Vorlage für das Pflichtenheft des Teleradiologie-Projektes Rhein-Neckar-Dreieck

Teleradiologie-Kommunikationsserver

Gefördert vom Sozialministerium Baden-Württemberg Zukunftsoffensive III

erstellt durch

Projektleitung Universitätsklinikum Mannheim
Dr. Gerald Weisser

Mannheim im November 2003

Inhaltsverzeichnis

Anlagenverzeichnis

1 EINLEITUNG

1.1 Überblick

Im Vordergrund dieses Projektes steht die Verbesserung der medizinischen Versorgung für die Akutbehandlung der Krankheitsbilder Schlaganfall und Schädel-Hirn-Verletzung. Dies soll über die Vernetzung der Schlaganfallstationen des Rhein-Neckar-Raumes sowie über die Vernetzung von Unfallchirurgischen Kliniken mit Neurochirurgischen Zentren erreicht werden.

Projektpartner sind insgesamt 13 Kliniken im Rhein-Neckar-Raum mit den Zentren
- Uniklinikum Heidelberg
- Uniklinikum Mannheim
- Städtisches Klinikum Karlsruhe

sowie den peripheren Kliniken
- Diakonie Mannheim
- Fürst-Stirum Klinikum Bruchsal
- KKH Schwetzingen
- KKH Sinsheim
- KKH Weinheim
- KKH Eberbach
- Vincentius-Kliniken Karlsruhe
- Klinikum Karlsbad-Langensteinbach
- Stadtklinik Baden-Baden
- KKH Mosbach

Die Koordination des Gesamtprojektes erfolgt über die Projektleitung im Institut für Klinische Radiologie, Universitätsklinikum Mannheim.

1.2 Ausführung der Angebotseinholungen und Ausschreibungen

Im Rahmen des Teleradiologie-Projektes Rhein-Neckar-Dreiecks werden eine Reihe von Angebotseinholungen und Ausschreibungen getätigt. Die Grundanforderungen an die einzelnen Komponenten werden dabei über zentrale Pflichtenhefte der Projektleitung definiert. Die Anschaffungen erfolgen über die beteiligten Partnerkliniken. Die jeweiligen Pflichtenhefte dieser Einzelausschreibungen basieren dabei auf den Vorlagen der zentralen Pflichtenhefte sowie aus zusätzlichen Anforderungen, die sich aus den lokalen Verhältnissen der Partnerkliniken ergeben.

2 STRATEGISCHE ZIELE

2.1 Kurzfristige Ziele

Die kurzfristigen Ziele sind die Vernetzung der angegebenen 13 Standorte, um einen schnellen und sicheren Informationsaustausch radiologischer Bilddaten über 24 Stunden hinweg bereit zu stellen.

2.2 Langfristige Ziele

Für die Zukunft möchte man einen landesweiten und Länder-übergreifenden Austausch von medizinischen Bilddaten und zugehörigen elektronischen Daten erreichen. Die hier vorgestellte Kommunikationslösung wird im Rahmen der 4 weiteren Landesprojekte der Zukunftsoffensive III des Landes Baden-Württemberg als Kommunikationsplattform zwischen allen beteiligten Kliniken und anderen Partnern eingesetzt. Ebenso ist eine Anbindung an andere Projekte, insbesondere das Landesprojekt Rheinland-Pfalz sowie das Radiologienetz Rhein-Neckar-Pfalz, vorgesehen.

3 VORGABEN (ORGANISATORISCHE, TECHNISCHE)

Ein wesentlicher Bestandteil ist die Kompatibilität des teleradiologischen Übertragungssystems zu bestehenden oder auch zukünftigen medizinischen Bildübertragungssystemen. Standard sind das DICOM-Protokoll sowie das zugehörige DICOM Dateiformat, das gemäß DICOM Supplement 54 als E-Mail-Anlage verschickt werden kann (siehe Anlage). Eine Einbindung von Textinformationen und Bildinformationen, die nicht im DICOM-Format vorliegen, ist erwünscht. Eine Rückübermittlung eines Befundes/Konsiles mit elektronischer Signatur ist angestrebt.

Die Realisierung dieser Aufgaben soll über eine Architektur mit Nutzung von verschlüsselten E-Mail-Nachrichten sowie automatisierter Umwandlung von DICOM-Protokoll zu E-Mail (und zurück) umgesetzt werden. Übermittlung von weiteren Informationen (zusätzlich zu Dateien im DICOM-Dateiformat) soll transparent über die E-Mail-Architektur mit Textinformationen und weiteren Dateianhängen erfolgen.

Dieses Teleradiologiekonzept soll über eine Client-Server Architektur umgesetzt werden. Es besteht aus 3 Kommunikationsservern in Heidelberg, Mannheim und Karlsruhe sowie aus ca. 20 Workstations in allen Standorten.

Die Konzeption der Kommunikationsserver und Workstations geht von einer Lage der Kommunikationsserver außerhalb der Firewall-Rechner in den Kliniken in Heidelberg, Mannheim und Karlsruhe aus. Die Kommunikationsserver verfügen über eine schnelle Internet-Anbindung (100 Mbit). Zusätzlich sind ISDN-Einwahlrouter (8-Kanal bzw. 30-Kanal) in den Zentren mit unmittelbarer Nähe zu den Kommunikationsservern vorgesehen. Hierüber können Häuser ohne ausreichend schnellen Internet-Zugang sich direkt in die Kommunikationsserver einwählen, zudem verfügen die Häuser mit primärer Verbindung über das Internet über kleine 2-Kanal-Router für die Verbindung zu den Kommunikationsservern bei Ausfall des Internet.
Für die Einwahlverbindungen in die Einwahlrouter der Zentren ist eine Rufnummer-Überprüfung des einwählenden Routers vorgesehen, es wird keine Leitungsverschlüsselung im Sinne eines VPN vorgenommen.

Für jeden Benutzer werden auf allen 3 Mailservern Mailkonten angelegt, die Inhalte dieser Mailkonten werden jedoch nicht repliziert auf die anderen Server. Die einzelnen Server arbeiten damit unabhängig von einander, die Benutzer fragen immer ihre Postfächer auf allen 3 Mailservern ab. Bei Ausfall eines Mailservers kann somit von jedem Benutzer einer der beiden anderen Mailserver zum Versenden von Bildern genutzt werden.

Die Clients (Teleradiologie-Workstations) sind im Intranet der jeweiligen Kliniken lokalisiert. Sie kommunizieren nach außen ausschließlich mit Mailprotokollen (POP3, IMAP4, SMTP bzw. deren SSL-Varianten). Die interne Kommunikation mit den Modalitäten und anderen Radiologie-Workstations geschieht über das DICOM-Protokoll. Die Umwandlung von DICOM-Bildern in verschlüsselte Mails geschieht innerhalb der Teleradiologie-Workstations.

Das Sicherheitskonzept der Installation besteht aus folgenden Bestandteilen:
- Leitungsverschlüsselung: Bei Übermittlung an oder Zugriff auf die Mailserver wird eine SSL-Verschlüsselung eingesetzt. Die Router kommunizieren untereinander unverschlüsselt.
- Inhaltsverschlüsselung: Die transportierten Dateninhalte werden mittels asymmetrischen Verschlüsselungsverfahren (OpenGP-kompatibel) verschlüsselt.
- Authentifizierung: Beim Versenden von Bildern (SMTPs) wird eine Benutzerauthentifizierung nach RFC gefordert. Eine weiter gehende Authentifizierung mittels Signatur der versandten Mails wird in der zweiten Phase des Projektes realisiert.

3.1 Konzeptskizze

In der folgenden Abbildung ist schematisch der Ablauf einer Versendung von Bildern aus der Klinik A und dem nachfolgenden Empfang der Bilder in der Klinik B dargestellt.

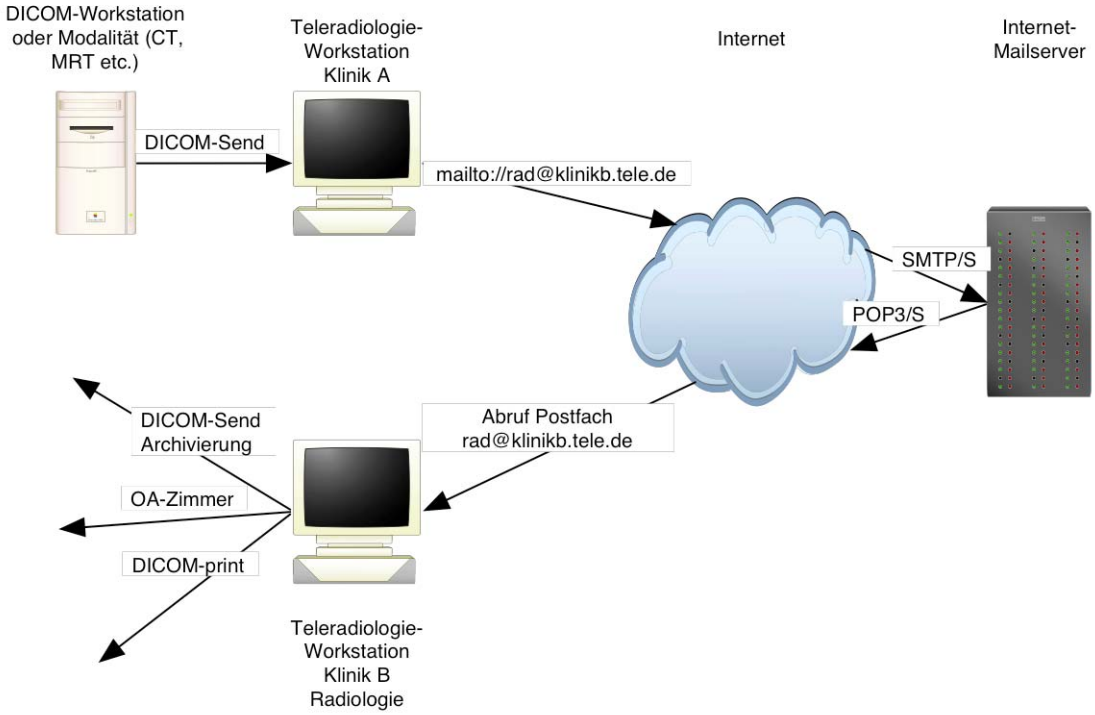

Abbildung 1: Schematischer Ablauf des Bildversands

Der Ablauf innerhalb einer Teleradiologie-Workstation beim Senden und Empfangen von Bildern sieht dabei wie folgt aus:

Versenden von Bildern:

- Empfang der Bilddaten über DICOM, Speicherung in der internen Datenbank der Teleradiologie-Workstation.
- Auswahl der zu versendenden Bilder durch den Arzt (z.B. 20 CT-Bilder).
- Hinzufügen von Informationen über Anamnese, Fragestellung und Rückrufnummer.
- Auswahl des Empfängers mit dem zugehörigen öffentlichen Schlüssel und der E-Mail-Adresse.
- Versenden der Einzelmails als verschlüsselte Mail nach OpenGP mit jeweils einem Attachment (jedes Bild als .dcm-Datei sowie Textinformationen als .txt-Datei mit der StudyInstanceUID als Dateinamen), insgesamt damit 21 Mails.

Empfang von Bildern:

- Automatisches Abfragen der Mailboxen auf den 3 Servern in MA, HD, KA
- Holen der 21 Mails vom Mailserver.
- Entschlüsseln der 21 Mails mit dem privaten Schlüssel, der auf der Festplatte gespeichert ist (keine Interaktion mit dem Benutzer).
- Einsortieren der enthaltenen DICOM-Dateien in die lokale Patientendatenbank.
- Anzeige der .txt-Datei in einem eigenen Fenster oder integriert in die Viewing-Applikation der Bilddateien.
- Automatisches Weiterleiten der Bilder z.B. an das Archiv oder eine weitere Workstation per DICOM (je nach lokaler Konfiguration).

Folgende Möglichkeiten sollen zusätzlich zu den oben genannten Arten der Bildversendung angeboten werden:

- Automatische Weiterleitung über die Teleradiologie-Workstation. Hierbei werden keine zusätzlichen Textinformationen erstellt. Die Empfängeradresse wird über den AET der DICOM-Verbindung definiert (z.B. AET=NCH_MA bedeutet eine automatische Weiterleitung der empfangenen DICOM-Bilder an die Mailadresse nch@ma.telerad.de). Die Konfiguration dieser Partner und Zuordnungen zur AET erfolgt in der Teleradiologie-Workstation. Damit ist eine automatische Versendung von Bildern von jeder DICOM-fähigen Modalität möglich.
- Erzeugung eines DICOMStructuredReport. Hier wird zusätzlich zur genannten .txt-Datei eine den DICOM-Normen entsprechende Befunddatei erzeugt und übertragen. Diese erlaubt in dazu ausgerüsteten Workstations eine einfache Zuordnung zu den entsprechenden Bilddaten, die im Falle der .txt-Datei nur über den Umweg des Dateinamens (StudyInstanceUID) möglich ist.
- Verwaltung mehrerer Benutzer der Teleradiologie-Workstation. Hierbei müssen mehrere Patientendatenbanken auf der Workstation angelegt werden und es muss ein Berechtigungskonzept für den Zugriff auf diese Datenbanken existieren (z.B. Datenbanken Neurologie und Neuroradiologie, Benutzer Müller hat Zugriff auf Neurologie, Benutzer Meier hat Zugriff auf Neuroradiologie). Damit müssen auch mehrere persönliche Schlüssel auf der Workstation existieren (ein Schlüssel Neurologie, ein Schlüssel Neuroradiologie), es muss dann auch auf mehrere Mailkonten zugegriffen werden (jeweils 3 Konten der Neurologie etc.). Die Benutzerauthentifizierung erfolgt in der ersten Projektphase über Name und Passwort, in der zweiten Projektphase wird dann eine Anmeldung mit Karte angestrebt.
- Unterstützung anderer Dateiformate: für andere Dateiformate (JPG, RTF, PNG, AVI etc.) sollte innerhalb der Teleradiologie-Applikation Möglichkeiten angeboten werden, diesen Dateiformaten Hilfsapplikationen zuzuordnen und diesen Hilfsapplikationen bei Empfang einer solchen Datei diese zu übergeben.
- Unterstützung von Bestätigungsmails: Es sollte die Möglichkeit bestehen, bei Bestätigungsmails des Mailservers (Mail wurde vom Empfänger abgerufen) diese als Empfangsbestätigung zu registrieren und diese Information an den Benutzer der Teleradiologie-Workstation weiterzugeben.

3.2 Sonderfall DICOM-Schnittstelle (Einbindung von Altsystemen)

Für die Anbindung von bestehenden einfachen Kliniksystemen, die in der Regel auf Einwahlleitungen mit ungesicherten DICOM-Verbindungen beruhen, wurde ein eigenes Konzept zur Integration entwickelt (siehe Abbildung 2: Konzeptskizze).

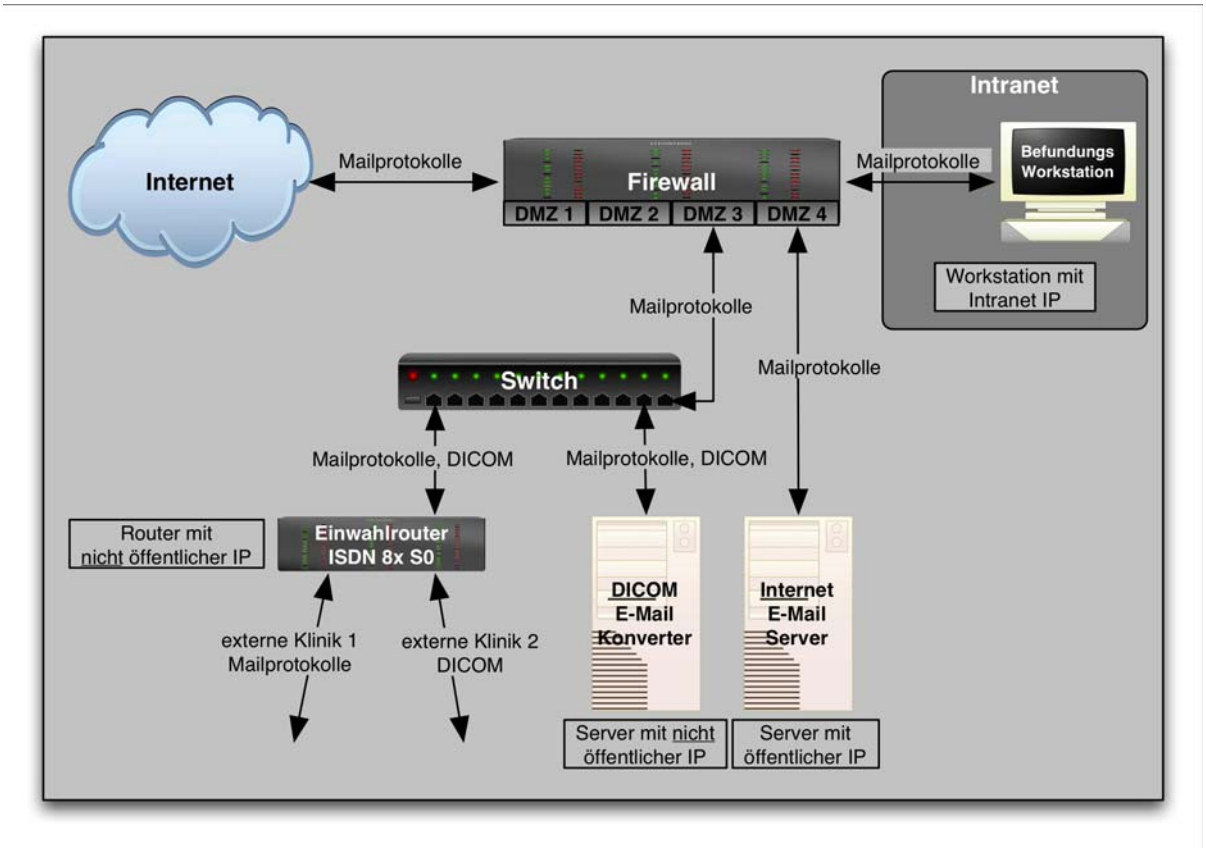

Abbildung 2: Konzeptskizze DICOM-/E-Mail-Zugang durch ISDN-Einwahlrouter.

Die Funktion des Sendens und Empfangens zwischen den peripheren Häusern und den Zentren mittels DICOM-Verbindungen kann mit geringem Aufwand einbruchssicher realisiert werden. Im Teleradiologie-Projekt übernimmt ein extra dafür eingerichteter DICOM-Server die Aufgabe eines automatischen DICOM-E-Mail/E-Mail-DICOM-Konverters:

In der Senderichtung nimmt der DICOM-Server direkte DICOM-Verbindungen über einen ISDN-Einwahlrouter entgegen und wandelt die eingehenden DICOM-Objekte in E-Mails um. Der Empfänger wird dabei anhand der AET erkannt, die Daten verschlüsselt und an das Postfach des Empfängers verschickt.

Umgekehrt ruft der DICOM-E-Mail-Konverter vom Mailserver E-Mails (über POP3 oder IMAP4) ab, entschlüsselt sie und schickt die darin enthaltenen DICOM-Objekte per DICOM-Verbindung über den ISDN-Einwahlrouter zu deren Bestimmungsort.

Der ISDN-Einwahlrouter wird so konfiguriert, dass er nur Anrufe von eingetragenen berechtigten Partnern entgegennimmt und auch nur zu Ihnen Verbindungen aufbaut. Zusätzlich werden die Verbindungen IPSec-verschlüsselt, soweit die peripheren Router dies unterstützen.

Der Mailserver ist über eine öffentliche IP-Adresse erreichbar und steht in einer der demilitarisierten Zonen der Firewall. Die Firewall sorgt dafür, dass nur über E-Mail-Protokolle auf dem Mailserver zugegriffen werden kann. Der DICOM-Server und der ISDN-Einwahlrouter sind über einen Switch miteinander verbunden und bilden zusammen einen nicht öffentlichen Subnetz, das wiederum in einer der anderen demilitarisierten Zonen der Firewall eingebunden ist.

Die Konstellation, bei dem der Mailserver direkt am Internet (außerhalb der Firewall, nicht in der DMZ) hängt ist auch zulässig, aber nicht zu empfehlen. Die E-Mails sind zwar alle verschlüsselt und durch Unbefugte geschützt, aber der Mailserver selbst wäre einen erhöhten Angriffsrisiko ausgesetzt (insbesondere DoS-Attacken).

Die DICOM-Kommunikation findet ausschließlich in dem Einwahlrouter-DICOM-Server Subnetz statt, am Mailserver werden keine DICOM-Verbindungen aufgebaut. Die Kommunikation zwischen DICOM-Server und Mailserver basiert ausschließlich auf Mailprotokollen. Private und PublicKeys sind nur auf dem DICOM-Server gespeichert. Die hierfür verwendeten Schlüsselpaare werden nur für diese Art der Kommunikation eingesetzt. Es sind zu keinem Zeitpunkt unverschlüsselte Daten auf dem Mailserver.

Die Server und alle Netzwerkkomponenten werden durch USV(s) gegen Stromausfälle geschützt (nicht abgebildet).

3.3 Schlüsselverwaltung, Zugriffsrechte

Im Rahmen des Projektes wird eine große Anzahl von asymmetrischen Schlüsselpaaren erzeugt. Grundprinzip der Verwaltung dieser Schlüssel im Projektzeitraum ist:

- Schlüsselpaare werden grundsätzlich vom lokalen Systemadministrator vor Ort erzeugt.
- Der öffentliche Schlüssel wird an die Projektleitung im Universitätsklinikum Mannheim weitergegeben und von dieser an die Projektpartner verteilt.
- Der private Schlüssel verbleibt beim lokalen Systemadministrator bzw. der Person des Schlüsselinhabers.

Es wird zwischen Verschlüsselung und Signatur unterschieden. Prinzipiell wird mit dem öffentlichen Schlüssel der Ziel-Workstation verschlüsselt und mit einem lokalen privaten Schlüssel signiert. In der ersten Phase des Projektes wird jedoch ausschließlich die Verschlüsselung genutzt, eine Verwendung der Signatur ist erst in einer zweiten Projektphase ab Mitte 2004 vorgesehen. Damit wird in der ersten Projektphase für jede Teleradiologie-Workstation ein Schlüsselpaar erzeugt. Es werden keine personenbezogenen Schlüsselpaare verwendet.

Fallbeispiel: Ablauf der Verschlüsselung beim Senden, als Sender wird Dr. Müller aus dem Kreiskrankenhaus angenommen, der Empfänger soll die Abteilung für Neurochirurgie im Zentrum sein.
Das Schlüsselpaar der Neurochirurgie wurde bei der Installation der Workstation dort erzeugt, der private Schlüssel liegt dort auf der Festplatte vor, der öffentliche Schlüssel wurde an Dr. Müller weitergegeben. Ebenso wurde auch auf der Teleradiologie-Workstation von Dr. Müller ein Schlüsselpaar erzeugt, dieses wird jedoch bei einem Sendevorgang von dieser Workstation nicht benötigt (nur beim Empfang von Bildern auf dieser Workstation).
Jedes Bild, das Dr. Müller an die Neurochirurgie schickt, wird damit zuvor mit dem öffentlichen Schlüssel der Neurochirurgie verschlüsselt, an eine E-Mail angehängt und an die E-Mail-Adresse der Neurochirurgie auf den Kommunikationsserver des Zentrums geschickt.

Die Teleradiologie-Workstation der Neurochirurgie fragt regelmäßig ihr Postfach auf dem Kommunikationsserver ab, lädt die E-Mails auf die lokale Festplatte und entschlüsselt die enthaltenen Bilddateien mit dem privaten Schlüssel, der sich ebenfalls auf der Festplatte befindet. Dieser Vorgang des Entschlüsselns muss vollautomatisch ablaufen (ohne Benutzerinteraktion). Der Neurochirurg meldet sich mit seinem Benutzernamen und Passwort an der Oberfläche der Teleradiologie-Workstation an und findet die Bilder des Patienten in der Patientendatenbank des Rechners.

Über dieses einfache Fallbeispiel hinausgehend kann es erforderlich sein, dass sich auf der Festplatte einer Teleradiologie-Workstation auch mehrere Schlüsselpaare befinden. Wenn sich z.B. die Abteilungen Neurochirurgie und Neurologie eine Workstation teilen, dann muss die Teleradiologie-Workstation mehrere verschiedene Postfächer abfragen und dem jeweiligen Postfach zusätzlich den korrekten Schlüssel zuordnen können. Dabei müssen aus rechtlichen Gründen auch unterschiedliche Patientendatenbanken auf dem Rechner existieren und den einzelnen Benutzern Rechte zum Zugriff auf diese Datenbanken zugeteilt werden.

4 ANFORDERUNGSKATALOG KOMMUNIKATIONSSERVER

Ziel der Angebotseinholung ist es, eine durchgängige und einheitliche Lösung für Übertragungen mit dem DICOM-Protokoll und Senden/Empfangen von E-Mail-Nachrichten mit DICOM-Anhängen und anderen Dateianhängen zu planen.

Die teleradiologische Versendung des Bildmaterials und der zusätzlichen Informationen (Text, nichtradiologische Bilder) soll den Arzt, die MTA sowie Mitarbeiter in den Funktionsbereichen unterstützen und nicht durch eine aufwändige Handhabung der Versandprozedur zeitlich unnötig lange binden. Eine elektronische Rückübermittlung der konsiliarischen Stellungnahme bzw. des radiologischen Befundes muss ebenso einfach und transparent möglich sein. Als Szenario steht die zeitkritische Patientenversorgung im Notfall im Vordergrund.

Anforderungen an derartige Systeme bestehen bezüglich Funktionalität, Schnittstellen und Technik. Einer weiteren Berücksichtigung bedürfen auch die Anbieterstruktur und die laufenden Kosten (Wartung, Instandhaltung und Verbindungskosten).

Die Anforderungen sind untergliedert für den Kommunikationsserver und die Workstations mit jeweils eigenen Pflichtenheften. Die Bedeutung der Kommunikationsserver wurde im Kapitel 3 erläutert, als Workstations sind z. B. die Arbeitsplatzrechner in der Radiologie und Neurologie definiert, die im Rahmen dieser Ausschreibung angeschafft werden sollen. Als DICOM-Geräte sind alle bereits vorhandenen Endgeräte mit DICOM-Protokoll-Fähigkeiten zu verstehen, insbesondere Untersuchungsgeräte (CT, MRT, etc.) und bereits vorhandene DICOM–Protokoll–fähige Befundungs-, Betrachtungs- oder Bildverarbeitungsworkstations sowie DICOM-Archive.

Geben Sie bitte zu jeder einzelnen Anforderung des Kapitels 4 an, ob sie bereits realisiert ist, bis wann sie realisiert wird oder ob sie im Entwicklungsplan nicht vorgesehen ist Beschreiben Sie bitte außerdem die Leistungsmerkmale jeder Anforderung, die realisiert ist oder sich in Realisierung befindet.

4.1 Kurzform

Als kurzen Abriss der Funktionalitäten des Kommunikationsservers sind folgende Punkte zu nennen, die im nächsten Abschnitt näher spezifiziert werden:

- Volle Funktionalität eines Internet-E-Mail-Servers. Insbesondere Unterstützung von mindestens 200 Benutzern mit POP3, IMAP4 und SMTP Diensten. Es müssen die SSL-Varianten dieser Dienste unterstützt werden, es muss eine Benutzerauthentifizierung nach RFC für den SMTP-Dienst unterstützt werden.
- Unterstützung von Bestätigungsmails an den Sender bei Abrufen von E-Mails durch den Empfänger.
- Automatisches Abfragen eines weiteren E-Mail-Servers (Uptime-Server).
- Eine Zeitsynchronisation soll mittels Network Time Protocol (NTP) möglich sein.
- Einbindung eines zweiten Servers mit nichtöffentlicher IP-Adresse mit folgender Funktionalität: Automatische Umwandlung von per DICOM empfangenen Bilddaten in zu sendende E-Mails. Definition des Empfängers über den AET. Automatische Entschlüsselung von per DICOM-E-Mail empfangenen DICOM-Elementen und Weiterleitung an DICOM-Partner. Definition des Empfängers über die E-Mail-Adresse.

4.2 Anforderungen an die Funktionalität

Die folgenden Funktionen und fachlichen Anforderungen sollten von dem Teleradiologiesystem unterstützt werden.

A1 Übertragungsfunktionen

E-Mail-Serverdienst

- Auf dem Kommunikationsserver muss ein E-Mail-Serverdienst eingerichtet sein, der POP3, IMAP4 und SMTP mit und ohne SSL-Verschlüsselung anbietet. Die Größe der Postfächer soll grundsätzlich unbeschränkt sein (Limitierung durch Festplattenspeicher).
- Es müssen mindestens 200 Benutzer konfigurierbar sein.
- Es sollen konfigurierbar Bestätigungsmails an den Absender bei Lesen der Mail durch den Empfänger möglich sein.
- Der auf dem Kommunikationsserver laufende E-Mail-Server soll über die Möglichkeit einer Steuerung (Überprüfen eines Postfaches, Senden, Weiterleiten und Löschen von einzelnen E-Mails und Gruppen von E-Mails, Änderung des eigenen Passwortes) über ein Webinterface mit personalisiertem, verschlüsseltem Zugriff (https) verfügen. Es sollen keine Einschränkungen bezüglich Plattform und Hersteller der Browsersoftware zum Zugriff auf dieses Webinterface vorhanden sein.

Verbindung zum Uptime-Server

- Es muss die automatische Abfrage eines Internet-Postfaches in wählbaren Zeitabständen (Sekunden, Minuten, Stunden und Tage) möglich sein (POP3-Protokoll mit SSL-Verschlüsselung).

A2 Sonderfall DICOM-Schnittstelle (Einbindung von Altsystemen)

Automatische DICOM <-> DICOM-E-Mail Konvertierung

Aus datenschutzrechtlichen Gründen darf die automatische Konvertierung nicht vom Kommunikationsserver selbst durchgeführt werden. Die Konvertierung muss von einen eigens dafür eingerichteter DICOM-Server, der indirekt (DMZ zu DMZ) mit dem Kommunikationsserver (Mailserver) in Verbindung steht, übernommen werden. Dieser DICOM-Server darf keine öffentlich erreichbare IP-Adresse haben und muss durch die Firewall gegen das Internet abgesichert sein. (vgl. Abbildung 2: Konzeptskizze)

Konvertierung DICOM-Protokoll zu E-Mail:

- Es muss ein DICOM-Empfang von beliebigen DICOM-Objekten über einen frei wählbaren Port möglich sein (DICOM Receive, SCP).
- Die per DICOM empfangenen Daten müssen als DICOM-Objekte abgespeichert werden und automatisch an einen oder mehrere E-Mail-Empfänger weiter versendet werden können mit anschließender, unmittelbarer Löschung der unverschlüsselten DICOM-Dateien.
- Die E-Mails müssen automatisch mit der auf dem Rechner gespeicherten öffentlichen Schlüssel des Empfängers verschlüsselt werden (OpenGP-kompatibel, PGP/MIME) und mit dem Schlüssel des DICOM-Servers signiert werden.
- Die Definition des Empfängers der DICOM-E-Mail muss über die Calling-AET des DICOM-Senders möglich sein (z.B. HDNCH als AET entspricht hdnch@hd.teleradiologie-rnd.de). Diese Zuordnungen müssen über eine graphische Benutzeroberfläche und einen entsprechenden Zugang administrierbar sein.

Konvertierung E-Mail zu DICOM-Protokoll:

- Der DICOM-Server muss ein zugeordnetes Postfach auf dem Kommunikationsserver per POP3 oder IMAP4 in einstellbaren, regelmäßigen Abständen abrufen. Die empfangenen Mails müssen automatisch mit dem gespeicherten privaten Schlüssel entschlüsselt werden. Die in der Mail

enthaltenen DICOM-Objekte werden über den zuvor konfigurierten Port per DICOM-Protokoll an ihren Bestimmungsort gesendet. Einer Empfangsadresse (Postfach auf dem Kommunikationsserver) muss ein DICOM-Partner fest zugeordnet werden können. Es müssen mindestens drei verschiedene Postfächer (und damit DICOM-Partner) verwaltet werden können. Diese Zuordnungen müssen über eine graphische Benutzeroberfläche und einen entsprechenden Zugang administrierbar sein.

A3 Dokumentation, Statistik

- Folgende Ereignisse müssen in einer Dokumentationsdatei protokolliert werden (jeweils mit Angabe von Datum, Uhrzeit und Benutzer):
  - Empfang von E-Mails (zusätzlich Angabe des Senders, der Zahl der Attachments, der Größe, der Auslastung des Speicherplatzes).
  - Empfang einer Untersuchung per DICOM (Angaben wie oben).
  - Jede Fehler- oder Warnmeldung.
  - Löschen von E-Mails.
- Die Dokumentationsdatei muss in einem allgemein lesbaren Format vorliegen (möglichst XML, wenn nicht möglich dann HTML o.ä.).
- Die Dokumentationsdatei muss für einen Zeitraum von mindestens 6 Monaten im direkten Zugriff vorliegen, bei Verwendung mehrerer Dateien muss eine eindeutige Zuordnung möglich sein.
- Folgende statistische Funktionen müssen innerhalb der Software oder in einem externen Modul vorliegen:
  - Zahl, Umfang, Übertragungszeit und Übertragungsprotokoll der empfangenen Untersuchungen und E-Mails innerhalb eines frei wählbaren Zeitraums (mindestens eines Tages, einer Woche, eines Monats und eines Jahres) mit Angabe von Summe, Mittelwert, Min, Max und Std.abw., soweit sinnvoll.
  - Aufgliederung der vorgenannten Statistik nach Sender, Empfänger, Art des Protokolls.

4.3 Technische Anforderungen

Nachfolgende technische Aspekte sollen vom Teleradiologiesystem unterstützt werden. Inwieweit ist dies durch das angebotene Produkt möglich?

B1 Datenschutz und Systemsicherheit

- Sicherstellung des allgemeinen Datenschutzes.
- Möglichkeit der Protokollierung der Eingaben, Änderungen und Löschungen von Daten.
- Passwortergänzende Verfahren zur Benutzeridentifikation (Karte, Schlüssel, Fingerabdruck).
- Möglichkeit zum schnellen und einfachen Benutzerwechsel (Login, Logout).
- Nach Eingabe des Passwortes möglichst Fortfahren mit der Benutzerführung entsprechend des Standes bei Beendigung der letzten Sitzung.
- Timeout nach x Minuten, einstellbar.
- Realisierung eines Zugriffsberechtigungskonzepts.
- Vorsorgemaßnahmen zur Datensicherheit, u. a. erprobte Datensicherung.
- Darlegung eines elektronischen Ausfallkonzeptes.
- Erprobtes Konzept für Desasterrecovery.
- Integration der Verschlüsselung.
- Vorschläge zur Integration der digitalen Signatur unter Berücksichtigung von Mehrfachsignaturen (Zertifikate nach Standard X509v3).

B2 Anpassung und Wartung

- Einfache und schnelle Parametrierung, Anpassung und Pflege der Anwendungssoftware.
- Customizing- und Parametrierungsunterstützung.
- Erweiterbare Struktur der Datenbank und der Anwendungssoftware.

B3 Systemadministration

- Operatorfreier 24-Stunden-Betrieb.
- Einfache Funktionen zur Systemüberwachung und –steuerung.
- Einfache Administrierung der DICOM/Teleradiologie-Partner (ohne Neustart, unter Beachtung von Datenschutzgesichtspunkten).
- Backup im laufenden Betrieb: zentral, automatisiert, permanent.
- Schnelle Recoverymechanismen.
- Automatisiertes Batchverfahren (z.B. Forwarding).
- Verzeichnisdienst inklusive anwendungsübergreifende Benutzerverwaltung (single sign-on).
- Unterstützung der zentralen Softwareverteilung (unter Beachtung von Datenschutzgesichtspunkten).

B4 Performance und Verfügbarkeit

- Aussagen zur Ausfallsicherheit des Systems (ggf. Ausfallstatistiken von Referenzhäusern).
- Angaben über benötigte Bandbreiten.

B5 Dokumentationen

- Benutzerhandbücher, soweit vorhanden.
- Programmdokumentationen, soweit vorhanden.
- Online-Hilfen und -Dokumentation, soweit vorhanden.

B6 Zertifizierung der Anwendungssoftware

- Liegen Zertifizierungen vor?

4.4 Fragen zum Anbieter

Wegen der vorgesehenen außergewöhnlichen Verbreitung des angestrebten Teleradiologie-Systems und des damit verbundenen hohen Investitionsvolumens ist die Zusammenarbeit mit einem erfahrenen und zuverlässigen Anbieter von großer Bedeutung. Daher bitten wir um Beantwortung der folgenden Fragen:

C1 Unternehmensstruktur

- Wie viele Mitarbeiter beschäftigt Ihr Unternehmen
  - insgesamt?
  - im Bereich Entwicklung ”Gesundheitswesen”?
  - im Bereich Support ”Gesundheitswesen”?
- Nennen Sie bitte die Standorte Ihrer Support-Niederlassungen in Rheinland-Pfalz, Baden-Württemberg und Hessen sowie die Anzahl der Mitarbeiter im Bereich Support in den verschiedenen Standorten.
- Nennen Sie bitte Ihren Umsatz im Bereich Gesundheitswesen für die Jahre 1998 bis 2000.

C2 Erfahrungen

- Wie lange haben Sie Erfahrung mit...
  - welchen relationalen Datenbanksystemen?
  - welchen graphischen Benutzeroberflächen?
  - Client-Server-Applikationen?
- Wie lange unterhält Ihre Firma bereits eigene Installationen im Gesundheitswesen?

- Nennen Sie die Art, das Einführungsjahr und die Anzahl Kunden Ihrer für die Bewertung in dieser Ausschreibung wesentlichen Produkte im Gesundheitswesen.
- Verfügen Ihre Mitarbeiter über langjährige Erfahrungen
  – in der Informations- und Kommunikationstechnologie?
  – in der Teleradiologie?
  – in der Radiologie?
  – in der Medizin?
  – mit Schnittstellen in Krankenhausinformationssystemen?
- Sind Sie im Besitz einer aktuellen Zertifizierung nach ISO 9000?

C3 Auswahlunterstützung

- Gibt es die Möglichkeit einer Demonstrationsinstallation?
- Zu welchen Konditionen bieten Sie eine Testinstallation an?
- Legen Sie bitte eine Referenzliste vor.
- Machen Sie bitte konkrete Angaben über die Häufigkeit bisher durchgeführter bzw. geplanter Releasewechsel. Geben Sie bitte den zeitlichen Aufwand sowie die Ausfallzeit für die Releasewechsel an. Beschreiben Sie bitte das Vorgehen beim Releasewechsel.

C4 Schulungsangebot

- Erläutern Sie Ihr Schulungskonzept.

C5 Wartung und Softwarepflege

- Haben Sie eine Hotline eingerichtet?
- In welcher Zeit an welchen Tagen ist diese erreichbar?
- In welcher Zeit an welchen Tagen stehen Mitarbeiter für Wartungsarbeiten zur Verfügung?
- Wie und in welchem Zeitrahmen werden funktionale Kundenwünsche bei der Weiterentwicklung Ihres Produktes realisiert?
- Ist oder wird eine Kopie des Quellcodes bei einem unabhängigen Notar zum Investitionsschutz hinterlegt und wird diese regelmäßig aktualisiert?

4.5 Kosten

Ohne eine Bewertung der Kosten ist eine Systemauswahl nicht möglich. Bitte nennen Sie jeweils die Annahmen, unter denen Ihre Kostenschätzungen gültig sind.

D1 Lizenzgebühren für die Serversoftware

- Lizenz für die Serversoftware (bis zu 200 User).
- Lizenzen bei der Ausweitung der Anwendung (User > 200).

D2 Kosten weiterer Software

- Betriebssystem.
- Datenbanksystem.
- Sonstige Systeme.

D3 Kosten für Implementierung und Organisationsunterstützung

- Auflistung des zeitlichen Aufwandes.
- Sonstige Kosten.

D4 Schulungskosten während der Einführung

- Als Gesamtpauschale, pro Benutzer.

D5 Kostenschätzung der Hardware

- Angabe der Leistungskennzahlen für die benötigte Hardware (einschließlich USV).
- Unterbreitung eines Angebotes für die vorstehend genannte Hardware einschl. eventuell weiterer auf Grund des Firmenkonzeptes notwendiger Hardware (die Hardware zum Betrieb der Standleitungen und Einwahlleitungen ist nicht Bestandteil des Angebotes, ebenso sind Firewall-Rechner nicht Bestandteil des Angebotes).
- Unterbreitung eines Ergänzungsangebotes für die zusätzliche Anschaffung eines weiteren Kommunikationsservers.

D6 Laufende Kosten für Software

- Pflegekosten Serversoftware.
- Pflegekosten sonstiger Software.
- Kosten für zukünftige Updates.

D7 Kosten für den Betrieb

- Wie hoch liegen die Kosten für eine externe Übernahme
  - der Betreuung der Anwendungs- und Systemsoftware (Second Level Support)?
  - der Betreuung der Anwender (z. B. Anlegen von Nutzern, Vergabe von Berechtigungen,...)?
  - des Betreibens der Hotline der Nutzer?
  - der laufenden Schulungen nach der Einführungsphase?
  - der Einführung neuer Auswertungen etc. sowie von fachspezifischen Dokumentationen?
- Wie hoch liegen die Kosten für eine externe Betreuung des Gesamtsystems (Hardware, Software, Betreuung, Schulung, Systempflege)?

D8 Externe Tagessätze für Dienstleistungen

- Wie hoch liegen die Tagessätze für
  - das Projektmanagement?
  - das Customizing?
  - die Softwareentwicklung?
  - die Beratung?
  - einen Techniker?
  - die Schulung?
- Wie hoch liegen die Reisekosten und sonstige Nebenkosten?

D9 Vorlage einer Firmen-Standard-Preisliste für

- Software.
- Hardware.
- Dienstleistungen.

4.6 Zeitplan für die Einführung der Serversoftware und die Hardware-Installation

E1 Vorlage eines nach Ihren Erfahrungen realisierbaren Zeitplanes

5 FORMALITÄTEN ZUR AUSSCHREIBUNG

Die Ausschreibung wird von Partnerkliniken durchgeführt. Dieses vorliegende Pflichtenheft wird Grundlage dieser Angebotseinholungen und Ausschreibungen sein und wird durch weitere Vorgaben des lokalen Ausschreibers ergänzt.

Ansprechpartner für technische Fragen des vorliegenden Pflichtenheftes ist die Projektleitung im Universitätsklinikum Mannheim.

Dipl. phys. Dr. med. Gerald Weisser
Projektleiter
Oberarzt des
Institut für Klinische Radiologie
Universitätsklinikum Mannheim
Theodor-Kutzer-Ufer 1-3
68167 Mannheim

Tel. 0621-383-1409/1410/1411/1412
Fax 0621-383-1457

teleradiologie@rad.ma.uni-heidelberg.de

6 VERSIONSHISTORIE

Version 1.0 vom 15.05.2003: Erste Veröffentlichung.
Version 1.1 vom 04.06.2003:
- Änderung der Formatierung.
- Telefonnummern ergänzt.
- Zeitsynchronisation mittels NTP hinzugefügt.

Version 1.2 vom 28.11.2003:
- Änderung der Formatierung.
- Anpassung und Erweiterung der automatischen DICOM-E-Mail-Konvertierung aus datenschutzrechtlichen Gründen. (Kapitel 3.2, 4.1 & 4.2). Hierbei wurde aus datenschutzrechtlichen Gründen eine Trennung zwischen DICOM-Verarbeitung (mit zum Teil unverschlüsselten Daten) und dem öffentlichen Mailserver hergestellt.