UNIVERSITÄT LEIPZIG

Medizinische Fakultät

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)

Ein Referenzmodell zur Integration der Telematikinfrastruktur für die Gesundheitskarte in ein Gesundheitsunternehmen

Diplomarbeit

Leipzig, Januar 2007

vorgelegt von:

Sandra Forberger
geb. am: 28.05.1983

Betreuer:

Dr. Gert Funkat

Inhaltsverzeichnis

Begriffs- und Abkürzungsverzeichnis

AES .....Advanced Encryption Standard

AMDOK.....Arzneimitteldokumentation

ATM25 .....Asynchronous Transfer Mode-Version bei der Daten 25,6 Mbit/s übertragen werden

BDSG .....Bundesdatenschutzgesetz

BMGS.....Bundesministerium für Gesundheit und Soziales

BNetzA.....Bundesnetzagentur

CA .....Zertifizierungsstelle

CAL.....Konnektorabstraktionsschicht (Connector Abstraction Layer)

CAMS.....Card Application Management System

DHCP ..... Dynamic Host Configuration Protocol

DMZ.....Demilitarized Zone

DNS.....Domain Name System

DSL .....Digital Subscriber Line

EAP-TLS.....Extensible Authentication Protocol- TLS

EDV.....elektronische Datenverarbeitung

eGK .....elektronische Gesundheitskarte

eKiosk.....elektronische Kiosk = Primärsystem des Versicherten

ePA.....elektronische Patientenakte

ESP.....Encapsulating Security Payload

eRezept.....elektronische Rezept

EU.....Europäische Union

eVerordnung.....elektronische Verordnung

Gematik .....Gesellschaft für Telematik

GKV .....Gesetzliche Krankenversicherung

GSM .....Global System for Mobile Communications

HBA .....elektronische Heilberufeausweis

HL7.....Health Level 7

IKE .....Internet Key Exchange

ISDN.....Integrated Services Digital Network

IT .....Informationstechnik

IPSec.....IP Security

KV .....Krankenversicherung

LAN.....Local Area Network

L2TP/PPP.....Layer 2 Tunnel Protokoll / Point to Point Protokoll

LTZ.....logische Telematik-Zugangsprovider

NAT.....Network Adress Traversal

NTP .....Network Time Protocol

OID.....Object Identifier

OCSP.....Online Certificate Status Protocol

PIN .....Persönliche Identifikationsnummer

PKI .....Public Key Infrastruktur

PPPoE.....Point to Point Protokoll over Ethernet

SGB V .....Sozialgesetzbuch V

SHA-1.....Secure Hash Algorithm

SICCT.....Secure Interoperable ChipCard Terminal

SMC .....Security Module Card = Institutionskarte (funktioniert nur in Verbindung mit HBA)

SSL/TLS.....Secure Sockets Layer /Transport Layer Security

TI .....Telematikinfrastruktur

TLS.....Transport Layer Security

UKL.....Universitätsklinikum Leipzig

UMTS.....Universal Mobile Telecommunication System

VERSA.....Verteilte Signaturarbeitsplätze

VLAN.....Virtual LAN

VSD.....Versichertenstammdaten

VSDD.....Versicherten-Stammdaten-DienstVODD Verordnungsdatendienst

VPN.....Virtuell Private Network

WAN .....Wide Area Network

XML .....Extensible Markup Language

ZDA.....Zertifizierungsdiensteanbieter

1 Einleitung

1.1 Gegenstand

Die elektronische Gesundheitskarte und der Aufbau einer Telematikinfrastruktur dienen der Modernisierung des deutschen Gesundheitssystems und der Verbesserung der Versorgungsqualität durch die erhöhte Verfügbarkeit von Patientendaten.

Mit Hilfe der elektronischen Gesundheitskarte können einige neue Anwendungen zur Verfügung gestellt werden. Dazu gehören die Speicherung von Notfalldaten, die Übermittlung des elektronischen Rezeptes, der Transport des elektronischen Arztbriefes und die Verwaltung der elektronischen Patientenakte. Zur Nutzung dieser Funktionen ist eine Datenkommunikation über eine Telematikinfrastruktur notwendig. Aufbau, Betrieb und Standardisierung dieser Infrastruktur ist Aufgabe der Gesellschaft für Telematik (Gematik[1]). Unter Telematikinfrastruktur versteht man nach SGB V §291a Absatz 7 eine "interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur".

Einige Sicherheitsvorkehrungen, wie zum Beispiel die Verwendung von elektronischen Signaturen oder die Verwendung von elektronischen Heilberufsausweisen, für die Erhebung, Verarbeitung und Nutzung der Patientendaten sind durch das SGB V vorgesehen. Die Definition von einheitlichen standardisierten Schnittstellen und Diensten, sowie die Festlegung technischer Vorgaben ist Aufgabe der Gematik. Für die Einhaltung der Vorschriften zum Schutz personenbezogener Daten nach dem Bundesdatenschutzgesetz und die Wahrung der Patientenrechte ist ebenfalls die Gematik verantwortlich.

In verschiedenen Modellregionen wird der Einsatz der elektronischen Gesundheitskarte und der elektronischen Heilberufsausweise getestet. Die Tests dienen der Überprüfung und Weiterentwicklung der Telematikinfrastruktur auf Funktionalität, Interoperabilität, Kompatibilität, Stabilität, und Sicherheit der einzelnen Komponenten und Dienste. Eine Integration der Telematikinfrastruktur in die teilnehmenden Gesundheitsunternehmen ist dazu unabdingbar. Neben den Vorgaben durch die Gematik müssen dabei auch zusätzliche Sicherheitsanforderungen und die vorhandene Kommunikationsinfrastruktur des Gesundheitsunternehmens beachtet werden. Ausgehend von den Modellregionen soll eine flächendeckende Einführung der elektronischen Gesundheitskarte in ganz Deutschland stattfinden.

1.2 Problemstellung

Vor der Einführung der elektronischen Gesundheitskarte im Universitätsklinikum Leipzig (UKL) wird ein Pilotprojekt durchgeführt werden bei dem ein Teil der Funktionen der elektronischen Gesundheitskarte getestet werden soll. Dazu ist eine Verknüpfung der Telematikinfrastruktur mit der klinikeigenen Infrastruktur erforderlich.

Problem 1: Die Rahmenbedingungen

Die Rahmenbedingungen für die Einführung der Telematikinfrastruktur sind noch unscharf und veränderlich. Daraus resultiert auch eine Zurückhaltung klinischer Rechenzentren bei der Vorbereitung der perspektivisch erforderlichen Integrationsleistung. Das Fundament für die Einführung der elektronischen Gesundheitskarte bilden folgende Gesetze:

- das GKV-Modernisierungsgesetz

[1] http://www.gematik.de/

- die entsprechenden Paragraphen des SGB V
- das Signaturgesetz

Der Inhalt der Gesetze ist dem Projektteam am UKL bekannt. Ein wichtiger Punkt in §291a SGB V ist die Gründung der Gematik.

Die Gematik ist für Aufbau, den Betrieb und die Standardisierungen der Telematikinfrastruktur verantwortlich. Die Gematik arbeitet an der technischen Spezifikation der Komponenten und der Konzeption der Gesamtarchitektur. Die dabei getroffenen Entscheidungen müssen durch das Pilotprojekt am UKL berücksichtigt werden, um eine korrekte Funktion der Telematikanwendungen in der Testphase zu gewährleisten. Der aktuelle Stand dieser Arbeiten ist nicht bekannt und soll deshalb analysiert und bewertet werden.

Die Vorgaben der Gematik, bezüglich der Komponenten und der Gesamtarchitektur, werden in Modellregionen getestet. Dabei wird eine Integration der Telematikinfrastruktur in die betreffenden Krankenhäuser und Arztpraxen durchgeführt. Die fertigen Architekturen und die darin verwendeten technischen Konstrukte können als Vorbild für die eigene Zielarchitektur dienen. Es sollte versucht werden Probleme, die während der Integration auftraten zukünftig zu vermeiden oder sie mit Hilfe der Lösungsansätze aus den Testregionen zu lösen. Die Erfahrungen aus den Modellregionen sind dem Projektteam am UKL unbekannt und sollen analysiert werden.

In der Vergangenheit gab es in der Gematik große Probleme, Beschlüsse mit der dafür notwendigen 2/3-Mehrheit zu fällen. Um die Arbeit voranzutreiben, hat das Bundesministerium für Gesundheit und Soziales (BMGS) eine Rechtsverordnung erlassen, durch die der Gematik nun Weisungen zur Durchführung der Tests gegeben werden. Der genaue Inhalt der Rechtsverordnung ist unbekannt, muss aber durch das Testprojekt am UKL ebenfalls eingehalten werden.

Problem 2: Anforderungsspezifikation

Aus der Unsicherheit über die Rahmenbedingungen resultiert auch, dass kein Lösungsvorschlag für die Integration der Telematikinfrastruktur ins UKL existiert. Da nur das Klinikum selbst eine Zielarchitektur spezifizieren kann und nicht zu erwarten ist, dass in naher Zukunft Hilfen für diese Aufgabe entwickelt werden, sollte dies so schnell wie möglich geschehen, um zukünftige Entwicklungen der Gematik zeitnah umsetzen zu können und nicht in einen Umsetzungsstau zu laufen.

Problem 3: Referenzmodell

Bisher gibt es kein Muster für die Integration der Telematikinfrastruktur in ein Gesundheitsunternehmen. Daraus resultiert eine Unsicherheit über die zu verwendenden technischen Konstrukte und die anzustrebende Zielarchitektur.

Für die Ausweitung des Pilotprojektes auf weitere Teile des UKL und für andere Häuser ist ein Muster interessant, weil es die Systemspezifikation für Nachfolgeprojekte stark vereinfacht. Durch das Mustermodell wird auf bereits bekannte Probleme und die zugehörigen Lösungsansätze hingewiesen. Dadurch können bei der Systemspezifikation Ressourcen gespart werden, die dann wiederum zur Verbesserung des Mustermodells eingesetzt werden können.

1.3 Zielsetzung

- Ziel 1 Überblick über die Inhalte der Rechtsverordnung, den Stand der Arbeiten der Gematik (technischen Spezifikationen, Konzeption der Gesamtarchitektur) und die Erfahrungen aus den Testregionen.
- Ziel 2 Sollkonzept für die Integration der Telematikinfrastruktur in das UKL
- Ziel 3 3LGM²-Referenzmodell zur Integration der Telematikinfrastruktur.

1.4 Aufgaben-/Fragestellung

- Arbeitspaket 1: Erarbeitung der Rahmenbedingungen

Es soll ein Überblick über die gesetzlichen Vorgaben, die das Fundament der Einführung der elektronischen Gesundheitskarte bilden, gegeben werden. Es muss besonders auf Aspekte der Sicherheit und des Datenschutzes geachtet werden. Hier liefert das SGB V, das Bundesdatenschutzgesetz sowie das Signaturgesetz wichtige Informationen.

Die bisherige Arbeit der Gematik ist zu untersuchen. Es sollen die technischen Spezifikationen und die Architekturspezifikationen analysiert und bewertet werden. Für Teile dieser Dokumente, die noch in Bearbeitung sind, sollen die vorläufigen Ergebnisse erarbeitet werden um Fehlentwicklungen, die zusätzliche Kosten verursachen, im eigenen Projekt zu verhindern.

Zu den Aufgabenbereichen der Gematik zählt auch das Durchführen von Tests. Das Testkonzept und die Testplanung sollen untersucht werden, um festzustellen wie die Telematikinfrastruktur in nächster Zeit wachsen wird. Ein Teil der Festlegungen zu den Tests wurde durch eine Rechtsverordnung des BMGS getroffen. Diese ist ebenfalls zu betrachten.

Die Fortschritte bei der Integration der Telematikinfrastruktur in die Modellregionen sind von besonderer Relevanz, um auf den gewonnenen Erfahrungen aufzubauen und bereits gefundene Lösungsansätze zu verfeinern.

- Arbeitspaket 2.1: Analyse des Ist-Zustands am UKL

  Vor der Spezifikation der Lösungsarchitektur müssen die technischen und organisatorischen Gegebenheiten sowie besonderen Anforderungen des UKL analysiert werden. Dabei soll besonders das Sicherheitskonzept betrachtet werden. Der Ist-Zustand ist zu modellieren und in Bezug auf die Eignung für die neuen Anwendungen zu bewerten.

- Arbeitspaket 2.2: Erstellen eines Anforderungskatalogs für die Lösungsarchitektur (Soll-Zustand)

  Unter Beachtung der Rahmenbedingungen und des in Arbeitspaket 2.1 beschriebene Ist-Zustand müssen nun die Anforderungen für eine Integration der Telematikinfrastruktur ins UKL erarbeitet werden. Insbesondere ist der Bereich Sicherheitsanforderungen zu beleuchten, dabei sind Einsatzmöglichkeiten für elektronische Signatur herauszuarbeiten. Aus den gefundenen Anforderungen ist ein Lösungsvorschlag für die Integration der Telematikinfrastruktur auszuarbeiten und zu modellieren.

- Arbeitspaket 3: Erstellung eines 3LGM²-Referenzmodells

  Die Lösungsarchitektur des UKL soll zu einem Referenzmodell verallgemeinert werden. Aus diesem Modell lassen sich dann konkrete Modelle für weitere Teile des UKL oder andere Häuser ableiten, was das Erstellen weiterer Soll-Zustände stark vereinfacht und zur Kostenminimierung beiträgt.

2 Grundlagen

2.1 Elektronische Gesundheitskarte (eGK)

Das Gesetz zur Modernisierung der gesetzlichen Krankenkasse trat am 1.1.2004 in Kraft. Dieses Gesetz bringt Änderungen ins Sozialgesetzbuch V ein, durch die unter anderem die Einführung der elektronischen Gesundheitskarte und die Gründung der Gematik geregelt werden.

Nach §291a des SGB V muss die elektronische Gesundheitskarte folgende Anwendungen unterstützen:

a) Nachweis der Berechtigung zur Inanspruchnahme von Leistungen;

b) Übermittlung von ärztlichen Verordnungen in elektronischer und maschinell verwertbarer Form (elektronisches Rezept);

c) Medizinische Daten zur Notversorgung;

d) Befunde, Diagnosen und Therapieempfehlungen für einrichtungsübergreifende fallbezogene Kooperation (elektronischer Arztbrief);

e) Daten zur Überprüfung der Arzneimitteltherapiesicherheit;

f) Daten über Diagnosen, Befunde, Therapiemaßnahmen, Behandlungsberichte und Impfungen für eine einrichtungs- und fallübergreifende Dokumentation (elektronische Patientenakte);

   a. durch vom Versicherten selbst oder für sie zur Verfügung gestellte Daten;

   b. Daten über in Anspruch genommene Leistungen und deren Kosten;

Auf diese Anwendungen soll im Folgenden näher eingegangen werden. Die Angaben wurden, wenn nicht anders vermerkt, aus den Veröffentlichungen des Bundesministeriums für Gesundheit [BMG] entnommen.

2.1.1 Versichertendaten

Die elektronische Gesundheitskarte enthält nach SGB V §291 folgende Daten:

- Krankenkasse,
- Name und Anschrift des Versicherten,
- Geburtsdatum und Geschlecht,
- Krankenversichertennummer, Versichertenstatus, Zuzahlungsstatus,
- Lichtbild, Unterschrift,
- Datum des Beginns des Versicherungsschutzes.

Mit Hilfe dieser Daten kann nach [FK_VSDM] die Berechtigung zur Inanspruchnahme von Leistungen geprüft werden. Diese Anwendung ist für alle Versicherten verpflichtend und stellt die Funktionalität der bisherige Krankenkassenkarte zur Verfügung. Bei vorhandenem Netzzugang können die Versichertenstammdaten auf der Karte auf Aktualität geprüft und gegebenenfalls mit den beim Kostenträger gespeicherten Daten aktualisiert werden. Die Rückseite der Karte dient als Europäische Krankenversicherungskarte. Sie ersetzt den Auslandskrankenschein innerhalb der EU und ermöglicht eine unkompliziertere Behandlung in diesen Ländern.

2.1.2 Das elektronische Rezept (eRezept)

Das elektronische Rezept dient der Vermeidung von Medienbrüchen bei der Übermittlung von ärztlichen Verordnungen. Bisher wurde bei der Verordnung von Medikamenten oder Leistungen mittels EDV ein Papierrezept erstellt. Dieses Papierrezept transportierte der Patient zum Leistungserbringer, der es dann zu Abrechnungszwecken wieder elektronisch verfügbar machte.

Mit der Einführung der elektronischen Gesundheitskarte wird dieses Verfahren durchgängig elektronisch ablaufen, da das elektronische Rezept zu den Pflichtanwendungen gehört. Mit der elektronischen Gesundheitskarte wird der Arzt das Rezept elektronisch erstellen und auf einem Server in der Telematikinfrastruktur ablegen. Der Leistungserbringer kann dann mit Hilfe der Gesundheitskarte des Patienten das eRezept vom Server abholen und direkt zur Abrechnung nutzen. Für die Durchführung des Verfahrens sind folgende Funktionen erforderlich [T-Stich]:

- Verordnung einfügen;
- Verordnungsliste per PIN oder per HBA anzeigen;
- Verordnung lesen;
- Verordnung einlösen;
- Verordnung sichtbar machen oder verbergen;
- Verordnung reservieren oder freigeben;
- Verordnung mit Zugangstoken abrufen.

Die Erstellung eines Rezeptes läuft nach [FK_VODM] folgendermaßen ab:

1. Auswahl eines Medikaments und Erstellen eines eRezepts für den Patienten. Das eRezept besteht aus den Versichertendaten, den Verordnungsdaten und den Daten des Verordners;
2. Abgleich mit der Arzneimitteldokumentation um unerwünschte Nebenwirkungen zu vermeiden;
3. Signieren des eRezepts mit der qualifizierten elektronischen Signatur des elektronischen Heilberufeausweises;
4. Verschlüsseln des eRezepts mit dem öffentlichen Schlüssel der eGK;
5. Überprüfung der Schreibberechtigung;
6. Speichern des Rezeptes auf der eGK oder auf einem Server der Telematikinfrastruktur;
7. Eventuell drucken eines Papierbelegs.

Nun hat der Patient die Möglichkeit wie bisher sein Rezept bei einer Apotheke oder im Versandhandel einzulösen.

Das Einlösen des Rezepts läuft nach [FK_VODM] dann folgendermaßen ab:

1. Prüfung der Zugriffsberechtigung;
2. Abrufen und Entschlüsseln des Rezeptes von der eGK oder mittels eGK oder Papierbeleg vom Server der Telematikinfrastruktur;
3. Gültigkeit der Verordnung prüfen (Signatur der Verordnung, Datum...);
4. Prüfung und Ergänzung der Arzneimitteldokumentation;
5. Löschen des Rezeptes von der eGK;
6. Ergänzung der Daten des Einlösers;
7. Signieren des eRezeptes durch den Einlöser;

8. Verschlüsseln des eingelösten Rezeptes mit dem öffentlichen Schlüssel der Abrechnungsstelle;
9. Übermittlung der Abrechnung zu einem Server.

Ein Modellierung der Abläufe zum Erstellen und Einlösen von elektronischen Rezepten wird in Kapitel 3.1.10 Modellierung des Architekturkonzeptes durchgeführt.

2.1.3 Medizinische Daten zur Notversorgung

Der Notfalldatensatz soll helfen im Notfall eine optimale Versorgung zu gewährleisten. Da der Notarzt am Unfallort den Patienten nicht kennt, ist es wichtig, dass er schnell einen Überblick über die wichtigsten Daten des Patienten erhält. Ist der Patient nicht ansprechbar und somit nicht in der Lage selbst Auskunft zu geben, ist es für den Notarzt schwierig diese Informationen zu erhalten. Der Notfalldatensatz kann helfen diese Daten zu bekommen. Er wird direkt auf der Karte gespeichert und kann nach [BMG] folgende Informationen enthalten:

- Blutgruppe,
- Diagnosen z.B. Allergien, chronische Organleiden, vorhanden Grunderkrankungen (Asthma, Herzkrankheiten),
- Arzneimittelunverträglichkeiten,
- Schutzimpfungen,
- Informationen zu Operationen und anderen Therapien, die im Notfall relevant sein können,
- eingenommene Medikamente, die im Notfall relevant sein können,
- Kontaktdaten zu nahestehenden Menschen oder dem behandelnden Arzt,
- sowie Hinweis auf Organspenderausweis oder Patientenverfügung.

Neben der Verbesserung der Qualität der Versorgung im Notfall, können diese Daten auch bei der Verordnung von Medikamenten wichtig sein, um nicht erwünschte Nebenwirkungen zu vermeiden.

Diese Anwendung ist nach [BMG] freiwillig und kann ohne Netzzugang verwendet werden. Der Datensatz kann nur nach direkter Autorisierung durch den Patienten geschrieben werden. Patient entscheidet selbst welche Daten über ihn gespeichert werden. Das Lesen der Daten ist für Angehörige aller Heilberufe möglich um im Notfall schnell Zugang zu den notwendigen Daten zu bekommen.

2.1.4 Daten zur Überprüfung der Arzneimitteltherapiesicherheit

Eine weitere freiwillige Anwendung ist die Arzneimitteldokumentation. In der Arzneimitteldokumentation werden nach [BMG] alle eingenommenen Medikamente gespeichert. Beim Verordnen weiterer Medikamente kann ein Arzt drauf zurückgreifen um mögliche Wechselwirkungen zu erkennen und somit Behandlungsfehler zu vermeiden.

2.1.5 Elektronischer Arztbrief

In Deutschland werden nach der Behandlung eines Patienten im Krankenhaus oder beim Facharzt die Diagnosen, Befunde und Prozeduren in einem Arztbrief zusammengefasst. Dieses Dokument dient der Kommunikation der behandelnden Ärzte untereinander und soll zukünftig mit Hilfe der elektronischen Gesundheitskarte übertragen werden. Der Patient kann nach [BMG] die in der Telematikinfrastruktur gespeicherten Arztbriefe freiwillig und selbstbestimmt den weiterbehandelnden Ärzten zur Verfügung stellen und so zur Verbesserung seiner Behandlung beitragen.

2.1.6 Elektronische Patientenakte (ePA)

Die elektronischen Patientenakte (ePA) bildet nach [BMG] die letzte Ausbaustufe der elektronischen Gesundheitskarte. Sie wird verschiedene medizinischen Daten eines Patienten enthalten. Neben der Arzneimitteldokumentation und dem elektronischen Arztbrief können in Zukunft Laborbefunde, Bilddaten, Operationsberichte und Daten anderer Untersuchungen gespeichert werden. Ziel ist der Aufbau einer vollständigen elektronischen Patientenakte, die eine gute Informationsbasis für den behandelnden Arzt darstellt. Daten können durch den Patienten selbst und durch den behandelnden Arzt in die ePA eingebracht werden. Der Patient entscheidet welche Dokumente in der elektronischen Patientenakte abgelegt werden und auf welche Dokumente der Arzt Zugriff erhält. Der Arzt bekommt dann mit Zustimmung des Patienten einen klar geregelten Zugriff auf die Daten, die der Patient für ihn freigegeben hat.

Ziel der elektronischen Patientenakte ist eine Verbesserung der einrichtungsübergreifenden Versorgung der Patienten. Durch die Vermeidung von teuren Doppeluntersuchungen trägt es zur Erhöhung der Effizienz der Versorgung bei.

2.2 Elektronischer Heilberufeausweis

Mit der Einführung der elektronischen Gesundheitskarte (eGK) wird auch die Einführung des elektronischen Heilberufeausweises(HBA) notwendig, da nach SGB V §291a Absatz 5 der Zugriff auf die Daten auf der eGK nur in Verbindung mit dem HBA erlaubt ist. Deshalb müssen alle Gesundheitsdienstberufe mit HBAs ausgestattet werden, um die eGK nutzen zu können.

Der HBA muss über eine qualifizierte elektronische Signatur verfügen. Zusätzlich ist das von der zuständigen Stelle bestätigte Attribut "Arzt", "Apotheker" in der Signatur eingebettet, um die Zugriffsberechtigung aufgrund der medizinischen Qualifikation zu prüfen. Es handelt sich nach [Hauser 2005] beim HBA also um ein qualifiziertes Schlüsselzertifikat mit Attributzertifikat .

Es gibt nach [Hauser 2005] 2 Typen von HBA: den personenbezogenen HBA und die Security Module Card (SMC) Typ A. Der personenbezogene HBA ist ein Sichtausweis. Er wird als elektronischer Ausweis für Online-Verbindungen, zum Aufbringen einer elektronischen Signatur und zur Entschlüsselung von Nachrichten für den Karteninhaber benötigt. Die SMC ist institutionsbezogen und hat die gleichen Funktionen wie der personenbezogenene HBA auf Institutionsebene. Sie dient außerdem der Erzeugung eines sicheren Tunnels für das VERSA-Konzept.

Durch das VERSA-Konzept (Verteilte Signatur Arbeitsplätze) soll nach [VERSA] die Möglichkeit gegeben werden, dass der HBA an zentraler Stelle gesteckt wird und von verschiedenen Arbeitsplätzen bedient werden kann. Dadurch soll es in Krankenhäusern und Apotheken möglich werden, dass ein Benutzer mehrere Arbeitsplätze hat, beziehungsweise mehrere Benutzer den selben Arbeitsplatz verwenden ohne das ständig wieder das Einstecken der Karte und das Eingeben der PIN nötig wird. VERSA sieht vor, dass der personenbezogene HBA an zentraler Stelle gesteckt wird. Möchte der Arzt nun z.B. eine Verordnung signieren, wird mit Hilfe einer SMC am Arbeitsplatz ein Trusted Channel zum HBA aufgebaut. Der Schutz der Remote-Verbindung erfolgt durch einen logischen Trusted Channel. Durch Eingabe der PIN des HBA wird die Karte für diesen Kanal freigeschaltet. Nun kann z.B. durch ein biometrisches Verfahren oder durch Eingabe einer Paraphe eine Verordnung signiert werden.

Den Herausgeber für die Heilberufeausweise legen nach SGB V die Länder fest.

2.3 Datenschutz und Datensicherheit

Die Daten der elektronischen Gesundheitskarte werden durch das Bundesdatenschutzgesetz [BDSG03] gesichert. Das Bundesdatenschutzgesetz gewährleistet einen sehr umfassenden Schutz der personenbezogenen Daten, da es eine Datenverarbeitung und Datenspeicherung verbietet, wenn sie nicht durch Gesetze oder Zustimmung des Patienten erlaubt wird. Der Patient hat das Recht, zu erfahren, welche Daten gespeichert sind und aus welchem Grund sie gespeichert sind. Er kann fehlerhafte Daten korrigieren lassen, die Weitergabe der Informationen untersagen und sogar eine

Sperrung oder Löschung der Daten veranlassen. Die Auskunft kann unter bestimmten Umständen verweigert werden, z.B. zur Wahrung des Geschäftsgeheimnisses u.ä. Außerdem sind bestimmte Institutionen von der Auskunftspflicht freigestellt.

Die Einhaltung des Bundesdatenschutzes ist auch im Sozialgesetzbuch [SGB V] verankert.

Die Erhebung, Verarbeitung und Nutzung der Daten der elektronische Gesundheitskarte darf nur nach Einwilligung des Versicherten und wenn es für die Versorgung des Patienten notwendig ist, erfolgen. Die Einwilligung wird auf der Karte dokumentiert, kann auf bestimmte Funktionen beschränkt werden und ist jederzeit widerruflich. Es wird außerdem die Möglichkeit geben die gespeicherten Daten über eKiosks einzusehen und die Daten nur für bestimmte Personen sichtbar zu machen. Der Versicherte kann auch die Löschung aller nicht abrechnungsrelevanter Daten verlangen. Abrechnungsrelevante Daten sind die Versichertenstammdaten und eRezepte. Durch diese Regelungen wird gewährleistet, dass der Patient "Herr seiner Daten" bleibt und die Rechte des Patienten nachdem BDSG gewahrt bleiben.

Die Daten dürfen nur durch Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten erhoben, verarbeitet und genutzt werden. In Krankenhäusern dürfen Gehilfen und zur Vorbereitung auf den Beruf tätige Personen unter Aufsicht ebenfalls Zugriff auf die Daten erhalten. Zur Verarbeitung des elektronischen Rezepts sind auch sonstige Leistungserbringer berechtigt Die Kontrolle der Zugriffsberechtigung erfolgt über den elektronischen Heilberufeausweis. Nach dem Bundesdatenschutzgesetz haben auch die Versicherten das Recht ihre Daten zuzugreifen.

Der Zugriff auf die Daten darf nur mit elektronischer Gesundheitskarte und elektronischem Heilberufeausweis (HBA) gemeinsam möglich sein. Die Nutzung der freiwilligen Daten darf nur nach Autorisierung durch den Versicherten erlaubt werden. Zugriff auf das elektronische Rezept kann auch erfolgen, wenn der Versicherte diesen mit einem geeigneten technischen Verfahren autorisiert. Die Einhaltung dieser Regeln muss durch technische Vorkehrungen, wie zum Bespiel ein PIN-Verfahren gewährleistet werden.

Zur Datenschutzkontrolle müssen nach SGB V die letzten 50 Zugriffe auf die Daten protokolliert werden. Diese Daten dürfen nur für die Datenschutzkontrolle genutzt werden und müssen vor Missbrauch geschützt werden. Das Zugriffprotokoll kann deshalb nur mit Hilfe der PIN ausgelesen werden.

2.4 Elektronische Signatur

Um die Authentizität der Daten zu gewährleisten müssen sie mittels elektronischer Signatur verschlüsselt und signiert werden. Dadurch wird gesichert, dass die Daten nach dem Absenden nicht geändert beziehungsweise von Dritten eingesehen werden. Zu diesem Zweck verfügen die HBA über eine qualifizierte elektronische Signatur. Damit die Patienten selbst Daten in die elektronische Patientenakte einfügen können, erhalten sie ebenfalls eine Signaturkarte mit qualifizierter elektronischer Signatur.

Im Signaturgesetz [SigG] werden 4 Arten elektronischer Signaturen unterschieden:

1. einfache elektronische Signatur;
2. fortgeschrittene elektronische Signatur;
3. qualifizierte elektronische Signatur;
4. qualifizierte elektronische Signatur mit Anbieter- Akkreditierung.

Die einfache elektronische Signatur ist nicht zweifelsfrei einer Person zugeordnet, erfüllt keine besonderen Sicherheitsanforderungen und hat daher wenig Beweiswert.

Die fortgeschrittene elektronische Signatur hat nach dem Signaturgesetz folgende Eigenschaften:

- ausschließlich dem Schlüsselinhaber zugeordnet;
- dient der Identifizierung des Schlüsselinhabers;

- Der Schlüsselinhaber hat die alleinige Kontrolle über die Mittel zur Signaturerzeugung, das heißt nur der Schlüsselinhaber kennt den Signaturschlüssel;
- mit den Daten auf die sie sich bezieht, so verknüpft sein, dass man nachträgliche Veränderungen erkennen kann. Damit ist die Integrität der Daten gewährleistet.

Die qualifizierte elektronische Signatur ist nach [SigR] rechtlich mit der eigenhändigen Unterschrift gleichgestellt. Sie hat zusätzlich zu den Eigenschaften der fortgeschrittenen elektronischen Signatur, folgende Eigenschaften:

- Identität des Unterzeichners durch qualifiziertes Zertifikat erkennbar machen;
- Erstellung der Signatur mit einer sicheren Signaturerstellungseinheit (Chipkarte).

Qualifizierte Zertifikate dürfen nach [SigG] nur durch Zertifizierungsdiensteanbieter (ZDA) ausgestellt werden. Der ZDA erzeugt den Signaturschlüssel und den Signaturprüfschlüssel in einer sicheren Umgebung. Der Signaturschlüssel wird unauslesbar auf einer Chipkarte gespeichert. Dann werden Signaturschlüssel und Identifikationsdaten in einem qualifizierten Zertifikat zusammengefügt und durch eine qualifizierte elektronische Signatur des ZDA bestätigt. Für den Heilberufeausweis erzeugt der ZDA zusätzlich das Attributzertifikat für den Heilberuf.

ZDA sind nach dem Signaturgesetz verpflichtet den Beginn des Betriebes bei der zuständigen Stelle anzuzeigen. Dabei muss ein Sicherheitskonzept vorgelegt werden. Im Sicherheitskonzept muss nach §4 [SigG] die erforderliche Zuverlässigkeit, Fachkunde, eine Deckungsvorsorge und die Erfüllung weiterer gesetzliche Voraussetzungen nach dem Signaturgesetz und der Signaturrichtlinie nachgewiesen werden. Deckungvorsorge heißt nach §12 [SigG], dass der ZDA mindestens 250000€ zur Verfügung haben muss, um seiner Schadenersatzpflicht nach §11 [SigG] nachzukommen. Die zuständige Behörde ist die Regulierungsbehörde für Telekommunikation und Post, die am 13.07.2005 in Bundesnetzagentur (BNetzA) umbenannt wurde.

Die höchsten Anforderungen erfüllt die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung. Sie unterscheiden sich laut §15 [SigG] von qualifizierten elektronischen Signaturen darin, dass der Zertifizierungsdienstanbieter die organisatorische und technische Sicherheit durch ein Gütesiegel nachweist. Für die Akkreditierung ist die Bundesnetzagentur zuständig.

Da Rezepte und Arztbriefe bisher durch den Arzt unterschrieben wurden, muss nun für die elektronische Realisierung das elektronische Äquivalent, die qualifizierte elektronische Signatur, verwendet werden um die Beweiskraft der Dokumente zu erhalten.

Für die Speicherung von Signaturschlüsseln und die Erstellung qualifizierter elektronischer Signaturen sind nach §17 [SigG] sichere Signaturerstellungseinheiten zu verwenden, die:

- Fälschungen der Signatur erkennbar macht;
- Verfälschungen der signierten Daten erkennbar macht;
- und unberechtigte Nutzung der Signaturschlüssel zur Signaturerstellung verhindern.

Bei der Prüfung einer qualifizierten elektronischen Signatur sind nach §17 [SigG] Signaturanwendungskomponenten zu verwenden, die zeigen:

- auf welche Daten sich die Signatur bezieht;
- ob die Daten verändert wurden;
- wer die Daten signiert hat;
- welchen Inhalt das zugehörige qualifizierte Zertifikat hat;
- welches Ergebnis die Nachprüfung des Zertifikats hatte.

Eine Signaturanwendungskomponente, die diese Anforderungen erfüllt, wird als Trusted Viewer bezeichnet.

Elektronische Signaturen verwenden das Public-Key-Verfahren. Für dieses Verfahren benötigt man ein Schlüsselpaar, welches aus Signaturschlüssel und Signaturprüfschlüssel besteht. Als erstes erzeugt man aus dem zu signierenden Dokument einen Hashwert, der wie ein digitaler Fingerabdruck eindeutig ist. Dieser Hashwert wird dann mit dem Signaturschlüssel verschlüsselt. Der Empfänger kann mit Hilfe des veröffentlichten Signaturprüfschlüssels die Signatur des Dokumentes testen. Die Zuordnung des Signaturprüfschlüssels zu einer Person wird bei der qualifizierten elektronischen Signatur durch das qualifizierte Zertifikat vorgenommen.

2.5 3LGM²-Modellierung

Das 3LGM²-Metamodell dient nach [3LGM²-HP] der Beschreibung, Bewertung und Planung von Informationssystemen im Gesundheitswesen. Es wurde vom Institut für Medizinische Informatik Statistik und Epidemiologie (IMISE) des UKL entwickelt. Die Abkürzung 3LGM heißt 3 Layer Graph-based Meta Modell. Bei der Modellierung mit dem 3LGM²-Metamodell entstehen demzufolge Graphen mit 3 Ebenen. Die 3 Ebenen repräsentieren 3 statische Sichtweisen auf das Informationssystem. Folgende Ebene werden im 3LGM²-Metamodel definiert:

- Fachliche Ebene,
- Logische Werkzeugebene,
- und Physische Werkzeugebene.

Um die Ebenen untereinander zu verknüpfen wurden Inter-Ebenen-Beziehungen definiert.

Die für das 3LGM²-Metamodell notwendigen Sprachkonzepte wurden mit UML-Klassendiagrammen beschrieben. Die Diagramme können im Anhang nachgeschlagen werden. Im folgenden sollen die Ebenen des 3LGM²-Metamodells näher beschrieben werden. Die Angaben wurden aus [Winter 2002] entnommen.

Auf der fachlichen Ebene werden Aufgaben eines Unternehmens modelliert. Die Aufgaben können in Teilaufgaben zerlegt werden, um einen höheren Detaillierungsgrad zu erreichen. Für die Erledigung der Aufgaben werden Informationen benötigt und es entstehen Informationen. Diese Informationen werden in Form von Objekttypen repräsentiert, die durch Aufgaben interpretiert bzw. bearbeitet werden können. Die Aufgaben können auf fachlicher Ebene bestimmten Organisationseinheiten des Unternehmens zugeordnet werden, in denen sie erledigt werden. Bei der Erledigung der Aufgaben werden die Mitarbeiter eines Unternehmens durch informationsverarbeitende Werkzeuge unterstützt. Auf logischer Werkzeugebene werden logische Werkzeuge in Form von Anwendungsbausteinen dargestellt. Die Anwendungsbausteine können in rechnergestützte und konventionelle Anwendungsbausteine eingeteilt werden. Rechnergestützte Anwendungsbausteine sind installierte und adaptierte Softwareprodukte, die eine Aufgabe teilweise oder komplett unterstützen. Konventionelle Anwendungsbausteine sind Organisationspläne oder papierbasierte Verfahren zur Erledigung von Aufgaben. Die Zuordnung zwischen Aufgaben und Anwendungsbausteinen wird über Anwendungsbausteinkonfigurationen vorgenommen. Eine Anwendungsbausteinkonfiguration beschreibt, welche Aufgabe durch welche Anwendungsbausteine gemeinsam unterstützt wird. Anwendungsbausteinkonfigurationen werden durch Inter-Ebenen-Beziehungen dargestellt. Weiterhin wird auf logischer Ebene dargestellt, wo die Objekttypen logisch gespeichert werden und wie die Anwendungsbausteine kommunizieren müssen, damit der Zugriff auf die benötigten Informationen ermöglicht wird. Im rechnerbasierten Fall werden Objekttypen durch Datensatztypen repräsentiert, im konventionellen Fall durch Dokumenttypen. Die Datensätze eines Datensatztyps werden in Datenbanken gespeichert, die Dokumente eines Dokumententyps in Dokumentensammlungen. Datenbanken und Dokumentensammlungen werden ebenfalls im Graph dargestellt. Die Kommunikation zwischen Anwendungsbausteinen geschieht über Bausteinschnittstellen, über die Nachrichten gesendet werden. Aufgaben können Ereignisse eines Types auslösen, die das Versenden von Nachrichten steuern.

Zur Realisierung von logischen Werkzeugen werden physische Werkzeuge benötigt. Physische Werkzeuge sind ohne installierte logische Anwendungsbausteine nicht nutzbar. Die Zuordnung zwischen physischen Datenverarbeitungsbausteinen und den darauf installierten logischen

Anwendungsbausteinen erfolgt über Datenverarbeitungskonfigurationen, die als Inter-Ebenen-Beziehungen im Graphen dargestellt werden. Physische Datenverarbeitungsbausteine sind Systeme aus Personen und konventionellen Werkzeugen (Regal, Telefon, Briefkasten) bzw. Rechnersysteme (PC, Drucker, Switche, Router....).

Für die Modellierung von Krankenhausinformationssystemen mit dem 3LGM²-Metamodell wird der 3LGM²-Baukasten verwendet. Die 3LGM²-Modelle dieser Arbeit wurden mit Version 2.7 (P51) des 3LGM²-Baukastens erstellt.

3 Rahmenbedingungen

Zur Schaffung der für die Einführung und Nutzung der elektronischen Gesundheitskarte notwendigen, Telematikinfrastruktur wurde die Gesellschaft für Telematik (Gematik) gegründet. Eine Telematikinfrastruktur ist nach SGB V §291a Absatz 7 eine "interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur". Die Gematik trifft Reglungen zur Telematikinfrastruktur und übernimmt deren Aufbau und Betrieb. Es sollen einheitliche Schnittstellen und Dienste definiert werden, die eine Kommunikation zwischen Kostenträgern, Krankenhäusern, Arztpraxen, Apotheken und sonstigen Leistungserbringern ermöglichen.

3.1 Architekturkonzept

Die Gesamtarchitektur ist nach [BARCH] in eine Basisarchitektur und die Facharchitekturen gegliedert. Die Basisarchitektur stellt die anwendungsneutralen Kommunikations- und Infrastrukturdienste bereit. Die Facharchitekturen sind auf die fachlichen Anforderungen der entsprechenden Anwendungen zugeschnitten und nutzen die Basisarchitektur. Da die Telematikinfrastruktur erweiterbar sein soll und von den bereits bekannten Anwendungen noch nicht alle Use-Cases bekannt sind, ist es notwendig eine Abstraktion von speziellen Use-Cases auf allgemein nutzbare Kommunikationsmuster vorzunehmen. Die Basisarchitektur stellt die Umsetzung von Kommunikationsmustern bereit und bildet damit den technischen Rahmen in dem die Fachanwendungen unterstützt werden und zu spezifizieren sind.

Es wurde bisher folgende Kommunikationsmuster von der Gematik definiert:

- Wirkbetrieb einer Fachanwendung;
- Einwilligung und Bereitstellung einer bestehenden freiwilligen Anwendung für einen Benutzer;
- Ausbringung einer neuen freiwilligen Anwendung in die Telematikinfrastruktur.

Die Gematik entwickelt die Gesamtarchitektur der Telematikinfrastruktur. Sie definiert und spezifiziert die Komponenten und beschreibt die Beziehungen und Kommunikationsverbindungen zwischen den Komponenten. Ein weiteres wichtiges Arbeitsgebiet ist die Sicherheit der Telematikinfrastruktur, da dieser Punkt die Akzeptanz der Architektur bei Versicherten und Leistungserbringern stark beeinflusst.

Im Folgenden sollen die Komponenten und Konzepte der geplanten Gesamtarchitektur betrachtet werden. Eine Modellierung des Architekturkonzeptes mit 3LGM² wird in Kapitel 3.1.10 durchgeführt. Die Angaben sind wenn nicht anders vermerkt aus [BARCH] entnommen.

3.1.1 Primärsystem

Die medizinischen Anwendungen in den Gesundheitsunternehmen werden als Primärsystem bezeichnet. Sie liegen außerhalb der Telematikinfrastruktur und werden deshalb hier nicht anwendungs- und sicherheitstechnisch betrachtet. Sie nutzen eine plattform- und betriebssystemunabhängige Schnittstelle des Konnektors, um mit der Telematikinfrastruktur zu kommunizieren. Das Primärsystem kann über die Schnittstelle die Fachanwendungen der Telematikinfrastruktur nach §291a SGB V, die Mehrwertdienste und Basisdienste des Konnektors ausführen.

Der Aufruf eines Dienstes wird im Primärsystem angestoßen. Dabei wird ein Fachdienst der Konnektorabstraktionsschicht (Connector Abstraction Layer, CAL) aufgerufen. Die CAL ruft dann über die Primärsystem-Konnektor-Schnittstelle den entsprechenden Fachdienst des Konnektors auf. Die CAL bildet die Middleware zwischen Primärsystem und Konnektor. Die Anwendungen und

Dienste werden der CAL über Funktionsaufrufe zur Verfügung gestellt. Das Transportprotokoll für die Kommunikation ist nach [SP-KON] SOAP. Die Kommunikation des Primärsystems mit dem Konnektor erfolgt über SOAP-Requests. Die Antwort an den Konnektor ist ein SOAP-Response. Die Nutzdaten werden nach [I-PS] in XML-Dokumenten auf Basis des Kommunikationsstandards HL7 versendet. Es wird synchrone Kommunikation verwendet, asynchrone Kommunkation darf aber für die Zukunft nicht ausgeschlossen werden. Außerdem kann sich das Primärsystem nach [SP-KON] beim Konnektor registrieren um über bestimmte Ereignisse informiert zu werden. Das Senden der Ereignisse vom Konnektor zum Primärsystem erfolgt dabei über HTTP-Post-Requests.

3.1.2 Konnektor

Der Konnektor bildet die sichere Verbindung zwischen dem lokalen Netzwerk des Leistungserbringers und dem Netzwerk der Telematikinfrastruktur. Er ist die Systemgrenze der Telematikinfrastruktur und besitzt Schnittstellen zu einem oder mehreren Primärsystemen, zu den Kartenterminals mit den Karten und zu den zentralen Diensten der Telematikinfrastruktur. Seine Aufgabe ist es eine sichere Kommunikation zwischen Primärsystem, Karte und Telematikinfrastruktur zu ermöglichen.

Der Konnektor ist nach [T-Stich] in Anwendungskonnektor und Netzkonnektor gegliedert. Der Anwendungskonnektor implementiert die Anbindung des Primärsystems, der Karten und der Kartenterminals an die zentrale Infrastruktur auf logischer Ebene. Der Netzkonnektor realisiert die Kommunikation mit der zentralen Infrastruktur auf Netzwerkebene.

Der Konnektor stellt dem Primärsystem Fachdienste und Basisdienste zur Verfügung. Die Basisdienste des Konnektors sind nach [T-Stich] und [BARCH]:

- Verwaltung von Ressourcen wie die Suche;
- Abrufen von Beschreibungen von Ressourcen;
- Eindeutige Objekt-Identifikator (OID) abrufen;
- Kryptographiedienste:
    - Verifikation der Gültigkeit eines Zertifikates und eines Zeitstempels;
    - Anzeige eines Dokuments zur Signatur in einem Trusted Viewer;
    - sicherer Transport des Dokuments zur Signaturerstellung;
    - Stapelsignatur;
    - Signatur erzeugen und prüfen;
    - Authentisierung;
    - und Entschlüsselung.
- Kartendienste ;
- Kartenterminaldienste;
- Ereignisdienst (nur nach Registrierung für ein bestimmtes Ereignis);
- Netzwerkdienste: Firewall, Routing und VPN;
- Managementdienst: Wartung und Betriebssicherheit

Die Fachdienste des Konnektors beinhalten die Kommunikation mit der zentralen Telematikinfrastruktur und Primärsystem, sowie die Ablauflogik der Anwendungen. Dazu werden die Basisdienste des Konnektors genutzt. Der Konnektor unterstützt die Fachdienste der Telematikinfrastruktur bei der Nutzung der Kartenterminals mit den Karten. Der Konnektor stellt den korrekten Informationsfluss sicher und führt ein syntaktische Prüfung der Daten durch, bevor diese der zur Telematikinfrastruktur gelangen. Die Kommunikation mit dem zentralen Teil der Fachdienste

erfolgt nach [SP-KON] über die von diesen angebotenen und die vom Broker vermittelten Schnittstellen.

Für die Fachanwendungen, die auch ohne Verbindung zur zentralen Telematikinfrastruktur verfügbar sein müssen, übernimmt der Konnektor im Offline-Fall den kompletten Ablauf. Im Konnektor selbst werden aber keine medizinischen Daten dauerhaft gespeichert.

Der Konnektor bietet nach [SP-KON] die sichere zertifizierte Umgebung für die Signaturanwendung. Es sollten nur zugelassene und sicherheitszertifizierte Konnektoren verwendet werden, um dem Versicherten und Leistunserbringern die Gewissheit zu geben, dass Datenschutz und Sicherheitsstandards eingehalten werden. Nach dem Signaturgesetz muss für die Erstellung und Prüfung einer qualifizierten elektronischen Signatur ein Trusted Viewer zur Verfügung gestellt werden. Der Konnektor muss also eine Schnittstelle zu einem Trusted Viewer zur Verfügung stellen. Die Kommunikation erfolgt über HTTP(s)-Post-Requests. Der Konnektor blockiert den Signaturvorgang bis ein Response von der Singnaturanwendungskomponente eingegangen ist und bricht unter Umständen die Signatur ab. Es handelt sich also um synchrone Kommunikation.

Der Konnektor stellt für das Primärsystem einen authentisierten Zugang zur Telematikinfrastruktur zur Verfügung und bildet die einzige Verbindung des Primärsystems zur Telematikinfrastruktur. Die Zugriffe des Konnektors zur Telematikinfrastruktur werden protokolliert, um der Forderung des SGB V nachzukommen. Der Konnektor baut nur dann eine Verbindung auf, wenn das Primärsystem eine Verbindung initialisiert. Abbildung 3-1 zeigt, dass der Zugang zur Telematikinfrastruktur mit Hilfe einer VPN-Verbindung auf Basis von IPSec über das Internet hergestellt wird. Den Endpunkt der VPN-Verbindung bildet der VPN-Konzentrator. Das Schlüsselmaterial für den Aufbau der VPN-Verbindung befindet sich auf einer Secure Module Card (SMC) Typ B. Diese Karte ist Träger der kryptographischen Identität der Institution und ermöglicht so die Verschlüsselung von Dokumenten an die Institution. Die Verantwortung für den VPN-Tunnel trägt der logische Telematik-Zugangsprovider. Die kryptographische Identität des Konnektors wird deshalb durch den Telematik-Zugangsprovider ausgegeben. Zwischen dem Konnektor und der zentralen Telematikinfrastruktur existiert genau ein VPN-Tunnel über den mehrere unabhängige Kommunikationskanäle geroutet werden können. Es muss durch den Konnektor sichergestellt werden, dass die zentralen Dienste nicht auf das lokale Netzwerk zugreifen können. Bricht die VPN-Verbindung ab, muss der Konnektor automatisch versuchen diese wieder aufzubauen.

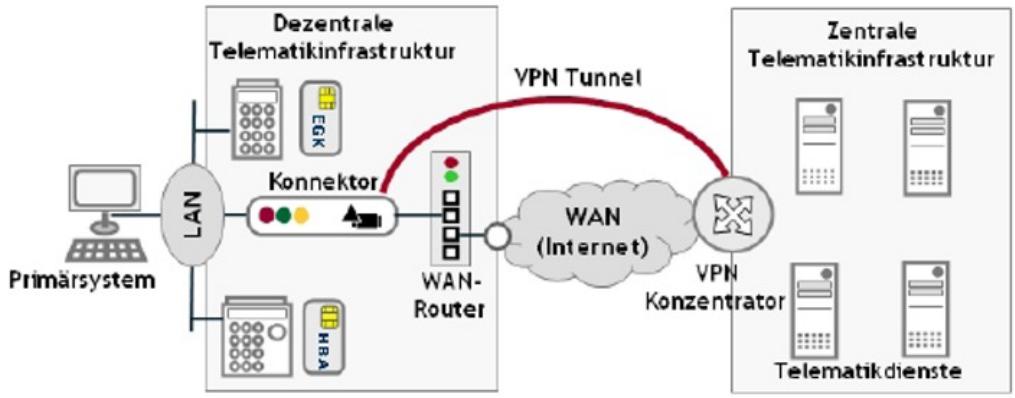


Abbildung 3-1: Nutzung des VPN Tunnels; Quelle: [SP-KON]

Der Konnektor stellt eine Managementschnittstelle zur Konfiguration, Wartung und Installation von Software zur Verfügung. Es gibt nach [T-Stich] eine lokale Schnittstelle und eine netzbasierte für das Systemmanagement über eine Servicezentrale. Ein zentrales Systemmanagement ist notwendig, da sehr viele Konnektoren im Einsatz sind, hohe Anforderungen an die Zuverlässigkeit gestellt werden und bei den Leistungserbringern häufig kein Personal für die Administration verfügbar ist. Die Schnittstelle stellt folgende Funktionen zur Verfügung:

- Meldung von Fehlern und Ausnahmesituationen vom Konnektor zur Servicezentrale
- Abfrage der Systemkonfiguration z.B. Einstellungen des Konnektors, installierte Softwarepakete

- Ändern der Systemkonfiguration, also das Bereitstellen von Softwareupdates

Mit Hilfe der lokalen Managementschnittstelle kann man zusätzlich zu den Möglichkeiten der netzbasierten Schnittstelle den Konnektor konfigurieren und Zugriff auf die Protokolldateien erhalten. Im Protokoll werden Daten zu Boot- und Resetvorgängen, zur VPN-Verbindung und zur SMC gespeichert.

Es kann außerdem eine Schnittstelle zur Online-Software-Aktualisierung geben. Diese Schnittstellen sind herstellerspezifisch. Bei allen Wartungsarbeiten ist sicherzustellen, dass die Zertifizierung des Konnektors nicht erlischt.

Der Zugriff auf die Dienste des Konnektors erfolgt ausschließlich über das Primärsystem. Der Betrieb des Konnektors muss ohne Eingriffe durch das Personal des Leistungserbringers möglich sein. Zur Unterstützung des Personals besitzt der Konnektor nach [SP-KON] geeignete Statusanzeigen anhand derer erkennbar ist, ob der Konnektor funktioniert und die Verbindungen zum lokalen Netzwerk und zur Telematikinfrastruktur aufgebaut sind. Die Statusanzeigen können z.B. LEDs am Konnektorgehäuse sein oder über die Managementschnittstelle realisiert werden. Der Konnektor muss den Dauerbetrieb bei den Leistungserbringern unterstützen und in kritischen Systemumgebungen eine ausfallsichere Konfiguration ermöglichen.

3.1.3 Kartenterminal

Die sichere Verbindung zwischen Konnektor, Chipkarte (HBA, eGK, SMC) und Benutzer wird mit Hilfe des Kartenterminals realisiert. Der Konnektor steuert und verwaltet die Kartenterminals über das Netzwerk des Gesundheitsunternehmens und stellt dem Primärsystem die Funktionen über die Konnektorschnittstelle zur Verfügung. Die Schnittstelle zwischen Konnektor und Kartenterminal wird über TCP/IP realisiert und ermöglicht:

- den Zugriff auf mehrere Kartenterminals/slots und mehrere Karten;
- die Kartenslots sind eindeutig adressierbar sind und einem Konnektor zugeordnet;
- gesteckte Karten sind eindeutig identifizierbar und lokalisierbar;
- Auflistung der aktuell gesteckten Karten;
- Koordination der Zugriffe auf Karten, so dass exklusive Zugriffe möglich sind;
- Aufbau eines Trusted Channels zur Karte (Secure Messaging);
- Ereignisübertragung und Nachrichtenanzeige auf bestimmten Terminals;
- Zuordnung von Karten und Kartenterminals zu bestimmten Arbeitsplätzen;
- Abstraktion herstellerspezifischer Kartenkommunikation;
- Abfrage des Funktionsumfangs.

In der Kartenterminalschnittstelle sind nach [T-Stich] drei Subsysteme identifizierbar. Das erste Subsystem ist die Clientkommunikation, die zwischen dem auslösenden System und dem Terminal stattfindet. Die Kommunikation läuft folgendermaßen ab:

1. Kartenterminal anhand seiner kryptographischen Identität zu authentisieren;
2. Auszuführende Transaktion zu übermitteln;
3. eventuelle Rückkommunikation während der Transaktion;
4. Transaktionsergebnisse zurückliefern.

Das 2. Subsystem ist der Eventkanal. Es handelt sich um einen aktiven Rückkanal zur Übermittlung betriebs- und sicherheitsrelevanter Ereignisse ohne vertrauliche Daten. Er besteht unabhängig von der Clientkommunikation und teilt hauptsächlich Kartensteckvorgänge und Kartenentfernungen mit.

Außerdem gibt es noch den Trusted-Channel für Kartenterminal-zu-Kartenterminal-Kommunikation. Bei der Card-To-Card-Authentication, die beim VERSA-Konzept benötigt wird, muss ein Trusted-Channel zwischen den beiden beteiligten Karten aufgebaut werden. Die PIN wird an einem Kartenterminal mit SMC Typ A eingegeben und über den Trusted-Channel verschlüsselt zum HBA im anderen Kartenterminal übertragen. Der Trusted-Channel wird entweder zwischen 2 Kartenterminals oder innerhalb eines Kartenterminals aufgebaut.

Die Anforderungen für das Kartenterminal werden nach [T-Stich] in der Spezifikation "eHealth-Kartenterminal-Spezifikation V 1.1.0"[SP-KT] beschrieben. Die Spezifikation basiert auf der SICCT-Spezifikation (Secure Interoperable ChipCard Terminal)[SICCT], die für die Nutzung im Gesundheitswesen erweitert beziehungsweise eingeschränkt wird. Die Spezifikation gibt exakte Vorgaben für zulässige technische Ausprägungen von Kartenterminals. Die Spezifikation enthält die technische Spezifikation auf Kommunikationsebene, eine Spezifikation auf Informationsebene und die Sicherheitsspezifikation. Es wird eine Basisfunktionalität mit dem minimalen Kartenterminaldiensten und –befehlen beschrieben.

Bei den Kartenterminals handelt es sich um netzwerkfähige Kartenterminals, die direkt an das Netzwerk angeschlossen werden. Werden die Kartenterminals über Drittkomponenten oder mit Kombigeräten ins Netzwerk integriert, müssen diese als virtuelle LAN-Kartenterminals betrieben werden, das heißt die Komponenten müssen ein netzwerkfähiges Terminal emulieren. Die Kommunikation zwischen Konnektor und Kartenterminal erfolgt über ein standardisiertes Protokoll. Die Kommunikation muss ohne die Installation eines kartenterminalspezifischen Treibers möglich sein.

Das Kartenterminal unterstützt Speicherchipkarten wie die abzulösende Krankenversicherungskarte und Prozessorchipkarten wie die eGK und der HBA. Diese Funktionalität ist in der Rollout-Phase besonders wichtig, da in dieser Phase Versicherte mit eGK und Versicherte mit Krankenversicherungskarte parallel versorgt werden müssen. Es kann damit vermieden werden, dass 2 Systeme parallel betrieben werden müssen und dadurch eventuell Seiteneffekte und Mehraufwand entstehen. Für die Architektur des Kartenterminals wird das Architekturmodell von Prozessorchipkarten nach ISO/IEC 7816 verwendet.

Das Kartenterminal besitzt technische Funktionen zur Anwenderauthentisierung, wie zum Beispiel KeyPad und biometrische Sensorik. Es muss in Verbindung mit einer geeigneten Signaturanwendungskomponente zur Erstellung von qualifizierten Signaturen verwendbar sein. Das Terminal besitzt ein oder mehrere Kartenkontaktiereinheiten in Normalgröße für HBA und eGK und zusätzlich Kontaktiereinheiten in Plugingröße für SMC.

Es ist eine eindeutige Benutzerführung erforderlich, um die Bedienbarkeit für alle Versicherten sicherzustellen. Es muss aus Sicherheitsgründen erkennbar sein, ob sich das Terminal in einem sicheren Modus befindet und somit nur mit vertrauenswürdigen Systemen kommuniziert. Es soll so verhindert werden, dass geheime Daten wie die PIN ausgespäht werden können. Die Sicherheitsanforderungen und die Stärke der Sicherheitsmechanismen werden in einem Schutzprofil festgelegt.

Um eine leichte Integrierbarkeit des Kartenterminals in Applikationen zu ermöglichen, sind die Details der Kommunikation und Ansteuerung der Chipkarten, der Benutzungsschnittstelle und die Transaktionssicherheit durch die Kartenterminalschnittstelle für Clientsysteme, wie zum Beispiel Primärsystem oder Konnektor, transparent zu halten. Gleichzeitig ist nach [T-Stich] auch die Erweiterbarkeit und Austauschbarkeit von Karten und Kartenapplikationen zu gewährleisten. Es ist zu berücksichtigen, dass über die Lebenszeit der Telematikinfrastruktur Erweiterungen und Anwendungen über Prozessorkarten ausgeführt werden können, die heute noch nicht absehbar sind. Deshalb sollte die Schnittstelle relativ unabhängig vom jetzigen Funktionsumfang. Diese Forderung verbietet nicht, dass es spezialisierte Zugriffsschichten gibt und schreibt auch nicht vor einen transparenten Kanal zur Karte zu verwenden.

Zukünftige Kartenterminals dürfen keine Anpassung der ansteuernden Logik erfordern. Des Weiteren muss die Ansteuerung durch Drittapplikationen möglich sein, um eine leichte Integration in Krankenhausinformationssysteme zu erlauben.

3.1.4 Karten

Die Karten dienen als Hilfsmittel zur funktionellen und sicheren Verbindung zwischen Benutzern und diesen Benutzern zugeordneten Daten.

Es sind derzeit vier Kartentypen vorgesehen:

- die elektronische Gesundheitskarte (eGK) für die Versicherten;
- der elektronische Heilberufeausweis (HBA bzw. BA) für alle Heilberufler, denen die Anwendungen der Telematikinfrastruktur zur Verfügung stehen sollen;
- Secure Module Card Typ A (SMC-A) als Stellverteter für den HBA in größeren Umgebungen;
- SMC Typ B als Träger für kryptographische Identitäten für den Konnektor und bei Bedarf durch die TI, durch Fachanwendungen oder durch Sicherheitsanforderungen auch für andere dezentrale Komponenten.

Die Interoperabilität ist durch folgende funktionale, sicherheitstechnische, organisatorische und operative Anforderungen gesichert.

Die Standardisierung der Chipkarten ist für einen interoperablen Betrieb erforderlich und basieren auf bestehenden Industriestandards, die durch weitere Vorgaben teilweise erweitert und teilweise eingeschränkt werden. Die Spezifikationen werden im Moment erstellt. Anforderungen für die Konzeption der Karten ergeben sich aus den gesetzlichen Gegebenheiten, die bereits im Kapitel Grundlagen behandelt wurden. Zur Sicherstellung der Interoperabilität wird ein Zulassungs- und Zertifizierungsverfahren eingeführt. Für die Zulassung ist eine sicherheitstechnische und funktionale Prüfung mit Zertifikaten notwendig. Die notwendigen Teilprüfungen und Teilzertifikate werden durch die Gematik festgelegt. Die erforderliche Performanz der auszugebenden Karten wird durch die Fachdienste, Anwendungen und die Leistungsfähigkeit der Chipkarten bestimmt. Bei der Abwägung Performanzanforderungen sind außerdem Kosten-Nutzenaspekte und die Akzeptanz der Benutzer zu berücksichtigen.

Um die Interoperabilität der Chipkarten zu erreichen, müssen diese der gleichen Spezifikation genügen. Die Spezifikation ist in mehrere Teile gegliedert. Den ersten Teil bildet die Betriebssystem-Schnittstelle. Sie beschreibt die Basisfunktionalität die einen bestimmten Funktionsumfang, Mechanismen und bestimmte Eigenschaften, insbesondere für die Sicherheitsmechanismen umfasst. In weiteren Teilen der Spezifikation wird beschrieben, wie die Fachdienste Daten, Funktionen und Mechanismen der Betriebssystem-Schnittstelle nutzen. Die Fachdienste werden unabhängig voneinander definiert, um die Migrationsfähigkeit des Systems nicht einzuschränken. Weiterhin werden Kartenmaterialien, Drucklayout und die Anforderungen an die Personalisierung einschließlich der zu personalisierenden Datenobjekte spezifiziert.

Es wird nach [T-Stich] vorausgesetzt, dass kartenseitig jede Version einer Anwendung identisch ist und damit jeder Konnektor die Anwendung unabhängig vom Kartentyp und Anwendungsanbieter verwenden kann. Die in den Testregionen ausgegebenen Chipkarten müssen von Beginn an migrationsfähig sein, um das Risiko eines erneuten Kartenaustauschs zu minimieren. Die Verwendung eines rudimentären CAMS (Card Application Management System) ist deshalb bereits in der Testphase notwendig.

CAMS dienen nach [T-Stich] der Verwaltung der Lebenszyklen von multifunktionalen Chipkarten insbesondere der eGK. Für die Testregionen sind die Funktionen und Prozesse zur Modifikation und Ergänzung der Datenstrukturen (Anwendungen) zur Verfügung zu stellen. Das CAMS verwaltet die kartenspezifischen Anwendung, so dass jede Anwendung nur auf einer der Karten des Versicherten vorkommen kann. In der Testphase besitzt jeder Versicherte nur eine Karte, später kann ein Versicherter auch mehrere Karten besitzen, aber zu jedem Zeitpunkt darf nur eine gültig sein. Die Karten sind dabei einem CAMS eindeutig zugeordnet. Für das CAMS werden Schlüsselmaterialien und -generatoren verwendet, die sich von denen für qualifizierte Signaturen unterscheiden. Das CAMS ist die einzige Instanz die den Schlüssel kennt, um die Datenstrukturen und Zugriffsrechte auf Rootebene zu ändern. Des Weiteren gibt es kartenspezifische Schlüssel, um die Applikationsstrukturen auf der Karte zu verändern. Die Anmeldung (binden) und Abmeldung (lösen)

von Anwendungen und die technische Einrichtung auf der eGK kann ebenfalls nur durch das CAMS durchgeführt werden. Die Anwendungsspezifischen Daten verwaltet nicht das CAMS sondern die Fachdienste. Das CAMS und die verschiedenen Anwendungsanbieter können über einen Verzeichnisdienst lokalisiert werden.

Das CAMS ist nach [T-Stich] an folgenden Prozessen beteiligt:

- Ausstellen einer neuen eGK;
- Verwaltung der Einwilligungen des Versicherten;
- Binden und Lösen von Anwendungen;
- Aufbringen, ändern und löschen der Applikationsstruktur (Datenstruktur, Zugriffsberechtigungen) auf die eGK;
- Import und Export der Anwendungskonfiguration bei Versicherungswechsel;
- Auskunftsfunktion für genutzte Anwendungen;
- Sperren einer eGK und Verteilung der Sperrinformationen;
- Verwaltung von Sperrinformationen.

3.1.5 Sicherheitskonzept

Die Sicherheit ist für die Akzeptanz der Telematikinfrastruktur von großer Bedeutung. Es wird ein gestuftes Sicherheitskonzept basierend auf Sicherheitszonen verwendet. In den verschiedenen Zonen werden unterschiedliche aufeinander abgestimmte Sicherheitskonzepte angewendet. Zonen mit hohen Sicherheitsanforderungen werden dadurch geschützt, dass der Zugriff nur aus bestimmten bereits geschützten Zonen erfolgen darf.

Abbildung 3-2 zeigt die geplanten Sicherheitszonen und die Datenflüsse, die administrativen Datenflüsse und die Netzverbindungen zwischen ihnen.

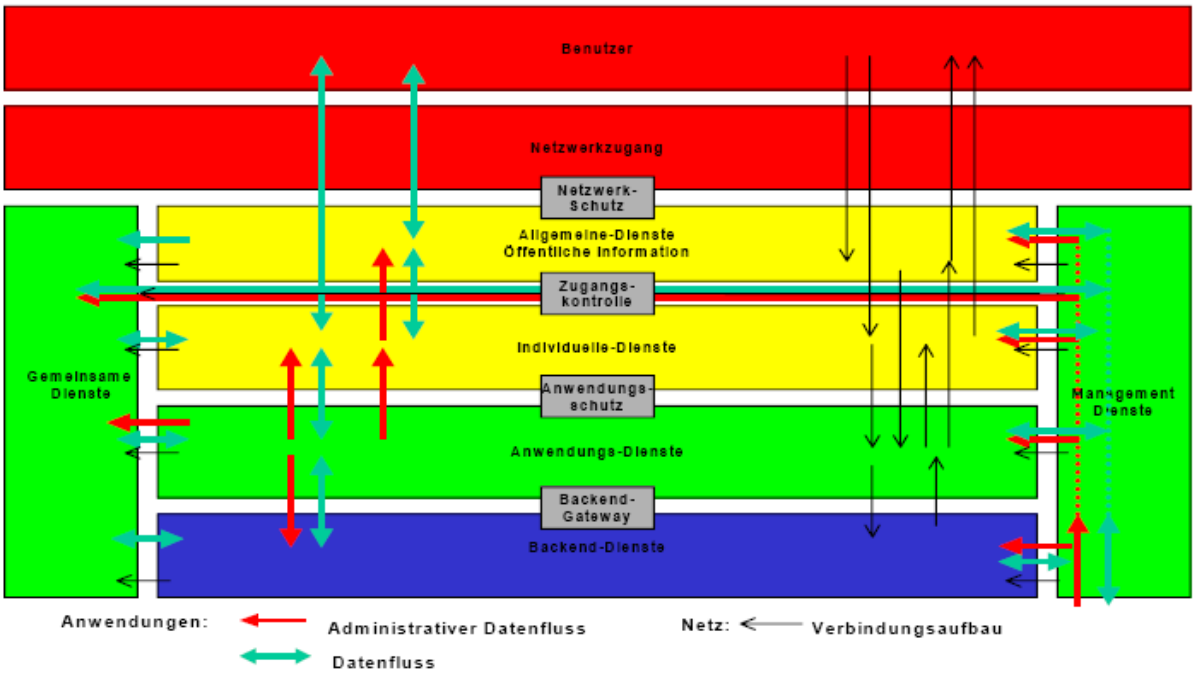


Abbildung 3-2: Sicherheitszonen; Quelle: [BARCH]

Bei einem solchen Konzept ist die Prüfung an den Zonengrenzen besonders wichtig. Es wird Prüfungen auf Applikationsebene und auf Netzwerkebene geben.

Die externen Zonen (rot) bilden den unsichersten Bereich. Es gibt keine Kontrollmöglichkeiten und unbekannte Verbindungen zu fremden Netzwerken. Es sind ausreichende Sicherheitsmaßnahmen zum Schutz vor Bedrohungen aus der externen Zone erforderlich.

Die Service-Zonen(gelb) beherbergt alle Komponenten, die eine direkte Kommunikation mit dem externen Bereich benötigen. In der Allgemeine-Dienste-Zone befinden sich Komponenten, die direkt mit der Außenwelt kommunizieren. Die Benutzer können direkt über TCP/IP auf die Dienste zugreifen und es gibt keine Benutzerauthentisierung. Durch die allgemeine Erreichbarkeit ist diese Zone sehr starken Bedrohungen ausgesetzt. Auf die Komponenten der Individuelle-Dienste-Zone können nur authentisierte Benutzer direkt zugreifen. Die Zugangskonrolle erfolgt in der Allgemeine-Dienste-Zone. Es wird die Autorisierung zum Zugriff auf die Anwendungen geprüft und gibt die Identität des Benutzers an die Anwendung weiter. Angriffe können in dieser Zone entdeckt und zurückverfolgt werden.

Die Komponenten der Support-Zonen (grün) überwachen die Dienste der Service-Zone, verarbeiten die Daten dieser Dienste weiter, beziehungsweise stellen Daten für diese bereit. Die Dienste werden unterteilt in Anwendungsdienste, gemeinsame Dienste und Managementdienste. In der Anwendungsdienstzone befinden sich die Speicher für sensitive Daten und die Server der Fachdienste. Die Zone ist durch Firewalls abgeschottet, so dass kein direkter Benutzerzugriff möglich ist. Die Gemeinsame-Dienste-Zone enthält Anwendungen, die von anderen Diensten genutzt werden können. Die Implementierung kann in verschiedenen LAN-Segmenten und Servern erfolgen. Durch diese Zone ist eine bessere Absicherung kritischer Systeme und Daten möglich. In der Managementdienst-Zone befinden sich Anwendungen zur Administration und Überwachung der Telematikinfrastruktur. Zugriff auf diese gesondert geschützten Anwendungen erhalten nur System- und Anwendungsadministratoren.

Die interne Zone (blau) ist der besonders gesicherte Bereich für interne Aufgaben. Hier befinden sich die Backend-Systeme und interne Server. Die Grenzen der Zone werden besonders kontrolliert und nur Administratoren erhalten Zugriff.

Der Konnektor nimmt in der Telematikinfrastruktur eine zentrale Rolle ein. Deshalb ist eine fundierte Analyse der Bedrohungen des Konnektors für die Sicherheit und Akzeptanz der Telematikinfrastruktur von entscheidender Bedeutung. Ausgehend von der Bedrohungsanalyse wurden in [T-Stich] folgende Sicherheitsfunktionen für den Konnektor identifiziert:

- Verwendung eines sicheren Tunnels zur Verbindung mit der Telematikinfrastruktur;
- Sicherheitsmechanismen in der Applikation;
- sichere Benutzerauthentisierung;
- Schutz der Integrität der Konnektorsoftware;
- sicheres Betriebsystem;
- Firewallfunktionalität, Intrusion Detection, Meldmechanismen;
- sichere Signaturanwendungskomponente;
- Fehlertoleranz;
- Sicherheitsmanagement.

Sicherheitsdienste werden nach [BARCH] dezentral durch den Konnektor und zentral in den Fachdiensten zur Verfügung gestellt. Das Primärsystem kann die Sicherheitsdienste des Konnektors über die Primärsystemschnittstelle nutzen. Die Sicherheit der übertragenen Daten in einer Transaktion wird auf Anwendungsebene unabhängig von Transport- und Netzwerkschicht gewährleistet. Die Zugriffskontrolle findet während der Transaktion im Fachdienst statt. In Abhängigkeit vom Fachdienst sind HBA, Authentisierung durch eGK und Autorisierung durch PIN-Eingabe notwendig. Das Schlüsselmaterial der beteiligten Karten ist bei jedem Zugriff online über OCSP (Online Certificate Status Protocol) zu prüfen. Aus Optimierungsgründen ist ein Caching der Gültigkeit für einen begrenzten Zeitraum möglich. Die Zugriffe werden protokolliert und bei Zugriffsverletzungen wird Sicherheitsalarm ausgelöst und das Sicherheitsmanagement benachrichtigt um weitere Maßnahmen einzuleiten.

Es muss nach [BARCH] ein Rechtemanagement auf Ebene einzelner Einträge eingeführt werden. Das komplette Verbergen von einzelnen Einträgen kann über die Fachanwendungen durch ein Rollenkonzept realisiert werden. Zeitversetzte Zugriffsverfahren sind über ein noch zu entwickelndes Ticketkonzept zu ermöglichen.

Eine übergreifende Public Key Infrastruktur (PKI) Architektur wird zentral für das Gesundheitswesen definiert. Es werden nach [BARCH] verschiedene PKI-Strukturen (Schlüsselpaare, Zertifikate, Zertifizierungsstellen(CA)...) für verschiedene Funktionen mit unterschiedlichen Sicherheitsniveaus verwendet. Die Public Key Strukturen für die Ausgabe von X.509-Zertifikaten werden als flache zweistufige Hierarchie implementiert. Die parallele Verwendung von Schlüsseln, Zertifikaten und Signaturen in der PKI des Gesundheitswesens und einer externen PKI sind nur möglich wenn die PK-Strukturen verbunden sind. Dies kann mit Hilfe einer Bridge-CA geschehen über die alle in die "Gematik Trust Service List" aufgenommenen Zertifizierungsstellen verbunden werden. Die "Gematik Trust Service List" definiert nach [SP-PKI] eine einheitliche Policy, um ein ausreichendes Sicherheitsniveau für die Zertifikate garantieren zu können. Durch dieses Konzept kann eine zentrale Abfrage von Zertifikatinformationen zur Überprüfung der Zertifikate ermöglicht werden.

3.1.6 Netzinfrastruktur

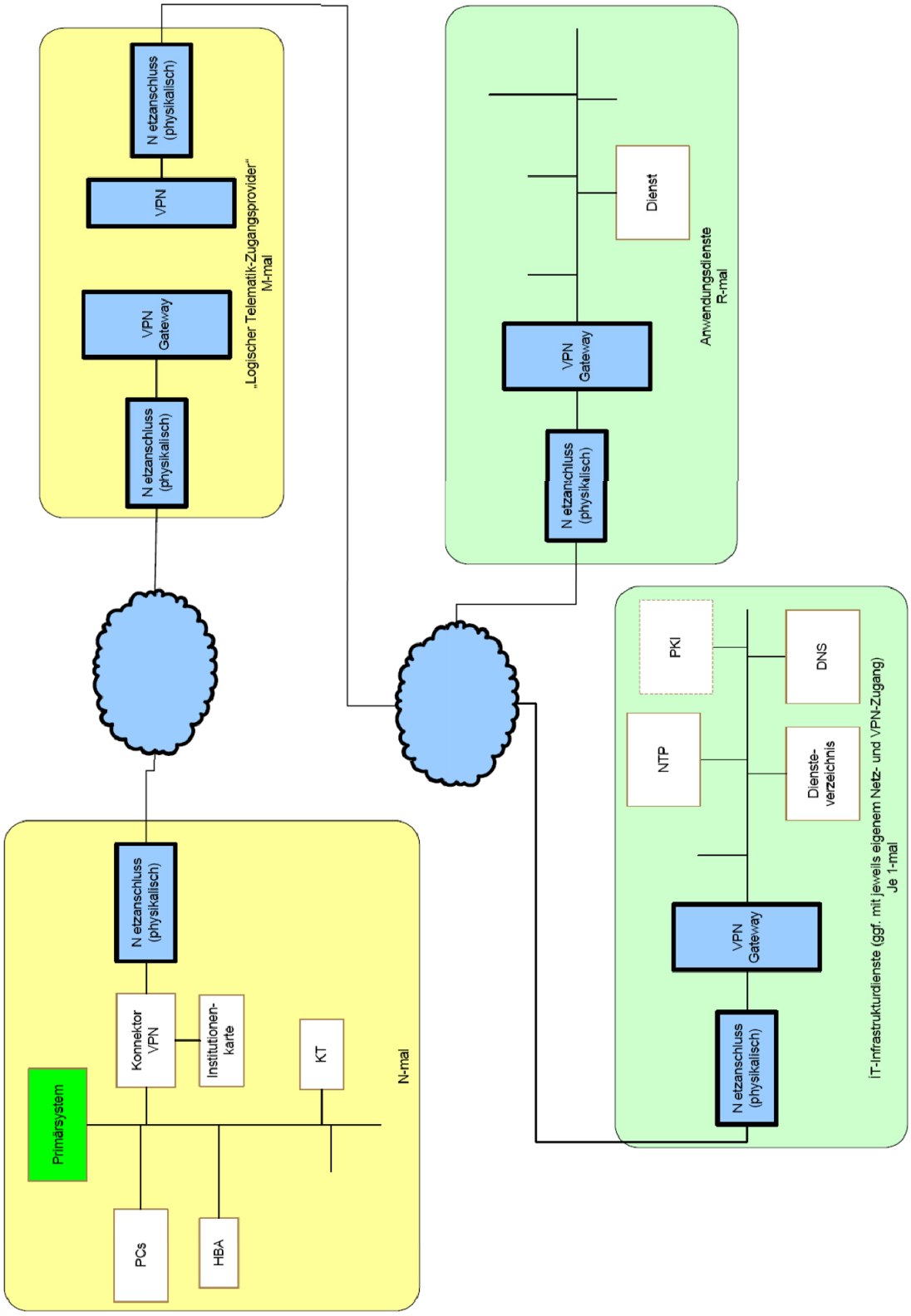


Abbildung 3-3: Netztopologie der Telematikinfrastruktur; Quelle: [BARCH]

Die Telematikinfrastruktur setzt auf Netzwerkebene auf einer Kommunikationsinfrastruktur auf Basis TCP/IP Technik auf. Die Kommunikationsinfrastruktur sollte von den Applikationen und Diensten unabhängig sein und flexibel auf neue Anforderungen reagieren können.

In der geplanten Netztopologie, die in Abbildung 3-3 dargestellt wird, gibt es nach [BARCH] fünf Zonen. Die 1. Zone enthält die Leistungserbringer. In dieser Zone ist eine heterogene Struktur auf Basis von TCP/IP vorhanden in der es keine systemweit eindeutige IP-Adressen gibt. Es ist deshalb ein einheitliches IP-Konzept für die gesamte Infrastruktur nötig. Die Kommunikation mit der Telematikinfrastruktur erfolgt ausschließlich über den Konnektor und einen physischen Netzzugang, der vom Leistungserbringer frei gewählt werden kann. Für Arztpraxen kommt hier ISDN oder DSL in Frage, für den mobilen Einsatz sind GSM oder UMTS möglich. Wird VLAN gemäß IEEE 802.1Q und ein mit bestehenden Firewalls gesichertes LAN beim Leistungserbringer verwendet, können nach [SP-KON] LAN- und WAN-Schnittstelle am Konnektor in einer physikalischen Schnittstelle zusammengefasst werden. Ist das LAN unsicher, müssen getrennte physikalische Schnittstellen genutzt werden.

Es sollte nach [SP-KON] der vom Netzzugangsprovider gestellte WAN-Zugangsrouter verwendet werden. Der Konnektor selbst kann ebenfalls eine WAN-Anschlussmöglichkeit, wie z.B. PPPoE oder ATM25-Anschluss für den direkten Zugang zu einem Provider implementieren. Die IP-Adresse des Konnektors an seiner WAN-Schnittstelle wird beim Zugang zum öffentlichen Netz am WAN-Router per NAT verändert. Deshalb muss die IPSec-Lösung NAT unterstützen. Die Veränderung der IP-Adresse erfolgt durch den Internet Service Provider oder den privaten Netzbetreiber und ist durch den Leistungserbringer nicht beeinflussbar. Beim Aufbau der IPSec-Verbindung zur zentralen Infrastruktur erhält der Konnektor dynamisch eine Tunnel-Schnittstellen-Adresse.

Für die Erfüllung dieser Anforderungen wurde in [SP-KON] ein Stufenplan für die eingesetzten Protokolle und Techniken entwickelt . In Stufe 1 wird ein L2TP/PPP-Tunnel verwendet. L2TP ist nach [SP-NW] eine in RFC 2661 definierte Erweiterung des PPP und wird als Remote VPN-Lösung verwendet. L2TP arbeitet auf Port 1701. Der Konnektor erhält über diesen Tunnel seine Tunnel-Schnittstellen-Adresse über den Mechanismus IPCP (Internet Protocol Control Protocol) und die DNS-Server-Adresse. Die Zugangskontrolle für den Tunnel erfolgt über EAP-TLS, weil es eine zertifikatbasierte Authentisierung ermöglicht. Die Schlüssel zur Verschlüsselung des Tunnels mit IPSec werden über das Internet Key Exchange Protokoll Version 1 (IKEv1) ausgetauscht. Es wird nach [SP-NW] der ESP (Encapsulating Security Payload) im Transportmodus mit dem Verschlüsselungsverfahren AES (Advanced Encryption Standard) und dem Authentisierungsverfahren SHA-1 verwendet. Das ESP-Protokoll ermöglicht eine Verschlüsselung der Daten und gewährleistet, dass die Herkunftsangabe und Inhalt der gesendeten Daten nicht unbemerkt verändert werden können. AES ist ein symmetrisches Verschlüsselungsverfahren, das heißt Ver- und Entschlüsselung werden mit dem gleichen Schlüssel durchgeführt. Bei AES handelt es sich um ein Blockchiffre. Die Funktionsweise des Algorithmus kann in [Daemen 2002] nachgelesen werden.. Bei der Authentisierung mit SHA-1 wird aus den Daten ein Hashwert ermittelt mit dessen Hilfe unautorisierte Änderungen festgestellt werden können. In weiteren Schritten entfällt die L2PT/PPP-Komponente, es wird IKEv2 eingeführt und die schrittweise Umstellung auf IPv6 erfolgt.

Es gibt genau eine aktive VPN-Verbindung vom Leistungserbringer zur Telematikinfrastruktur. Es sollte aber eine alternative Verbindung bei Ausfall der Primärverbindung zur Verfügung stehen.

In Abbildung 3-3 folgt auf die Zone der Leistungserbringer der Logische-Telematik-Zugangsprovider(LTZ). Er erlaubt den Leistungserbringern den Zugang zu den Anwendungsdiensten und den IT-Infrastrukturdiensten über die VPN-Verbindungen. Der LTZ managt und administriert die VPN-Verbindungen für die Leistungserbringer.

Für große Krankenhäuser kann der Zugang zur Telematikinfrastruktur über eine Direktanbindung erfolgen. Sicherheit und Verfügbarkeit wird auf Basis einer verbindlichen Policy durch das Krankenhaus selbst realisiert.

Die IT-Infrastrukturdienste bilden in Abbildung 3-3 eine weitere Zone. Die IT-Infrastrukturdienste kommen systemweit nur einmal als Master vor, können aber hierarchisch und verteilt realisiert werden. Zu den IT-Infrastrukturdiensten gehören:

- Zentrale Verzeichnisdienste zur Lokalisierung, Registrierung und Berechtigungsvergabe z.B. DNS;
- Zentraler Dienst zur Zeitsynchronisation (NTP);

- Trustcenter für die Sicherung der internen Kommunikation und die Ausstellung von Echtheitszertifikaten für Diensten;
- Zentrales Netzwerkmanagement;
- Zentrale Kommunikationsdienste um die Systemkopplung für eine Integration mit externen Trustcentern oder anderen Gesundheitsnetzen zu realisieren.

Die letzte Zone bilden in Abbildung 3-3 die Anwendungsdienste. Zu den Anwendungsdienste gehören die zentralen Fachdienste und die Mehrwertdienste. Aufgrund des Bandbreitenbedarfs können unterschiedliche Übertragungstechniken verwendet werden. Das physikalische Netz, das die Komponenten verbindet arbeitet mit den Protokollen TCP/IP und IPSec (RFC 2401-2409). Das Schlüsselmanagement wird über das Protokoll Internet Key Exchange(IKE) implementiert. Neben den standardisierten Diensten nach SGB V §291a sollen auch Mehrwertdienste durch die Telematikinfrastruktur unterstützt werden, die direkt mit dem Primärsystem kommunizieren. Um eine unkontrollierte Kommunikation zwischen dem Primärsystem und den standardisierten Diensten zu verhindern, kann es notwendig werden die Dienste strikt zu trennen.

3.1.7 Konfiguration des Konnektors

Für die Interoperabilität und Austauschbarkeit der Konnektoren ist es wichtig, dass der Konnektor eines Herstellers durch einen anderen Konnektor mit gleicher Konfiguration jeder Zeit ersetzt werden kann. Deshalb ist es notwendig die Konfigurationsparameter der Konnektoren zu spezifizieren.

Für die Inbetriebnahme des Konnektors müssen nach [SP-KON] einige Einstellungen vorgenommen werden. Zum Einen muss die SMC B zur Identifikation der Institution gegenüber der Telematikinfrastruktur in den Konnektor eingesetzt werden. Von der SMC müssen die Daten für die VPN-Verbindung ausgelesen und in den Konnektor eingetragen werden. Sind keine VPN-Verbindungsdaten auf der SMC B gespeichert, können diese Eintragungen auch manuell über die Managmentschnittstelle des Konnektors erfolgen. Wenn im Netzwerk des Leistungserbringers kein DHCP-Server vorhanden ist, muss der Konnektor für das Netzwerk mit IP-Adresse, Subnetz-Maske, Gateway und DNS-Server konfiguriert werden. Ist ein DHCP-Server vorhanden, darf dieser keine DNS- oder DHCP-Adresse übermitteln, da diese Angaben vom Internet Service Provider oder der Telematikinfrastruktur zur Verfügung gestellt werden.

Die Konfiguration der Kartenterminal am Konnektor kann verschieden erfolgen. Eine automatische Konfiguration ist mit Hilfe der in SICCT (Secure Interoperable ChipCard Terminal) definierten Standard Protokolle möglich. Es gibt darin Protokolle zum Bekannt machen und zum Auffinden der Kartenterminaldienste. Bei der Verwendung des Protokolls zur Bekanntmachung der Kartenterminaldienste sendet das Kartenterminal Multicast-Pakete durch das LAN. Der Konnektor muss das Protokoll zur Bekanntmachung implementieren, um diese Pakete zu empfangen und zu interpretieren. Der Konnektor kann optional auch das Protokoll zum Auffinden der Dienste unterstützen. Ist das Kartenterminal direkt am Konnektor angeschlossen, erfolgt die Konfiguration ebenfalls automatisch. Des Weiteren ist eine manuelle Zuweisung am Konnektor mit Hilfe der Identifier der Kartenterminals möglich. Sollen dem Konnektor nicht automatisch alle gefundenen Kartenterminals zugewiesen werden, kann man in der Konfiguration des Konnektors die Kartenterminals manuell zuweisen und die automatische Zuweisung ausschalten.

Beim Start verbindet sich der Konnektor automatisch mit allen zugewiesenen Kartenterminals über eine mit SSL/TLS verschlüsselte TCP-Verbindung. Ist ein Kartenterminal beim Start nicht verfügbar, wird die Verbindung aufgebaut, wenn sich das Kartenterminal über das SICCT Protokoll zur Bekanntmachung der Kartenterminaldienste meldet oder es erfolgt automatisch ein weiterer Versuch nach einem Zeitintervall.

Damit das Primärsystem die Fachdienste nutzen kann, muss dem Arbeitsplatz über eine Konfigurationsdatei der Identifikator eines Kartenterminals und es kann ein Anwendungskonnektor zugewiesen werden.

3.1.8 Primärsystemarchitektur und Konnektor

Der Konnektor ermöglicht die sichere Kommunikation zwischen Karte, Primärsystem und der Telematikinfrastruktur. Um diese Aufgabe zu erfüllen, muss der Konnektor in ein bestehendes Informationssystem integriert werden. Über die Benutzungsschnittstelle des Primärsystems kann der Leistungserbringer mit Hilfe des Konnektors die zentralen Dienste der Telematikinfrastruktur nutzen.

In Abhängigkeit von der Primärsystemarchitektur und den unterschiedlichen Einsatzumgebungen bei den Leistungserbringern sind nach [T-Stich] unterschiedliche Integrationsvarianten denkbar. Im Folgenden sollen 3 Primärsystemarchitekturen betrachtet werden:

- die Thin-Client-Architektur,
- die Rich-Client-Architektur,
- die Terminalserver-Architektur.

Weiterhin sollen die Integrationsmöglichkeiten der Einsatzumgebungen:

- Einzelpraxis,
- Praxisgemeinschaft,
- Gemeinschaftspraxis,
- Hausbesuch,
- Apotheke,
- Krankenhaus
- und eKiosk

untersucht werden.

3.1.8.1. Thin-Client-Architektur

In dieser Architektur läuft das Anwendungssystem auf einem Zentralrechner. Die Clients dienen nur der Präsentation der Daten und der Interaktion mit dem Benutzer. Da die Anwendungslogik auf dem Anwendungsserver ausgeführt wird, dient dieser auch als Client für den Konnektor (siehe Abbildung 3-4). Für die Ansteuerung der Kartenterminals muss der Anwendungsserver dem Konnektor den Identifikator des sendenden Thin-Clients liefern.

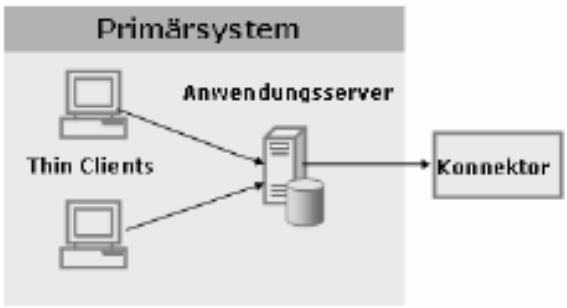


Abbildung 3-4: Konnektor in einer Thin-Client-Architektur; Quelle: [T-Stich]

3.1.8.2. Rich-Client-Architektur

In dieser Architektur wird die Anwendungslogik auf den Clients ausgeführt. Im Normalfall wird die Datenbank auf einen Server ausgelagert. Handelt es sich beim Primärsystem um eine Einzelplatzinstallation können sich Datenbank und Anwendungssystem auf dem Rich-Client befinden. Wie Abbildung 3-5 dargestellt, bildet in beiden Fällen der Rich-Client den Client für den Konnektor.

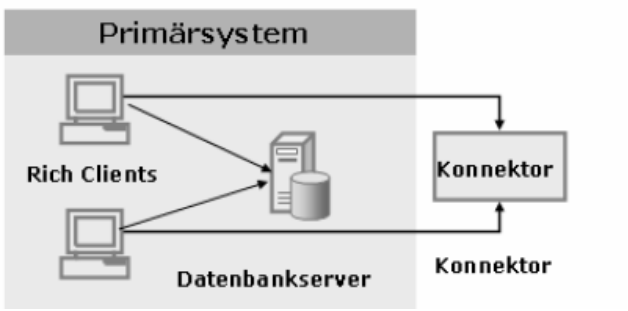


Abbildung 3-5: Konnektor in einer Rich-Client-Architektur; Quelle: [T-Stich]

3.1.8.3. Terminalserverarchitektur

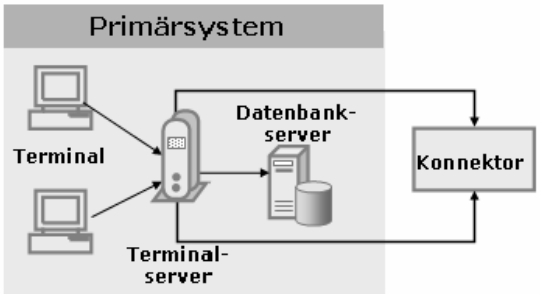


Abbildung 3-6: Konnektor in einer Terminalserver-Architektur; Quelle: [T-Stich]

Die Terminalserverarchitektur ist der Thin-Client-Architektur sehr ähnlich. Die Terminals dienen nur der Präsentation und der Interaktion mit dem Benutzer. Die Anwendungslogik läuft auf dem Terminalserver und greift auf den Datenbankserver zu. Der Terminalserver ist der Client für den Konnektor (siehe Abbildung 3-6). Wie auch bei der Thin-Client-Architektur muss der Terminalserver dem Konnektor für die Ansteuerung der Kartenterminals den Identifikator des Terminals liefern.

3.1.8.4. Einzelpraxis

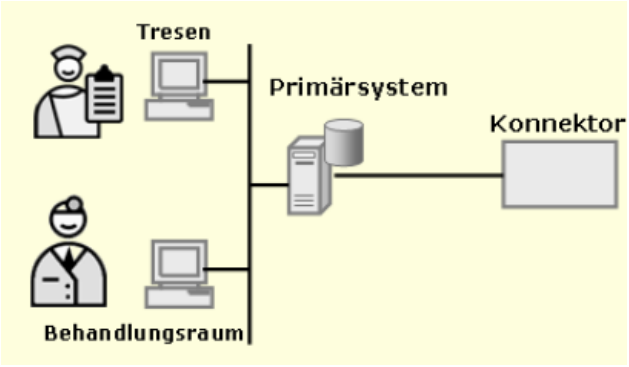


Abbildung 3-7: Konnektor in einer Einzelpraxis; Quelle: [T-Stich]

In einer Einzelpraxis arbeitet ein Arzt mit seinen Angestellten. Es ist eine Infrastruktur mit wenigen Rechnern vorhanden. Meist ist, wie in Abbildung 3-7 dargestellt, ein Arbeitsplatz am Tresen und ein oder mehrere Arbeitsplätze in den Behandlungsräumen vorhanden. An diesen Arbeitsplätzen ist Zugriff auf das Primärsystem möglich. Über das Primärsystem kann der Benutzer mit Hilfe des Konnektors die Dienste der Telematikinfrastruktur nutzen.

3.1.8.5. Praxisgemeinschaft

In einer Praxisgemeinschaft teilen sich mehrere Ärzte die technische Infrastruktur und das Personal. Die Ärzte haben aber eigene Patienten und eigene Abrechnung (siehe Abbildung 3-8). Um die aus

Datenschutzgründen geforderte getrennte Datenhaltung zu realisieren, nutzen die Ärzte entweder verschiedene Primärsysteme oder ein mandantenfähiges Primärsystem.

Jeder Arzt der Praxisgemeinschaft muss sich aufgrund der getrennten Abrechnung gegenüber der Telematikinfrastruktur mit einer eigenen SMC identifizieren. Deshalb müssen auch am Konnektor die Ärzte unterschieden werden. Es gibt die Möglichkeit getrennte Konnektoren oder einen mandantenfähigen Konnektor zu verwenden. Der mandantenfähige Konnektor kann mehrere SMC verwalten und zwischen den verschiedenen Primärsystemen bzw. den Mandanten des Primärsystems unterscheiden.

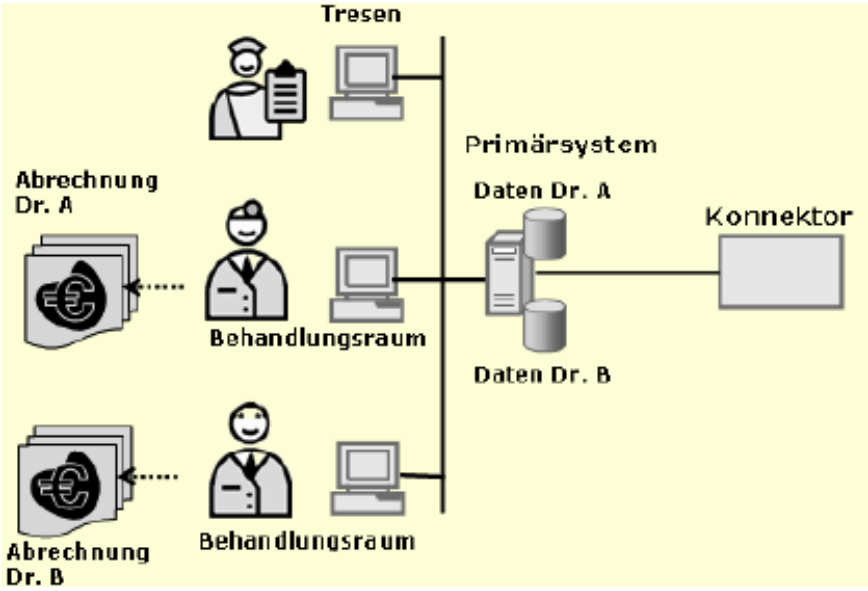


Abbildung 3-8: Konnektor in einer Praxisgemeinschaft; Quelle: [T-Stich]

Bei Verwendung von getrennten Konnektoren müssen auch verschiedene Primärsysteme verwendet werden, durch die Auswahl des Primärsystems wird dabei die Trennung vorgenommen. Diese Variante widerspricht jedoch der Philosophie der Praxisgemeinschaft die technische Infrastruktur gemeinsam zu nutzen.

3.1.8.6. Gemeinschaftspraxis

In einer Gemeinschaftspraxis teilen sich mehrere Ärzte Personal und technische Infrastruktur. Sie behandeln ihre Patienten gemeinsam und rechnen auch gemeinsam ab. Wie in Abbildung 3-9 dargestellt, ist bei einer Gemeinschaftspraxis auch eine gemeinsame Datenhaltung erlaubt. Deshalb kann ein Konnektor mit einer SMC verwendet werden. Im Unterschied zur Einzelpraxis gibt es mehrere Heilberufeausweise, die bei bestimmten Diensten wie zum Beispiel beim Signieren unterschieden werden müssen.

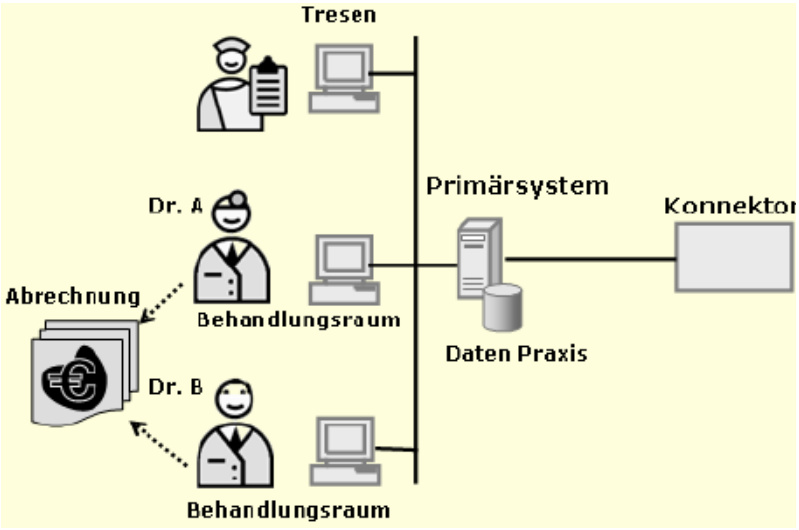


Abbildung 3-9: Konnektor in einer Gemeinschaftspraxis; Quelle: [T-Stich]

3.1.8.7. Hausbesuch

Beim Hausbesuch benutzt der Arzt ein mobiles Gerät (siehe Abbildung 3-10) mit einem Offline-Konnektor und einen mobilen Drucker. Ein Offline-Konnektor ist ein Konnektor der bei Nicht-Verfügbarkeit einer Verbindung zur Telematikinfrastruktur den kompletten Ablauf der bestimmten Fachdienste übernimmt. Auf dem Gerät wird ein Primärsystem mit geringer Funktionalität, d.h. Stammdaten von der Karte lesen und Verordnung erstellen zur Verfügung gestellt. In der Praxis werden die Daten dann ins Primärsystem übertragen und die Verordnung in der Telematikinfrastruktur gespeichert.

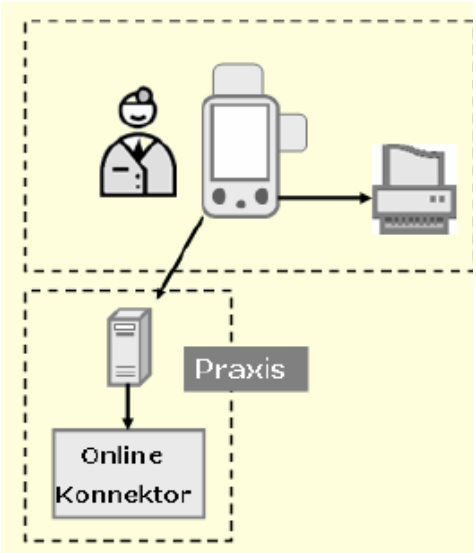


Abbildung 3-10: Mobiler Einsatz des Konnektors; Quelle: [T-Stich]

3.1.8.8. Apotheke

In der Apotheke gibt es mehrere Bedienplätze (siehe Abbildung 3-11), die auf ein Primärsystem zugreifen. An den Bedienplätzen muss es Kartenterminals für die eGK und den Berufsausweis geben, da die Apothekenhelfer an wechselnden Arbeitsplätzen bedienen.

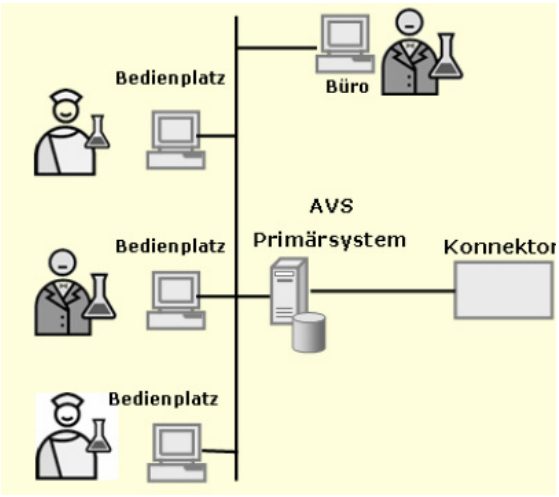


Abbildung 3-11: Konnektor in einer Apotheke; Quelle: [T-Stich]

In einer Apotheken mit vielen Bedienplätzen müssen unter Umständen sehr viele Steckvorgänge durchgeführt werden, was zum Verschleiß der Berufsausweise führt. Für diesen Anwendungsfall wurde das VERSA-Konzept entwickelt. Das VERSA-Konzept ermöglicht, wie im Kapitel Grundlagen erläutert, die Verwendung eines zentral gesteckten Berufsausweis.

Der Apotheker muss die Rezepte nach der Einlösung signieren. Dieser Vorgang kann gesammelt in einer Stapelsignatur passieren, um den Zeitaufwand zu verringern.

Der Apothekenkonnektor muss höhere Verfügbarkeitsanforderungen erfüllen. Während der Arzt entscheiden kann, ob das Rezept auf die eGK speichern oder in die Telematikinfrastruktur speichert, kann das Rezept in der Apotheke bei Ausfall der Telematikinfrastruktur nicht eingelöst werden, wenn es auf die Infrastruktur gespeichert wurde.

3.1.8.9. Krankenhaus

Im Krankenhaus werden hohe Anforderungen an Leistung und Verfügbarkeit gestellt, da es sehr viele Arbeitsplätze gibt (siehe Abbildung 3-12). Zur Erfüllung dieser Anforderungen sollte eine verteilte Realisierung mit mehreren Konnektoren gewählt werden.

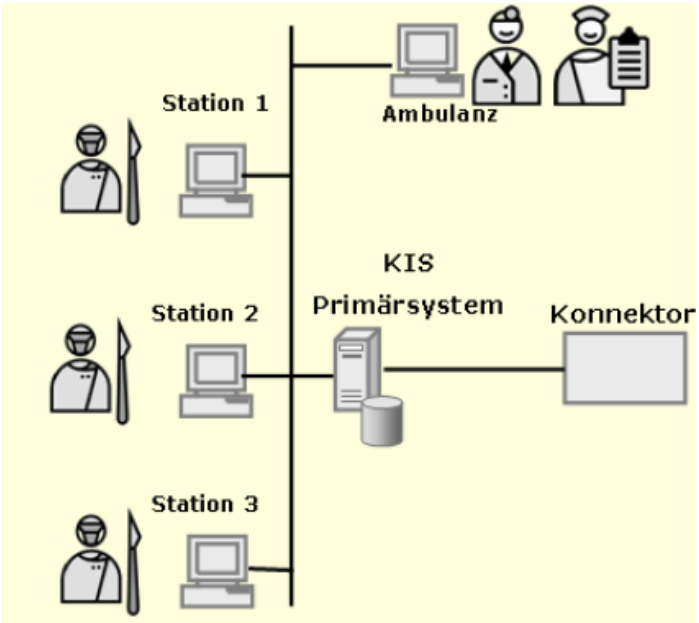


Abbildung 3-12: Konnektor in einem Krankenhaus; Quelle: [T-Stich]

Die Nutzung der elektronischen Gesundheitskarte wird sich im stationären Bereich des Krankenhaus anfangs auf die Aufnahme und Entlassung von Patienten beschränken. Im ambulanten Bereich muss

zwischen Patienten einer Institutsambulanz und Patienten eines ermächtigten Arztes unterschieden werden. Ein ermächtigter Arzt arbeitet wie ein niedergelassener Arzt, deshalb erfolgt die Integration auch wie in einer Arztpraxis. Patienten einer Institutsambulanz sind Patienten des Krankenhauses. Die Abrechnung erfolgt jedoch über eine eigene KV-Arztvertragsnummer. Dieses Anwendungsszenarium ist am besten mit dem einer Gemeinschaftspraxis vergleichbar.

Neben der Ausstellung von elektronischen Rezepten für öffentliche Apotheken, können für ambulante Patienten auch Rezepte für Arzneimittel aus der Krankenhausapotheke erstellt werden. In diesem Fall ist der behandelten Arzt Ersteller und Einlöser des Rezeptes.

3.1.8.10.eKiosk

Das Kioskterminal ist das Primärsystem über das der Versicherte die über ihn gespeicherten Daten lesen kann. Er kann Zugriffsberechtigungen vergeben, indem er Einträge sichtbar oder unsichtbar macht, er kann nicht abrechnungsrelevante Daten löschen und Rezepte bei einer Versandapotheke einlösen. Das Kioskterminal hat nach Abbildung 3-13 einen integrierten Konnektor, wenn es sich nicht innerhalb eines LANs einer Apotheke oder einer Arztpraxis befindet.

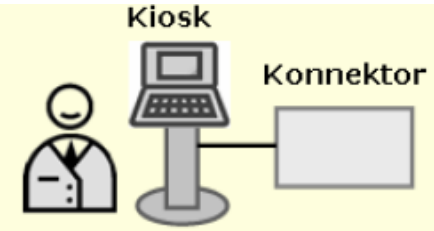


Abbildung 3-13: Konnektor am eKiosk; Quelle: [T-Stich]

3.1.9 Verteilung der Konnektorfunktionalität

Aufgrund der unterschiedlichen Einsatzumgebungen beim Leistungserbringer können nach [SP-KON] unterschiedliche Anforderungen an die Ausprägungen des Konnektors in Bezug auf Funktionsumfang, Leistungsmerkmal und physikalische Funktionsverteilung entstehen. Wichtig ist, dass für alle Verteilungslösungen die Sicherheitsanforderungen nach dem Schutzprofil gelten.

In der Einbox-Lösung befinden sich Anwendungs- und Netzkonnektor innerhalb einer Hardwarekomponente. Die Sicherheitsanforderungen werden überwiegend durch technische Maßnahmen erfüllt.

Wird eine Mehrkomponentenlösung gewählt sind Anwendungs- und Netzkonnektor voneinander getrennt. Der Anwendungskonnektor kann als Software in die existierende Infrastruktur eingebunden werden. Hier ist es auch möglich Hochverfügbarkeit herzustellen, indem der Anwendungskonnektor verteilt auf mehreren Servern vorhanden ist. Der Netzkonnektor kann ebenfalls als Software oder als Hardware realisiert werden. Bei diesen Software-Lösungen sind die Sicherheitsanforderungen durch organisatorische Maßnahmen zu gewährleisten, dass keine unberechtigten Personen Zugriff zu den Servern erhalten und so die Konnektorsoftware manipulieren können. Sehr wichtig ist es zu verhindern, dass das Primärsystem direkt mit dem Netzkonnektor kommuniziert oder der Anwendungskonnektor ohne den Netzkonnektor eine Verbindung zum Internet aufbaut.

3.1.10 Modellierung des Architekturkonzeptes

3.1.10.1.Fachliche Ebene

Auf der fachlichen Ebene sollen nur die Pflichtanwendungen betrachtet werden. Die verschiedenen Aufgaben wurden in mehrere Teilmodelle aufgeteilt, um eine übersichtliche Darstellung zu ermöglichen. In Ambulanzen wird bei der Aufnahme die Prüfung der Berechtigung zur Inanspruchnahme von Leistungen durchgeführt. Dabei wird durch das Lichtbild festgestellt, ob der Patient zur Verwendung dieser eGK berechtigt ist. Durch Ablaufdatum der Karte und die zentrale Sperrliste der Gematik wird die Gültigkeit der Karte geprüft. Danach wird festgestellt, ob die

Versichertenstammdaten auf der Karte aktuell sind und bei Bedarf wird eine Aktualisierung durchgeführt. Die Daten von der eGK werden in das Primärsystem kopiert. Zum Abschluss findet die Prüfung des Anspruchszeitraums statt, indem der Beginn des Versicherungsschutzes und das Ende des Leistungsanspruchs mit dem Leistungsdatum verglichen werden. Die Überprüfung der Berechtigung zur Inanspruchnahme von Leistungen und ihre Teilaufgaben wird in Abbildung 3-14 dargestellt.

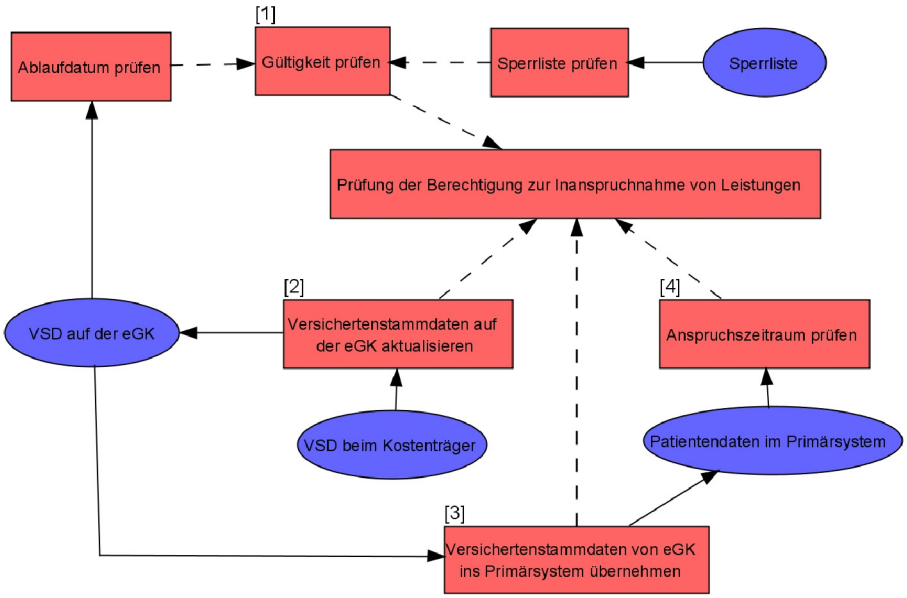


Abbildung 3-14: 3LGM²-Teilmodell für die Prüfung der Berechtigung zur Inanspruchnahme von Leistungen

Eine 2. Aufgabe ist das Ausstellen von elektronischen Verordnungen und wird in Abbildung 3-15 dargestellt. Die Verordnungsdaten müssen wie bisher im Primärsystem eingetragen werden. Dann erfolgt die Prüfung der Vordnung durch den Arzt und Signatur mittels HBA und die anschließende Übertragung auf die eGK oder in die Telematikinfrastruktur. Wenn die eVerordnung in die Telematikinfrastruktur übertragen wurde, kann ein Papierbeleg gedruckt werden. Mit Hilfe dieses Belegs kann eine eVerordnung ohne die Anwesenheit der eGK eingelöst werden.

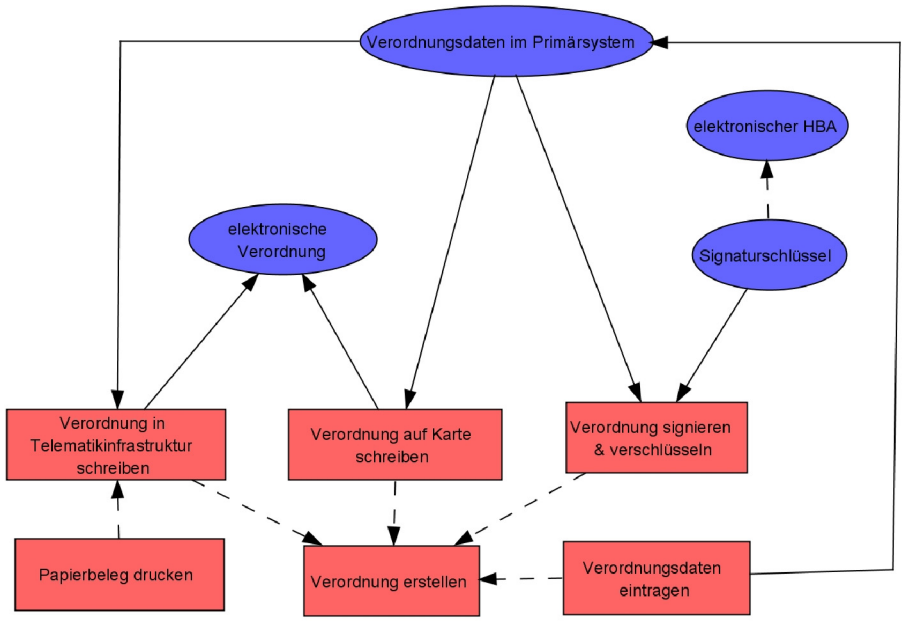


Abbildung 3-15: 3LGM²-Teilmodell für die Erstellung von elektronischen Verordnungen

Die letzte Pflichtanwendung ist das Einlösen von eVerordnungen. Diese Aufgabe kann in Ambulanzen und im stationären Bereich stattfinden. Im stationären Bereich werden Verordnungen von

Krankenhausbehandlungen (Einweisungen) eingelöst. Im Ambulanten Bereich können Überweisungen oder Verordnungen von bestimmten Behandlungen eingelöst werden. Das Einlösen von eVerordnungen ist in Abbildung 3-16 modelliert. Bei einer Einlösungen mit anwesender eGK werden alle einlösbaren Verordnungen von der eGK und aus der TI für diesen Versicherten aufgelistet, bei Einlösung eines Papierbelegs nur die Verordnungen aus der TI. Daraus kann nun eine Verordnung zur Einlösung ausgewählt und die Gültigkeit überprüft werden. Die ausgewählte Verordnung wird eingelöst und die Einlösedaten werden ergänzt. Nun kann die Verordnung vom Transportmedium gelöscht werden.

Für die Abrechnung der Verordnung muss diese vom Einlöser signiert, verschlüsselt und anschließend zur Abrechnungsstelle übermittelt werden.

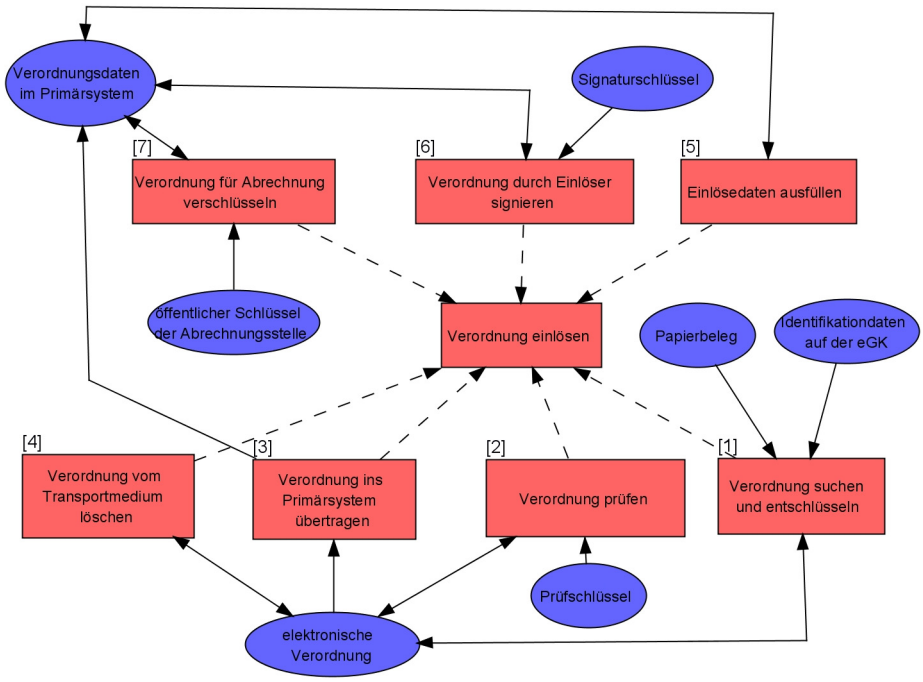


Abbildung 3-16: 3LGM²-Teilmodell für die Einlösung einer elektronischen Verordnung

3.1.10.2.Logische Werkzeugebene

Die logische Werkzeugebene (siehe Abbildung 3-17) kann in 2 Bereiche unterteilt werden. Ein Teil befindet sich im Gesundheitsunternehmen und der andere im zentralen Teil der Telematikinfrastruktur. Im Gesundheitsunternehmen befinden sich die im Architekturkonzept beschriebenen Bausteine Konnektor und Primärsystem. Für die Anwendung der elektronischen Signatur existiert ein Trusted Viewer. Für die Verwendung der Karten wurden die Kartenterminaldienste und das Kartenbetriebssystem der Prozessorkarten modelliert.

Im zentralen Teil der Infrastruktur befinden sich Infrastrukturdienste und die einzelnen Fachdienste. Als Gegenstelle für die VPN-Verbindung vom Konnektor zur zentralen Infrastruktur gibt es den Telematik-Zugangsprovider (VPN-Konzentrator), der die einzige Zugangsmöglichkeit zur zentralen Infrastruktur bietet.

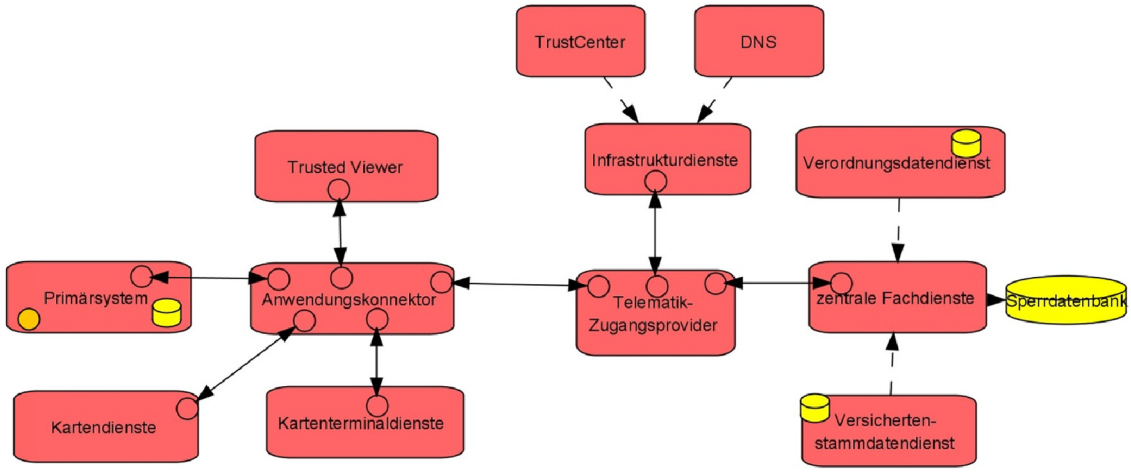


Abbildung 3-17: Logische Werkzeugebene des 3LGM²-Modells zum Architekturkonzept

3.1.10.3.Physische Werkzeugebene

Auf physischer Ebene wurden Arbeitsplatzrechner, Kartenterminals und Server modelliert. Die physische Werkzeugebene des Modells ist in Abbildung 3-18 dargestellt. Wie im Architekturkonzept beschrieben werden LAN-Terminals verwendet. Es sind Kartenterminals dargestellt, die selbst LAN-fähig sind und sich direkt im Netzwerk befinden. Eine 2. Möglichkeit ist die Verwendung von virtuellen Kartenterminals, die an Arbeitsplatzrechner angeschlossen werden. Dabei emuliert der Arbeitsplatzrechner ein LAN-Kartenterminal.

In der Abbildung ist der Konnektor zu finden. Er baut wie in Kapitel 3.1.6 Netzinfrastruktur beschrieben, eine VPN-Verbindung über den WAN-Router zum VPN-Konzentrator auf, der den Zugang zur zentralen Telematikinfrastruktur bildet. Der Datenverarbeitungsbaustein "Zentrale Telematikinfrastruktur" steht für alle Server, auf denen die zentralen Fach- und Infrastrukturdienste laufen.

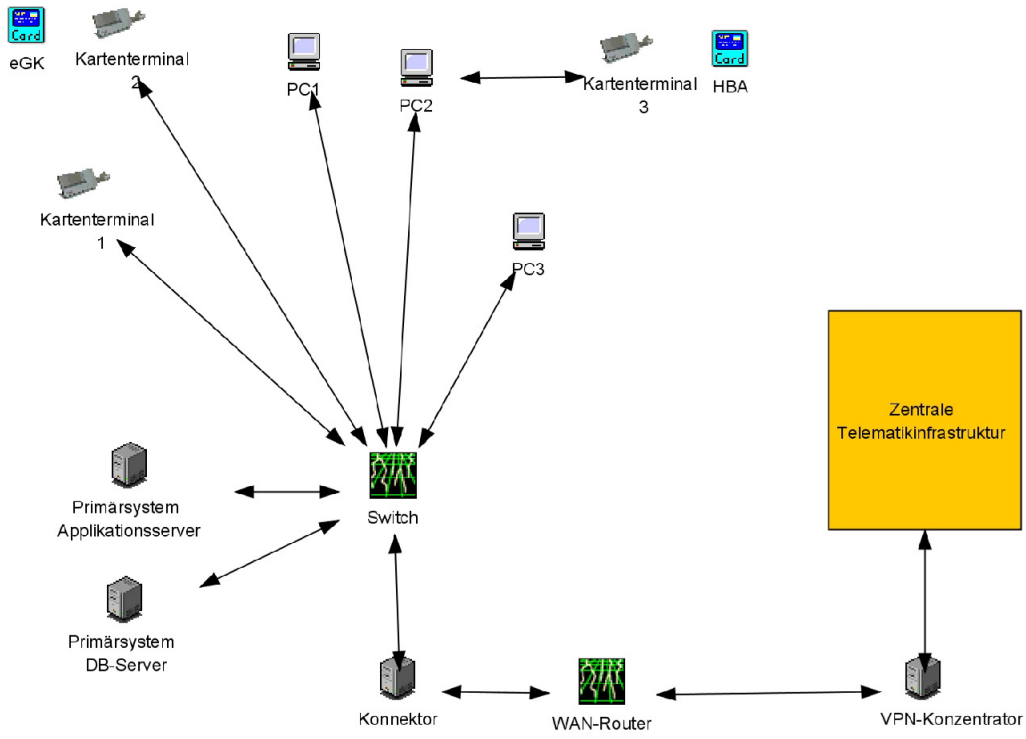


Abbildung 3-18: Physische Werkzeugebene des 3LGM²-Modells zum Architekturkonzept

3.1.11 Bewertung des Architekturkonzeptes

3.1.11.1. Integration in das Primärsystem

Die Telematikinfrastruktur soll nach dem Architekturkonzept mit Hilfe des Connector Abstraction Layer direkt ins Primärsystem integriert werden. Im Architekturkonzept wird festgelegt, dass die Kommunikation über SOAP-Aufrufe erfolgt und die Nutzdaten durch XML-Dokumente auf Basis von HL7 übertragen werden.

Das Primärsystem muss also durch den Hersteller um ein Connector Abstraction Layer (CAL) erweitert werden. Der CAL realisiert die Kommunikation über SOAP und die Erzeugung der XML-Dokumente.

Da auf dem Markt nur eine begrenzte Anzahl von Patientenverwaltungssystemen für Krankenhäuser existiert und diese bereits HL7 implementieren, ist der Aufwand für die Erweiterung dieser Primärsysteme vertretbar. Wie gut Datenintegration erreicht wird, hängt von der Datenintegration im KIS ab und von der Realisierung der CAL durch die Primärsystemhersteller. Der Grad an Zugriffs-Präsentations- und Kontextintegration hängt ebenfalls vom Stand der Integration im KIS ab und ist unabhängig vom Architekturkonzept. Die Präsentationsintegration hängt stark davon ab in wie weit sich die Primärsystemhersteller abstimmen, wird aber in der Regel nicht hergestellt werden können.

Die Festlegung auf HL7 als Kommunikationsstandard ist für die Integration in Praxisverwaltungssysteme schwierig, da dort meist die Kommunikationsstandards der xDT –Familie zum Einsatz kommen. Um die Integration zu ermöglichen, besteht die Möglichkeit die Praxisverwaltungssysteme um eine CAL-Komponente mit HL7-Schnittstelle zu erweitern. Auf dem Markt sind sehr viele Produkte für Arztpraxen vorhanden, die um eine entsprechende Schnittstelle erweitert werden müssen. Wird für ein Produkt keine solche Schnittstelle realisiert, ist der Arzt gezwungen ein neues Praxisverwaltungssystem einzuführen um mit der eGK arbeiten zu können. Da der Kauf eines neuen Produktes teuer ist und zusätzlichen Einarbeitungsaufwand verursacht, könnte die Akzeptanz der eGK weiter sinken. Für niedergelassene Ärzte, die Eigenentwicklungen verwenden, ist der Aufwand für die Entwicklung einer Schnittstelle zur Telematikinfrastruktur nicht vertretbar und der Arzt muss zu einem kommerziellen Produkt wechseln. Durch die Einführung der elektronischen Gesundheitskarte würde dadurch die Auswahl an Praxisverwaltungssystemen am Markt zurückgehen.

Eine weitere Möglichkeit, um die Entwicklung einer HL7-Schnittstelle zu umgehen, ist nach [Stäubert 2006] die Entwicklung von Adapterkomponenten. Die Adapterkomponente empfängt die Nachrichten des Praxisverwaltungssystems, wandelt diese in HL7-Nachrichten um und versendet die HL7-Nachrichten dann weiter. Adapterkomponenten werden bereits für die Kommunikation zwischen Krankenhäusern und dem niedergelassenen Bereich entwickelt. Ein großer Vorteil dieser Variante wäre, dass der Arzt bei seinem bereits gewohnten Praxisverwaltungssystem bleiben kann und so Einarbeitungsaufwand und Investitionskosten spart. Diese Lösung wird jedoch nicht funktionieren, weil trotzdem eine CAL-Komponente auf Basis eines anderen Kommunikationsstandards entwickelt werden muss. Die Nachrichten dieser Schnittstelle könnte die Adapterkomponente dann in HL7-Nachrichten umwandeln. Am Entwicklungsaufwand für die Erweiterung des Praxisverwaltungssystems ändert sich dadurch jedoch nichts.

Haben die Hersteller der Primärsysteme eine Connector-Abstraction-Layer-Komponente in ihre Produkte integriert, sollte der Integrationsaufwand im Gesundheitsunternehmen auf Ebene der Anwendungsbausteine nur noch gering sein.

3.1.11.2. Integration in das Sicherheitskonzept

Das Sicherheitskonzept eines Unternehmens dient dem Schutz der Integrität, Vertraulichkeit und Verfügbarkeit von IT-Systemen. In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische IT-Systeme empfohlen. Durch die organisatorischen, personellen, infrastrukturellen und technischen Maßnahmen des Katalogs kann ein Schutzniveau erreicht werden, das für den normalen Schutzbedarf ausreicht und für die Absicherung von IT-Systeme mit erhöhtem Schutzbedarf erweitert werden kann.

In den IT-Grundschutz-Katalogen werden Bausteine definiert aus denen ein typisches IT-System besteht. Darauf aufbauende wird die erwartete Gefährungslage beschrieben und ein Maßnahmenpaket zum Schutz des Bausteins vor den beschriebenen Gefährdungen vorgeschlagen.

Das Kernstück für die Integration der Telematikinfrastruktur in das Sicherheitskonzept eines Gesundheitsunternehmens bilden die Maßnahmen zum Schutz des Konnektors. Handelt es sich beim Konnektor um eine eigene Hardware so ist diese entsprechend des Sicherheitskonzeptes zu schützen. Handelt es sich um einen Softwarekonnektor so sind die Server zu schützen. Der Raum in dem sich die Hardware befindet ist ebenfalls zu schützen.

Nach [SP_KON] ist vorgesehen, dass der Konnektor in einem "nur für Befugte zugänglichen Raum" oder einem "abschließbaren Schrank" aufgestellt werden soll. Außerdem ist festgelegt, dass die SMC Typ B in einem Kartenterminal im selben Raum oder Schrank gesteckt werden muss. Im IT-Grundschutzkatalog werden Maßnahmen zum Schutz von Serverräumen (B2.4) beschrieben. Dazu gehören Maßnahmen zum Schutz vor Stromausfall, Feuer- und Wasserschäden, gesicherte Türen und Fenster sowie Zutrittsbeschränkungen und Fernanzeige für Störungen. Die Fernanzeige ist nach [SP-KON] durch die Management-Schnittstelle für den Konnektor vorgesehen. Ist ein bereits ein Serverraum bzw. ein Serverschrank mit den entsprechenden Schutzmaßnahmen vorhanden so kann dieser verwendet werden. Sonst muss zumindest ein Serverschrank angeschafft werden, um die nach [SP-KON] notwendigen Zutrittsbeschränkungen zu realisieren. Um nur Befugten den Zugriff auf den Konnektor zu ermöglichen, sollte auf eine restriktive Rechtevergabe für den Server geachtet werden.

Im Krankenhaus ist eine hohe Verfügbarkeit des Konnektors wichtig, da hier sehr viele Arbeitsplätze am Konnektor angeschlossen sind. Im Falle eines Ausfalls kann an keinem Arbeitsplatz auf die Telematikinfrastruktur zugriffen, was große Verluste für das Krankenhaus bedeutet. Deshalb sollte in einem Krankenhaus Hochverfügbarkeit für den Konnektor realisiert werden. Dies kann nach [T-Stich] entweder durch die Realisierung auf einem hochverfügbaren Server oder durch eine verteilte Realisierung auf mehreren Konnektoren geschehen. Des Weiteren sollten Stromversorgung und Kommunikationsverbindungen redundant vorhanden sein, um hier Ausfälle auszuschließen.

Ein weiteres Problem ist die Realisierung der VPN-Verbindung zum zentralen Teil der Telematikinfrastruktur, wenn das Netzwerk des Gesundheitsunternehmens durch einen Sicherheitsgateway (Firewall) geschützt ist. Jede Kommunikation mit einem externen Netz muss über den Paketfilter erfolgen. Abbildung 3-18 verdeutlicht, dass sich der Konnektor direkt am internen Netzwerk angeschlossen ist und von dort aus über einen WAN-Router die Verbindung zur Telematikinfrastruktur herstellt. Durch diese Architektur wird der Paketfilter umgangen, was mit dem Sicherheitskonzept unvereinbar ist.

Weitere sicherheitsrelevante Komponenten der Telematikinfrastruktur sind die Karten und Kartenterminals. Um die Karten vor Missbrauch zu schützen, sind diese mit einem Lichtbild versehen. Des Weiteren kann für die eGK ein Gültigkeitsdatum festgelegt werden und es gibt in der zentralen Infrastruktur Sperrlisten für Karten. Außerdem kann der Versicherte selbst seine eGK vor Missbrauch schützen indem er die allgemeinen Sicherheitsregeln für eine EC-Karte einhält. Dazu gehört, dass die PIN nicht aufgeschrieben wird, bzw. PIN und Karte getrennt aufbewahrt werden oder dass der Versicherte darauf achtet, was mit der Karte geschieht, wenn er sie dem Personal weiter gibt.

Der HBA ist ebenfalls vor Missbrauch zu schützen, da der Inhaber des HBA im Namen des Arztes qualifizierte elektronische Signaturen leisten kann. Neben technischen Maßnahmen ist hier ebenfalls auf organisatorische Maßnahmen bei der Integration in den Workflow zurückzugreifen. Wird in einem Gesundheitsunternehmen das VERSA-Konzept realisiert, sollten die HBAs in Kartenterminals an einer organisatorisch und technisch gesicherten zentralen Stelle gesteckt werden. An den Arbeitsplätzen muss sich dann ein Kartenterminal mit SMC-A befinden über das eine Card-To-Card-Authentisierung durchgeführt werden kann. Da die SMC-A nicht gesteckt werden muss, kann diese durch technische Maßnahmen am Kartenterminal gegen Diebstahl gesichert werden.

Die Kartenterminals für die eGK und den HBA an den Arbeitsplätzen müssen insbesondere vor Diebstahl und Manipulation geschützt werden. Dies kann durch geeignete Aufstellorte und eventuell technische Maßnahmen realisiert werden. Die Maßnahmen, die zum Schutz der Kartenterminals für die Krankenversicherungskarte verwendet werden, können hier wiederverwendet werden.

Weitere Teile der Architektur wie das Primärssystem und die Verkabelung für die Kommunikationsverbindungen der Komponenten innerhalb des Gesundheitsunternehmens werden hier nicht betrachtet, da diese Teile bereits vorhanden und ausreichend geschützt sind.

Besondere Sicherheitsmaßnahmen sind für eKiosks und im mobilen Betrieb notwendig, da das Gefährdungspotential höher ist und die hier beschriebenen Maßnahmen zum Teil nicht angewendet werden können.

3.1.11.3. Integration in den Workflow

Für die Nutzung der Versichertenstammdaten (VSD) werden nach [FK_VSDM] Institutionen autorisiert, somit haben auch berufsmäßige Gehilfen von Leistungserbringern die Berechtigung diese Daten zu lesen. Dieser Schritt ist notwendig, um die Integration in den Workflow zu vereinfachen. Bei einem niedergelassenen Arzt besteht so die Möglichkeit, dass eine Arzthelferin an der Rezeption wie bisher die Berechtigung zur Inanspruchnahme von Leistungen prüfen kann. Auch im Krankenhaus ist diese Funktion notwendig, damit eine zentrale Patientenaufnahme realisiert werden kann.

Bei der Ausstellung einer eVerordnung ist zu beachten, dass die eVerordnung zwar durch berufsmäßige Gehilfen ausgestellt werden dürfen, aber nur Inhaber eines HBAs dürfen sie signieren. Bisher war es jedoch ebenso notwendig, dass ein Arzt das Rezept unterschreibt. Deshalb ergeben sich dadurch keine Änderungen am Workflow. Für das Einstellen des Rezeptes in die Telematikinfrastruktur bzw. das Speichern auf der eGK ist das Vorhandensein der eGK zwingend erforderlich. Das Abholen eines Rezeptes beim Arzt durch eine Vertretung ist deshalb ohne Weitergabe der Karte nicht möglich.

Das Einlösen des Rezeptes in der Apotheke kann auch durch in der Apothekenbetriebsordnung festgelegtes Apothekenpersonal erfolgen. Die Integration in den Workflow der Apotheke sollte also kein Problem sein. Für die Abrechnung muss der Apotheker mit seinem HBA die eingelösten Verordnungen mittels Stapelsignatur signieren und die signierten Verordnungen zum Kostenträger übermitteln.

3.2 Modellregionen

Die Gematik ist auch für den Test der entwickelten Architektur verantwortlich. Dafür wurde ein Testkonzept und eine Testplanung entwickelt. Letztendlich wurden die Festlegungen zu den Tests durch die Rechtsverordnung beschlossen.

3.2.1 Zulassungsverfahren

Zur Erhöhung der Akzeptanz durch die Versicherten und Leistungserbringer sollten nur zugelassene Kartenterminals und Konnektoren verwendet werden, die ein sicherheitstechnische und funktionale Prüfung mit Teilzertifikaten und Validierungen durchlaufen haben. Es ist nach [T-Stich] Aufgabe der Gematik ein einheitliches Test- und Zulassungsverfahren und eine zentrale Zulassungsstelle zu etablieren. Die Erfüllung der Anforderungen muss durch geeignete Prüfstellen bestätigt werden. Die Prüfstellen werden durch die Gematik akkreditiert und müssen Fachkunde, Zuverlässigkeit und Unabhängigkeit nachweisen. Mit der Erteilung der Zulassung wird bestätigt, dass die Komponente alle Anforderungen im Bezug auf Sicherheit und Fachlogik erfüllt und deshalb für Zwecke der Gesundheitstelematik verwendet werden darf.

Die Konnektoren müssen nach [T-Stich] eine fachlogische und sicherheitstechnische Prüfung durchlaufen. Bei der fachlogischen Prüfung werden bereits vorhanden Prüfungs- und Zulassungsverfahren für IT-Systeme im Gesundheitswesen verwendet. Bei der sicherheitstechnischen Prüfung wird festgestellt, ob die implementierten Sicherheitsmaßnahmen geeignet sind Bedrohungen entgegen zu wirken. Es werden Maßnahmen an der Systembasis, in der Anwendungslogik der Dienste und am Netzkonnektor betrachtet. Weiterhin wird der Konnektor bezüglich seiner Eignung zur Erstellung von qualifizierten elektronischen Signaturen überprüft.

Für eine Zulassung der Karten eGK, HBA und SMC werden funktionale Tests durch die Gematik, eine Materialprüfung und Sicherheitstests durchgeführt. Die Sicherheitstests erfolgen nach einem Common Criteria (ISO/IEC 15408) Schutzprofil durch akkreditierte Prüfstellen.

3.2.2 Testkonzept

Die Testmaßnahmen dienen nach der Rechtsverordnung [VTE2005] "Überprüfung und Weiterentwicklung der für die Einführung und Anwendung der elektronischen Gesundheitskarte erforderlichen Telematikinfrastruktur. Sie richten sich insbesondere auf Funktionalität, Interoperabilität, Kompatibilität, Stabilität und Sicherheit der einzelnen Komponenten und Dienste." Die wichtigsten Ziele der Testmaßnahmen sind:

- Nachweis der Funktionalität, Interoperabilität, Stabilität und Sicherheit;
- Auswirkung der eGK auf die Organisation z.B. Ablaufprozesse, Datenlage;
- Optimierung von Betrieb und Schulungsmaßnahmen;
- Akzeptanz bei Versicherten und Leistungserbringern.

Die Gematik betreibt das zentrale Testlabor. Dieses umfasst Plattformen für Test und Abnahme der dezentralen Komponenten, sowie der zentralen und dezentralen Anwendungs- und Infrastrukturdienste. Die Gematik entwickelt die Testverfahren. Die funktionalen Abnahmetests werden durch die Gematik durchgeführt. Des Weiteren wird die zentrale Testinfrastruktur und eine Musterumgebung betrieben. Das Testmanagement gehört ebenfalls zu den Aufgaben der Gematik.

Die Gematik leistet in den Testregionen technische und organisatorische Unterstützung und bindet die Regionen in das Testmanagement ein.

Die Test werden in 4 Teststufen durchgeführt. Stufe 1 bilden die Labortests. Dabei werden die nach den Spezifikationen erstellten Komponenten bezüglich ihrer Funktionalität und der technischen Eigenschaften getestet. Neben den Komponententests werden auch Integrationstest zur Prüfung des Zusammenspiels zwischen den Komponenten und der Test der Datenschutzanforderungen durchgeführt. Am Ende der Labortests werden die Prozessabläufe der Anwendungen in der Musterumgebung getestet. Danach folgen in Stufe 2 die Anwendertests mit Testdaten in einer zentralen Musterumgebung. In dieser Phase testen zukünftige Anwender der Gesundheitskarte die Praxistauglichkeit. Es dürfen Komponenten ohne Zulassung verwendet werden. In den Stufen 3 und 4 werden in den Modellregionen Tests unter realen Einsatzbedingungen durchgeführt. In Stufe 3 werden 10000 Versicherte mit ihren Kostenträgern und Leistungserbringern eingebunden. Es ist eine beschränkte Zulassung der Komponenten nötig. In Stufe 4 werden in 2 Modellregionen die Tests auf 100000 Versicherte ausgeweitet. Bis zu diesen Tests sollte die vollständige Zulassung erfolgen. Nach erfolgreichen Tests in Stufe 4 wird der Rollout des Gesamtsystems durchgeführt.

Die Testung findet in 4 Funktionsabschnitten statt. Im 1. Funktionsabschnitt wird elektronische Gesundheitskarte ohne Netzzugang als Nachweis der Berechtigung zur Inanspruchnahme von Leistungen getestet. Im 2. Abschnitt wird ein Netzzugang geschaffen, über den die Gültigkeit des Versicherungsnachweises überprüft und die Daten auf der Karte mit den Daten der Krankenkasse aktualisiert werden können. Nach Funktionsabschnitt 2 sind die unter 2.1.1. beschriebenen Anwendungen getestet. Den 3. Funktionsabschnitt bilden das eRezept für apothekenpflichtige Arzneimittel außer Betäubungsmittel und sonstige Produkte die nur durch Apotheken vertrieben werden. Im 4. Abschnitt wird das eRezept auf andere Produkte, wie zum Beispiel Betäubungsmittel, Heil- und Hilfsmittel ausgeweitet und die Funktionen Notfalldaten und Arzneimitteldokumentation werden getestet.

Der durch die Rechtsverordnung aufgestellte Zeitplan kann nicht mehr eingehalten werden. Eine neue Verordnung wird nach [Goetz] in Kürze folgen.

Es wurde ein neuer Zeitplan (siehe Abbildung 3-19) für die Tests ausgearbeitet (Stand 7.8.2006):

	FA 1 (offline VSD, Notfalldaten, eRezept)	FA 2 (+online VSD)	FA 3 (+VODD)	FA 4 (+VODD, freiw. Anw.)
Stufe 1 (Labortest)	A 19.09.06	B 28.11.06	C 06.02.07	D 01.05.07
Stufe 2 (dez. Anwendertest)	E 28.11.06	F 06.02.07	G 01.05.07	H 24.07.07
Stufe 3 (10.000er)	I 06.02.07	J 01.05.07	K 07.08.07	L 13.11.07
Stufe 4 (100.000er)	M 19.02.08			

Abbildung 3-19: Zeitplan der Baymatic; Quelle: [Jedamzik 2006]

Der Zeitplan muss durch die Gesellschafter der Gematik beschlossen werden. Bis dahin bleibt der Plan aus der Rechtsverordnung vom 2.11.2005 der offizielle Zeitplan.

Nach der Verordnung über Testmaßnahmen hat "die Gesellschaft für Telematik darauf hinzuwirken, dass nach der dritten Stufe der Tests dezentrale Komponenten nicht mehr auszutauschen und Geschäftsprozesse weitgehend nicht mehr zu verändern sind". Diese Regelung bietet eine Investitionssicherheit für Unternehmen, die außerhalb der von der Gematik festgelegten Testregionen ebenfalls Pilotprojekte durchführen möchten.

3.2.3 Projektstand in der Modellregion Löbau-Zittau

In der Region Löbau-Zittau sind 6 Krankenkassen, 1 Klinikum, 1 Altenheim, 30 Apotheken, 170 niedergelassene Ärzte, 130 Heil- und Hilfsmittelerbringer und 130 000 Versicherte am Projekt beteiligt (Stand April 2006). Die Informationen zur Modellregion wurden aus [Seibt 2005] und von der Projekt-Homepage von SaxMediCard[2] entnommen. Die Initiierung des Projektes erfolgte im Januar 2004. Nachdem die Region alle Kriterien der Gematik im Mai 2005 erfüllte, wurde am 05.04.2006 der Vertrag mit der gematik unterzeichnet. Die Leitung des Projekt obliegt der AOK Sachsen, die Projektsteuerung der Firma ehealth consulting. Die regionale Projektleitung hat die Managementgesellschaft Gesundheitszentrum Löbau-Zittau mbH.

Die Ziele des Projektes sind:

- Umsetzung der Pflichtanwendungen nach §291a SGB V;
- Durchführung von Testszenarien nach den Vorgaben der Gematik/BMGS;
- Tests der Interoperabilität und Akzeptanz von eGK und HBA;
- Test der Telematikdienste (Versichertenmanagement, eRezept, Notfalldaten, Arzneimitteldaten und ePA).

Insbesondere soll der Versichertenstammdatensatzes (VSDD), die Verwendung des eRezeptes im Offline- und Online-Betrieb, das Zusammenspiel zwischen eGK und den Primärsystemen und der Aufbau des Kartenmanagementsystems der Krankenkassen getestet werden.

Im Minitest, das heißt der Startphase des Projektes, wurden nach [Sax2005] 500 Versicherte mit eGKs und 20 Arztpraxen mit HBAs ausgestattet. Die Ausstattung aller Apotheken ist in Planung. Im Klinikum Löbau-Zittau ist der HBA in den Radiologien bereits seit 2001 mit den Funktionen

[2] http://www.gesundheitskarte-sachsen.de/

Authentisierung und elektronische Signatur im Routinebetrieb. Im Klinikum existiert ein LDAP-Server, HL7-Server, Firewall, PACS und ePA..

Die Sächsische Landesärztekammer wurde nach [SachsSM] als Ausgabepilot für den HBA bestätigt. Es sollen die administrativ-organisatorischen Prozesse und Abläufe zwischen Ärztekammern, Ärzten und den Zertifizierungsdiensteanbietern getestet werden.

Seit Oktober 2006 ist nach [SaxMediCard] die Musterumgebung der Gematik installiert und das Testlabor fertiggestellt. Es besteht für Ärzte und Apotheker die Möglichkeit sich über die Komponenten zu informieren und Schulungen zu besuchen.

Ab Dezember 2006 werden nach [SaxMediCard] 25 niedergelassene Ärzte der Region mit Kartenterminals ausgestattet und 10000 Versicherte erhalten eine elektronischen Gesundheitskarte. Es können dann Tests der elektronischen Gesundheitskarte mit der Funktionalität der Krankenversicherungskarte (Funktionsabschnitt 1) durchgeführt werden. Ab März 2007 sollen weitere Funktionsabschnitte folgen.

4 Analyse des Ist-Zustands am UKL

Der folgende Abschnitt beschäftigt sich mit der Analyse des Ist-Zustandes eines Uniklinikums. Es werden die für die Integration der Telematikinfrastruktur relevanten Ausschnitte dargestellt. Den Schwerpunkt der Analyse bildet die Darstellung des Sicherheitskonzeptes und der Architektur auf physischer Werkzeugebene. Die Analyse basiert auf Gesprächen mit dem Bereich Informationsmanagement. Zur Darstellung der aktuellen Situation wird ein 3LGM²-Modell mit den wesentlichen Merkmalen erstellt.

4.1 Modell des Ist-Zustandes

4.1.1 Fachliche Ebene

Für die Beschreibung der Aufgaben ist eine Gliederung in stationären und ambulanten Bereich notwendig. Es sollen hier nur Aufgaben betrachtet werden, die von der Einführung der eGK mit den Pflichtanwendungen betroffen sind.

Im stationären Bereich wird sich die Anwendung der eGK auf die Aufnahme von Patienten beschränken. Die Patientenaufnahme wird in Abbildung 4-1 modelliert. Bei der Aufnahme wird im Normalfall eine Verordnung zur stationären Behandlung eingelöst. Im Notfall gibt es keine Verordnung. Die Patientenstammdaten werden dabei von der Krankenversicherungskarte ins Primärsystem übermittelt. Die Verordnung wird durch das Aufnahmepersonal überprüft und die Daten der Verordnung werden ins Primärsystem übertragen. Danach werden die Einlösedaten ausgefüllt, auf die Verordnung aufgedruckt und die Verordnung wird unterschrieben. Zu einem späteren Zeitpunkt erfolgt die Abrechnung.

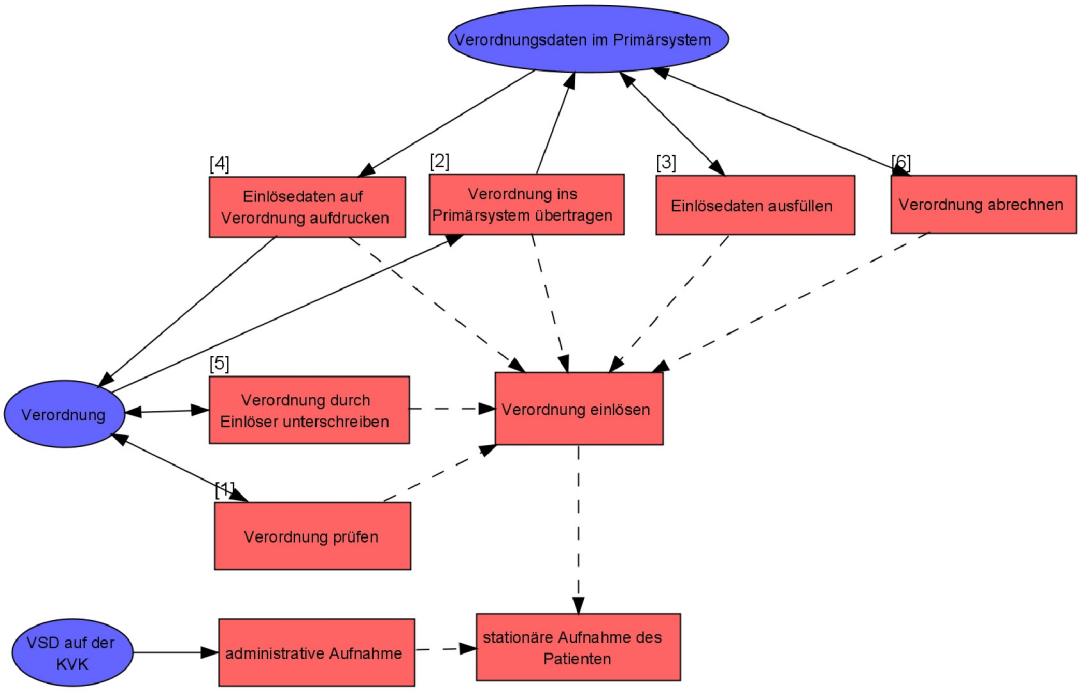


Abbildung 4-1: Fachliche Ebene des 3LGM²-Modells zum Ist-Zustand für den stationären Bereich

Im ambulanten Bereich können die Aufgaben Prüfung der Berechtigung zur Inanspruchnahme von Leistungen, Einlösung von Verordnungen und Erstellung von Verordnungen für Arzneimittel identifiziert werden. Die Einlösung von Verordnungen wird wie bei stationären Aufnahmen

durchgeführt und ist in Abbildung 4-1 dargestellt. Bei der Prüfung der Berechtigung zur Inanspruchnahme von Leistungen (siehe Abbildung 4-2), muss die KVK vorhanden sein. Das aufgedruckte Ablaufdatum muss geprüft werden und im Folgenden werden die Daten von der Karte ins Primärsystem eingelesen. Bei der Verordnung von Arzneimitteln (siehe Abbildung 4-2), füllt der Arzt im Primärsystem die Verordnung aus und druckt diese dann auf das entsprechende Formular. Danach prüft er noch einmal die Daten auf der Verordnung und unterschreibt das Formular. Der Patient bekommt die Verordnung und kann diese in jeder Apotheke einlösen.

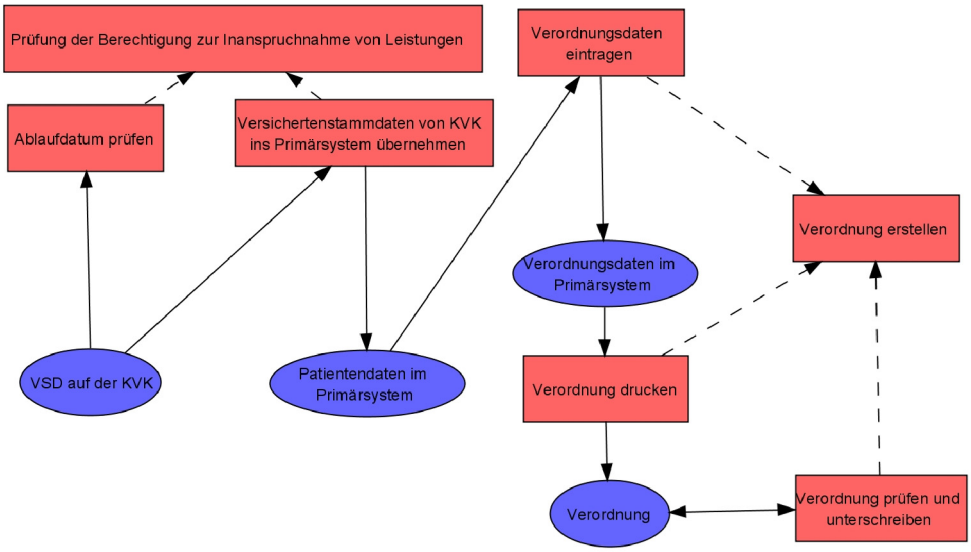


Abbildung 4-2: Fachliche Ebene des 3LGM²-Modells zum Ist-Zustand für den ambulanten Bereich

4.1.2 Logische Werkzeugebene

Auf logischer Werkzeugebene sollen nun die Anwendungsbausteine mit ihren Datenbanken und Schnittstellen modelliert werden mit Hilfe deren die Aufgaben erledigt werden. Ein Teil der Aufgaben wird, wie man im Modell in Abbildung 4-3 sieht, derzeit ohne Rechnerunterstützung durchgeführt. Dazu gehört die Prüfung der Gültigkeit der Karte, die Einlösung der Verordnung der Krankenhausbehandlung und das Prüfen und Unterschreiben der Verordnung. Die Übernahme der Patientendaten ins Primärsystem und das Erstellen einer Verordnung werden mit Hilfe des Primärsystems erledigt.

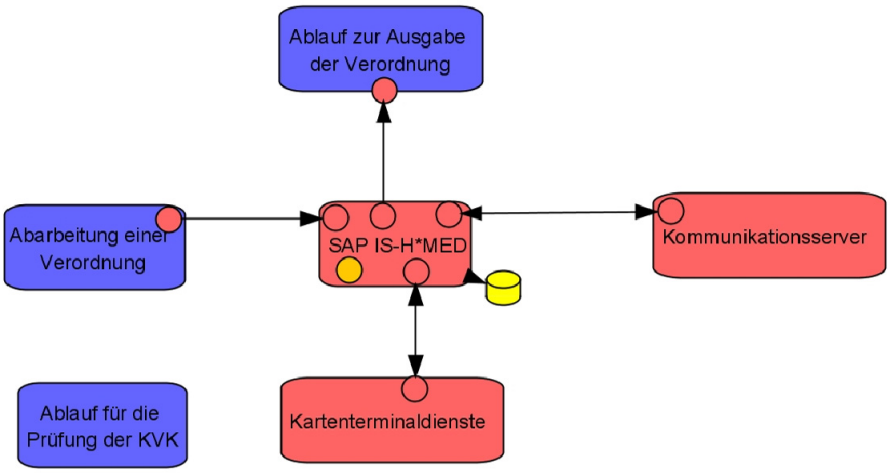


Abbildung 4-3: Logische Werkzeugebene des 3LGM²-Modells zum Ist-Zustand

In Abbildung 4-3 ist zu erkennen, dass im Ist-Zustand auf logischer Werkzeugebene sehr viele Medienbrüche vorhanden sind. Im Modell sind diese als Kommunikationsbeziehungen zwischen konventionellen und rechnerbasierten Anwendungsbausteinen dargestellt.

4.1.3 physische Werkzeugebene

Auf den Workstations läuft das Primärsystem, das im Fall des UKL SAP IS-H*MED ist. Die Kommunikation zwischen den Workstations in der zentralen Patientenaufnahme und der Krankenversicherungskarte läuft über ein Kartenterminal für Speicherkarten, das direkt an der entsprechenden Workstation angeschlossen ist.

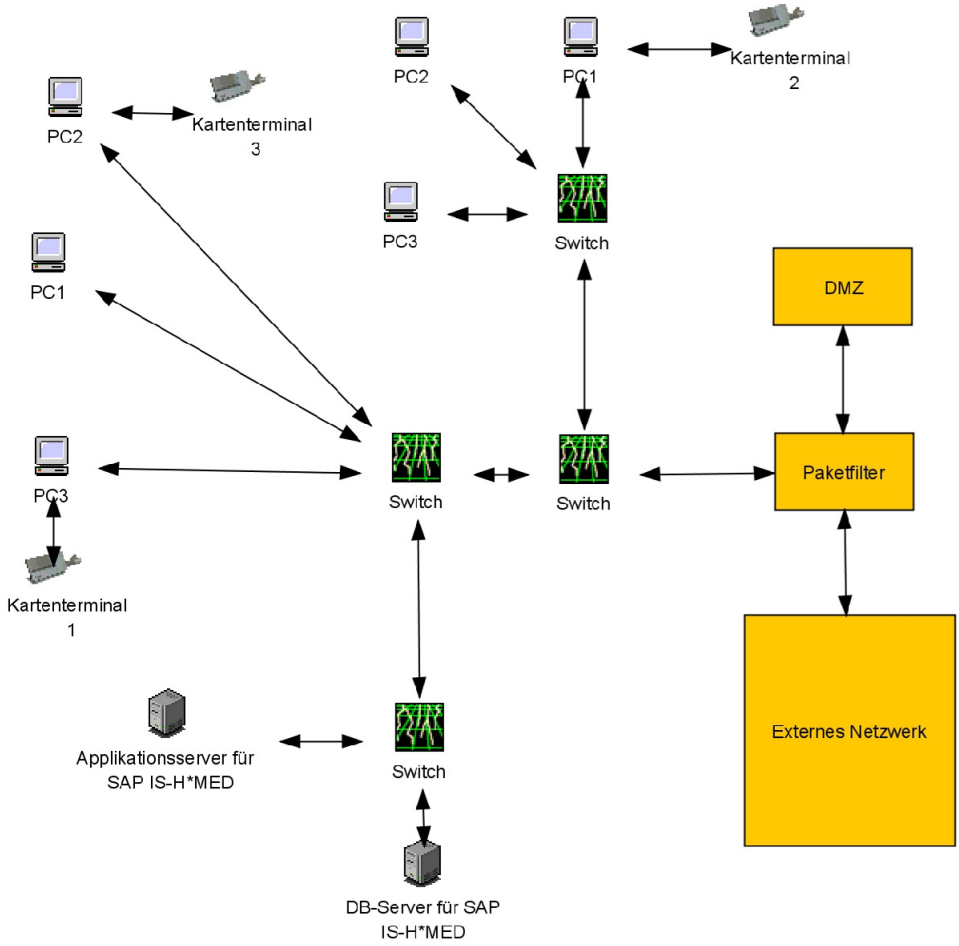


Abbildung 4-4: Physische Werkzeugebene des 3LGM²-Modells zum Ist-Zustand

Das interne Netzwerk besteht auf physischer Ebene aus vielen IP-Segmenten. Die unterschiedlichen Segmente sind in Abbildung 4-4 durch die verschiedenen Switche dargestellt. In der Realität ist das Netzwerk sehr viel komplexer und die Trennung der unterschiedlichen Segmente muss sich nicht an den Switchen orientieren.

Jede Kommunikation mit dem externen Netz erfolgt über einen Paketfilter. Alle nicht explizit benötigten Ports sind geschlossen. Die Server und Dienste des internen Netzes sind aus dem externen Netz nicht erreichbar. Der Datenverarbeitungsbaustein externes Netzwerk steht für alle Server des Internets. Über dieses nicht vertrauenswürdige Netz erfolgt jede Kommunikation mit externen Partnern. Auf die Sicherheit dieses Netzwerks hat das Rechenzentrum des UKL keinen Einfluss und es wird deshalb als unsicher eingestuft.

Einige Dienste müssen sowohl vom internen als auch vom externen Netzwerk erreichbar sein. Für solche Anwendungen wurde das getrennte Teilnetzwerk Demilitarized Zone(DMZ) eingerichtet. Die DMZ ist durch den Paketfilter gegenüber dem internen und externen Netz abgeschirmt. Der Zugriff auf die DMZ ist auf die gewünschten Dienste beschränkt. Dadurch sind nur Angriffe über den

entsprechenden Dienst möglich. Ist ein Angriff dennoch erfolgreich, ist der Nutzen für Folgeangriffe durch die Abschirmung ebenfalls stark eingeschränkt.

4.2 Bewertung des Ist-Zustandes

4.2.1 Integration in das Primärsystem

Das Primärsystem des UKL für die Pflichtanwendungen der Telematikinfrastruktur ist SAP IS-H*MED. Für die Verwendung der freiwilligen Anwendungen könnten in Zukunft weitere rechnerbasierte Anwendungsbausteine des Krankenhausinformationssystems wie zum Beispiel das Radiologieinformationssystem benötigt werden. Für die Kommunikation der rechnerbasierten Anwendungsbausteine untereinander wird ein Kommunikationsserver verwendet. Die dadurch entstehende Sternarchitektur hat den Vorteil, dass pro Anwendungsbaustein nur eine Schnittstelle zum Kommunikationsserver definiert werden muss und nicht je eine Schnittstelle zu jedem Anwendungsbaustein mit dem Daten ausgetauscht werden müssen. Dieser Architekturstil führt zu einer leichteren Wartbarkeit der Kommunikationsschnittstellen.

Am UKL wird als Kommunikationsserver die Eigenentwicklung Kodix verwendet. Da alle bisherigen Schnittstellen ausschließlich asynchrone Kommunikation verwenden, ist in Kodix nur asynchrone Kommunikation realisiert. Eine Weiterentwicklung des Kommunikationsservers kann jedoch durchgeführt werden.

Die Kommunikation zwischen SAP IS-H*MED und weiteren Anwendungsbausteinen erfolgt über HL7. Deshalb existiert bereits eine Schnittstelle zwischen Kommunikationsserver und SAP IS-H*MED, die für die Integration der Telematikinfrastruktur lediglich erweitert werden muss. Das Produkt besitzt derzeit keinen Connector Abstraction Layer (CAL). Für die Integration in die Telematikinfrastruktur muss SAP diese Komponente entwickeln.

4.2.2 Integration in das Sicherheitskonzept

Es existieren am UKL Server für die hoher Schutzbedarf besteht. Diese befinden sich in Serverräumen, für die Maßnahmen der IT-Grundschutzkataloge zum Schutz von Serverräumen realisiert wurden. Die vorhandenen Server sind auch auf Softwareebene vor unbefugtem Zugriff geschützt. Für einige Anwendungssysteme wurde am UKL bereits Hochverfügbarkeit realisiert. Die verwendeten Konzepte und Maßnahmen können für den Konnektor wieder verwendet werden.

Das Sicherheitskonzept des UKL besagt, dass jede Kommunikation aus dem internen Netz durch den Paketfilter kontrolliert wird. Kommunikation aus dem externen Netz in das interne Netzwerk ist durch den Paketfilter nicht möglich. Um Kommunikation aus dem externen Netz zu ermöglichen, wurde die DMZ eingerichtet. Diese Zone ist gegenüber dem externen und internen Netz über den Paketfilter geschützt, der nur die für den Dienst notwendige Kommunikation erlaubt.

Zum Schutz des HBA und der eGK gibt es am UKL keine Erfahrung, da es bisher keine Karten mit vergleichbarer Funktionalität und dem damit verbundenen Schadenspotential gab. Anhand der Krankenversichertenkarte(KVK) kann man jedoch sehen, dass die Versicherten mit den Karten sorglos umgehen und Aufklärungsbedarf besteht. Die Kartenterminals mussten auch bisher vor Manipulation und Diebstahl geschützt werden. Bisher gab es jedoch für die KVK kein PIN, die vor Ausspähung zu geschützt werden musste. In wie weit die bisherigen Maßnahmen weiter verwendet werden können und welche zusätzlichen Maßnahmen erforderlich sind, bleibt abzuwarten.

4.2.3 Integration in den Workflow

Der Workflow des UKL entspricht dem Workflow einer Praxis im niedergelassenen Bereich. Die Prüfung der Berechtigung zur Inanspruchnahme von Leistungen wird durch die eGK erweitert. Der Arbeitsablauf in der Praxis ändert sich dadurch jedoch nicht. Da bisher die Ärzte in den Ambulanzen die Rezepte im Primärsystem erstellten und dann für den Patienten druckten und unterschrieben, wird hier lediglich die Rechnerunterstützung ausgeweitet. Änderungen am Workflow sind nicht zu erwarten.

Bei der zentralen Patientenaufnahme im stationären Bereich wird ebenfalls die Rechnerunterstützung ausgeweitet. Bisher wurde die Einweisung zwar papierbasiert bearbeitet, mussten jedoch für die Abrechnung ins Primärsystem übertragen werden. Hier führt die Einführung der eVerordnung ebenfalls zur Vereinfachung des Workflows.

5 Anforderungsspezifikation

In den vorangegangen Abschnitten wurden die externen Rahmenbedingungen und der Ist-Zustand am UKL analysiert. Es wurden Modelle erstellt um die wesentlichen Merkmale des Ist-Zustandes und der von der Gematik geplanten Integration erstellt. Nun sollen darauf aufbauend die Anforderungen des UKL und der Gematik spezifiziert werden.

5.1 Integration in das Primärsystem

Für die Integration ins das UKL ist es notwendig, dass eine Connector Abstraction Layer (CAL) für das Produkt SAP IS-H*MED entwickelt wird. Diese Aufgabe muss durch den Hersteller des Primärsystems durchgeführt werden und kann durch das UKL nicht beeinflusst werden. Ohne diese Entwicklungsleistung durch SAP ist eine Integration der Telematikinfrastruktur in das UKL nicht möglich.

Zur Verwendung der freiwilligen Anwendung kann es in Zukunft notwendig werden weitere Teile des Krankenhausinformationssystems wie zum Beispiel das Radiologieinformationssystem für die Befundübermittlung als weiteres Primärsystem zu integrieren. Solange nur ein Primärsystem mit dem Konnektor integriert werden muss, ist es möglich diese Schnittstelle direkt zu realisieren. Kommen jedoch weitere hinzu entsteht auf diese Weise eine schwer wartbare Architektur, die vermieden werden soll. Es wird deshalb empfohlen die Kommunikation des Konnektors mit dem Primärsystem über den Kommunikationsserver zu realisieren. Dazu muss der Kommunikationsserver in der Lage sein SOAP-Aufrufe mit HL7-Inhalt zu transportieren. Für die Kommunikation zwischen Primärsystem und Konnektor ist derzeit synchrone Kommunikation vorgesehen, asynchrone Kommunikation ist aber für die Zukunft nicht ausgeschlossen. Der Kommunikationsserver muss also sowohl synchrone als auch asynchrone Kommunikation unterstützen. Im UKL wird die Eigenentwicklung Kodix als Kommunikationsserver verwendet. Kodix unterstützt derzeit nur asynchrone Kommunikation und muss deshalb für die Integration des Konnektors in das Krankenhausinformationssystem weiterentwickelt werden.

5.2 Verwendung der elektronischen Signatur

Bei der Erstellung von qualifizierten elektronischen Signaturen können ebenfalls einige Anforderungen identifiziert werden. Zur Überprüfung der qualifizierten Signaturen muss Zugriff auf das zentrale Trust Center der Gematik möglich sein. Für die Erstellung der Signatur wird außerdem ein Signaturanwendungskomponente (Trusted Viewer) benötigt. Der Trusted Viewer muss nach [SP-KON] auf dem Arbeitsplatz des Benutzers laufen. Sollte die elektronische Signatur in Zukunft auch für andere Anwendung genutzt werden, kann dies durch eine direkte Nutzung der Basisdienste des Konnektors realisiert werden.

Im ersten Schritt ist die Einführung der Pflichtanwendungen der elektronischen Gesundheitskarte vorgesehen. Hier muss die qualifizierte elektronische Signatur beim Erstellen und Einlösen von Verordnungen verwendet werden. Die elektronische Signatur ersetzt beim Erstellen der Verordnung die Unterschrift des Arztes auf der Papierverordnung. Die Ärzte sollten deshalb mit der qualifizierten elektronischen Signatur ebenso sorgfältig umgehen wie mit ihrer eigenhändigen Unterschrift. Dazu gehört das sorgfältige Prüfen der Verordnung im Trusted Viewer vor dem Signieren. Nach dem Einlösen einer Verordnung kann der Arzt die Verordnung für die Abrechnung signieren. Er bestätigt damit gegenüber der Krankenkasse, dass er die Leistung erbracht hat. Hier gilt ebenfalls, dass die qualifizierte elektronische Signatur rechtlich bindend ist und der Arzt für eventuelle Betrugsfälle und Fehler haftbar gemacht werden kann. Den Ärzten muss vor der Einführung des HBA deutlich gemacht werden, dass die qualifizierte elektronische Signatur die eigenhändige Unterschrift ersetzt und deshalb mit ihr ebenso sorgfältig umzugehen ist wie mit der eigenhändigen Unterschrift. Mit der Einführung der freiwilligen Anwendungen werden auch die Anwendungsbereiche für die elektronische Signatur

größer. Alle medizinischen Daten eines Patienten, die in die Telematikinfrastruktur übertragen werden, müssen zur Sicherung der Vertrauenswürdigkeit der Daten vor der Übermittlung signiert werden. Bringt der Patient selbst Daten in die ePA ein, muss er diese mittels einer eigenen Signaturkarte signieren. Die elektronische Signatur dient hier zur Feststellung der Urheberschaft. Der Empfänger der Daten kann dann selbst entscheiden, ob er Daten vertraut, die von diesem Autor stammen.

Ein weiterer wichtiger Punkt im Zusammenhang mit der elektronischen Signatur ist die Verschlüsselung. Alle Patientendaten, die in die Telematikinfrastruktur eingebracht werden, müssen mit Hilfe der elektronischen Gesundheitskarte verschlüsselt und beim Zugriff auf die Daten wieder entschlüsselt werden. Es muss den Versicherten deutlich gemacht werden, was mit der eGK alles möglich ist und dass sie die eGK wie eine EC-Karte behandeln sollten.

5.3 Anforderungen an den Konnektor

Es muss möglich sein, dass UKL über einen zentralen Konnektor an die Telematikinfrastruktur angeschlossen wird. Da es sich bei den verschiedenen Ambulanzen und dem stationären Bereich bei der Abrechnung mit der Krankenkasse um verschiedene Institutionen handelt, müssen diese in der Telematikinfrastruktur unterscheidbar sein. Die Identifikation der Institutionen erfolgt in der TI durch die SMC Typ B. Es ist also notwendig verschiedene SMC Typ B für die verschiedenen Ambulanzen und den stationären Bereich zu verwenden. Eine Möglichkeit ist die Verwendung unterschiedlicher Konnektoren für die Bereiche. Diese Möglichkeit kann jedoch aus Kostengründen nicht akzeptiert werden. Eine weitere Möglichkeit ist die Verwendung eines mandantenfähigen Konnektors. Ein mandantenfähiger Konnektor kann mit mehreren SMC Typ B betrieben werden und verwendet für die Verbindung die SMC der jeweiligen Institution. Ein Nachteil dieser Variante ist, dass sehr viele Arbeitsplätze über einen Konnektor Zugang zur Telematikinfrastruktur erhalten. Dadurch kann es zu Verbindungsüberlastungen und Abbrüchen kommen. Eine verteilte Realisierung mit mehreren Konnektoren zur Lastverteilung kann dann notwendig sein.

Wie bereits erwähnt, werden in Zukunft sehr viele Arbeitsplatzrechner den Zugang zur Telematikinfrastruktur über den Konnektor nutzen. Für eine effektive Arbeit in der Patientenaufnahme und in den Ambulanzen ist es notwendig, dass die Verbindung zur Telematikinfrastruktur funktioniert. Es soll deshalb Hochverfügbarkeit für den Konnektor gewährleistet sein.

Der Konnektor muss wie in der Spezifikation vorgesehen in einem Serverraum stehen, um ihn vor Diebstahl und Manipulation zu schützen. Es sollten die in den IT-Grundschutzkatalogen vorgeschlagenen Maßnahmen zum Schutz von Serverräumen (B2.4) realisiert werden. Dazu gehören Maßnahmen zum Schutz vor Stromausfall, Feuer- und Wasserschäden, gesicherte Türen und Fenster sowie Zutrittsbeschränkungen und Fernanzeige für Störungen.

5.4 Integration in das Sicherheitskonzept

Aus Sicherheitsgründen darf die VPN-Verbindung zwischen Konnektor und VPN-Konzentrator nicht am Paketfilter des UKL vorbei aufgebaut werden. Es gehört zum Sicherheitskonzept des UKL, dass alle Kommunikationsverbindungen mit dem externen Bereich über den Paketfilter aufgebaut werden müssen. Da Dienste auf Servern im internen Bereich aus dem externen Netz nicht erreichbar sind, ist es nicht möglich den Konnektor im internen Netzwerk zu betreiben. Der Konnektor muss demzufolge in einem Netzwerkteil außerhalb des internen Netzes eingesetzt werden.

Für die Einführung der elektronischen Gesundheitskarte mit den Pflichtanwendungen müssen die Patientenaufnahme und die Ambulanzen mit Kartenterminals ausgestattet werden. Wenn die Verwendung der freiwilligen Anwendungen realisiert wird, ist eine breitere Ausstattung mit Kartenterminals im stationären Bereich erforderlich.

Es wird vorgeschlagen in den Ambulanzen das VERSA-Konzept zu realisieren. Dabei kann der HBA an zentraler Stelle in einer Ambulanz gesteckt werden. Zum Schutz des Raumes sind Zutrittsreglung erforderlich und der Raum sollte wenn möglich verschlossen werden.

Die Kartenterminals für die Card-to-Card-Authentisierung und die eGK befinden sich an den Arbeitsplätzen. Da diese Räume selten ausreichend durch organisatorische Maßnahmen gesichert werden können, sollte ein Diebstahl- und Manipulationsschutz angebracht werden. Die SMC-A in Kartenterminals für Card-to-Card-Authentisierung muss normalerweise nicht gesteckt werden und kann deshalb technisch vor Diebstahl und Manipulation gesichert werden.

Bei der Realisierung des VERSA-Konzeptes kann es leicht passieren, dass die Kartenterminals bei der Card-to-Card-Authentisierung in verschiedenen Netzwerksegmenten liegen. Es muss also möglich sein, diese Art der Kommunikation über verschiedene Netzwerksegmente zu realisieren.

5.5 Zusammenfassung der Anforderungen

Zur Zusammenfassung der Anforderungen sollen diese hier noch einmal zusammengestellt werden.

1. Integration des Primärsystems:
    a. Connector Abstraction Layer für das Primärsystem;
    b. Kommunikation über den Kommunikationsserver;
    c. Unterstützung von synchroner und asynchroner Kommunikation durch Kommunikationsserver;
2. Verwendung der elektronischen Signatur:
    a. Trust Center zur Zertifikatausstellung und -prüfung;
    b. Trusted Viewer am Arbeitsplatz des Benutzers;
    c. Sorgfältiger Umgang der Karteninhaber mit den Karten;
3. Anforderungen an den Konnektor:
    a. Anschluss aller Teile des UKL an die Telematikinfrastruktur über einen Konnektor;
    b. Hochverfügbarkeit des Konnektors;
    c. Schutzmaßnahmen für den Konnektor nach den IT-Grundschutzkatalogen;
4. Sicherheitsanforderungen:
    a. Aufbau von Verbindungen vom internen Netz zur TI nur über den Paketfilter;
    b. Erreichbarkeit des Konnektors aus der TI;
    c. Verwendung des VERSA-Konzept;
    d. Schutz der zentralen Stelle zum Stecken der HBA;
    e. Schutz der Kartenterminals an den Arbeitsplätzen;
5. Kommunikation über verschiedene Netzwerksegmente.

6 Referenzmodell

In Kapitel 3 wurde das Architekturkonzept der Gematik vorgestellt. Für die Integration dieses Architekturkonzeptes in das Krankenhausinformationssystem des UKL ist es notwendig die relevanten Teile des aktuellen Krankenhausinformationssystems zu analysieren und bezüglich der Eignung für die neuen Anwendungen zu bewerten. Die gewonnen Informationen wurden in Kapitel 4 dargestellt. Kapitel 5 beschäftigt sich mit der Spezifikation der Anforderungen für die Integration der Telematikinfrastruktur in das Krankenhausinformationssystem des UKL. Aus den dargestellten Anforderungen soll nun ein 3LGM²-Referenzmodell abgeleitet werden.

6.1 Modellierung der fachlichen Ebene

Die Einführung der elektronischen Gesundheitskarte führt zu einer Erweiterung der Rechnerunterstützung der betroffenen Aufgaben. Von den Pflichtanwendungen sind die Aufgaben "Prüfung der Berechtigung der Inanspruchnahme von Leistungen", "Erstellen von Verordnungen" und "Einlösen von Verordnungen" betroffen.

Die Prüfung der Berechtigung der Inanspruchnahme von Leistungen wird in Abbildung 6-1 modelliert. Dabei wird als erstes das Lichtbild auf der elektronischen Gesundheitskarteund dann wie bisher das Ablaufdatum der Karte überprüft. Um eine eventuelle Sperrung der Karte zu erkennen, wird eine zentrale Sperrliste der Gematik durchsucht. Nach der Prüfung der Gültigkeit der Karte, wird überprüft, ob eine Aktualisierung der Kartendaten mit den Daten der Krankenkasse erforderlich ist. Diese wird gegebenenfalls durchgeführt und die Versichertenstammdaten werden wie bisher in das Primärsystem übertragen. Im Vergleich zum Ablauf bei Verwendung der KVK, wird die Gültigkeitsprüfung ausgeweitet und eine Aktualisierung der Stammdaten auf der Karte wird ermöglicht.

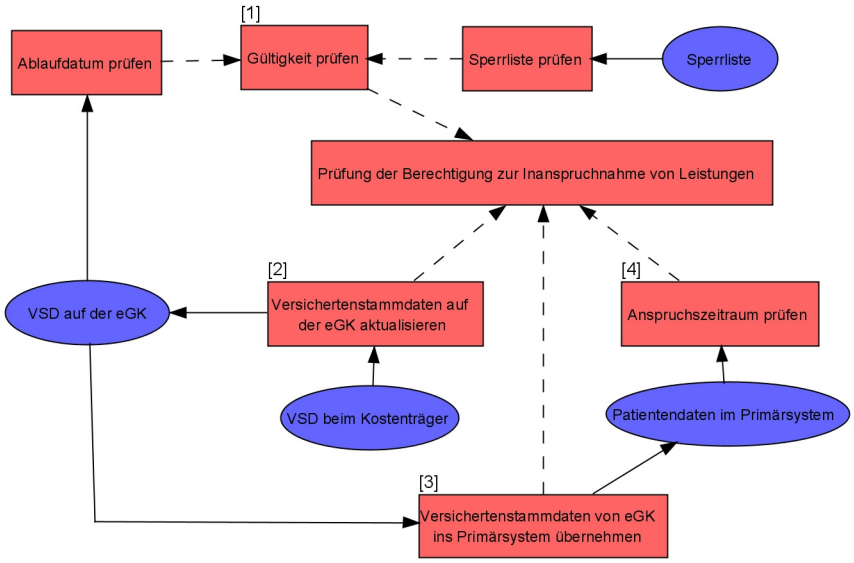


Abbildung 6-1: 3LGM²-Teilmodell für die Prüfung der Berechtigung zur Inanspruchnahme von Leistungen

Bei der Erstellung von Verordnungen erfolgt ebenfalls eine Erweiterung der Rechnerunterstützung. Die Daten werden im Primärsystem eingetragen. Statt dem Ausdrucken der Verordnung erfolgt die Prüfung und Signatur der Verordnung mit Rechnerunterstützung innerhalb der Telematikinfrastruktur(TI). Danach erfolgt die Übertragung der verschlüsselten und signierten Verordnung auf die elektronische Gesundheitskarte oder in den zentralen Teil der Telematikinfrastruktur. Um die Einlösung einer Verordnung durch einen Stellvertreter zu

ermöglichen, kann ein Papierbeleg für den Zugriff auf die Verordnung im zentralen Teil der TI gedruckt werden. Der Vorgang zur Erstellung von eVerordnungen ist in Abbildung 6-2 modelliert.

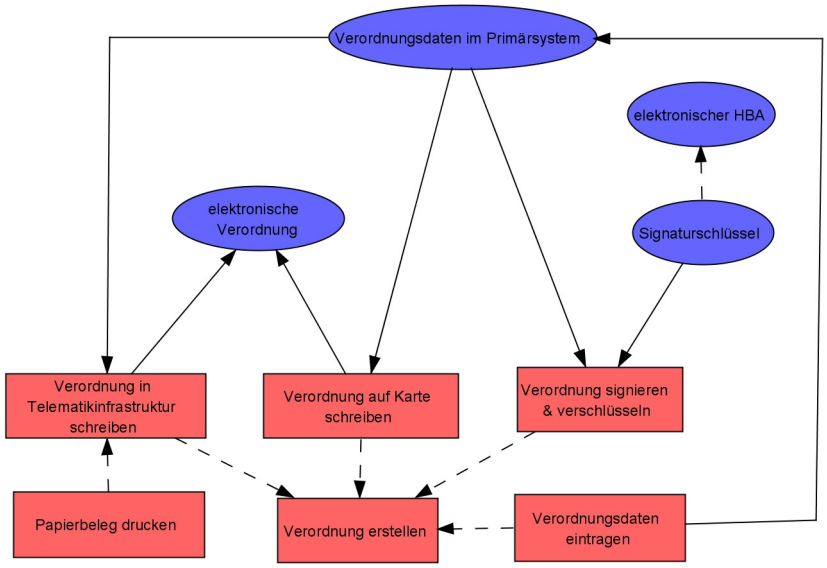


Abbildung 6-2: 3LGM²-Teilmodell für die Erstellung von elektronischen Verordnungen

Auch beim Einlösen von Verordnung wird die Rechnerunterstützung ausgeweitet. Im ambulanten Bereich werden Verordnungen von Behandlungen eingelöst, im stationären Bereich hauptsächlich Verordnungen von Krankenhausbehandlungen. Der Ablauf der Einlösung ist in beiden Fällen gleich und ist in Abbildung 6-3 modelliert. Ist bei der Einlösung die eGK des Patienten vorhanden, werden alle Verordnungen auf der eGK und in der TI angezeigt. Bei Einlösung mit einem Papierbeleg, werden nur die Verordnungen in der TI aufgelistet. Ob eine Verordnung angezeigt wird hängt davon ab, ob die Institution die entsprechende Berechtigung zur Einlösung besitzt und ob die Verordnung sichtbar ist. Bei der anschließenden Gültigkeitsprüfung werden das Verordnungsdatum und die Signatur überprüft. Es werden die Einlösedaten ergänzt und die Verordnung wird vom Transportmedium, d.h. eGK oder TI gelöscht. Zur Abrechnung der Verordnung erfolgt wiederum die Signatur und Verschlüsselung durch den Einlöser und eine Übermittlung zur Abrechnungsstelle.

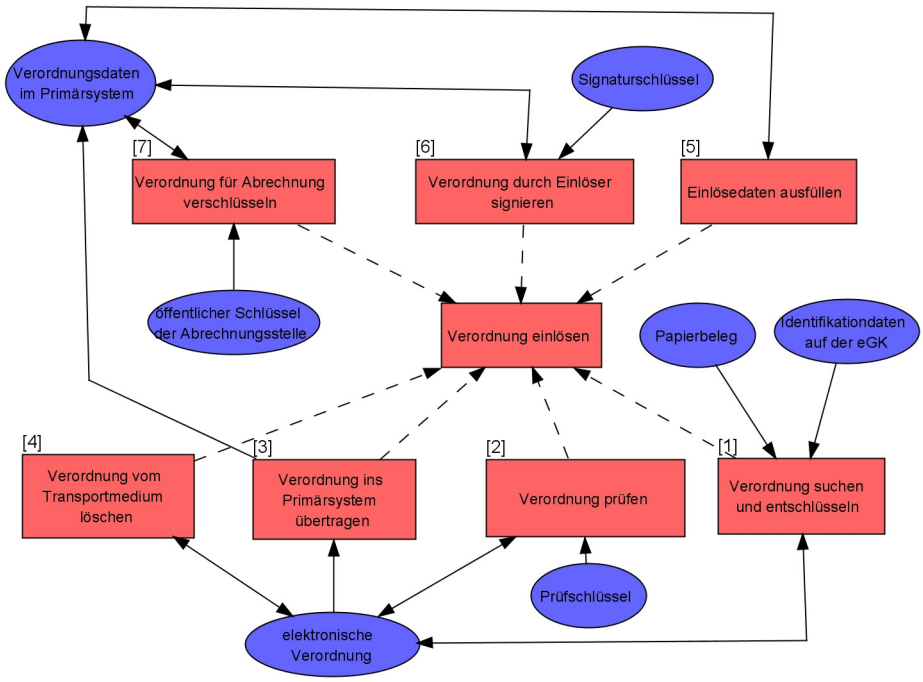


Abbildung 6-3: 3LGM²-Teilmodell für die Einlösung einer elektronischen Verordnung

Bei den Fachkonzepten handelt es sich um verbindliche Vorgaben der Gematik, deshalb entspricht die fachliche Ebene des Referenzmodells der fachlichen Eben des Architekturkonezptes. Die Abbildung 3-14, Abbildung 3-15, Abbildung 3-16 wurden an dieser Stelle erneut verwendet, um das Referenzmodell zu vervollständigen.

6.2 Modellierung der logischen Werkzeugebene

6.2.1 Primärsystem

Das Krankenhausinformationssystem eines großen Krankenhauses enthält viele verschiedene Anwendungssysteme um die Aufgaben der Einrichtung möglichst gut zu unterstützen. Für eine Integration der Telematikinfrastruktur in das Krankenhausinformationssystem ist es deshalb notwendig die Primärsysteme zu identifizieren. Für die Pflichtanwendungen wird dies in der Regel das Patientenverwaltungssystem sein. Für die freiwilligen Anwendungen der elektronischen Gesundheitskarte kann es in Zukunft erforderlich werden weitere Teile des Krankenhausinformationssystems wie zum Beispiel das Radiologieinformationssystem als Primärsysteme zusätzlich einzubinden.

Die verschiedenen vorhandenen Anwendungssysteme sind durch Kommunikationsbeziehungen verknüpft. Zur Realisierung der Kommunikation wird nach [Winter 2002] häufig eine Sternarchitektur mit einem Kommunikationsserver im Zentrum verwendet. Die Sternarchitektur wird verwendet, weil für jedes Anwendungssystem nur eine Schnittstelle zum Kommunikationsserver realisiert werden muss und dadurch die Menge der Schnittstellen zwischen Anwendungssystemen klein gehalten werden kann. Die bereits vorhandene Sternarchitektur kann genutzt werden indem der Konnektor über eine Schnittstelle an den Kommunikationsserver angeschlossen wird. Zur Integration der Primärsysteme muss dann nur die schon vorhandene Schnittstelle zwischen dem Primärsystem und Kommunikationsserver angepasst werden. Abbildung 6-4 zeigt die dabei entstehende Architektur.

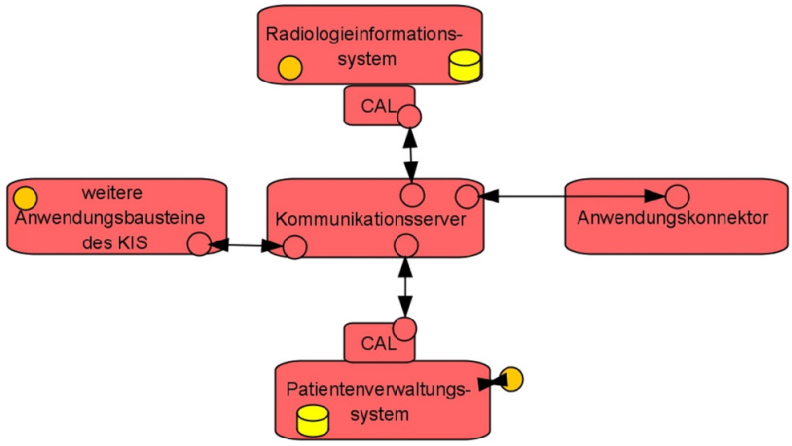


Abbildung 6-4: Integration mehrerer Primärsysteme

Die Hersteller der Primärsysteme müssen eine Middle-Ware-Komponente für die Kommunikation mit dem Konnektor für ihre Produkte zur Verfügung stellen. Diese Komponente wird als Connector Abstraction Layer bezeichnet und erzeugt aus den Daten des Primärsystems HL7-Nachrichten an den Konnektor. Die Verwendung des Kommunikationsstandards HL7 ist für Krankenhäuser kein Problem, da hier auch bisher mit HL7 gearbeitet wurde und die vorhandenen HL7-Schnittstellen zwischen Primärsystem und Kommunikationsserver nur angepasst werden müssen.

6.2.2 Anwendungskonnektor

Der Anwendungskonnektor ist die Kernkomponente der Telematikinfrastruktur bei den Leistungserbringern. Er bildet die sichere Schnittstelle zwischen Primärsystem, Kartenterminal, Karte und den zentralen Dienste. Der Anwendungskonnektor stellt dem Primärsystem Basisdienste und Fachdienste zur Verfügung. Die Basisdienste enthalten Kryptographiedienste, Kartenterminaldienste

und Kartendienste. Die Fachdienste realisieren einen Teil der Ablauflogik des Dienstes und die Kommunikation mit dem Primärsystem und den zentralen Fachdiensten. Dazu werden die Basisdienste verwendet. Nähere Informationen zum Konnektor können in Kapitel 3.1.2 nachgelesen werden.

6.2.3 Zentrale Dienste

Der zentrale Teil der Telematikinfrastruktur besteht aus Fachdiensten und Infrastrukturdiensten (siehe Abbildung 6-5). Der Zugang zum zentralen Teil wird über eine Kommunikationsverbindung zwischen dezentralem Konnektor und dem Logischen Telematik-Zugangsprovider hergestellt.

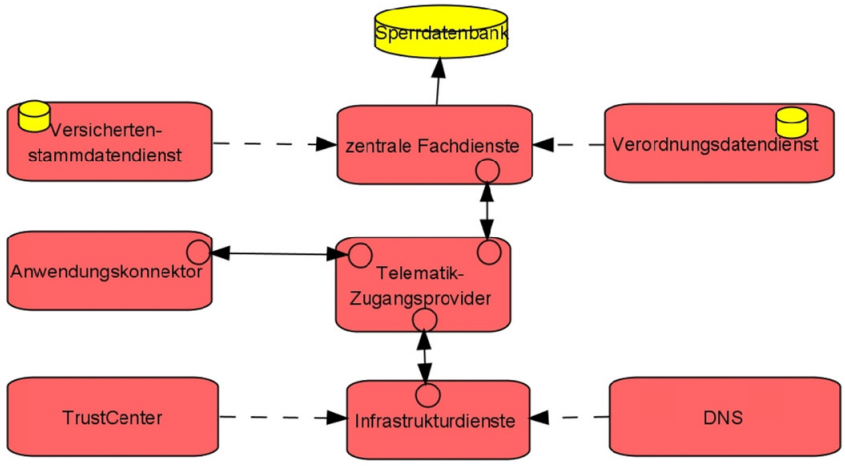


Abbildung 6-5: Zentrale Dienste

Die Fachdienste beinhalten die zentral durchführbaren Teile der Ablauflogik und speichern die Nutzdaten. Im zentralen Teil wird immer mit verschlüsselten medizinischen Daten gearbeitet. Die Entschlüsselung der Daten ist nur mit Hilfe der elektronischen Gesundheitskarte möglich.

Die Infrastrukturdienste sind Dienste, die nicht nur in der Telematikinfrastruktur vorhanden sind, sondern auch in anderen Bereichen Anwendung finden. Dazu gehört zum Beispiel das TrustCenter, der Broker zur Lokalisierung der Dienste oder der DNS.

6.2.4 Elektronische Signatur

Für die Erstellung einer qualifizierten elektronischen Signatur ist die Verwendung einer zertifizierten Signaturanwendungskomponente erforderlich. Die von der Gematik zugelassenen Konnektoren sind für die Erzeugung qualifizierter elektronischer Signaturen geeignet. Laut Signaturgesetz ist für die Erstellung und Prüfung von Signaturen ein Trusted Viewer erforderlich. Der Konnektor besitzt eine Schnittstelle einem Trusted Viewer, der als eigenständiger Anwendungsbaustein auf dem Arbeitplatz des Benutzers verfügbar sein muss.

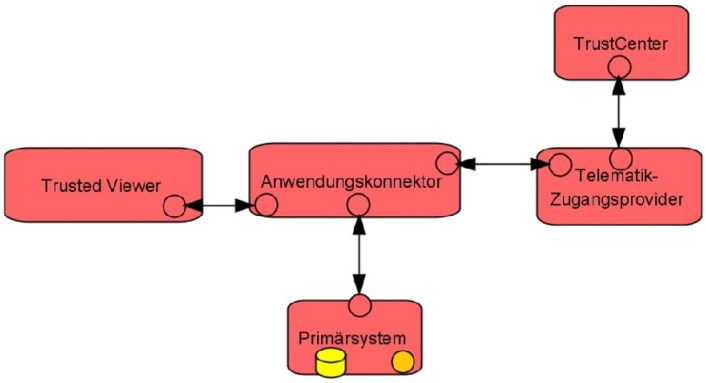


Abbildung 6-6: Komponenten für die Anwendung einer Elektronischen Signatur

Für die Prüfung einer qualifizierten elektronischen Signatur ist die Verbindung zum zentralen Trust Center der Gematik erforderlich, über das alle in der Telematikinfrastruktur benötigten Zertifikatinformationen abgerufen werden können. In Abbildung 6-6 sind die Komponenten für die Anwendung der elektronischen Signatur und deren Kommunikationsbeziehungen dargestellt.

6.2.5 Weitere dezentrale Komponenten

Für die Verwendung der Anwendungen der Telematikinfrastruktur ist die Nutzung der elektronischen Gesundheitskarte und des elektronischen Heilberufausweises zur Prüfung der Zugriffsberechtigung notwendig. Weiterhin dient der elektronische Heilberufeausweis der Erzeugung qualifizierter elektronischer Signaturen auf medizinischen Dokumenten. Die Nutzung der Karten durch das Primärsystem erfolgt über den Konnektor. Dieser ordnet den Arbeitplätzen Kartenterminals zu und besitzt eine Schnittstelle zum Kartenterminal. Über diese Schnittstelle kann der Status des Terminals und der Karten bestimmt werden und eine Steuerung des Kartenterminals ist ebenfalls möglich. Durch das Kartenterminal kann der Konnektor auch auf die einzelnen Prozessorkarten zugreifen und die durch die Karten angebotenen Dienste ausführen.

6.2.6 Modell der logischen Werkzeugebene

Die genannten Aspekte können im 3LGM²-Modell dargestellt werden. Abbildung 6-7 zeigt die logischer Werkzeugebene des 3LGM²-Modells.

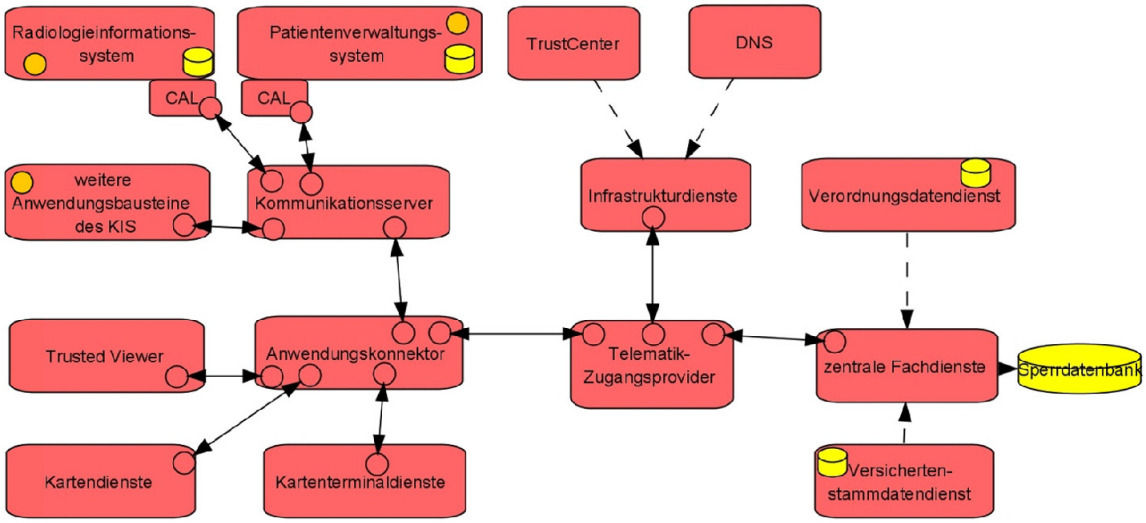


Abbildung 6-7: Logische Werkzeugebene des 3LGM²-Referenzmodells

6.3 Modellierung der Physische Werkzeugebene

6.3.1 Hardware

Die Anwendungsbausteine sind auf verschiedenen Datenverarbeitungsbausteinen installiert. In einem Krankenhausinformationssystem wird es einen oder mehrere Server für jeden Anwendungsbaustein geben. Durch die Verwendung von virtuellen Servern können auch mehrere Anwendungsbausteine auf einem physischen Datenverarbeitungsbaustein installiert sein. Die Server befinden sich im internen Netzwerk des Krankenhauses und können mit den Clients kommunizieren. Im Referenzmodell sind diese internen Server als ein Datenverarbeitungsbaustein dargestellt. Es sei angemerkt, dass dieser Datenverarbeitungsbaustein im realen Fall sehr komplex sein kann. Der für die Datenintegration der Anwendungsbausteine benötigte Kommunikationsserver ist ebenfalls auf einem Server installiert. und befindet sich im internen Netzwerk des Krankenhauses.

Der Anwendungskonnektor kann einer eigenen Hardware oder auf einem Server installiert sein. Der Konnektor ist für den Aufbau der Verbindung zur zentralen TI verantwortlich. Es wird eine VPN-

Verbindung auf Basis von IPSec aufgebaut. Das Schlüsselmaterial und die Authentisierungsdaten für den Verbindungsaufbau befinden sich auf der SMC-B. Die SMC-B (Secure Module Card Typ B) ist eine Institutionskarte und dient in der Telematikinfrastruktur als Träger der kryptograpischen Identität einer Institution. Für die Nutzung der SMC-B am Konnektor muss ein Kartenterminal zur Verfügung gestellt werden. Das Kartenterminal muss sich Sicherheitsgründen im selben Raum, bzw. Schrank befinden. Die Gegenstelle für die VPN-Verbindung ist der VPN-Konzentrator. Der VPN-Konzentrator stellt die Hardwareumsetzung des logischen Telematik-Zugangsprovider auf logischer Werkzeugebene dar. Der logische Telematik-Zugangsprovider, bzw. der VPN-Konzentrator erlaubt den Leistungserbringer den Zugriff auf die TI über VPN-Verbindungen. Informationen zu den technischen Details der VPN-Verbindung werden in Kapitel 3.1.6 dargestellt.

Für die Verwendung der elektronischen Gesundheitskarte sind Kartenterminals erforderlich. Im Architekturkonzept der Gematik ist festgelegt, dass netzwerkfähige Kartenterminals verwendet werden müssen. Diese können direkt in das interne Netzwerk integriert werden. Die Zuordnung der Kartenterminals erfolgt über durch den Konnektor. Werden nicht netzwerkfähige Kartenterminals verwendet, besteht nach dem Architekturkonzept die Möglichkeit, dass diese an einen Arbeitsplatzrechner angeschlossen werden und der Arbeitsplatzrechner ein netzwerkfähiges Kartenterminal emuliert.

Die Hardwareimplementierung der zentralen Dienste ist für die Integration der Telematikinfrastruktur in ein Krankenhaus nicht relevant. Im Referenzmodell wird dieser Serververbund deshalb als ein Datenverarbeitungsbaustein dargestellt.

6.3.2 Sicherheitskonzept

Die bereits vorhandenen Server des internen Netzwerkes sollten durch das Sicherheitskonzept des Krankenhauses bereits ausreichend gesichert sein. Diese Komponenten werden hier nicht betrachtet. Der zentrale Teil der Telematikinfrastruktur und der VPN-Konzentrator werden ebenfalls nicht betrachtet, weil sie nicht im Verantwortungsbereich des Krankenhauses liegen. In [SP-KON] werden Maßnahmen zum Schutz der Konnektorhardware beschrieben. Weitere Maßnahmen können aus dem Betriebskonzept für die IT-Infrastruktur abgeleitet werden. Die Maßnahmen zum Schutz des Konnektors wurden bereits in Kapitel 3.1.11.2 erläutert.

Zum Schutz der Kartenterminals für den HBA kann das VERSA-Konzept (VERteilte Signatur Arbeitsplätze) verwendet werden. Dabei wird der HBA an zentraler Stelle gesteckt. Die zentrale Stelle kann durch organisatorische und technische Maßnahmen gut gesichert werden. Zur Verwendung des HBA muss am Arbeitsplatz ein Kartenterminal mit fest eingebauter SMC-A verfügbar sein. Der Besitzer des HBA kann an diesem Kartenterminal seine PIN eingeben, die dann über einen sicheren Kanal zum HBA weitergeleitet wird, wo die Authentisierung findet statt. Das Kartenterminal am Arbeitsplatz sollte gegen Manipulation und Missbrauch geschützt werden. Für die Benutzung der eGK müssen ebenfalls Kartenterminals am Arbeitsplatz vorhanden sein. Diese Kartenterminals müssen technisch gegen Manipulation geschützt werden. Da sich der Konnektor sowie die verschiedenen Kartenterminals und Arbeitplätze in einem großen Krankenhaus in verschiedenen Netzwerksegmenten befinden können, ist es wichtig, dass Segment übergreifende Kommunikation realisiert werden kann.

Im Referenzmodell wird der Konnektor in einem eigenen Netzwerkbereich am Paketfilter aufgestellt. Nach dem Architekturkonzept der Gematik soll die Verbindung zur zentralen Infrastruktur über einen WAN-Router aufgebaut werden. Der WAN-Router ist für NAT zuständig. Ist der Paketfilter der Institution in der Lage NAT durchzuführen, kann die Verbindung zur zentralen Infrastruktur über den Paketfilter aufgebaut werden. Beschränkt man zusätzlich am Paketfilter die Kommunikation zwischen Konnektor und VPN-Konzentrator auf die durch die Gematik definierten Dienste, ist der Konnektor vor Angriffen aus dem externen Netz geschützt. Die Kommunikation zwischen Konnektor und dem internen Netz mit Kartenterminals und Primärsystem erfolgt ebenfalls über den Paketfilter. Das ist notwendig da die Sicherheitskonzepte der Krankenhäuser eine Erreichbarkeit von Diensten aus dem externen Netzwerk verbieten und der Konnektor deshalb aus dem internen Netz ausgelagert werden muss. Die Erreichbarkeit ist notwendig für Rückkommunikation aus der zentralen TI und für die Unterstützung der zentralen Dienste bei der Nutzung von Kartenterminals und Karten.

6.3.3 Modell der physischen Werkzeugebene

Die in den vorangegangenen Abschnitten beschriebenen Komponenten sollen nun im 3LGM²-Modell dargestellt werden. Abbildung 6-8 zeigt die physische Werkzeugebene des 3LGM²-Modells.

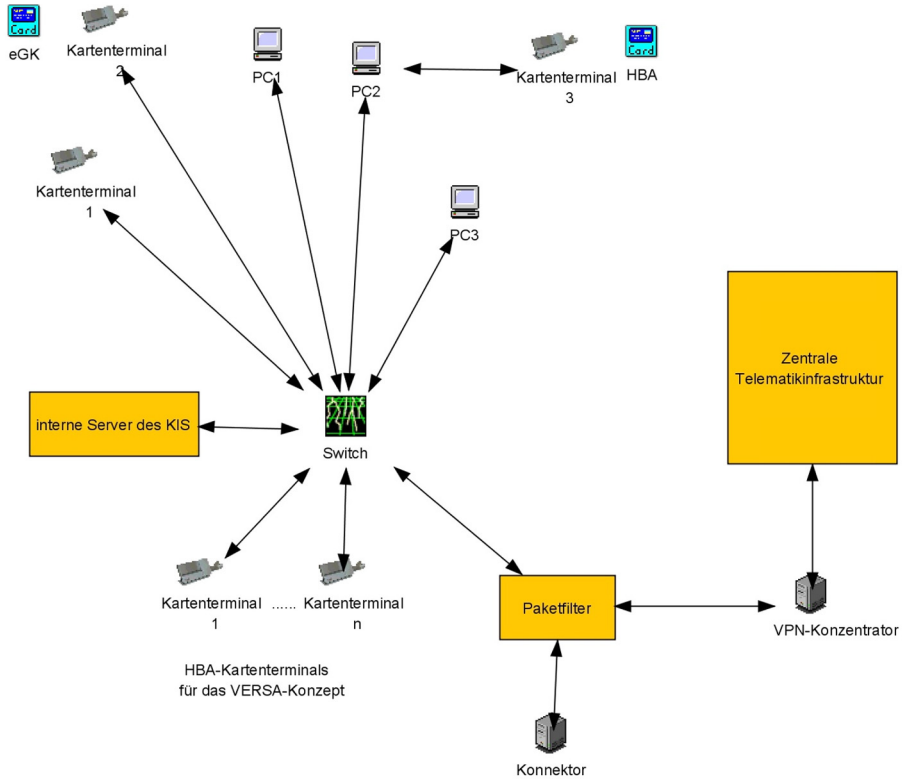


Abbildung 6-8: Physische Werkzeugebene des 3LGM²-Referenzmodells

7 Anwendung des Referenzmodells auf das UKL

Beim Ableiten von speziellen Modellen aus einem Referenzmodell müssen die allgemeinen Komponenten des Referenzmodells durch die konkreten Komponenten aus der entsprechenden Institution ersetzt werden.

7.1.1 Fachliche Ebene

Da die Vorgehensweisen durch die Fachkonzepte der Gematik verbindlich vorgegeben werden, entspricht die Fachliche Ebene der Fachlichen Ebene des Referenzmodells. In der Bewertung bezüglich der Integration in den Workflow (siehe Kapitel 3.1.11.3) wurden kritische Punkte beleuchtet. Durch die Einführung der Autorisierung von Institutionen wurden bereits die größten Probleme für die Integration in den Workflow beseitigt. Sollten dennoch Abweichungen zwischen Workflow des UKL und dem vorgesehenen Workflow vorhanden sein, muss der Workflow des UKL angepasst werden.

7.1.2 Logische Werkzeugebene

In Abbildung 7-1 ist die logische Werkzeugebene des abgeleiteten Modells dargestellt. Für die Ableitung eines speziellen Modells aus dem Referenzmodell müssen auf logischer Werkzeugebene die Primärsysteme identifiziert werden. Das Primärsystem für die Pflichtanwendungen der TI ist nach dem Referenzmodell das Patientenverwaltungssystem. Am UKL handelt es sich um das Anwendungssystem SAP IS-H*MED. Da im ersten Schritt nur die Pflichtanwendungen realisiert werden, ist die Integration weiterer Anwendungsbausteine des KIS in die TI nicht notwendig. Die Kommunikation zwischen Primärsystem und Anwendungskonnektor erfolgt über den Kommunikationsserver.

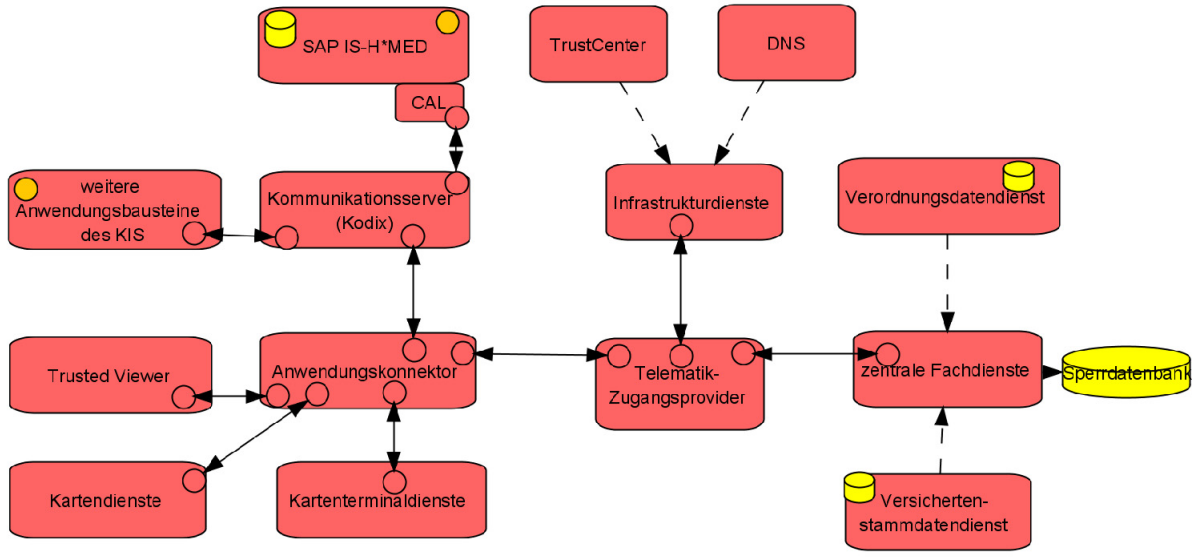


Abbildung 7-1: Logische Werkzeugebene des 3LGM²-Modells zur indirekten Realisierung

Das heißt, die vorhandene Schnittstelle zwischen Primärsystem und Kommunikationsserver wird ausgebaut und eine Schnittstelle zwischen Anwendungskonnektor und Kommunikationsserver eingerichtet. Die Konfiguration des Kommunikationsservers muss dabei gegebenenfalls angepasst werden. Der Vorteil dieser Realisierung besteht darin, dass bei einer Integration weiterer Teile des Krankenhausinformationssystems als Primärsystem für die Telematikinfrastruktur, keine neuen Schnittstellen geschaffen werden müssen, sondern die bestehenden Schnittstellen ausgebaut werden können. Ein Nachteil am UKL ist, dass die Eigenentwicklung Kodix keine synchrone Kommunikation

beherrscht und deshalb eine Weiterentwicklung des Kommunikationsservers notwendig ist. Aus diesem Grund kann es notwendig werden die vorgeschlagene Architektur nicht zu verwenden sondern eine andere Realisierung zu wählen.

Es besteht die Möglichkeit eine direkte Realisierung der Schnittstelle zwischen Anwendungskonnektor und Primärsystem zu verwenden.

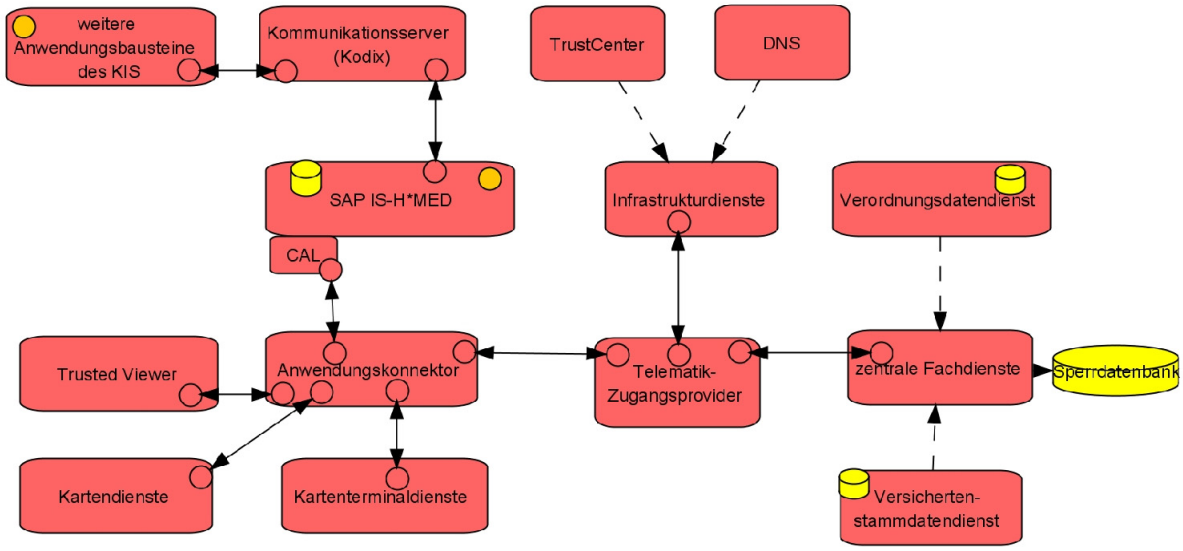


Abbildung 7-2: Logische Werkzeugebene des 3LGM²-Modells zur direkten Realisierung

Der Vorteil dieser Variante (siehe Abbildung 7-2) besteht darin, dass am Kommunikationsserver keine Änderungen notwendig sind. Für das UKL kann dadurch die Weiterentwicklung des Kommunikationsservers um synchrone Kommunikation gespart werden. Wird in Zukunft jedoch die Integration weiterer Teile des KIS notwendig, ist ein größerer Aufwand notwendig. Es besteht dann die Möglichkeit auf die im Referenzmodell vorgeschlagene Lösung umzusteigen oder auf die Realisierung weiterer direkter Schnittstellen zum Anwendungskonnektor zurückzugreifen. Die zweite Möglichkeit führt dazu, dass eine schwer wartbare Architektur entsteht. Das sollte unbedingt vermieden werden. Die indirekte Realisierung über den Kommunikationsserver sollte dieser Variante deshalb vorgezogen werden.

7.1.3 Physische Werkzeugebene

Für die Ableitung der physischen Werkzeugebene aus dem Referenzmodell, muss die Struktur des Netzwerks der Institution abgebildet werden. Es soll hier nur ein stark vereinfachtes Modell des internen Netzwerkes verwendet werden (siehe Abbildung 7-3).

Im Referenzmodell wird der Konnektor in einen Netzwerkteil außerhalb des internen Netzwerkes verlagert. Die VPN-Verbindung wird über den Paketfilter aufgebaut. Der Paketfilter kann den Konnektor vor Angriffen aus dem externen Netz schützen, indem die Kommunikation zwischen VPN-Konzentrator und Konnektor auf die von der Gematik definierten Dienste beschränkt wird.

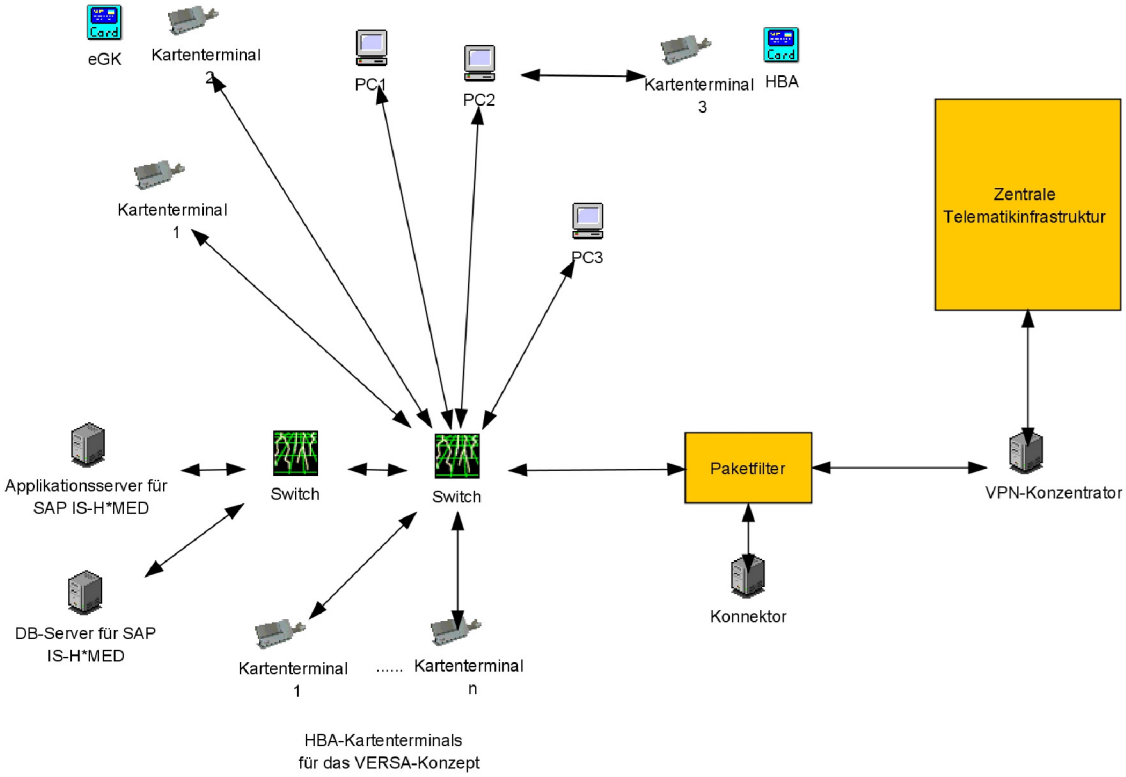


Abbildung 7-3: Physische Werkzeugebene des 3LGM²-Modells zur Realisierung ohne WAN-Router

Wird in einer Institution ein Paketfilter eingesetzt der kein NAT durchführen kann, ist es nicht möglich die VPN-Verbindung über den Paketfilter aufzubauen. Es muss dann wie von der Gematik vorgeschlagen ein NAT-fähiger WAN-Router verwendet werden. Bei der in Abbildung 7-4 dargestellen Lösung ist der Konnektor nicht durch den Paketfilter vor Angriffen aus dem externen Netz geschützt. Deshalb ist die Lösung aus dem Referenzmodell dieser Lösung vorzuziehen.

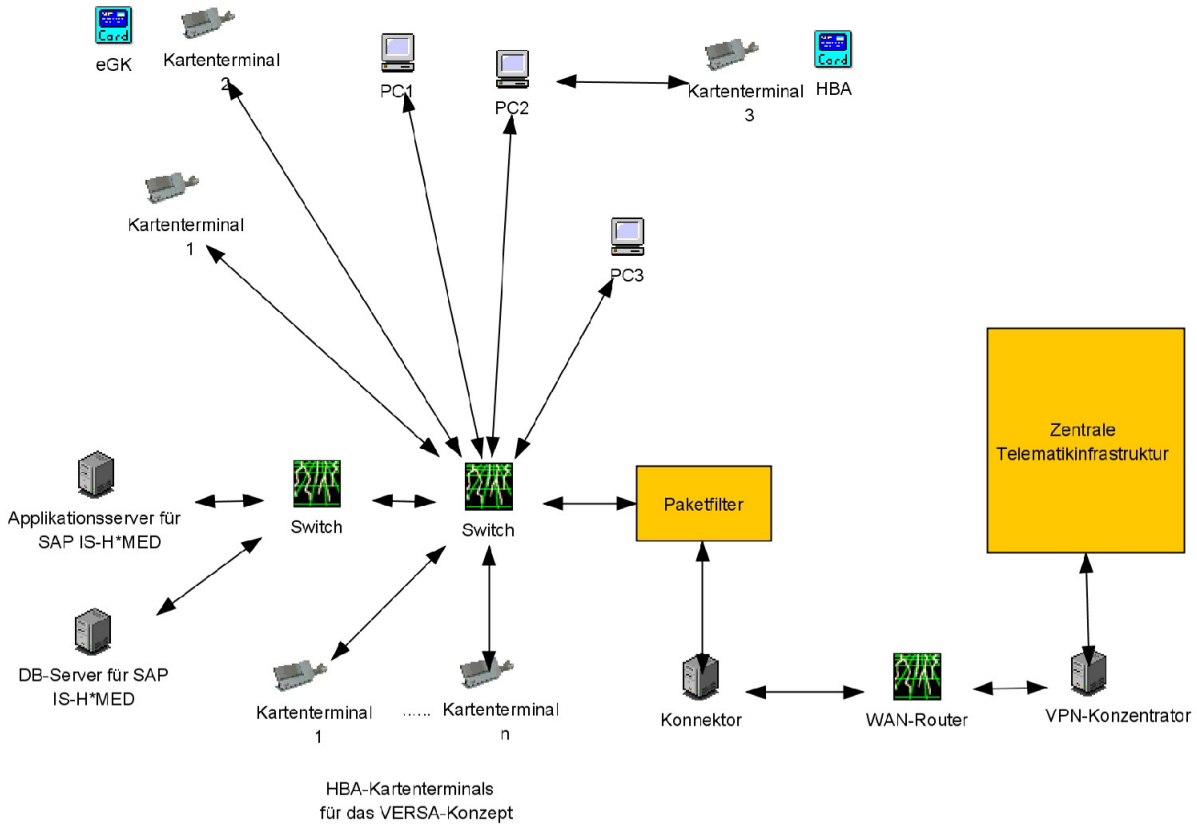


Abbildung 7-4: Physische Werkzeugebene des 3LGM²-Modells zur Realisierung mit WAN-Router

8 Zusammenfassung

Im Folgenden sollen nun die Ergebnisse zu den in Kapitel 1.4 formulierten Aufgaben zusammengestellt werden.

Arbeitspaket 1: Erarbeitung der Rahmenbedingungen

Es sollte ein Überblick über die gesetzlichen Vorgaben für die Einführung der elektronischen Gesundheitskarte(eGK) gegeben werden. Das Fundament für die Einführung der elektronischen Gesundheitskarte bildet SGB V §291a. Es werden darin die Anwendungen der eGK beschrieben, grundlegende Maßnahmen zu Datenschutz und Datensicherheit, sowie die Aufgaben der Gematik. Die Anwendungen der eGK werden in Kapitel 2.1 dargestellt. Die Maßnahmen zu Datenschutz und Datensicherheit nach SGB V sind in Kapitel 2.3 beschrieben. Weiterhin wurden in Kapitel 2.3 die Inhalte des Bundesdatenschutzgesetz betrachtet. Für den Zugriff auf die Daten der eGK und das Einbringen von Daten in die Telematikinfrastruktur (TI) ist nach dem SGB V §291a ein elektronischer Heilberufeausweis(HBA) mit der Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen notwendig. Die gesetzlichen Festlegungen für den Einsatz der elektronischen Signatur können in Kapitel 2.4 nachgelesen werden.

Im zweiten Teil des Arbeitspaketes sollte die Arbeit der Gematik untersucht werden. Es wurde eine Analyse der technischen Spezifikationen und Architekturspezifikationen durchgeführt. In Kapitel 3.1 wurde das Architekturkonzept der Gematik als Ergebnis dieser Analyse dargestellt, modelliert und bewertet.

Eine weitere Aufgabe der Gematik ist die Durchführung von Tests. Die Rahmenbedingungen für die Testmaßnahmen, sowie ein Zeitplan wurden durch eine Ersatzvornahme des BMGS vorgegeben. Diese Rahmenbedingungen wurde in Kapitel 3.2.2 vorgestellt. Weiterhin sollten die verwendeten Architekturen in den Modellregionen analysiert werden. Diese Aufgabe wurde stellvertretend für alle Modellregionen an der Modellregion Löbau Zittau durchgeführt. In den Modellregionen wurden bisher keine 10000er Tests durchgeführt und deshalb liegen auch keine Erfahrungen bei der Integration in ein Gesundheitsunternehmen vor. Von der Gematik wurden einige Einsatzszenarien ausgearbeitet und Hinweise für die Integration des Konnektors gegeben. Diese Szenarien wurden in Kapitel 3.1.8 dargestellt. Praktische Erfahrung mit der Integration konnten nicht dargestellt werden.

Arbeitspaket 2.1: Analyse des Ist-Zustands am UKL

In Kapitel 4 wurde der Ist-Zustand des UKL analysiert und modelliert. Den Schwerpunkt bildete die Darstellung des Sicherheitskonzeptes und die Architektur auf physischer Werkzeugebene. Eine Bewertung des Ist-Zustands der Eignung für die neuen Anwendungen wurde in Kapitel 4.2 durchgeführt. Die Bewertung wurde bezüglich der Integration des Primärsystems in die TI, der Integration des Sicherheitskonzeptes des UKL mit dem der TI und der Integration des Workflows des UKL mit dem der TI vorgenommen. Es werden die bei der Integration der TI nutzbaren Konzepte und auftretenden Problemfelder dargestellt.

Arbeitspaket 2.2: Erstellen eines Anforderungskatalogs für die Lösungsarchitektur (Soll-Zustand)

In Kapitel 5 werden die Anforderungen für eine Integration der TI in das UKL spezifiziert. Es werden Anforderungen bezüglich der Integration des Primärsystems dargestellt. Im folgenden werden Einsatzgebiete der elektronischen Signatur beschrieben und Anforderungen die sich aus der Verwendung der elektronischen Signatur ergeben. Es werden dabei technische Anforderungen und Anforderungen an die Inhaber der benötigten Karten (eGK, HBA) beschrieben. In Kapitel 5.3 sind Anforderungen an den Konnektor formuliert. Dazu gehören Anforderungen zum Schutz des Konnektors, Verfügbarkeitsanforderungen und Anforderungen für die Verwaltung verschiedener Institutionen für die Abrechnung mit der Krankenkasse. Ein weiterer Anforderungsblock sind die

Sicherheitsanforderungen für die VPN-Verbindung und die Kartenterminals. Diese werden in Kapitel 5.4. Am Ende des Kapitels werden unter 5.5 die Anforderungen zusammengefasst.

Arbeitspaket 3: Erstellung eines 3LGM²-Referenzmodells

In Kapitel 6 wird aus den Anforderungen für die Integration der TI am UKL ein 3LMG²-Referenzmodell abgeleitet. Bei der Erstellung des Referenzmodells wurde eine Zielarchitektur ausgearbeitet und modelliert. Mit Hilfe des Referenzmodells soll die Spezifikation der Sollarchitektur in Projekten zur Integration der Telematikinfrastruktur in ein Gesundheitsunternehmen vereinfacht werden, da durch das Mustermodell auf bekannte Probleme hinweist und Lösungsansätze bietet. Die Anwendung des 3LGM²-Referenzmodells erfolgt durch Ableitung von speziellen Modellen indem die allgemeinen Komponenten aus dem Referenzmodell durch die konkreten Komponenten der Institution ersetzt werden. In Kapitel 7 der Arbeit wurde aus dem 3LGM²-Referenzmodell ein spezielles Modell für das UKL abgeleitet. Weiterhin werden alternative Lösungsarchitekturen aufgezeigt, die aufgrund besonderer Rahmenbedingungen zum Einsatz kommen können. Es werden die Gründe für die Abweichung vom Referenzmodell genannt und die Vor- und Nachteile der alternativen Lösungsmöglichkeit genannt.

9 Diskussion

In der Arbeit wurde das Architekturkonzept der Gematik dargestellt, modelliert und bewertet. Es ist zu beachten, dass es sich um ein vorläufiges Architekturkonzept handelt, da die Spezifikationen der Komponenten und der Architektur noch nicht abgeschlossen sind. Deshalb sollte das Architekturkonzept in Zukunft an die neuen Versionen der Spezifikationen der Gematik angepasst werden. Haben die Änderungen Auswirkungen auf die Anforderungsspezifikation und das 3LGM²-Referenzmodell, müssen diese ebenfalls angepasst werden. Es ist nicht zu erwarten, dass sich in Zukunft grundlegende Änderungen am Architekturkonzept ergeben, da in den Testregionen mit den Testmaßnahmen begonnen wird und somit eine Investitionssicherheit für die teilnehmenden Krankenkassen und Leistungserbringer gegeben sein muss.

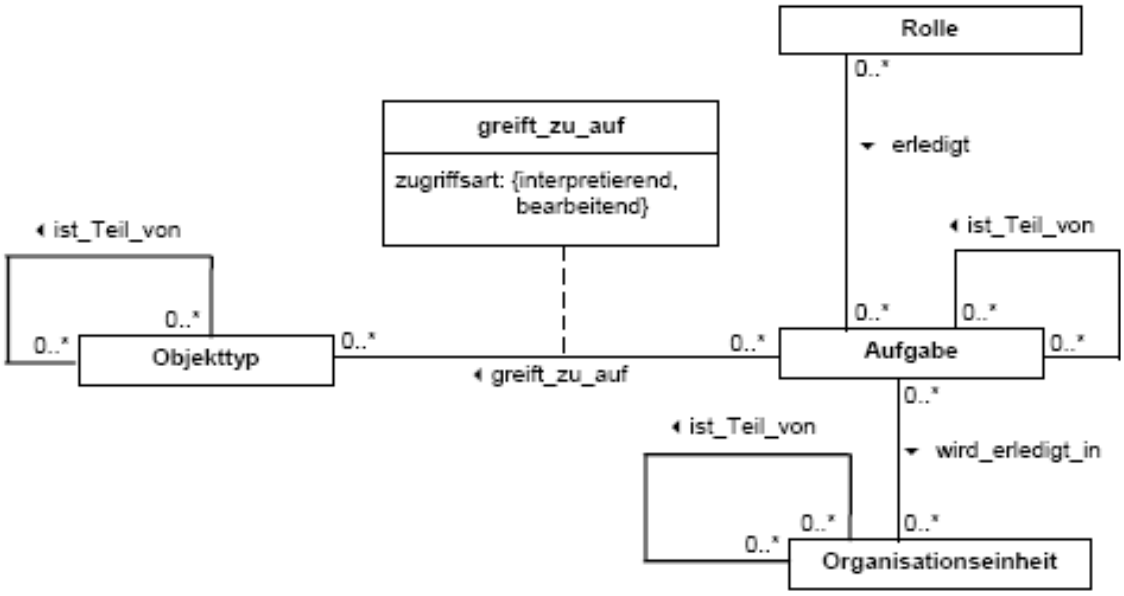
Wie bereits in Kapitel 8 erwähnt, konnten keine praktischen Erfahrungen mit der Integration der TI in ein Gesundheitsunternehmen dargestellt werden, weil die 10000er Tests in den Modellregionen zum Zeitpunkt der Arbeit noch nicht begonnen hatten. Da die Gematik die erforderlichen Spezifikationen nicht fertiggestellt hat, konnten die Hersteller nur Prototypen entwerfen. Die Modellregionen sind davon abhängig, funktionsfähige Komponenten für die 10000er Tests zur Verfügung gestellt zu bekommen und konnten somit keine Integrationsarbeiten durchführen. Der Stand der Modellregionen wurde am Beispiel Löbau Zittau beschrieben. Die anderen Modellregionen befinden sich in einem ähnlichen Entwicklungsstadium. Wenn Anfang Jahr 2007 die 10000er Tests in der Modellregion Löbau Zittau begonnen haben, sollten die fertigen Architekturen der Modellregionen analysiert und mit dem Referenzmodell verglichen werden. Das 3LGM²-Referenzmodell muss gegebenenfalls angepasst werden.

Einige Anforderungen für die Integration der TI in ein Gesundheitsunternehmen können nicht durch das Gesundheitsunternehmen selbst erfüllt werden. Dazu gehört zum Beispiel die Erstellung der CAL-Komponente für das Primärsystem, die durch den Primärsystemhersteller zur Verfügung gestellt wird. Eine weitere Anforderung ist die Unterstützung der Kommunikation über verschiedene Netzwerksegmente durch den Konnektor. Diese Anforderungen müssen erfüllt werden, bevor eine Integration in das UKL möglich wird.

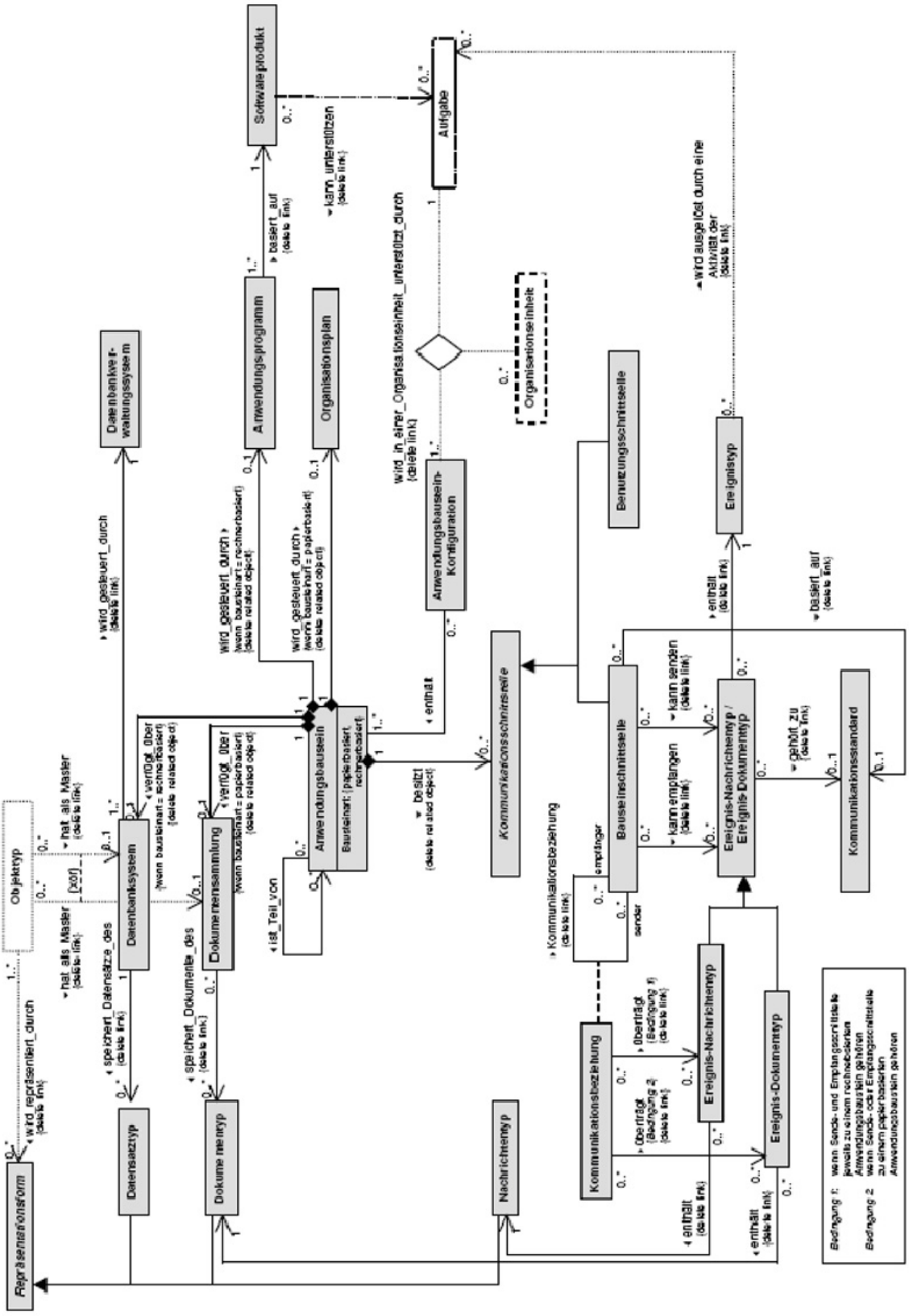
Anhang

UML-Diagramme zum 3LGM²-Metamodell:

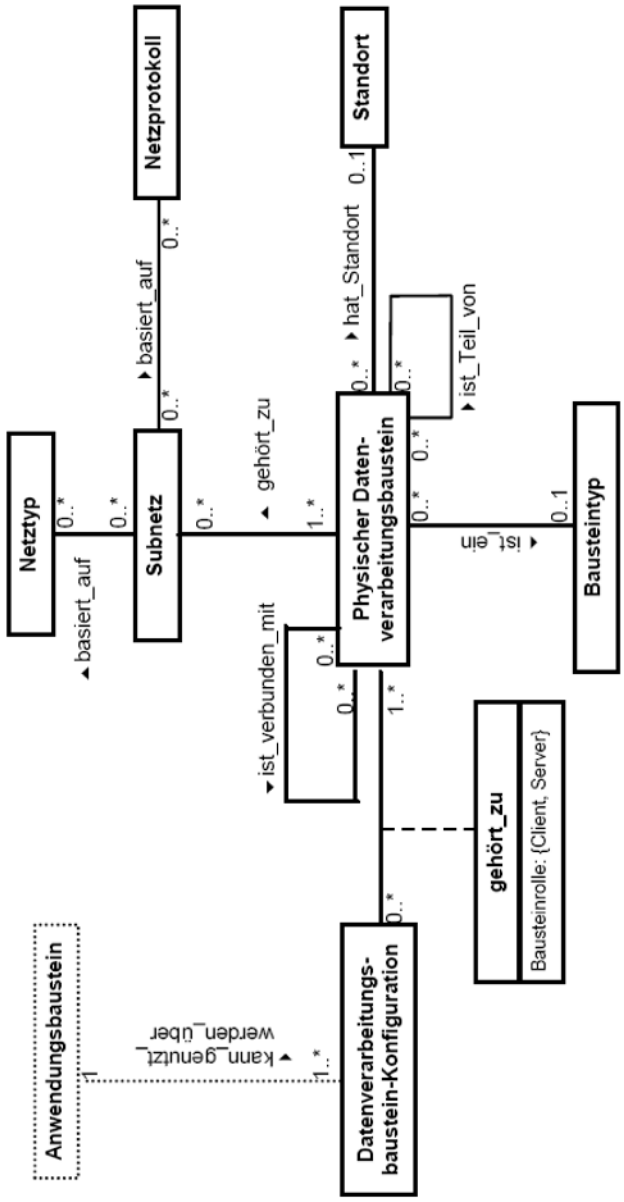
Fachliche Ebene (Quelle: [3LGM²-HP]):



Logische Werkzeugebene (Quelle: [3LGM²-HP]):



Physische Werkzeugebene (Quelle: [3LGM²-HP]):



Glossar

Common Criteria

Kriterienwerk zur Durchführung von Sicherheitsuntersuchungen an IT-Sicherheitsprodukten. Es gibt eine variable Prüftiefe von EAL1-7. Zertifikate sind international anerkannt.

Protection Files

Dokument in dem die Sicherheitsanforderungen an eine Gruppe von Produkten festgelegt werden.

Paraphe

verkürztes Namenszeichen oder Namensstempel. Es weißt nicht genügend Merkmale zur sicheren Authentisierung aus. Bei der elektronischen Signatur dient die Paraphe zur Auslösung einer Signatur, wenn die Karte bereits durch PIN-Eingabe freigeschaltet ist und damit bereits eine Authentisierung des Benutzers stattgefunden hat.

SOAP

Protokoll mit dessen Hilfe Daten zwischen Systemen ausgetauscht werden können. SOAP verwendet XML zur Repräsentation der Daten.

xDT-Familie

Nach [Stäubert 2006] findet diese Protokollfamilie hauptsächlich im niedergelassenen Bereich Anwendung. DT steht dabei für Datenträger in neueren Versionen für Datentransfer. Folgende Standards gehören zur xDT-Familie:

- ADT (Abrechnungsdatenträger): Austausch von Abrechnungsdaten zwischen KV und Praxis;
- KVDT (KV Katenträger): Ablösung des ADT;
- BDT (Behandlungsdatenträger): Austausch von Behandlungsdaten;
- LDT (Labordatenträger);
- GDT (Gerätedatenträger): Austausch zwischen Praxisverwaltungssystem und Messgeräten;
- SDKT (Stammdaten-Kostenträger): Austausch der Stammdaten der Krankenkassen und sonstiger Kostenträger;
- SDGO/SDRW(Stammdatei Gebührenordnung/Regelwerk): Austausch der Gebührenordnungen und Regelwerke.

Literaturverzeichnis

Im Text werden Literaturhinweise durch die angegebenen Kürzel gekennzeichnet.

[3LGM²-HP]: IMISE: www.3lgm.de aufgerufen am 06.11.2006

[BARCH]: Gematik (2006), Gesamtarchitektur, Basisarchitektur für Testvorhaben, Version 0.8

[BDSG2003]: Bundesdatenschutzgesetz vom 14.01.2003

[BMG]: Bundesministerium für Gesundheit (2006), Die Gesundheitskarte, Gesundheitskarte aktuell, http://www.die-gesundheitskarte.de/index.html aufgerufen am 10.7.2006

[Daemen 2002]: Daemen J.,Rijmen V.(2002): The Design of Rijndael, AES- Advanced Encryption Standard, Springer

[FK_VODM]: Gematik (2006), Fachkonzept Verordnungsdatenmanagement, Version:1.0.0

[FK_VSDM]: Gematik (2006), Fachkonzept Versichertenstammdatenmanagement, Version: 1.0.0

[Goetz]: Goetz C., Elektronische Heilberufsausweise, Sowie: Stand der Umsetzung in den Modellregionen, http://www.trends-tagung.de/Resources/download/vortrag_dr_goetz_trends_20060708.pdf

[Hauser 2005]: Hauser R. (2005): Die Einführung des elektronischen Heilberufeausweises gemäß §291a SGB V, http://www.uke.uni-hamburg.de/institute/medizinische-informatik/downloads/institut-medizinische-informatik/KIS2005Hauser.pdf abgerufen am 13.6.2006

[I-PS]: Gematik (2006): Informationsveranstaltung für Primärsystemanbieter (Vortragssammlung), http://www.gematik.de/(S(jovmp245bp2m1jfootkxyn45))/Presse___Praesentationen.Gematik?ActiveID=1372 abgerufen am 24.8.2006

[Jedamzik 2006]: Jedamzik S.(2006): eGK - Stand der Umsetzung in den Modellregionen, http://www.trends-tagung.de/Resources/download/vortrag_dr_jedamzik_trends_20060708.pdf abgerufen am 24.8.2006

[SachsSM]: Sächsisches Staatsministerium für Soziales, Sachsen wird Testregion für elektronischen Heilberufeausweis für Ärzte, 7.10.2005

[Sax2005]: SaxMediCard, Elektronische Gesundheitskarte - Weichen in Sachsen gestellt in: e-health Journal, 06/2005

[SaxMediCard]: SaxMediCard, SaxMediCard- Die elektronische Gesundheitskarte im Freistaat Sachsen, http://www.gesundheitskarte-sachsen.de/aktuelles.php, 31.10.2006

[Seibt 2005]: Seibt R. (2005), SaxMediCard, Aktueller Stand der Einführung der eGK und des HBA in Sachsen, http://www.gesundheitskarte-sachsen.de/download/SaxMediCard_IT_Ostsachsen.PDF aufgerufen am 31.7.2006

[SGB V]: Sozialgesetzbuch V §291, §291a, §291b

[SigG]: Gesetz über Rahmenbedingungen für elektronischen Signaturen (Signaturgesetz), vom 16.05.2001

[SigR]: Signaturrichtlinie (2000) Umsetzungsfrist für alle EU-Staaten: 19.7.2001

[SP-KON]: Gematik (2006), Spezifikation Konnektor Version: 0.5.0

[SP-KT]: Gematik (2006), Spezifikation eHealth-Kartenterminal Version:1.1.0

[SP-NW]: Gematik(2006), Netzwerkspezifikation Version: 1.0.0 [SP-PKI]: Gematik (2006), Festlegung einer einheitlichen X.509-Zertifikatsinfrastruktur für die Telematik im Gesundheitswesen, Version: 1.0.0

[SICCT]: TeleTrust (2006): SICCT Secure Interoperable ChipCard Terminal, Version 1.0.3

[Stäubert 2006]: Stäubert S.(2006), Referenzmodell für die Kommunikation eines Universitätsklinikums mit dem niedergelassenen Bereich, Universität Leipzig

[T-Stich]: TU Wien, INSO, BMGS (2005), T-Stich: Architektur der dezentralen Dienste und Komponenten, http://www.dimdi.de/dynamic/de/ehealth/karte/downloadcenter/technik/loesungsarchitektur/loesungsarchitektur_archiv/egk_t-stich_v1-0.pdf aufgerufen am 10.07.2006

[VERSA]: Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH, VERSA – Ein Überblick: http://www.wuv-gmbh.de/media/versa_abstract.pdf, abgerufen am: 14.6.2006

[VTE2005]: Verordnung über die Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte (2005)

[Winter 2002]: Winter A., Ammenwerth E., Brigl B., Haux R. (2002). Krankenhausinformationssysteme. In Lehmann T., Bexten E.M.z. (eds) (2002). Handbuch der Medizinischen Informatik. Hanser, München.

Abbildungsverzeichnis

Erklärung

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

Leipzig, 11. Januar 2007

Sandra Forberger