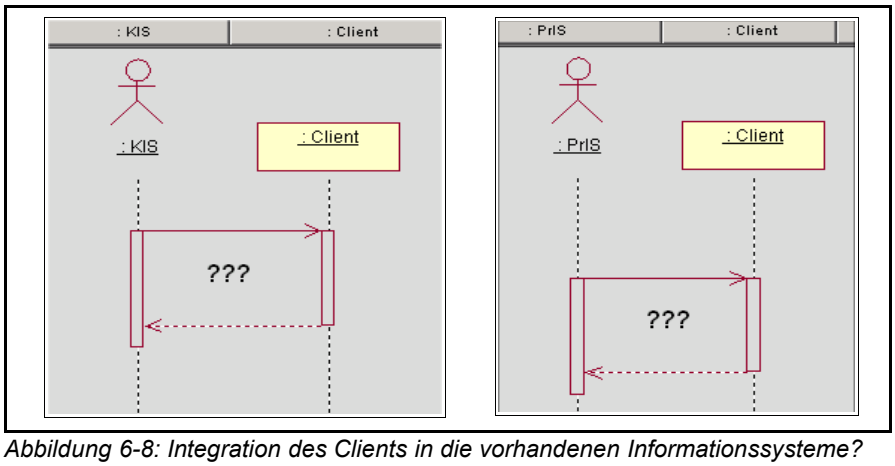

Abbildung 6-8: Integration des Clients in die vorhandenen Informationssysteme?

Eine Lösung der Integrationsanforderungen wäre die Integration des Clients oder die Implementierung einer Schnittstelle zum Client in die vorhandenen Informationssysteme.

Die derzeitige Situation im niedergelassenen Bereich ist diesbezüglich so, dass die Hersteller der Praxissoftware konservativ mit der Implementierung neuer Kommunikationsmöglichkeiten umgehen und weiterhin auf die etablierte BDT-Schnittstelle setzen. Andererseits sind die niedergelassenen Ärzte nicht bereit die hohen Investitionskosten einer integrierten Lösung zu tragen oder sich die Praxissoftwarelösung eines Herstellers vorschreiben zu lassen. Diese Situation hat eine Nische für Softwarehersteller im Gesundheitswesen geschaffen, die eine Schnittstelle zwischen Client und vorhandenem Praxisinformationssystem anbieten und so die Integrationsanforderungen erfüllen [GMCHP]. Die gesuchte Schnittstelle zwischen Client und Zielsystem wird unter der Komponentenbezeichnung Adapter eingeführt.

Im stationären Bereich gibt es ebenfalls noch keine Lösung, die einen Client integriert oder eine Schnittstelle zum Client bereitstellt. Die im klinischen Sektor weit verbreitete Kommunikationsserverarchitektur könnte hier einen möglicher Ansatzpunkt für eine Integration sein. Vorstellbar ist auch der Einsatz eines Adapters am klinischen Arbeitsplatz, welcher das Bindeglied zwischen KIS und Client darstellt. Dieser Adapter könnte auch vorhandene Schnittstellen des Kommunikationsservers bedienen und die Integration auf diesem Wege unterstützen.

Wie eine Integrationslösung im Einzelfall auch aussehen mag, so lässt sich eine Lösung des Integrationsproblems für das Referenzmodell mit dem Einsatz des Adapters modellieren. Die Funktionen, die der Adapter dabei im Rahmen der Integrationsanforderungen leisten muss, gelten für stationären wie für niedergelassenen Bereich. Der Adapter muss folgende Fähigkeiten besitzen:

- Bedienung der Clientschnittstelle
- Bereitstellen von Schnittstellen zum verwendeten Informationssystem (KIS, PrIS)
- Zuordnung von abgerufenen Nachrichten (Mapping)
- Konvertieren von Nachrichten

Bei der Bereitstellung von Schnittstellen zum jeweiligen Informationssystem sollte der Adapter im niedergelassenen Bereich die BDT-Schnittstelle unterstützen. Im stationären Bereich ist in Verbindung mit einem Kommunikationsserver die Unterstützung der HL7-Schnittstelle sinnvoll.

Die Zuordnung von abgerufenen Nachrichten stellt durch das Fehlen eines einrichtungsübergreifenden Master Patient Index ein großes Problem dar. Hier kann vorerst nur eine Zuordnung über die Patientenstammdaten erfolgen. Dazu muss der Adapter Zugriff auf die Patientenstammdaten des Informationssystem haben. Während im niedergelassenen Bereich eine manuelle Zuordnung der Patienten zu den abgerufenen Nachrichten denkbar ist, muss im stationären Bereich zumindest eine Vorsortierung bezüglich der in Frage kommenden Fachgruppe (HPG) stattfinden.

Für den einrichtungsübergreifenden Austausch medizinischer Daten bieten sich die im Grundlagenkapitel vorgestellten CDA-Dokumente an. Abbildung E-2 (Anhang E, Seite 31) zeigt beispielhaft die Verarbeitung eines CDA-Dokuments beim Versenden anhand eines Zustandübergangsdiagramms. Die strukturierten CDA-Dokumente kann der Adapter direkt an das Zielsystem weiterleiten, falls dieses eine entsprechende Unterstützung bietet. Andernfalls ist eine Konvertierung der CDA-Dokumente aufgrund der strukturiert gespeicherten Informationen in ein Format, dass vom Zielsystem verarbeitet werden kann, möglich. Eine Konvertierung in das HL7-Format Version 3 ist bei CDA-Dokumenten durch das beiden Formaten zu Grunde liegende

RIM gesichert, siehe Kapitel 2.2.3. Eine Konvertierung zu HL7 Version 2 und BDT ist aufgrund semantischer Inkompatibilitäten mit Abstrichen möglich.

Die Sequenzdiagramme in Abbildung 6-9 und Abbildung 6-10 zeigen nun, wie der Kommunikationsprozess mit Adapter abläuft.

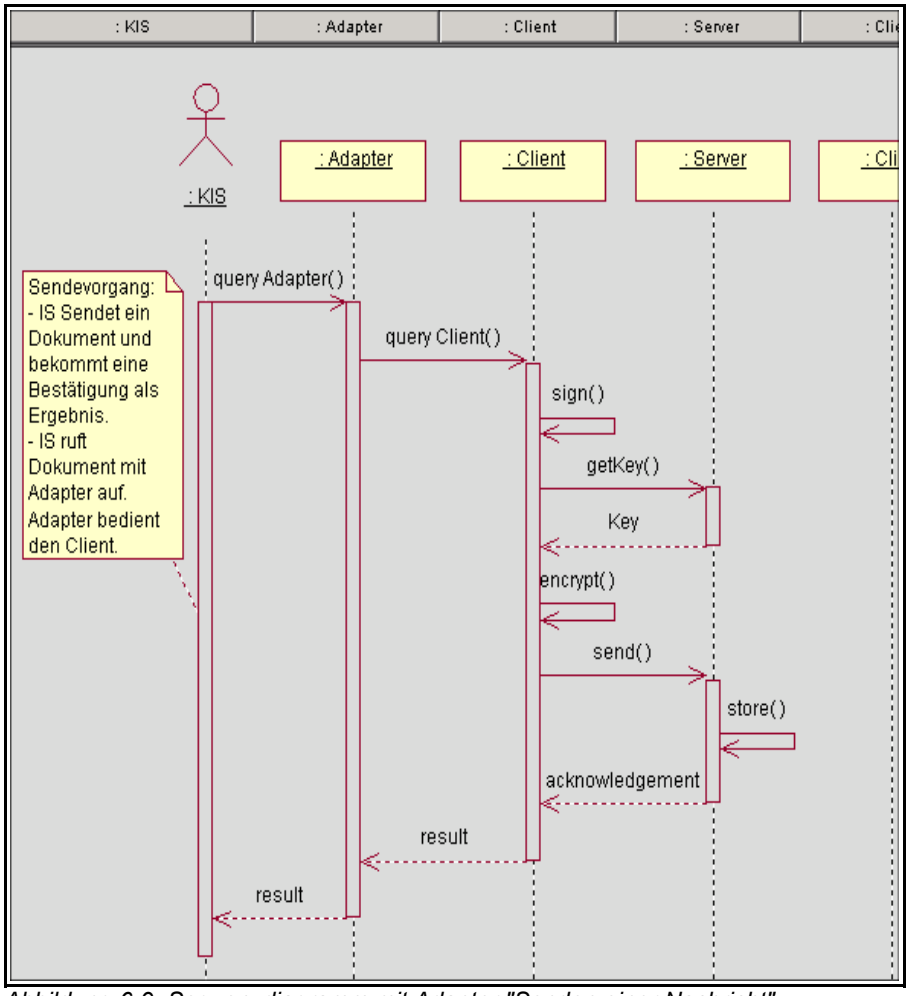

Abbildung 6-9: Sequenzdiagramm mit Adapter "Senden einer Nachricht"

In *queryAdapter()* und *queryClient()* Abbildung 6-9 stecken die oben Beschriebenen Fähigkeiten des Adapters, die eine Integration des Client in das KIS bzw. PrIS leisten sollen.

Ein ähnliches Sequenzdiagramm lässt sich nun für den Abruf der Nachrichten vom Server erstellen Abbildung 6-10 (Seite 91).

Im Gegensatz zum Sendevorgang hat der Adapter beim Empfang von Nachrichten zusätzliche Probleme zu lösen. Die empfangene Nachricht muss für das Zielsystem aufbereitet (*konvert_result()*) und einem Patienten zugeordnet werden. Diese Zuordnung von Nachricht und Patient wird durch die selbst delegierte UML-Nachricht *map_result()* modelliert. Dieses Mapping kann manuell durch die Präsentation von Auswahllisten oder halbautomatisch durch eingeschränkte Auswahllisten realisiert sein. Ein vollautomatisches Verfahren wird an dieser Stelle wohl erst Einzug halten können, wenn ein bisher fehlender eindeutiger Identifikator für einen Patienten in Form eines Master Patient Index eingeführt wird. Bis dahin wird die fehlerbehaftete Identifikation der Patienten über die Patientenstammdaten benutzt und mit einer manuell durch den Arzt durchgeführten Zuordnung umgesetzt.

Mit den beiden Informationssystemen KIS und PrIS, dem Adapter, Client und Server sind nun alle wesentlichen Komponenten für eine sektorübergreifende Kommunikation identifiziert. Mit diesen Erkenntnissen kann nun zur 3LGM²-Modellierung übergegangen werden.

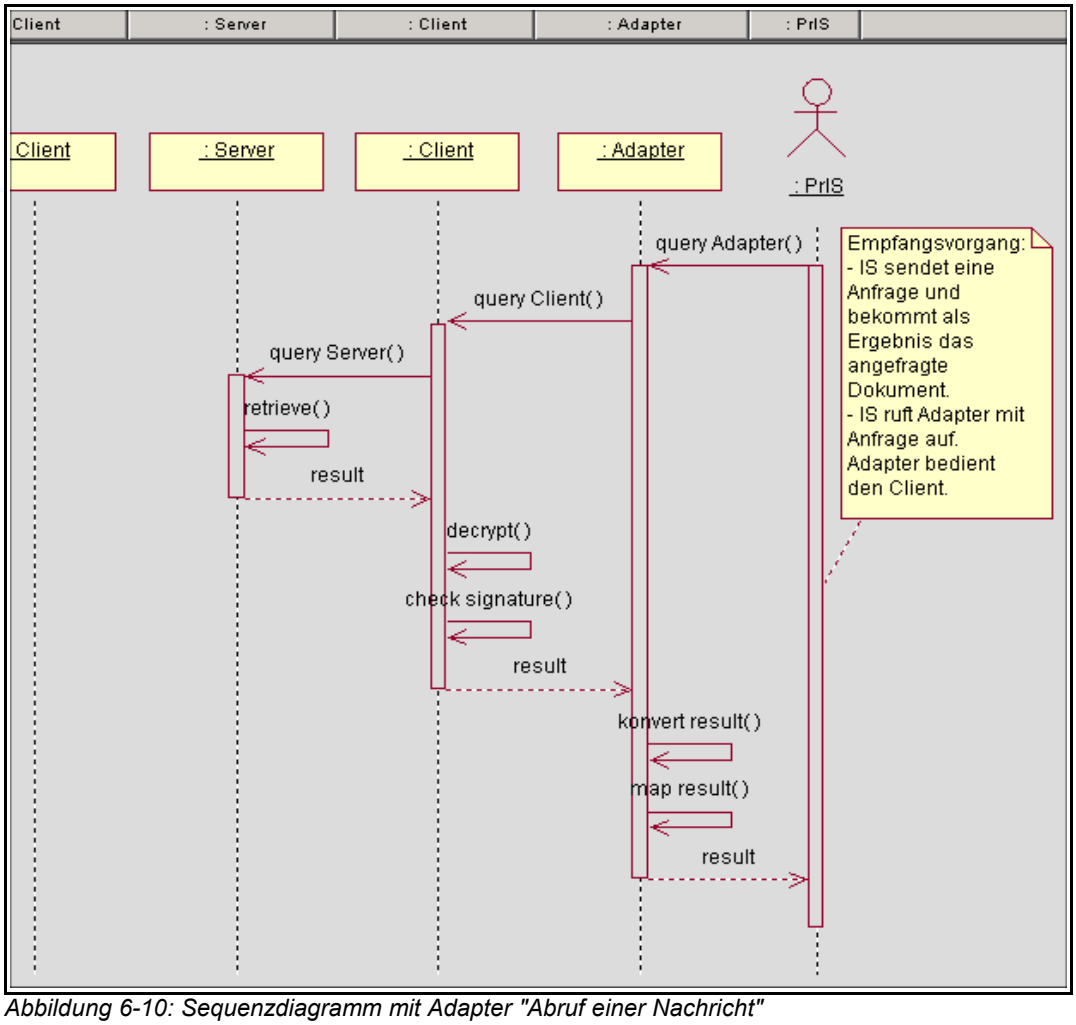

Abbildung 6-10: Sequenzdiagramm mit Adapter "Abruf einer Nachricht"

6.5 3LGM²-Referenzmodell

Das in Kapitel 5.1.4 erstellte Ist-Modell dient als Basis für die Modellierung des 3LGM²-Referenzmodells. Die im Ist-Modell modellierten Aufgaben, Objekttypen, Anwendungsbausteine, physischen Datenverarbeitungsbausteine und Prozesse werden unverändert in das Referenzmodell übernommen und finden als Übergangs- bzw. Ausfallkonzept Verwendung. In den folgenden Abschnitten werden die Ebenen und Interebenenbeziehungen des 3LGM²-Referenzmodells vorgestellt.

6.5.1 Fachliche Ebene

Auf der fachlichen Ebene sind gegenüber dem Ist-Modell im Wesentlichen zwei Modifikationen zu verzeichnen.

Es wird ein neuer Objekttyp eingeführt: 'computerbasierter Auszug der Patientengeschichte'. Dieser leitet sich wie sein papierbasiertes Gegenstück 'konventioneller Auszug der Patientengeschichte' vom Objekttyp 'Patientengeschichte' ab und kann damit sämtliche Objekttypen der Patientengeschichte (Abbildung D-1 Anhang D, [UMIT2005]) enthalten. Repräsentiert wird er durch ein CDA-Dokument.

Die zweite Modifikation widmet sich der Problematik des fehlenden Master Patient Index und der dadurch notwendig werdenden Aufgabe der Zuordnung von ausgetauschten Dokumenten und im Informationssystem angelegten Patienten. Im Modell wird dem begegnet, indem eine neue Aufgabe 'Dokumenten-Mapping' und der Objekttyp 'Patientenstamminformationen' eingeführt wird. Der Objekttyp 'Patientenstamminformationen' ist virtuell und beinhaltet die für die Aufgabe 'Dokumenten-Mapping' benötigten Informationen, d.h. Patientenstammdaten aus den Informationssystemen und aus dem Header des CDA-Dokuments.

Abbildung 6-11 zeigt die fachliche Ebene des 3LGM²-Referenzmodells.

Abbildung 6-11: Fachliche Ebene 3LGM²-Referenzmodell

Zurückblickend auf das Use Case Diagramm in Abbildung 6-2 lassen sich die Anwendungsfälle 'behandeln' und 'Patienten verwalten' als 'Patientenbehandlung' bzw. 'Patientenadministration' im

3LGM²-Referenzmodell wiederfinden. Diese beiden Aufgaben leiten sich aus der Aufgabe 'Patientenbehandlung' ab, siehe „Referenzmodell der fachlichen Ebene“ [UMIT2005] - angepasst 'Aufgaben der Patientenbehandlung' Abbildung D-2 Anhang D. Alle anderen Anwendungsfälle werden bei der 3LGM²-Modellierung als inhärent angesehen und werden durch die Beziehungen zwischen Aufgaben und Objekttypen abgedeckt.

6.5.2 Logische Werkzeugebene

Zur logischen Ebene des 3LGM² Ist-Modells kommen nun weitere Komponenten hinzu, die in Kapitel 6.3 (Client, Server) und 6.4 (Adapter) identifiziert wurden. In Abbildung 6-12 (Seite 94) ist die logische Ebene des 3LGM²-Referenzmodells zu sehen.

Als zentrale Komponente für den Nachrichtenaustausch wird der Anwendungsbaustein 'IV Kommunikationssystem' eingeführt. Dieser ist eine Art Black-Box zur Abwicklung der Kommunikation über das PaDok-Verfahren. Lediglich bekannte Komponenten wie Server, Datenbank und Verzeichnisdienst sind angedeutet. Über die Bausteinschnittstelle des 'IV Kommunikationssystem' Abbildung 6-12 (a) kommunizieren nun die 'Schnittstellenbausteine (Client)' (b, c) und stellen den Verbindungspunkt zwischen KIS bzw. PrIS und 'IV Kommunikationssystem' dar. Als Integrationskomponente ist der Anwendungsbaustein 'Adapter' (d, e) modelliert. Er bietet sowohl Bausteinschnittstellen zum PaDok-Client als auch zum 'Kommunikationsserver' bzw. zum 'Patientenverwaltungssystem Praxis'.

6.5.3 Physische Werkzeugebene

Die physische Ebene des 3LGM²-Referenzmodells wurde gegenüber dem Ist-Modell in punkto Netzwerkkomponenten (gelb dargestellt) erweitert. Sie ist in Abbildung 6-13 (Seite 95) dargestellt. Durch die Einführung von 'Medizin Netzwerk' und 'VPN Gateway' eines Medizin Netz Providers sind die Router und damit die Netzwerke der beteiligten physischen Datenverarbeitungsbausteine miteinander verbunden. Dies ist die Grundlage für den Nachrichtenaustausch auf der logischen Werkzeugebene. Das 'VPN Gateway' beim Medizin Netz Provider stellt den transportgesicherten Zugang zum 'Datenaustausch Server' des 'IV Kommunikationssystem' (PaDok-Server) über eine lokal verfügbare Zugangstechnik (ISDN, DSL, UMTS etc.) her.

Die Router, die bereits im Ist-Modell vorhanden waren, wurden bisher, wenn überhaupt vorhanden, für den Internetzugang genutzt. Es bleibt im Einzelfall zu prüfen, ob bei diesen Geräten alle Voraussetzungen für eine VPN-Einwahl gegeben sind. Bei der Modellierung wird von Routern mit entsprechenden Fähigkeiten ausgegangen.

Das 'Intranet IV Kommunikationssystem' ist wie auf der logischen Werkzeugebene nur so dargestellt, wie es der Spezifikation [D2D2005] zu entnehmen ist. Für die Modellierung und das Verständnis der Kommunikationsvorgänge ist dies jedoch ausreichend und die Serverkomponenten können als Black-Box angesehen werden.

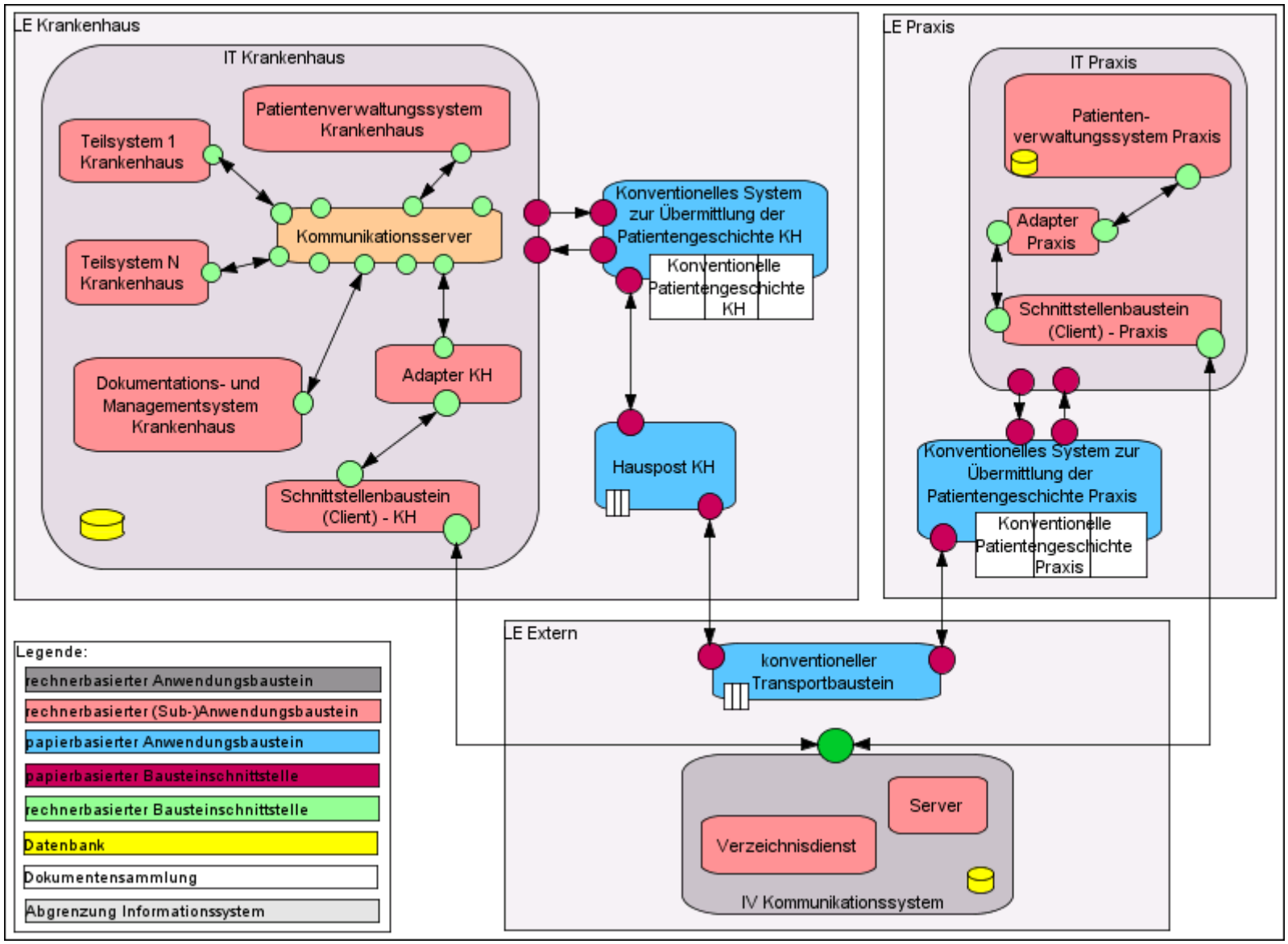

Abbildung 6-12: Logische Ebene des 3LGM2-Referenzmodells

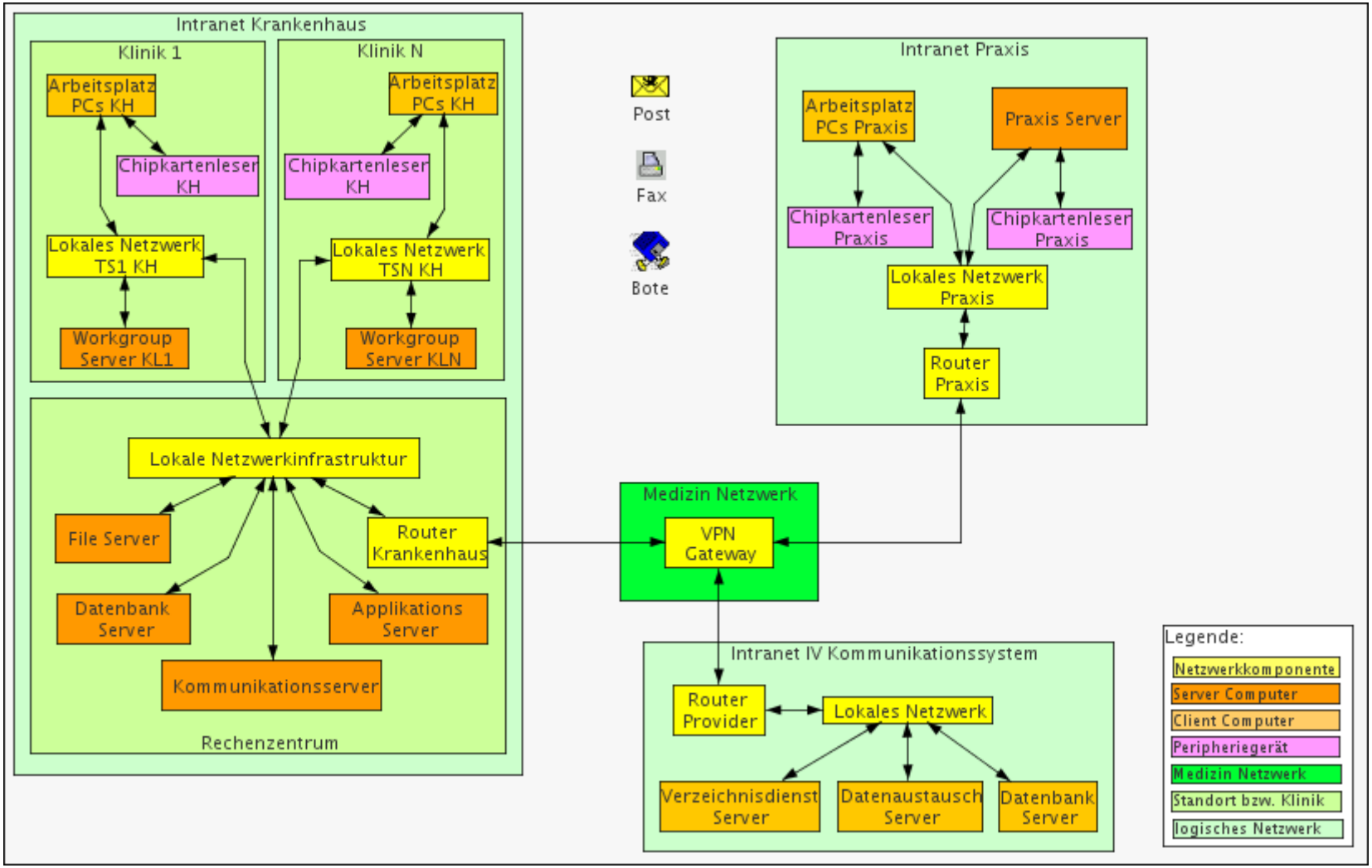

Abbildung 6-13: Physische Ebene des 3LGM2-Referenzmodells

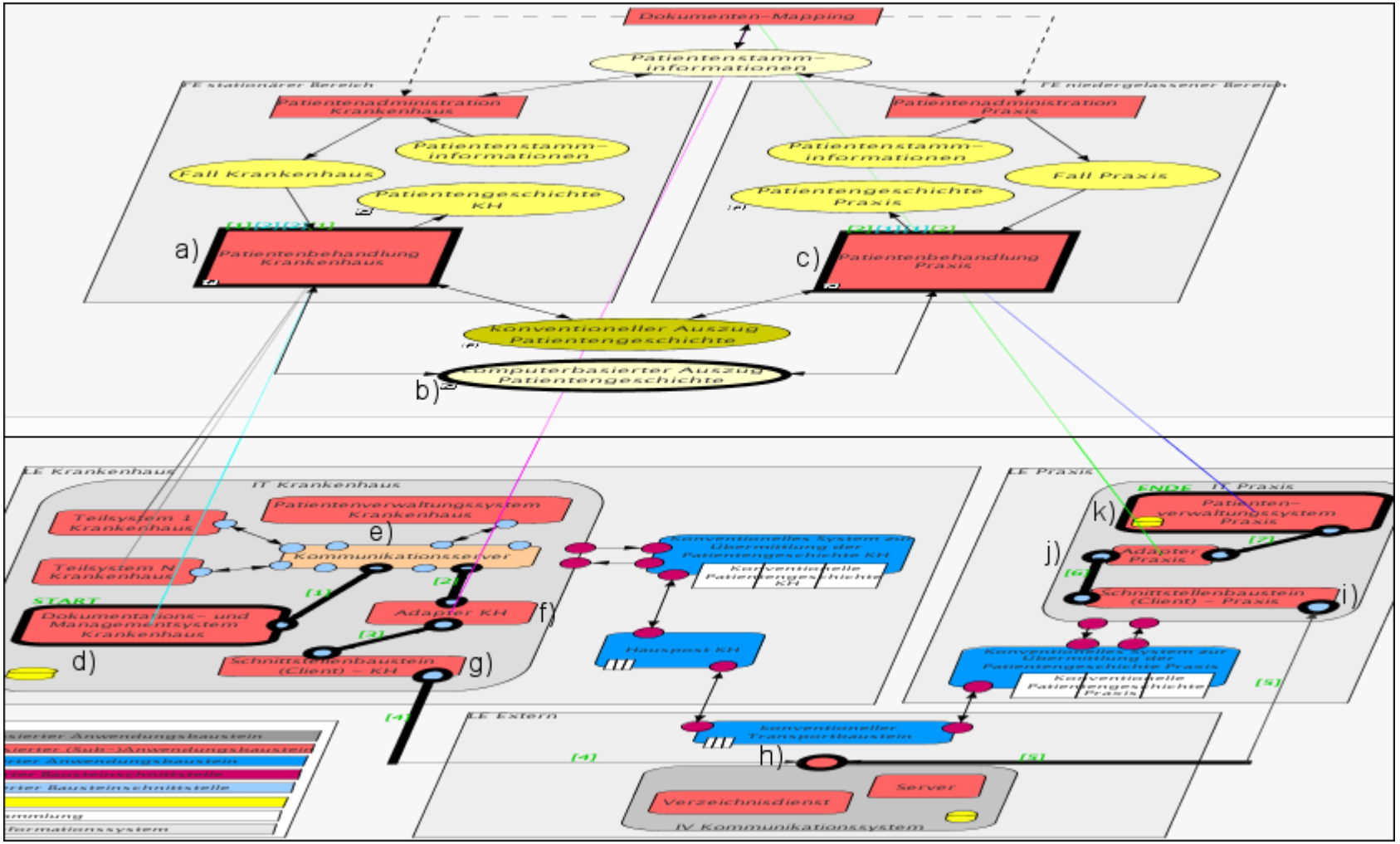

Abbildung 6-14: Interebenenbeziehungen und computerbasierter Kommunikationsprozess des 3LGM2-Referenzmodells

6.5.4 Interebenenbeziehungen und computerbasierter Kommunikationsprozess

Die in Abbildung 6-14 (Seite 96) dargestellten Interebenenbeziehungen zeigen ausgewählte Beziehungen zwischen den am modellierten Kommunikationsprozess beteiligten Aufgaben der fachlichen Ebene und den korrespondierenden Anwendungsbausteinen der logischen Werkzeugebene (a↔d bzw. c↔k). Die am Kommunikationsprozess beteiligten Komponenten sind fett hervorgehoben und mit kleinen Buchstaben versehen.

Der computerbasierte Kommunikationsprozess wird von der Aufgabe 'Patientenbehandlung Krankenhaus' initiiert (a). Auf der fachlichen Ebene drückt sich der Prozess durch die gemeinsame Bearbeitung/Interpretation des Objekttyps 'computerbasierter Auszug der Patientengeschichte' (b) durch 'Patientenbehandlung Krankenhaus' (a) und 'Patientenbehandlung Praxis' (c) aus.

Auf der logischen Werkzeugebene setzt sich der Kommunikationsprozess im Krankenhaus über die Anwendungsbausteine d→e→f→g fort. Dabei sorgen 'Kommunikationsserver' (e) und 'Adapter' (f) für die Anbindung der Schnittstellen und die Konvertierung der zu versendenden Nachricht. Die auf diesem Wege vorbereitete Nachricht kann nun vom 'Schnittstellenbaustein (Client)' (g) nach dem PaDok-Verfahren signiert, verschlüsselt und an den PaDok-'Server' (h)gesendet werden. Dieser Prozessabschnitt bildet den im Sequenzdiagramm Abbildung 6-9 (Seite 90) modellierten Kommunikationsprozess „Senden einer Nachricht“ mit den Möglichkeiten des 3LGM²-Metamodells ab. Der im Sequenzdiagramm Abbildung 6-10 (Seite 91) dargestellte „Abruf einer Nachricht“ wird durch Beziehungen der Anwendungsbausteine k→j→i→h im 3LGM²-Referenzmodell nachempfunden.

6.6 Spezielle Modelle

Die Benutzung des Referenzmodells, d.h. die Ableitung spezieller Modelle, lässt sich durch eine Instantiierung der Modellkomponenten erreichen. In den UML-Sequenzdiagrammen sind die Objekte in Form von Klassen modelliert (z.B. ':KIS'). Diese können für ein spezielles Modell instantiiert werden (z.B. 'Uni-Klinikum_Musterstadt:KIS'). Ähnlich verhält es sich mit den im 3LGM²-Modell verwendeten Komponenten. Es können bspw. aus den 'Teilkliniken 1-N' des Referenz-Krankenhauses auf der logischen Ebene konkrete Kliniken, wie z.B. eine Radiologie, modelliert werden. Ebenso ist im Referenzmodell offen, welche Softwarelösung für ein 'Patientenverwaltungssystem im Krankenhaus' bzw. in der Praxis oder welches 'Dokumentations- und Managementsystem' im Krankenhaus eingesetzt wird. In einem aus dem Referenzmodell abgeleiteten speziellen Modell werden diese Modellkomponenten auf die existierenden Installationen festgelegt.

Es ist weiterhin Möglich über die Serverkomponente eine Vielzahl von Kliniken und Arztpraxen anzubinden. Dies kann z.B. durch die Vervielfachung der Arztpraxiskomponenten auf der logischen und physischen Ebene unterstützt werden. Ein Beispielszenario für die logische Ebene zeigt Abbildung 6-15 auf der folgenden Seite. Dort sind ausschließlich computerbasierte Anwendungsbausteine dargestellt. Die konventionellen Anwendungsbausteine sind aufgrund einer besseren Übersichtlichkeit ausgeblendet. Das Szenario ist typisch für die Vernetzung von Arztpraxen und Krankenhaus mit Hilfe des PaDok-Verfahren bzw. seiner Implementierung D2D.

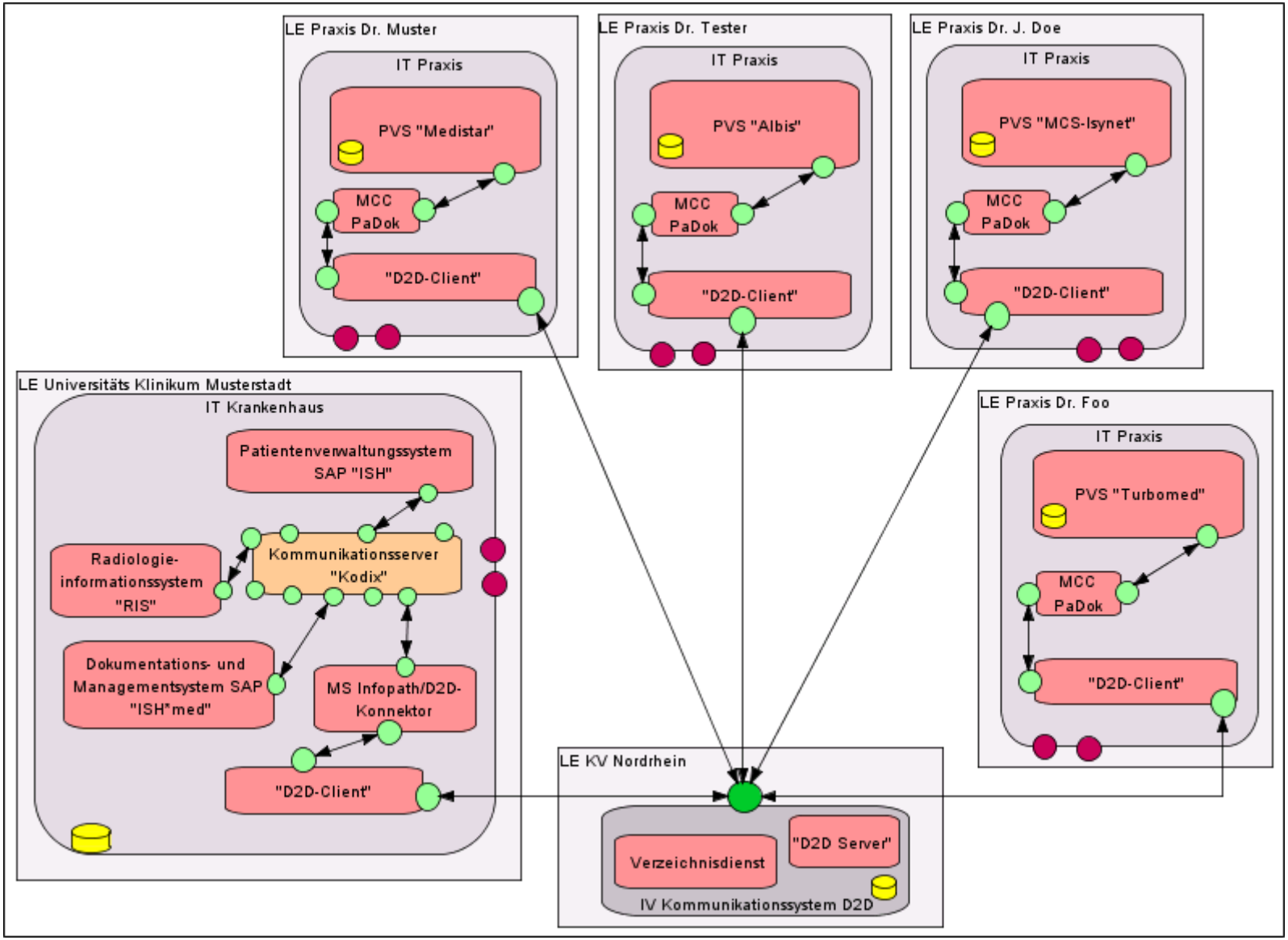

Abbildung 6-15: Beispielszenario für die logische Werkzeugebene. Dargestellt ist die Anbindung von einem Klinikum und vier Arztpaxen per D2D.

Bei der Erstellung der konkreten Modell ist darauf zu achten, dass die Kernelemente des 3LGM²-Referenzmodells für die sektorübergreifende Kommunikation in das abzuleitende Modell übernommen werden. Die Kernelemente definieren die Klasse der Sachverhalte, d.h. die zentralen Komponenten der Kommunikationsarchitektur, siehe Kapitel 2.5.1 „Definition Referenzmodell“. Abbildung 6-16 zeigt die Kernelemente der logischen Werkzeugebene. Dazu gehören: der Betreiber des Servers und der dazugehörenden Infrastruktur, d.h. Datenbank und Verzeichnisdienst, ein Schnittstellenbaustein und ein Adapter. Über die 3LGM2-Referenzmodell gespeicherten Interebenenbeziehungen lassen sich weitere Kernelemente auf der fachlichen Ebene und der physischen Werkzeugebene finden.

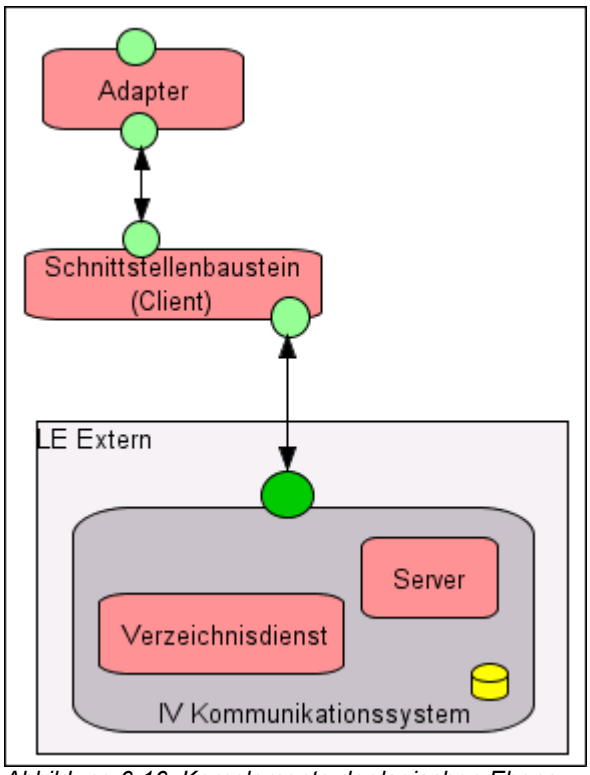

Abbildung 6-16: Kernelemente der logischen Ebene

6.7 Abschlussbetrachtungen zum Referenzmodell

Die Herleitung des 3LGM²-Referenzmodells über Use Case und Sequenzdiagramme bietet viele Vorteile. Zum einen wird durch die Erstellung der Use Case Diagramme die Modellierung der fachlichen Ebene des 3LGM²-Modells vorbereitet. Zum anderen bieten Use Case Diagramme zusätzliche Aspekte indem sie die an den Aufgaben beteiligten Aktoren berücksichtigen. Aufgaben und Aktoren werden direkt in Beziehung gestellt. Beim 3LGM²-Modell sind die Aktoren ebenfalls vorhanden, sie sind jedoch aufgrund der Modellspezifikation auf logische und physische Ebene verteilt. Eine Beziehung zwischen beiden Komponenten ist über die Interebenenbeziehungen realisiert.

Ein weiterer Vorteil der Berücksichtigung zusätzlicher Diagramme ist die erleichterte Identifikation von Modellkomponenten. Mit Hilfe von Sequenzdiagrammen lassen sich Prozessabläufe und Kommunikationsvorgänge in einer übersichtlichen Form darstellen. Eine

schrittweise Verfeinerung der Vorgänge ist durch das Hinzufügen weiterer Komponenten möglich. Auf diese Weise wird ein vorerst grob skizzierter Vorgang bis zum gewünschten Detailgrad präzisiert und wesentliche Modellkomponenten identifiziert. Die Prozessmodellierung mit dem 3LGM²-Metamodell setzt eine genaue Kenntnis der zu modellierenden Prozessabläufe und ihrer beteiligten Prozesselemente voraus. UML-Sequenzdiagramme bieten hier eine Unterstützung beim Verständnis und bei der Modellierung von Kommunikationsprozessen.

Das in diesem Kapitel vorgestellte Referenzmodell wurde auf diese Weise schrittweise erstellt. Die beteiligten Komponenten finden sich daher sowohl in Use Case und Sequenzdiagrammen als auch im 3LGM²-Referenzmodell wieder und beschreiben die selben Kommunikationsprozesse. Alle Sichten sind für ein umfassendes Verständnis von Bedeutung. Use Case Diagramme mit ihrer auf die Anwendungsfälle zentrierten Sicht, stellen die Unternehmensaufgaben in Beziehung mit ihren Aktoren dar. Die Stärke der Sequenzdiagramme liegt in der zeitlichen Auflösung der interagierenden Komponenten und der Hervorhebung wichtiger Prozessabläufe und Funktionsaufrufe, wie dem Signieren oder Verschlüsseln der Nachrichten. Die Vorteile der 3LGM²-Modellierung liegen in der Verknüpfungen aller Teilaspekte. Von den Aufgaben der fachlichen Ebene über die Anwendungsbausteinen der logischen Werkzeugebene werden durch Interebenenbeziehungen die erfassten Sachverhalte abgebildet. Durch die grafischen Darstellung des Kommunikationspfades über die involvierten Anwendungsbausteine, Bausteinschnittstellen und deren Kommunikationsbeziehungen werden Kommunikationsvorgänge ebenenübergreifend darstellbar. Über die Interebenenbeziehungen zwischen logischer und physischer Werkzeugebene wird der Zusammenhang zwischen Anwendungsbausteinen und physischen Datenverarbeitungsbausteinen hergestellt.

7 Schlussbetrachtung und Diskussion

7.1 Erfüllung der Zielsetzung und Diskussion

Im Folgenden werden die in Kapitel 1.3 formulierten Ziele auf ihre Erfüllung untersucht. Es wird weiterhin überprüft, inwiefern die in Kapitel 1.2 festgestellten Probleme gelöst werden konnten.

Problem 1:

> *Es gibt eine Vielzahl von Anforderungen an die sektorübergreifende Kommunikation. Diese komplexen Anforderungen sind bisher noch nicht umfassend katalogisiert. Es fehlt eine Übersicht der Gesetzeslage und der Technologiesituation.*

Aus diesem Problem leitete sich Ziel 1 ab: Die Erstellung eines Anforderungskataloges auf dessen Basis eine Entscheidung für den Einsatz eines geeigneten Verfahren getroffen werden kann. Dabei sollte die Gesetzeslage und technische Anforderungen herausgearbeitet werden.

Die Erstellung des Anforderungskatalogs ist Gegenstand von Kapitel 3. Dort werden in drei Abschnitten die gesetzlichen, technischen und ökonomischen Anforderungen erarbeitet und am Ende jedes Abschnittes zusammengefasst. In Kapitel 3.1 werden umfassend die gesetzlichen Rahmenbedingungen dargelegt, die bei der sektorübergreifenden elektronischen Kommunikation gelten. Am Ende dieses Abschnittes steht Tabelle 3-2 (Seite 37) bereit. Sie enthält eine detaillierte Übersicht der Gesetzeslage. Aus ihr leiten sich die in Kapitel 3.4 Tabelle 3-9 (Seite 48) dargelegten gesetzlichen Anforderungen ab. Diese auf die wesentlichen Anforderungen komprimierte Tabelle beinhalten zu einem großen Teil datenschutzrechtliche Vorgaben aber unter anderem auch die Anforderungen nach Aufklärung der Patienten und der freien Arztwahl. Die gesetzlichen Anforderungen werden in Kapitel 5.3 als K.O.-Kriterien für die Auswahl der Verfahren genutzt.

Kapitel 3.2 beschäftigt sich mit den technischen Anforderungen. Diese gliedern sich in die funktionalen Anforderungen der Nutzer und die technischen Rahmenbedingungen, welche an Hardware und Software gestellt werden. Im Ergebnis steht in Kapitel 3.2.3 eine Übersicht der technischen Anforderungen bereit.

Die finanziellen Ressourcen des deutschen Gesundheitswesen sind begrenzt. Sie sind zudem Motivation für eine verbesserte sektorübergreifende Kommunikation. Dadurch wird die Einsparung von Kosten, wie sie z.B. durch Medienbrüche entstehen, erhofft. In Kapitel 3.3 werden deshalb zusätzlich ökonomische Anforderungen aufgestellt. Diese sollen als Richtlinie für einen effizienten Umgang mit den begrenzten finanziellen Ressourcen verstanden werden.

In Kapitel 3.4 steht schließlich der Katalog der gesetzlichen, technischen und ökonomischen Anforderungen bereit. Aus dem Katalog wurden die zur Bewertung der Verfahren in Kapitel 5.3 benötigten Kriterien abgeleitet.

Problem 2:

> *Es fehlt weiterhin ein Katalog von Produkten und Verfahren, die sich zur Erstellung der benötigten Kommunikationsarchitekturen eignen. In diesem Katalog müssten außerdem Verweise zu den jeweils zu beachtenden Anforderungen im Anforderungskatalog bzw. Hinweise, Funktionen und Einschränkungen verfügbar sein. Bei der Vorauswahl der Produkte und Verfahren widmet sich diese Arbeit der Frage, wie zwischen stationären und niedergelassener Bereich medizinische Daten ausgetauscht werden können, um dem Ziel Integrierte Versorgung näher zu kommen.*

Aus Problem 2 leitet sich Ziel 2 ab: Die Ermittlung von Verfahren, die für die bereichsübergreifende Kommunikation schutzwürdiger Daten im Gesundheitswesen geeignet sind.

Zur Lösung dieser Aufgabe wurden zunächst generell weit verbreitete Techniken wie z.B. die E-Mail-Kommunikation vorgestellt. Detaillierter wurden im Anschluss dessen zwei Verfahren untersucht, die speziell für die Gegebenheiten des deutschen Gesundheitswesen entwickelt wurden. Beide Verfahren, VCS und PaDok, verwenden kryptografische Methoden, um datenschutzrechtliche Anforderungen zu erfüllen.

Als Ergebnis steht in Kapitel 4.5 eine Übersicht der vorgestellten Verfahren zu Verfügung. Diese Übersicht stellt die wichtigsten Eckdaten der Verfahren gegenüber und bereitet die Analyse und Bewertung der Verfahren vor.

Problem 3:

> *Es gibt keine Musterlösungen bzw. kein Referenzmodell für die einrichtungsübergreifende Kommunikation zwischen stationären und niedergelassen Bereich.*
>
> *Es fehlt ein auf einem Referenzmodell basierendes Werkzeug, welches den Informationsmanager bei der Erfüllung seiner Aufgaben unterstützt.*
>
> *Bisher entwickelte Methoden folgen keinem Standard und es ist nicht garantiert, dass sie untereinander kompatible Architekturen erzeugen. Ein Vergleich ist problematisch und sie sind aufgrund unterschiedlichster Konzepte nur schwer zu evaluieren.*

Aus Problem 3 leiten sich zwei Ziele ab. Zunächst muss aus den in Kapitel 4 vorgestellten Verfahren mit Hilfe der in Kapitel 3 zusammengetragenen Anforderungen ein anforderungskonformes Verfahren für die Kommunikation zwischen stationärem und niedergelassem Bereich gefunden werden. Die Lösung dieser Aufgabe wurde in Kapitel 5.3 beschrieben. Dazu wurden die gesetzlichen Anforderungen als K.O.-Kriterien genutzt, um eine Vorauswahl zu treffen. Anschließend wurden technische und ökonomische Anforderungen in die Analyse einbezogen. Auf diese Weise wurde das PaDok-Verfahren als derzeit optimale Kommunikationslösung ermittelt.

Das zweite Ziel ist zugleich das Hauptziel der Arbeit: Die Erstellung des Referenzmodells für die Kommunikation zwischen stationären und niedergelassen Bereich.

Bei der Erstellung des Referenzmodells wurden die Komponenten der Kommunikationsarchitektur mit Hilfe von Use Case und Sequenzdiagrammen identifiziert. Mit

diesen Ergebnissen und des in Kapitel 5.1 erstellten Ist-Modells wurde das 3LGM²-Referenzmodell auf Basis des PaDok-Verfahrens entwickelt.

Mit dem 3LGM²-Baukasten und dem 3LGM²-Referenzmodell für die sektorübergreifende Kommunikation ist der Informationsmanager eines Krankenhauses in der Lage, die Kommunikation mit angebundenen niedergelassenen Ärzten zu modellieren. In Kapitel 6.6 wurde gezeigt, dass sich durch Instantiierung und Modifikationen, wie z.B. der Vervielfältigung der Praxiskomponenten, spezielle Modelle aus dem Referenzmodell ableiten lassen. Die aus dem Referenzmodell abgeleiteten konkreten Modelle sind miteinander Vergleichbar, da ihnen ein gemeinsamer Sachverhalt zu Grunde liegt, d.h. sie die gleichen Kernelemente benutzen. Mit diesen Überlegungen wurde gezeigt, dass es sich bei dem erstellten 3LGM²-Modell tatsächlich um ein Referenzmodell handelt.

7.2 Ausblick

Das entwickelte 3LGM²-Referenzmodell unterstützt den Informationsmanager bei der Modellierung der sektoübergreifenden Kommunikation mit dem 3LGM²-Baukasten. Ein sinnvoller Schritt bei der Weiterentwicklung des 3LGM²-Baukastens ist die Implementierung dieser und weiterer Musterlösungen. Das Ziel der Entwicklung sollte ein Assistent sein, der Musterlösungen für die wichtigsten Informationssystemarchitekturen vorhält und abhängig vom umzusetzenden Modellierungsproblem, den Informationsmanager diese zur Verfügung stellt. Der Assistent sollte dabei in der Form zu beeinflussen sein, dass er je nach Anforderungen die Kernelemente einer Lösungsarchitektur oder wahlweise ein vollständiges Referenzmodell bereitstellt.

Das in dieser Arbeit erstellte Referenzmodell beinhaltet zur Herstellung der Datenintegration die Adapterkomponente. Sie soll einen reibungslosen Datenaustausch über die Systemgrenzen und damit über Formate und Protokolle mit unterschiedlichen Datenmodellen ermöglichen. In der Praxis stellt sich dies als problematisch heraus, da eine Vielzahl von Einschränkungen bei den Protokollübergängen zwischen Softwareprodukten verschiedener Hersteller zu beachten ist. Weniger problematisch ist die syntaktische Heterogenität, der mit entsprechenden Transformationen begegnet werden kann. Große Schwierigkeiten treten auf wenn semantische Inkompatibilitäten zwischen den Kommunikationspartnern bestehen, siehe Kapitel 5.3.2. Um so spannender sind die aktuellen Bemühungen, den XML-basierten CDA-Standard weiter voran zu treiben. Datenformate, die standardisiert, austauschbar, lesbar und allgemein akzeptiert werden, sind die Voraussetzung für den Informationsaustausch zwischen unterschiedlichen Einrichtungen. Nur mit einer gemeinsamen semantischen Basis ist eine Vernetzung im Sinne einer Integrierten Patientenversorgung möglich.

Mit den in dieser Arbeit vorgestellten Verfahren VCS und PaDok wird ein datenschutzkonformer Datenaustausch zwischen den Teilnehmern am Gesundheitswesen ermöglicht. Ein wichtiger Punkt bei der Einführung derartiger Verfahren ist die Aufklärung der Nutzer. Auch die aufwendigste Verschlüsselung ist wirkungslos, wenn bspw. unsachgemäß mit Chipkarten oder Passwörtern umgegangen wird.

Nach der Einführung von Verfahren zum elektronischen Datenaustausch sollte stets eine Kosten/Nutzenanalyse erfolgen, um Einsparung- und Qualitätssteigerungseffekte nachweisen zu können. In diesem Zusammenhang müssen immer auch Analysen bzgl. Nutzerakzeptanz und Bedienbarkeit durchgeführt werden, um frühzeitig auf Nutzerprobleme eingehen zu können.

Zufriedene, aufgeklärte Nutzer sind in Anbetracht des enormen technischen Aufwandes ein wichtiger Erfolgsgarant bei der Einführung neuer Verfahren in die eingespielten Prozessabläufe im Gesundheitswesen.

Abzuwarten bleibt die Einführung und Weiterentwicklungen der elektronischen Gesundheitskarte und der zugehörigen Telematikinfrastruktur. Die eGK wird jedoch voraussichtlich erst ab 2007 die Speicherung von Gesundheitsdaten ermöglichen, siehe Kapitel 2.3.3. Bis dahin bleibt die Verwendung von Alternativkonzepten, wie die Verwendung provisorischer Chipkarten, für die Authentifizierung der Teilnehmer einer vernetzten Infrastruktur.

Literaturverzeichnis

[3LGM2HP]: Institut für Medizinische Informatik Statistik und Epidemiologie (IMISE); "Home Page 3LGM2"; http://www.3lgm2.de/; September 2005

[3LGM2HP]: (IMISE), Institut für Medizinische Informatik Statistik und Epidemiologie; "Home Page 3LGM2"; http://www.3lgm2.de/; September 2005

[BDSG]: "Bundesdatenschutzgesetz"; Bundesregierung Deutschland; Aktualisierte, nicht amtliche Fassung, Stand: Dezember 2002; http://www.bfd.bund.de/information/BDSG_neu.pdf; Dezember 1990

[BDT1994]: Lichtner Friedrich, Sembritzki Jürgen "BDT-Satzbeschreibung - Schnittstellenbeschreibung zum systemunabhängigen Datentransfer von Behandlungsdaten"; Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland; Version 02/94; ; Februar 1994

[Beyer2004]: Beyer Mario, Kuhn Klaus A., Meiler Christian, Jablonski Stefan, Lenz Richard; "IT-basierte Integration in medizinischen Versorgungsnetzen"; CEUR Workshop Proceedings; "Enterprise Application Integration 2004, Proceedings of the GI-/GMDS Workshop on Enterprise Application Integration (EAI-04), Oldenburg, Germany, February 12-13, 2004"; Institut für Medizinische Informatik der Philipps-Universität Marburg, Lehrstuhl für Informatik der Friedrich-Alexander-Universität Erlangen; 2004

[BITTHP]: BitTorrent, Inc.; "Home Page BitTorrent"; http://www.bittorrent.com/; November 2005

[BMGeGK2006]: Bundesministerium für Gesundheit - BMG; "Ab wann wird es die elektronische Gesundheitskarte geben?"; http://www.die-gesundheitskarte.de/fragen_und_antworten/details/start_egk.html; 2005

[BNAHP]: Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen; "Home Page Bundesnetzagentur"; http://www.bundesnetzagentur.de; Dezember 2005

[Brigl2003]: Brigl Birgit, Wendt Thomas, Winter Alfred; "Ein UML-basiertes Meta-Modell zur Beschreibung von Krankenhausinformationssystemen"; Institut für Medizinische Informatik Statistik und Epidemiologie - IMISE, Universität Leipzig; Mai 2003

[Brigl2004]: Brigl Birgit, Häber Anke, Wendt Thomas, Winter Alfred; Ein 3LGM² Modell des Krankenhausinformationssystems des Universitätsklinikums Leipzig und seine Verwertbarkeit für das Informationsmanagement; IMISE, Uni Leipzig; 2004

[Bultmann2002]: Bultmann Marion, Wellbrock Rita, Biermann Heinz, Engels Jürgen, Ernestus Walter, Höhn Udo, Wehrmann Rüdiger, Schurig Andreas; "Datenschutz und Telemedizin - Anforderungen an Medizinnetze"; Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Oktober 2002

[CEN13606]: CEN 13606 "Health informatics - Electronic healthcare record communication"; Europäisches Komitee für Normung - CEN; 13606 - Revised final draft for formal vote; http://www.centc251.org/TCMeet/Doclist/TCdoc99/N99-040.pdf; May 1999

[D2D2005]: "D2D-Technisches Handbuch - Technisches Handbuch des Kommunikationskonzeptes für patientenbezogene medizinische Daten "; Kassenärztliche Vereinigung Nordrhein (KVNo), Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung; Version 4.01; http://kvno.arzt.de/importiert/d2d_habu_soft.pdf; August 2005

[D2DHP]: Kassenärztlichen Vereinigungen Nordrhein (KVNO); "Home Page KVNO D2D"; http://www.d2d.de/; September 2005

[DGIV2005]: Deutsche Gesellschaft für Integrierte Versorgung e.V. (DGIV); "Gemeldete, zum Stichtag geltende Verträge zur integrierten Versorgung nach Versorgungsregion" (Stichtag: 31.03.2005); http://www.dgiv.org/BQS-Uebersicht_IV_Vertraege.pdf; März 2005

[DGIVHP]: (DGIV), Deutsche Gesellschaft für Integrierte Versorgung e.V.; "Homepage DGIV"; http://www.dgiv.org; March 2005

[DGNHP]: Deutsches Gesundheitsnetz Service GmbH (DGN); "Home Page DGN"; http://www.dgn.de; November 2005

[Dierks1999]: Dierks Christian; "Rechtliche und praktische Probleme der Integration von Telemedizin in das Gesundheitswesen in Deutschland"; Humboldt-Universität zu Berlin; Februar 1999

[Dierks2005]: Dierks, Christian; "Rechtliche Aspekte der Gesundheitstelematik"; Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, Band 48, Nummer 6, S635-639; June 2005

[eGKHPC2005]: Katja Möhrle; "Der elektronische Heilberufeausweis (Health Professional Card/ HPC)"; http://www.laekh.de/Presse-Forum/Mitteilungen/mitteilungen_2005/quartal1/hpc.html; Jan 2005

[Fowler1998]: Fowler Martin, Scott Kendall; "UML konzentriert - Die neue Standard-Objektmodellierungssprache anwenden"; 1. Ausgabe; Addison-Wesley, 1998

[GDSGNRW]: NRW, Landesregierung "Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen"; Landesregierung NRW; geänderte Fassung von 17.12.1999 (§2); http://www.duesseldorf.de/datenschutz/rechtsgrundlagen/gdsg.pdf; Febuary 1994

[Geissbuhler2004]: Geissbuhler A, Spahni S, Assimacopoulos A, Raetzo MA, Gobet G.; "Design of a patient-centered, multi-institutional healthcare information network using peer-to-peer communication in a highly distributed architecture."; Medinfo, Band 11, Nummer 2, S1048-1052; 2004

[GMCHP]: (GMC), Gesellschaft für medizinische Computersysteme mbH; "Homepage GMC-Systems"; http://www.gmc-systems.de; Juni 2005

[GMG]: "Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz - GMG)"; Bundesregierung Deutschland; Fassung von 14.11.2003; http://www.die-gesundheitsreform.de/gesundheitspolitik/gesetze/pdf/gkv-modernisierungsgesetz-gmg.pdf; November 2003

[Goetz2005]: Goetz Christoph F-J; "Strukturgefüge künftiger Heilberufsausweise im deutschen Gesundheitswesen" erschienen in [TMFS2005]; Kapitel S1, S28-31, Minerva KG; 2005

[Graetz2005]: Grätzel von Grätz Philipp; "Vernetzte Medizin - Patienten-Empowerment und Netzinfrastrukturen in der Medizin des 21. Jahrhunderts"; 1. Ausgabe; Verlag Heinz Heise, 2005

[Haensch2005]: Hänsch H., Fleck E.; "Vernetzung und integrierte Versorgung - Vor- und Nachteile aus medizinischer Sicht"; Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, Band 48, Nummer 7, S755 - 760; July 2005

[Haux1998]: Haux Reinhold, Lagemann Anita, Knaup Petra, Schmücker Paul, Winter Alfred; "Management von Informationssystemen - Analyse, Bewertung, Auswahl, Bereitstellung und Einführung von Informationssystemkomponenten am Beispiel von Krankenhausinformationssystemen"; 1. Ausgabe; B. G. Teubner Stuttgart, 1998

[Heitmann2001]: Heitmann, Kai U.; "Zusammenfassung zur Clinical Document Architecture(CDA)"; SCIPHOX GbR mbH, Universität zu Köln; March 2001

[Hl723]: Quinn John "Spezifikation HL7 Version 2.3"; Health Level Seven, Inc.; Final Edition; http://www.hl7.org/library/General/v231.zip; May 1999

[HL7CDA]: Dolin Robert H., Alschuler Liora, Boyer Sandy, Beebe Calvin, Behlen Fred M., Biron Paul V. "HL7 Clinical Document Architecture"; Health Level Seven, Inc.; Release 2.0; ; August 2004

[HL7DE]: HL7 Benutzergruppe in Deutschland, e.V.; "Home Page HL7 DE"; http://www.hl7.de; September 2005

[HL7DT]: Schadow Gunther, Biron Paul, McKenzie Lloyd, Grieve Grahame, Pratt Doug "Data Types - Abstract Specification"; Health Level Seven, Inc.; ANSI/HL7 V3 DT, R1-2004 11/29/2004; http://www.hl7.org/v3ballot/html/infrastructure/datatypes/datatypes.htm; November 2004

[HL7M15]: Blobel Bernd; "Quo vadis HL7?"; HL7 Mitteilungen, Band -, Nummer 15, S5-6; April 2003

[HL7RIM]: Beeler George, Case James, Curry Jane, Hueber Ann, Mckenzie Lloyd, Schadow Gunther, Shakir Abdul-Malik "HL7 Reference Information Model"; Health Level Seven, Inc.; V 02-04; https://www.hl7.org/library/data-model/RIM/C30204/rim.htm; July 2004

[HL7USA]: Health Level Seven, Inc.; "Home Page HL7 Inc."; http://www.hl7.org; September 2005

[Horsch2002]: Horsch Alexander, Handels Heinz; "Telematik im Gesundheitswesen" erschienen im Handbuch der medizinischen Informatik [Lehmann2002]; Kapitel 12, S567-606, Hanser Verlag; 2002

[IBMTHP]: Fraunhofer Institut für Biomedizinische Technik (IBMT); "Home Page IBMT"; http://www.ibmt.de/; September 2005

[IETFHP]: IETF; "Home Page IETF"; http://www.ietf.org; November 2005

[ISOHP]: ISO; "Home Page ISO"; http://www.iso.org;

[IVB2004]: Richter Klaus H., Mehl E., Schütz J., Ulrich G., Weigeldt U., Becker F., Homan P.; "Vertrag zur Integrierten Versorgung durch Hausärzte und Hausapothelen ('Integrationsvertrag') gem. §§140a ff. SGB V"; http://www.hausaerzteverband-bremen.de/download/vertragbarmer.pdf; September 2004

[KBV_SS]: Kassenärztliche Bundesvereinigung (KBV); "Schnittstellen: xDT - Synonym für elektronischen Datenaustausch in der Arztpraxis"; http://www.kbv.de/ita/4274.html; 2005

[Keading2005]: Keading Andre; "Datenmanagement in der medizinischen Praxis"; http://www.imise.uni-leipzig.de/Lehre/Semester/2005/SGKI/DatenmanagementPraxis.pdf; 2005

[KHG]: "Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze"; Bundesregierung Deutschland; Zuletzt geändert: 22.6.2005; http://www.bmgs.bund.de/cln_040/nn_603204/SharedDocs/Gesetzestexte/Krankenhaeuser/KHG,templateId=raw,property=publicationFile.pdf/KHG.pdf; Juni 1972

[Koehler2002]: Köhler Claus O.; "Integration des Patienten in medizinische Informationskreisläufe" erschienen im Handbuch der medizinischen Informatik [Lehmann2002]; Kapitel 11, S553-565, Hanser Verlag; 2002

[Krcmar2003]: ; "Informationsmanagement"; 3. Auflage; Springer Verlag, 2003

[Krueger2005]: Krüger-Brand Heike E.; "Telemedizin: Erfolgreiche Geschäftsmodelle"; Deutsches Ärzteblatt, Band 102, Nummer 7, A-441 / B-374 / C-349; February 2005

[Lehmann2002]: Lehmann Thomas, Meyer zu Bexten Erdmunde; "Handbuch der medizinischen Informatik"; 2. Ausgabe; Hanser Verlag, 2002

[Lenz2005]: Lenz Richard , Beyer Mario, Meiler Christian, Jablonski Stefan, Kuhn Klaus A.; "Informationsintegration in Gesundheitsversorgungsnetzen Herausforderungen an die Informatik"; Informatik-Spektrum, Band 28, Nummer 2, S105-119; April 2005

[LIV2005]: Beckmann H., Biet Th., Blattmann J., Bosenius M., Dietrich Th., Dörje F., Elsner M., Henze H., Klitza K., Latz V., Liebsch B., Pesch C., Schiefer D., Schnettger K., Sunderhaus M., Uhl A., et. al.; "Leitfaden zur Integrierten Versorgung aus der Praxis"; Rheinische Fachhochschule Köln; March 2005

[Lux2005]: Lux A.; "Ökonomische Aspekte der Gesundheitstelematik"; Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz, Band 48, Nummer 6, S640-645; Juni 2005

[MCSDEG2004]: MCS AG, DOCexpert Gruppe; "Die MCS AG und die DOCexpert Gruppe erklären ihren Austritt aus dem VDAP"; http://www.docexpert.de/docs/deg/presse/archiv/vdap.html; März 2003

[Mueller2005]: Müller J. H.; "Gesundheitstelematik und Datenschutz"; Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz, Band 48, Nummer 6, S629-634; Juni 2005

[MuellerU2005]: Müller U., Funkat G., Jaekel D., Kaeding A., Winter A.; "Communication Support for Managed Care"; The Journal on Information Technology in Healthcare, Band 3, Nummer 5, S295-300; 2005

[MuellerU20051]: Müller Ulrike, Funkat Gert, Pilz Uwe, Smers Stefan; "IT-Konzept zur Integrierte Versorgung"; Institut für Medizinische Informatik, Statistik und Epidemiologie - IMISE, Universitätsklinikum Leipzig - UKL (Bereich 1); Juni 2005

[Noelle2001]: Noelle Guido, Heitmann Kai U.; "SCIPHOX - elektronische Kommunikation im Gesundheitswesen: Auf dem Weg zur integrierten Versorgung"; Deutsches Ärzteblatt, Band 98, Nummer 45, S2-6; November 2001

[Oestereich1997]: Oestereich, Bernd; "Objektorientierte Softwareentwicklung mit der Unified Modeling Language"; 3; R. Oldenbourg Verlag, 1997

[OID2005]: Heitmann, Kai U.; "Object Identifier (OID) Konzept für das deutsche Gesundheitswesen"; HL7-Benutzergruppe Deutschland e.V., Arbeitsgemeinschaft SCIPHOX GbR mbH, Kassenärztliche Bundesvereinigung - KBV, Deutsches Institut für medizinische Dokumentation und Information - DIMDI; March 2005

[PADOKHP]: Fraunhofer Institut für Biomedizinische Technik (IBMT); "Home Page PaDok"; http://padok.ibmt.fhg.de/; September 2005

[Paland2005]: Paland N, Riepe C; "Politische Aspekte und Ziele der Gesundheitstelematik"; Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz, Band 48, Nummer 6, S623-628; Juni 2005

[PAS1011]: Verband Deutscher Arztpraxis-Softwarehersteller e.V. (VDAP) "VCS Kommunikationskonzepte für das Gesundheitswesen"; Verband Deutscher Arztpraxis-Softwarehersteller e.V. (VDAP); DIN PAS1011; ; Januar 2001

[RFC1939]: Network Working Group "Post Office Protocol - Version 3 (POP3)"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc1939.txt; August 1982

[RFC2045]: Network Working Group "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2045.txt; November 1996

[RFC2251]: Network Working Group "Lightweight Directory Access Protocol (v3) - LDAP (v3)"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2251.txt; Dezember 1997

[RFC2440]: Network Working Group "OpenPGP Message Format"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2440.txt; November 1998

[RFC2518]: Network Working Group "HTTP Extensions for Distributed Authoring - WEBDAV"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2518.txt; Februar 1999

[RFC2633]: Network Working Group "S/MIME Version 3 Message Specification"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2633.txt; Juni 1999

[RFC2821]: Network Working Group "SIMPLE MAIL TRANSFER PROTOCOL (SMTP)"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2821.txt; April 2001

[RFC2822]: Network Working Group "Internet Message Format"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc2822.txt; April 2001

[RFC959]: Network Working Group "FILE TRANSFER PROTOCOL (FTP)"; The Internet Engineering Task Force - IETF; ; http://www.ietf.org/rfc/rfc959.txt; Oktober 1985

[Roche03]: Reiche Dagmar; "Roche Lexikon Medizin"; 5. Auflage; Urban & Fischer, 2003

[SaechsDSG]: "Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz - SächsDSG)"; Freistaat Sachsen; Stand 25.08.2003; http://www.saxonia-verlag.de/recht-sachsen/212_2bs.pdf; Juli 2003

[SaechsGDG]: "Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen"; Freistaat Sachsen; Stand 03.05.2003; http://www.saxonia-verlag.de/recht-sachsen/250_1bs.pdf; Mai 2003

[SAPHP]: SAP AG; "Home Page SAP AG"; http://www.sap.de; November

[Schmidt2004]: Schmidt Ulla; "Standpunkt: Chancen"; Deutsches Ärzteblatt, Band 101, Nummer 47, A-3220; November 2004

[Schneider2005]: Schneider Uwe K.; "Datenschutz in der vernetzten Medizin" erschienen in [Graetz2005]; Kapitel 3, S136-162, Verlag Heinz Heise; 2005

[Schneier1996]: Schneier Bruce; "Angewandte Kryptographie"; 1. Ausgabe; Addison-Wesley, 1996

[SCIPHOXHP]: SCIPHOX Gbr mbH; "Home Page SCIPHOX"; http://www.sciphox.de; Juli 2005

[SCIPHOXP1]: Heitmann Kai U., Noelle Guido, Schweiger Ralf, et. al. "Phase I - Kommunikationsumfang und -inhalt (Spezifikation zum standardisierten elektronischen Kurzbericht)"; SCIPHOX GbR mbH, HL7-Benutzergruppe in Deutschland e.V., Universität zu Köln, medicine online GmbH, Universität Gießen; v1.0 Working Draft 15; http://www.sciphox.de/atwork/tools/WD-sciphox-v15.pdf; Juni 2002

[Secaritas2004]: Schlüter, Hühnlein; "Ausgabe der Health Professional Card durch die Landesärztekammer"; Secaritas AG, secunet Security Networks AG; Jun 2004

[SGBV]: "Sozialgesetzbuch - Fünftes Buch (V) - Gesezliche Krankenversicherung"; Bundesregierung Deutschland; Zuletzt geändert: 29.08.2005; http://bundesrecht.juris.de/bundesrecht/sgb_5/gesamt.pdf; Dezember 1988

[SIG]: "Gesetz über die Rahmenbedingungen für elektronische Signaturen"; Bundesregierung Deutschland; geänderte Fassung von 16.05.2001; http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf; Mai 2001

[SPEZHPC]: Struif Bruno, et. al. "German Health Professoinal Card and Security Module Card - Spezification"; Fraunhofer-Institute for Secure Telecooperation (FhG-SIT); Version 2.0; http://www.zi-berlin.de/hpc/downloads/HPC_Apotheker_Aerzte_V2_0.pdf; Juli 2003

[SPEZLA]: Projektgruppe FuE-Projekt "Lösungsarchitektur"; "Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte"; Fraunhofer für Software- und Systemtechnik, Fraunhofer Institut Arbeitswirtschaft und Organisation, Fraunhofer Institut Sichere Inforamtionstechnologie; Version 1.0; http://www.dimdi.de/dynamic/de/ehealth/karte/technik/loesungsarchitektur/ergebnisse/index.htm; März 2005

[Stock2002]: Stock Stephanie, David Dagmar M., Lauterbach Karl W., Rosenthal Barbara, Schäfer Robert D.; "Institutionen des Gesundheitswesens und deren Verpflechtung (Healthmanagement)" erschienen im Handbuch der medizinischen Informatik [Lehmann2002]; Kapitel 2, S25-44, Hanser Verlag; 2002

[Tanenbaum2000]: Tanenbaum Andrew S.; "Computernetzwerke"; 3rd Edition; Prentice Hall, 2000

[TelemedHP]: telemed Online Service für Heilberufe GmbH; "Home Page telemed Online Service für Heilberufe GmbH"; http://www.telemed.de; November 2005

[TMF2006]: Jäckel Achim; "Telemedizinführer Deutschland - 2006"; 7. Ausgabe; Minerva KG, 2006

[TMFS2005]: Hempel Volker, Jäckel Achim, Reum Lutz; "Sonderausgabe Telemedizinführer Deutschland - elektronische Gesundheitskarte"; 1. Sonderausgabe 2005; Minerva KG, 2005

[UMIT2005]: Hübner-Bloder G. "Referenzmodell für die Fachliche Ebene des 3LGM²"; Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT); Version 1; ; Oktober 2005

[UMLV2]: Object Management Group, Inc. "Unified Modeling Language: Superstructure"; Object Management Group, Inc. - OMG; Version 2.0, 05-07-04; http://www.omg.org/technology/documents/formal/uml.htm; August 2005

[VDAPHP]: Verband Deutscher Artzinformationssystemhersteller und Provider e.V. (VDAP); "Home Page VDAP"; http://www.vdap.de/; August 2005

[VHitG2005]: Naumann Jens; "Aspekte der Telematik-Einführung aus Sicht der Anbieter von Arztpraxis-EDV"; http://www.initiative-praxis-edv.de/docs/e_health.pdf; 2005

[W3XML]: Bray Tim, Paoli Jean, Sperberg-McQueen C. M., Maler Eve, Yergeau François, Cowan John "Extensible Markup Language (XML) 1.1"; World Wide Web Consortium - W3C; REC-xml11-20040204; http://www.w3.org/TR/2004/REC-xml11-20040204/; February 2004

[Wendt2004]: Wendt Thomas, Häber Anke, Brigl Birgit, Winter Alfred; "Modeling Hospital Information Systems (Part 2) - Using the 3LGM2 Tool for Modeling Patient Record Management"; Methods of Information in Medicine, Band 43, Nummer 3, S256-267; 2004

[Wendt2005]: Wendt Thomas; "Modellierung und Bewertung von Intergration in Krankenhausinformationssystemen"; Medizinische Fakultät der Universität Leipzig, Institut für Medizinische Informatik Statistik und Epidemilogie - IMISE; 2005

[Winter1995]: WINTER A., ZIMMERLING R; "Die Bedeutung von Referenzmodellen für das Management von Krankenhausinformationssystemen" erschienen in Herausforderungen eines globalen Informationsverbundes für die Informatik; Kapitel , S703-710, Springer; 1995

[Winter2002]: Winter Alfred, Ammenwerth Elske, Brigl Birgit, Haux Reinhold; "Krankenhausinformationssysteme" erschienen im Handbuch der medizinischen Informatik [Lehmann2002]; Kapitel 10, S473-552, Hanser Verlag; 2002

[Winter2003]: Winter Alfred, Brigl Birgit, Wendt Thomas; "Modeling Hospital Information Systems (Part 1) - The Revised Three-layer Graph-based Meta Model 3LGM2"; Methods of Information in Medicine, Band 42, Nummer 5, S544-551; 2003

[Winter2004]: Winter Alfred, Brigl Birgit, Heller Oliver, Mueller Ulrike, Struebing Alexander, Wendt Thomas; "Supporting Information Management for Regional Health Information Systems by Models with Communication Path Analysis"; IDEAS Workshop on Medical Information Systems: The Digital Hospital (IDEAS-DH'04), Band 1, Nummer 1, S139-146; 2004

[WinterAF1999]: Winter AF, Winter A, Becker K, et al.; "Referenzmodelle für die Unterstützung des Managements von Krankenhausinformationssystemen"; Informatik, Biometrie und Epidemiologie in Medizin und Biologie, Band 30, Nummer 4, 173-189; 1999

[WinterM2005]: Winter Mario; "Methodische objektorientierte Softwareentwicklung"; 1. Ausgabe; dpunkt.verlag, 2005

[Wozak2004]: Wozak Florian; "Gewährleistung von End-to-End Security in telemedizinischen Befundnetzwerken"; Institut für Informationssysteme des Gesundheitswesens, private Universität für medizinische Informatik und Technik Tirol (UMIT); 2004

[XMLD2D]: Marschall Hans-Joachim; "XML in D2D"; http://kvno.arzt.de/mitglieder/d2d/xml_anwen.html; Oktober 2005

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

A: xDT Spezifika und Auszug einer BDT-Datei

B: HL7-Nachrichten und CDA-Dokumente

C: Klassendiagramme logische und physische Werkzeugebene

D: 3LGM^2-Modelle

E: UML-Diagramme

F: CD-Rom mit 3LGM^2-Modellen und zugehörigen Programmen

Anhang A: xDT-Spezifika

Aufbau und Struktur am Beispiel BDT

Der BDT ist in Anlehnung an den ADT zur Übermittlung von Behandlungsdaten zwischen Praxisverwaltungssystemen entwickelt worden. Dazu wurden einige abrechungsrelevante Teile des ADT nicht in den BDT übernommen und Strukturen zur Aufnahme von Behandlungsdaten eingeführt. Teile, die in ADT und BDT übereinstimmen, werden identisch bezeichnet. ADT ist demnach keine echte Teilmenge des BDT und besteht parallel.

Gröbste Strukturierungseinheit ist das Datenpaket. Das Datenpaket stellt die Übertragungseinheit innerhalb eines BDT-Transfers dar. Ein Datenpaket besteht seinerseits aus Sätzen, die über mehrere Datenträger verteilt sein können. Der Datenträger ist eine mit DOS (ab Version 2) formatierte Diskette, auf dem die Informationen im ASCII Format gespeichert werden. Tabelle 2-2 stellt die Struktur des Datenpakets dar.

Datenpaket	Datenträger	Sätze
Datenpaket	Datenträger 1	Datenträger-Header
		Datenpaket-Header
		Praxisdaten
		Behandlungsdaten
		Datenträger-Abschluß
	Datenträger 2 bis n-1	Datenträger-Header
		Behandlungsdaten
		Datenträger-Abschluß
	Datenträger n	Datenträger-Header
		Behandlungsdaten
		Datenpaket-Abschluß
		Datenträger-Abschluß

Tabelle B-1: Struktur Datenpaket bei BDT

Die Sätze beinhalten sowohl Strukturinformationen, wie z.B. die Länge des Feldes oder die Datenträgerkennung, als auch inhaltliche Informationen, wie die Behandlungsdaten. Jeder BDT-Satz besteht aus mindestens 2 Feldern, die durch „Wagenrücklauf/Zeilenumbruch“ (CR/LF, ACSII 13/10) getrennt sind. Die beiden ersten Felder kennzeichnen stets die Feldlänge und die Feldkennung. Anschließend folgen Felder mit dem eigentlichen Inhalt.

Feld#	Feldlänge	Feldkennung	Feldinhalt
1	013	8000	6100
2	014	8100	00815
3-n	nnn	nnnn	xxxx

Tabelle B-2: Beispiel Feldstruktur bei BDT

Im Beispiel in Tabelle 2-3 berechnet sich die Feldlänge für Feld 1 wie folgt:

3Byte (Feldlänge) + 4Byte (Feldkennung) + 4Byte (Feldinhalt) + 2Byte (CR/LF) = 13Byte → 013

Die Bedeutung der Feldkennung ist in Tabellen der Satzarten, Feldkategorien und in der Feldtabelle im BDT Standard [BDT1994] definiert und wird eindeutig durch eine vierstellige Zahl identifiziert. Im Beispiel ist die Feldkennung für Feld 1 8000, was die Satzidentifikation kennzeichnet. Die Satzidentifikation, also der Feldinhalt von Feld 1, ist 6100, was für den Patientenstamm steht. Bei dem Beispiel BDT (Teil-) Datensatz aus Tabelle 2-3 handelt es sich also um Patientenstammdaten. Feld 2 mit der Feldkennung 8100 (Satzlänge) wird die Länge des Datensatzes mit 815 Byte angegeben. In Feld 3-n können nun inhaltliche Felder folgen. Tabelle 2-4 zeigt dies exemplarisch für die Feldkennung 3000 (Patienten ID), Feldkennung 3101 (Nachname), Feldkennung 3102 (Vorname) und Feldkennung 3103 (Geburtstag). Weitere Felder von Satzart 6100 (Patientenstamm) können folgen.

Feld#	Feldlänge	Feldkennung	Feldinhalt
3	015	3000	123456
4	019	3101	Mustermann
5	019	3102	Maximilian
6	017	3103	11031952

Tabelle B-3: Beispiel inhaltliche Felder

Feldkennungen und Feldinhalt werden vom Schnittstellenmodul der Praxissoftware mit Hilfe der Feldtabelle ausgewertet. Die Feldtabelle ordnet der Feldkennung eine Bezeichnung, Länge, Typ und Regel ID zu. Einen Auszug aus der Feldtabelle zeigt Tabelle 2-5 für Feldkennung 3103.

Feldkennung	Bezeichnung	Länge	Typ	RegelID
3103	Geburtstag	8	Datum	020

Tabelle B-4: Auszug Feldtabelle

Die RegelID gibt das Format vor und wird in der Regeltabelle definiert.

RegelID	Kategorie	Prüfung
020	Format	TTMMJJJJ

Tabelle B-5: Auszug Regeltabelle

So ergibt sich ein Zusammenhang zwischen Feld, Feldtabelle und Regeltabelle, wie in Abbildung B-17 dargestellt.

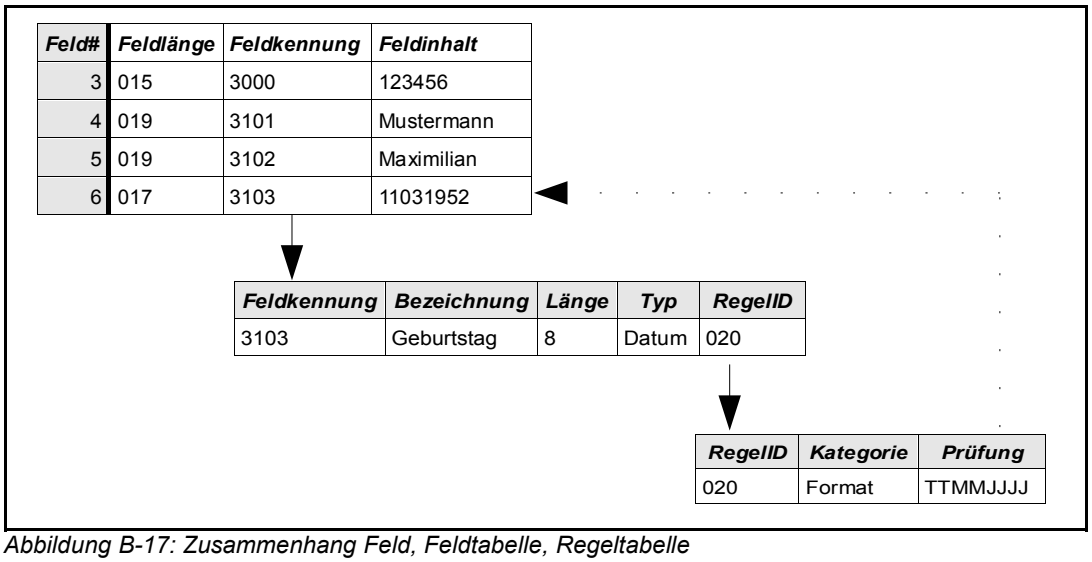

Abbildung B-17: Zusammenhang Feld, Feldtabelle, Regeltabelle

Auszug einer BDT-Datei mit den Beispieldaten:

```
...
01380006100
014810000815
0153000123456
0193101Mustermann
0193102Maximilian
017310311031952
...
```

Anhang B: HL7-Nachrichten und CDA-Dokumente

Aufbau und Struktur am Beispiel einer HL7-Version 2 Nachricht

Die Struktur einer HL7-Nachricht wird durch die *Abstract Message Definition* beschrieben. Eine Nachricht ist die kleinste Einheit, die zwischen den Systemen ausgetauscht wird. Sie besteht aus Segmenten, die in einer vorgegebenen Reihenfolge angeordnet sind. Jede Nachricht hat einen Nachrichtentyp (Abbildung B-1 a)). Mit dem Nachrichtentyp wird der Einsatzzweck für eine Nachricht festgelegt. Beispiele für den Nachrichtentyp sind Administrative Patientendaten (ADT), Befunde (ORF) oder Bestellungen (ORM). Nachrichtentypen können weiter in Ereignisse (Events) unterteilt werden (Abbildung B-1 b)), die die spezifische Segmentkombination für eine Nachricht festlegen (Abbildung B-1 c)). Beispiele für ADT Events sind A01 (Aufnahme eines Patienten), A02 (Verlegung), A03 (Entlassung) und so weiter.

Wie in Abbildung B-1 c) zu erkennen, wird bei der Definition der Segmentabfolge eine Backus-Naur ähnliche Syntax verwendet. Die Segmente MSH (Message Header Segment) und PID (Patienten Information Segment) sind in diesem Fall obligatorisch. Segment PD1 (zusätzliche soziale Angaben) ist demnach optional. Segment OBX (Beobachtung/Befund) kann mehrfach vorkommen.

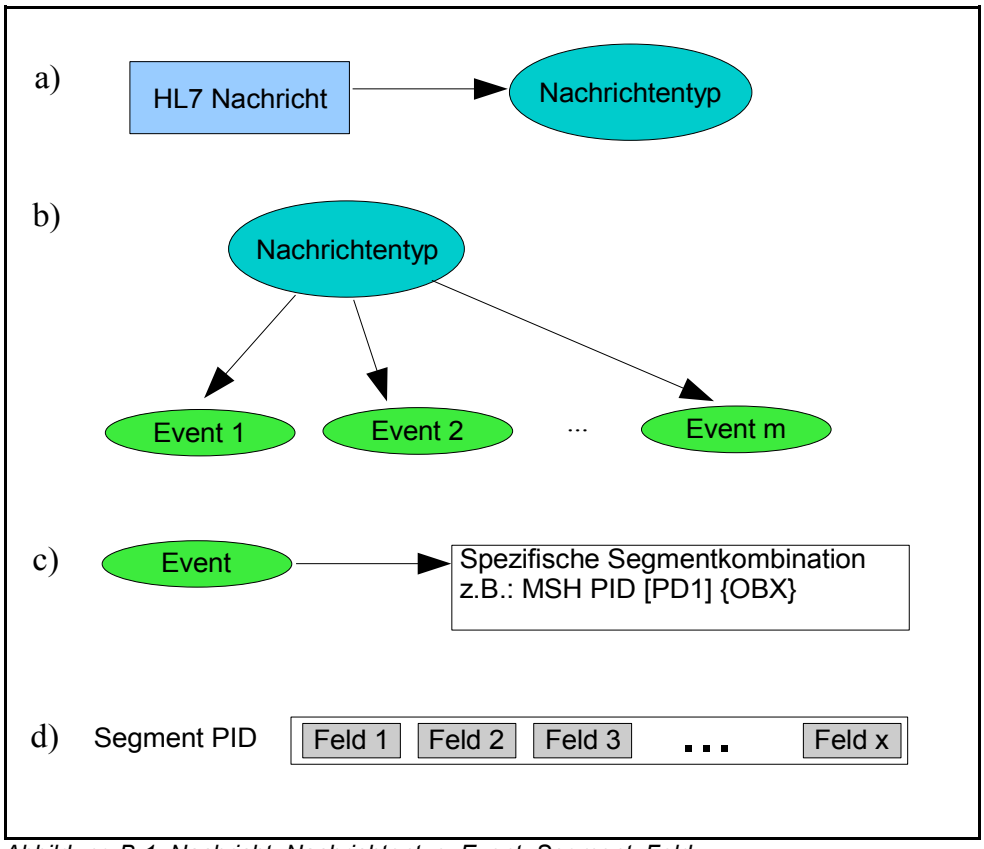

Abbildung B-1: Nachricht, Nachrichtentyp, Event, Segment, Feld

Segmente bestehen aus Feldern und werden immer mit 3 Buchstaben bezeichnet. Die Nummerierung, Länge und Inhalt sowie Typ und Format der Felder ist ebenfalls spezifiziert (Abbildung B-1 d)).

Mit den *Encoding Rules* wird die Kodierung der Inhalte der Felder und der Trennzeichen definiert. Felder werden durch „|“ von einander getrennt. Trennzeichen innerhalb eines Feldes ist „^“. Segmente werden durch einen Zeilenumbruch voneinander getrennt, sodass jedes Segment auf einer Zeile steht.

Das folgende Beispiel zeigt das PID (Patienten Information) Segment von Patient Max Mustermann, geboren am 11.3.1952, interne Patienten ID ist 1234, alternative Patienten ID ist 4321:

PID| | |1234|4321|Max^Mustermann^“”^“”^“”^“”| |19520311|....

Die Bedeutung und Kodierung der Felder ist in den Anhängen des HL7 Standards [Hl723] definiert.

z-Segmente

Um auf die landesspezifische Bedürfnisse eingehen zu können, bietet der HL7 Standard die Möglichkeit zusätzliche Segment zu definieren – die z-Segmente. In Deutschland wird ebenfalls davon Gebrauch gemacht und es kam zur Definition folgender z-Segmente:

- ZBD – Bankverbindungsdaten
- ZKA – Küchenanforderung
- ZPF – Pflegestufenerfassung
- ZWL – nicht-medizinische Wahlleistungen
- ZBE – Bewegungsdaten
- ZB1 – Zusatzsegment der Bundeswehr

Die Definition der z-Segmente ist Aufgabe der nationalen Nutzergruppen. Z-Segmente werden auch landesübergreifend zwischen den Nutzergruppen ausgetauscht und diskutiert. Wenn die Einführung landesspezifischer Segmente auch international von den Nutzergruppen als sinnvoll erachtet wird, können sie in den internationalen Standard aufgenommen werden.

Beispiel: Auszug eines levelone-CDA-Dokument in der XML-Code Ansicht und mit einem Stylesheet versehen in einem Browser dargestellt.

```
<?xml version="1.0" encoding="iso-8859-1"?>
<?xml-stylesheet type="text/xsl" href="../../xml/stylesheets/eArztBrief.xsl"?>
<levelone xmlns="urn::hl7-org/cda" xmlns:sciphox="urn::sciphox-org/sciphox"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="urn::hl7-org/cda sciphox-cda.xsd">
  <clinical_document_header>
       <id EX="a123" RT="2.16.840.1.113883.3.933"/>
       <document_type_cd V="11490-0" S="2.16.840.1.113883.6.1" DN="Arztbrief"/>
  </clinical_document_header>
  <body>
       <section>
            <caption>Arztbrief</caption>
            <section>
                 <caption>Medikamente<caption_cd V="10160-0"
                      S="2.16.840.1.113883.6.1"/></caption>
              <paragraph>
```

```
                        <content>
                              <local_markup ignore="all"
                                    descriptor="sciphox">
                                    <sciphox:sciphox-ssu type="medications"
                                          country="de" version="v1">
                                    <sciphox:Medikationen/></sciphox:sciphox-ssu>
                              </local_markup>
                        </content>
                  </paragraph>
            </section>
            <section>
                  <caption>Anamnese<caption_cd V="11492-6"
                        S="2.16.840.1.113883.6.1"/></caption>
                  <paragraph>
                        <content>
                              <local_markup ignore="all" descriptor="sciphox">
                                    <sciphox:sciphox-ssu type="anamnese"
                                          country="de" version="v1">
                                    <sciphox:anamnese/></sciphox:sciphox-ssu>
                              </local_markup>
                        </content>
                  </paragraph>
            </section>
...
```

Abbildung B-2: Auszug eines elektronischen Arztbriefes (Quelle: GMC-Systems [GMCHP])

Anhang C: Klassendiagramme logische und physische Werkzeugebene

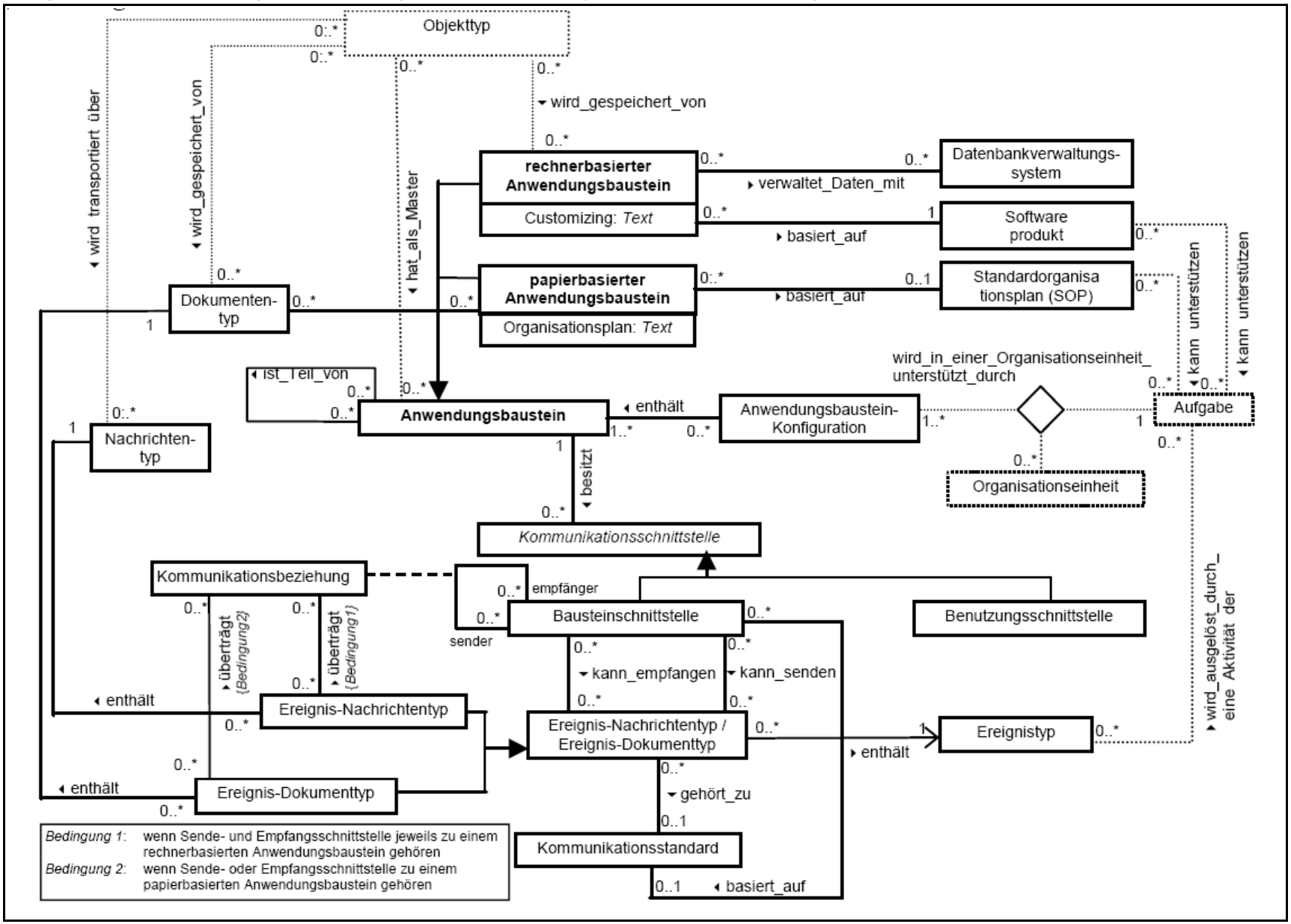

Abbildung C-1: UML-Klassendiagramm logische Werkzeugebene (Quelle: [3LGM2HP])

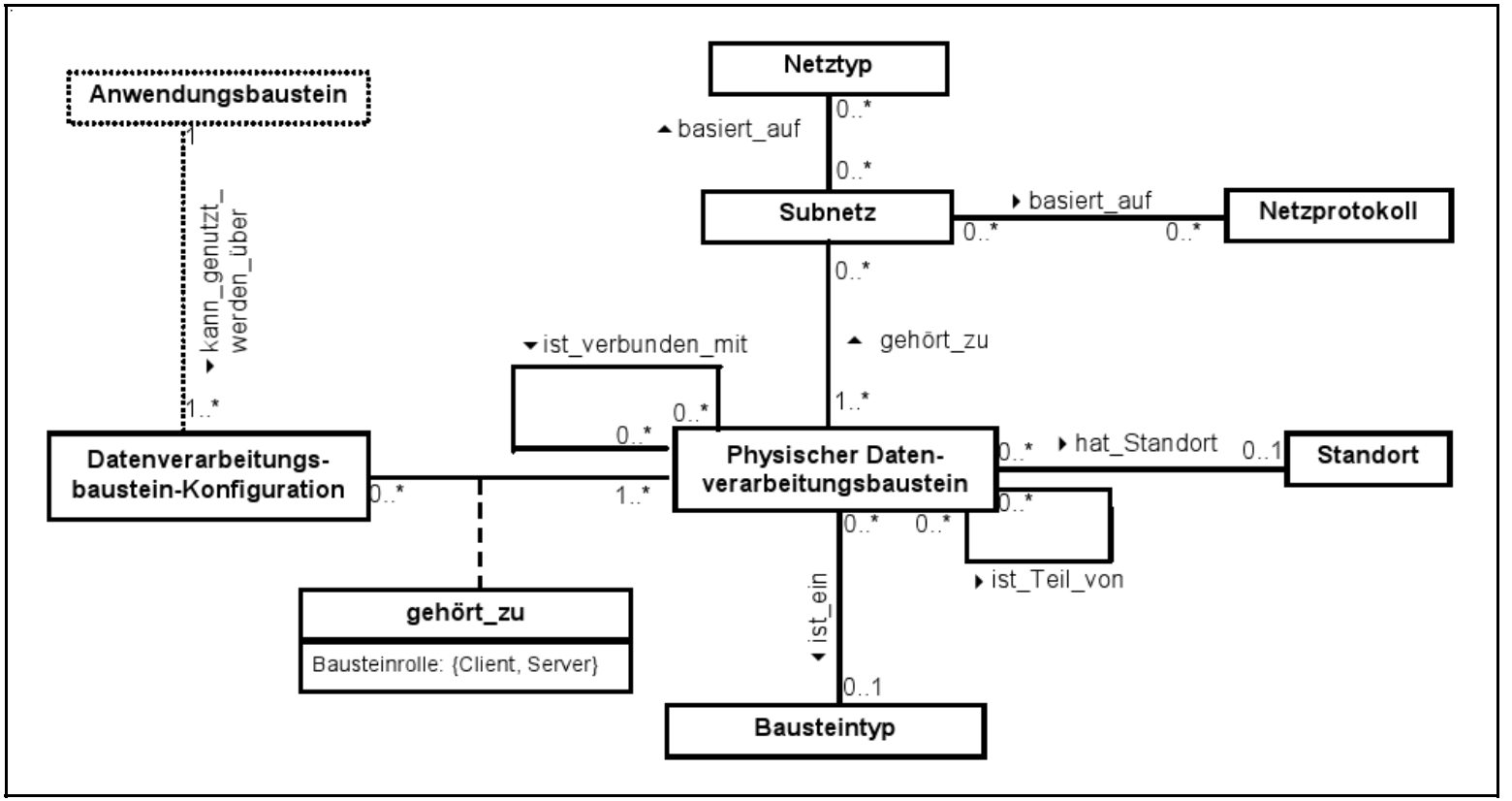

Abbildung C-2: UML-Klassendiagramm physischen Werkzeugebene (Quelle: [3LGM2HP])

Anhang D: 3LGM²-Modelle

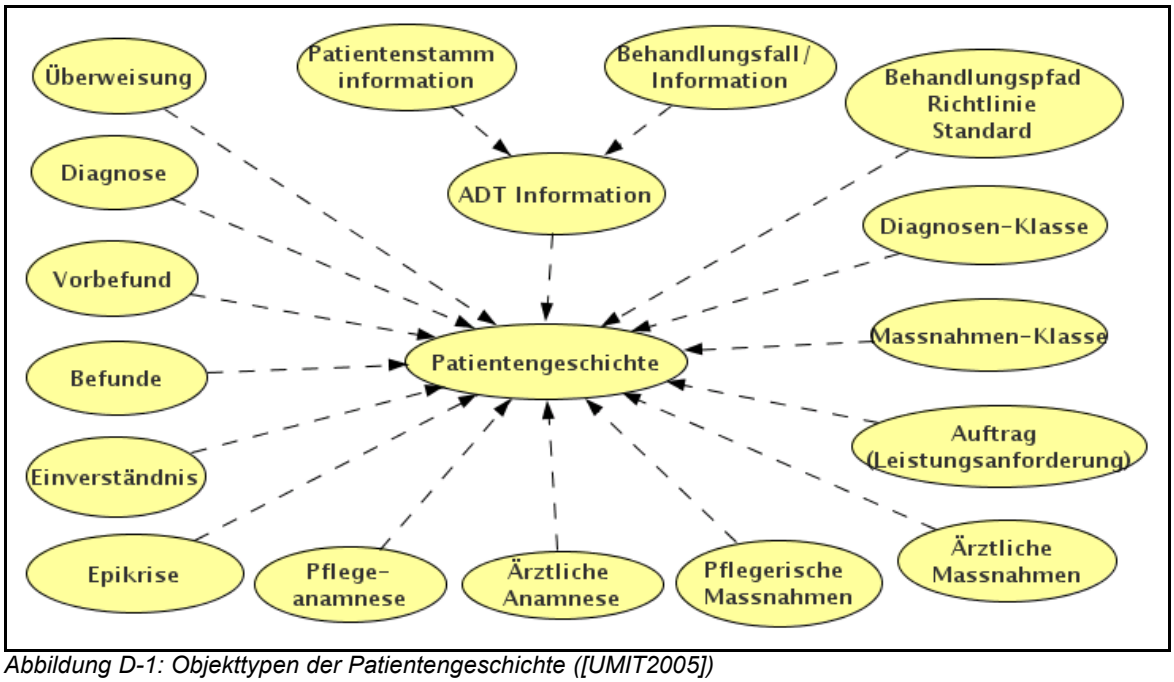

Abbildung D-1: Objekttypen der Patientengeschichte ([UMIT2005])

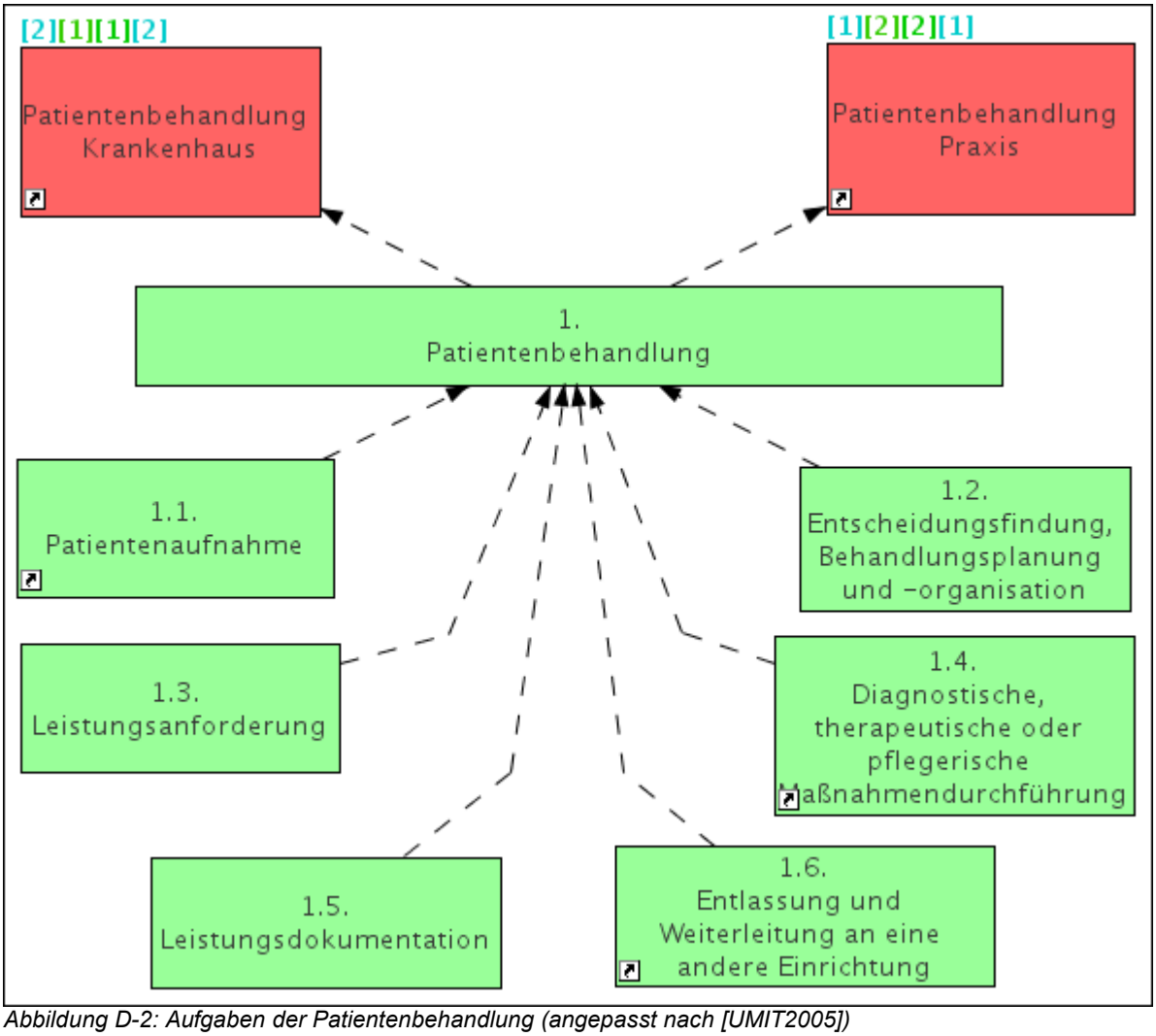

Abbildung D-2: Aufgaben der Patientenbehandlung (angepasst nach [UMIT2005])

Anhang E: UML Diagramme

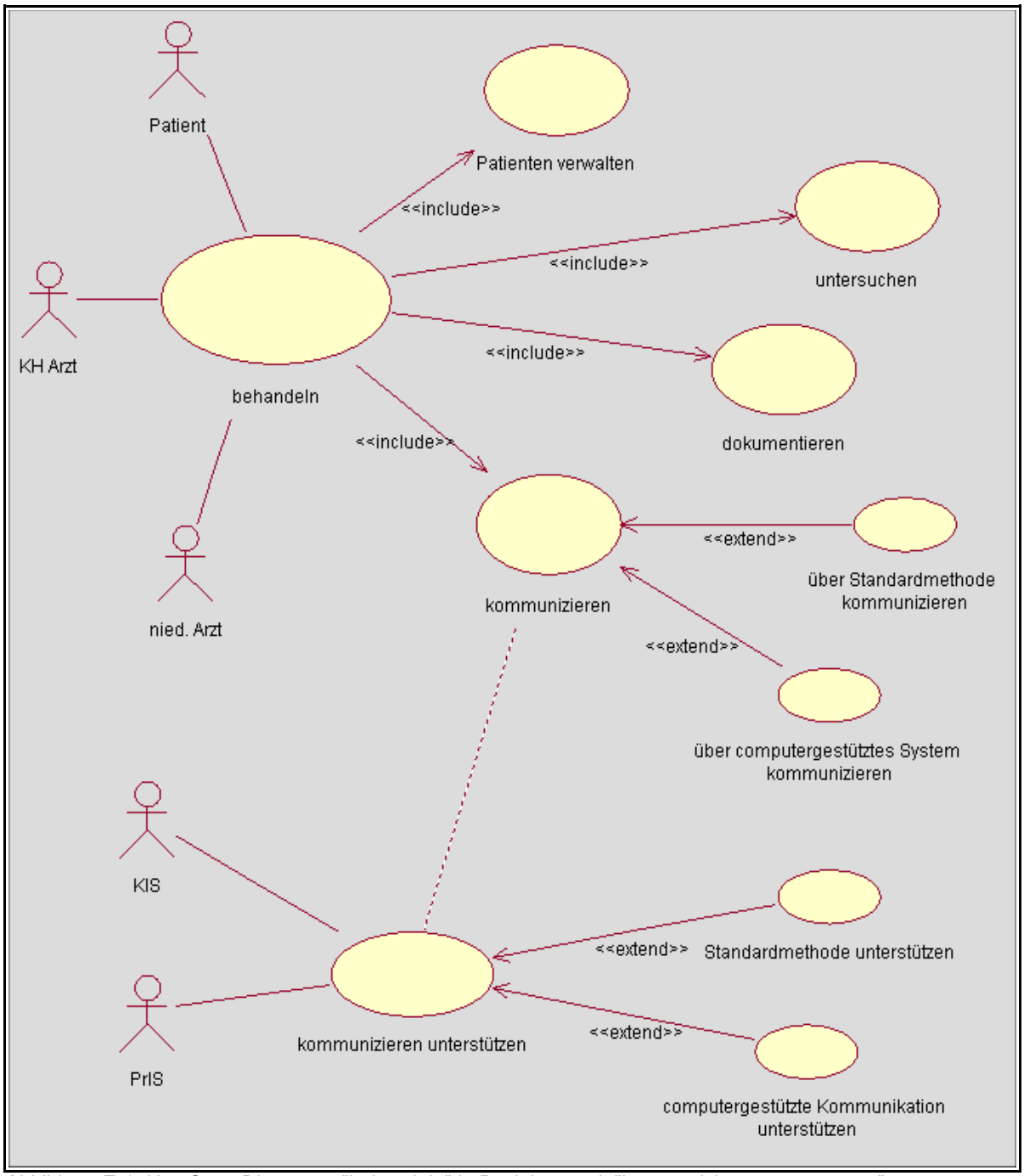

Abbildung E-1: Use Case Diagramm "behandeln" in Beziehung mit "kommunizieren unterstützen"

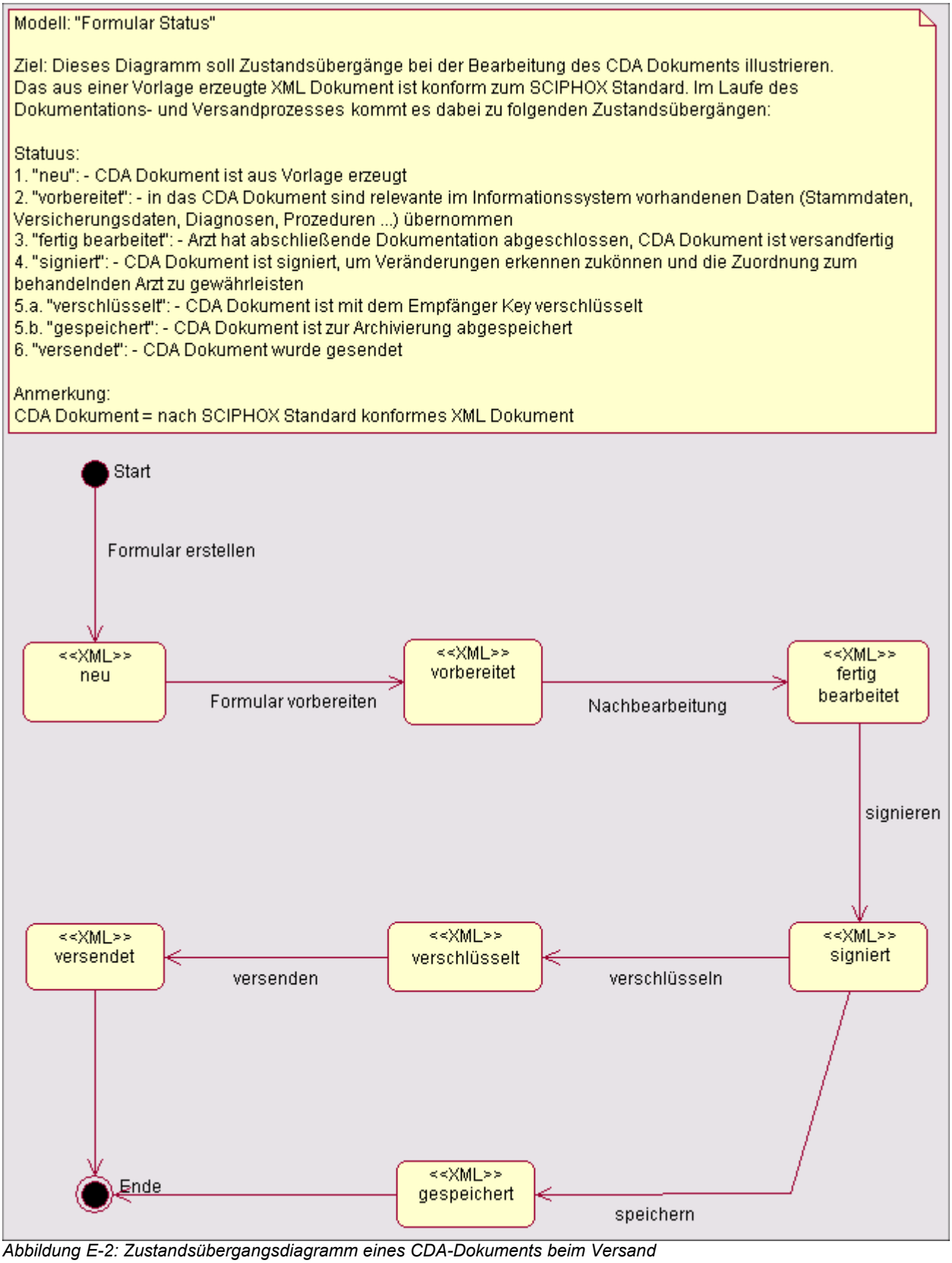

Abbildung E-2: Zustandsübergangsdiagramm eines CDA-Dokuments beim Versand

Anhang F: CD-Rom mit 3LGM²-Modellen und zugehörigen Programmen

Inhalt der CD-Rom:

- Diese Diplomarbeit im PDF-Dateiformat
- Java Runtime 1.5.x für Windows und Linux
- 3LGM²-Baukasten für Windows und Linux
- 3LGM²-Modell für den in Kapitel 2.6.1 vorgestellten Kommunikationsprozess (BeispielKommunikationsprozess.z3lgm)
- 3LGM²-Modell Ist-Zustand und Referenzmodell (gesamt-Modell.z3lgm)
- Quellen und BIBTex Datei (soweit in elektronischer Form vorhanden)

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Leipzig, 23. Februar 2006