Schreier G, Hayn D, Hörbst A, Ammenwerth E, editors. Proceedings of the eHealth2012. 2012 Mai 10-11; Vienna, Austria. OCG; 2012.

ENDE-ZU-ENDE SICHERHEIT: EIN LÖSUNGSANSATZ FÜR EIN NATIONALES NETZWERK ZUR TELEKOOPERATION

Staemmler M[1], Walz M[2], Weisser G[3], Engelmann U[4], Weininger R[5], Ernstberger A[6], Sturm J[7]

Kurzfassung

Die Telekooperation dient der zeitnahen Versorgung von Schwerverletzen durch den Austausch von Behandlungs- und Bilddaten. Für eine datenschutzkonforme Umsetzung erfolgt eine 2-Faktor Authentisierung durch Besitz und Wissen, personenbezogene Zugriffsrechte und eine Aufteilung der Verantwortungsbereiche zwischen einem Verzeichnisdienst, dem Betreiber und einem externen Sicherheitsdienstleister. Die Plattform ist seit Herbst 2011 erfolgreich in Betrieb.

Abstract

Telecooperation supports immediate care for trauma patients by facilitating a mutual exchange of treatment and image date. To comply with data protection regulation a 2-factor authentication using ownership and knowledge, personalized access rights and a distributed responsibility for the directory services, the operation of the infrastructure and external security services has been established. The platform is in routine-operation since autumn 2011.

Keywords – telecooperation, authentication, trauma, end-to-end security

1. Einleitung

Eine hochwertige Versorgung von Schwerverletzten erfordert die einrichtungsübergreifende Kooperation aller Beteiligten. Typische Szenarien ergeben sich einerseits aus der Notfallsituation wie z.B. „zweite Meinung“, „Abklärung einer Verlegungsindikation“, oder „Verlegung“ und andererseits aus der Weiterbehandlung wie z.B. zur „Rehabilitation“, „Physiotherapie“ oder „ambulanten Nachbehandlung“.

Die deutsche Gesellschaft für Unfallchirurgie (DGU) hat mit dem Aufbau ca. 55 Traumanetzen in Deutschland, die ca. 800 Traumazentren repräsentieren, die organisatorische Grundlage für eine umfassende Telekooperation gelegt [5]. Dabei gewährleistet die Zertifizierung der Traumazentren

1 Medizininformatik, Fachbereich ETI, Fachhochschule Stralsund

2 Ärztliche Stelle für Qualitätssicherung in der Radiologie Hessen, TÜV SÜD Life Service GmbH, Frankfurt

3 Radiologie und Geschäftsfeld Informationstechnologie und Qualitätssicherung, Universitätsmedizin Mannheim

4 Chili GmbH, Heidelberg

5 Pegasus GmbH, Regenstauf

6 Abteilung für Unfallchirurgie, Universitätsklinikum Regensburg

7 Akademie der Unfallchirurgie GmbH, München

die Struktur- und Prozessqualität entsprechend Vorgaben im Weißbuch zur Versorgung Schwerverletzter [12]. Auch Kliniken in Österreich sind bereits zertifiziert [10]. Technisch gesehen erfordert die Telekooperation zudem die Kommunikation von Bild- und Behandlungsdaten. Um den Aufwand nicht in jedem der Traumanetze zu duplizieren hat die Akademie der Unfallchirurgie (AUC) dazu eine bundesweite Plattform aufgebaut.

Ziel dieses Beitrags ist es - ausgehend von den funktionalen Anforderungen - die Systemarchitektur zur Gewährleistung einer datenschutzkonformen Authentisierung, Autorisierung und Transportsicherheit vorzustellen.

2. Methoden

Aus Sicht der Anwender sollen der Zugang und die Anbindung an die bundesweite Plattform zur Telekooperation in unterschiedlichen Funktionsstufen möglich sein.

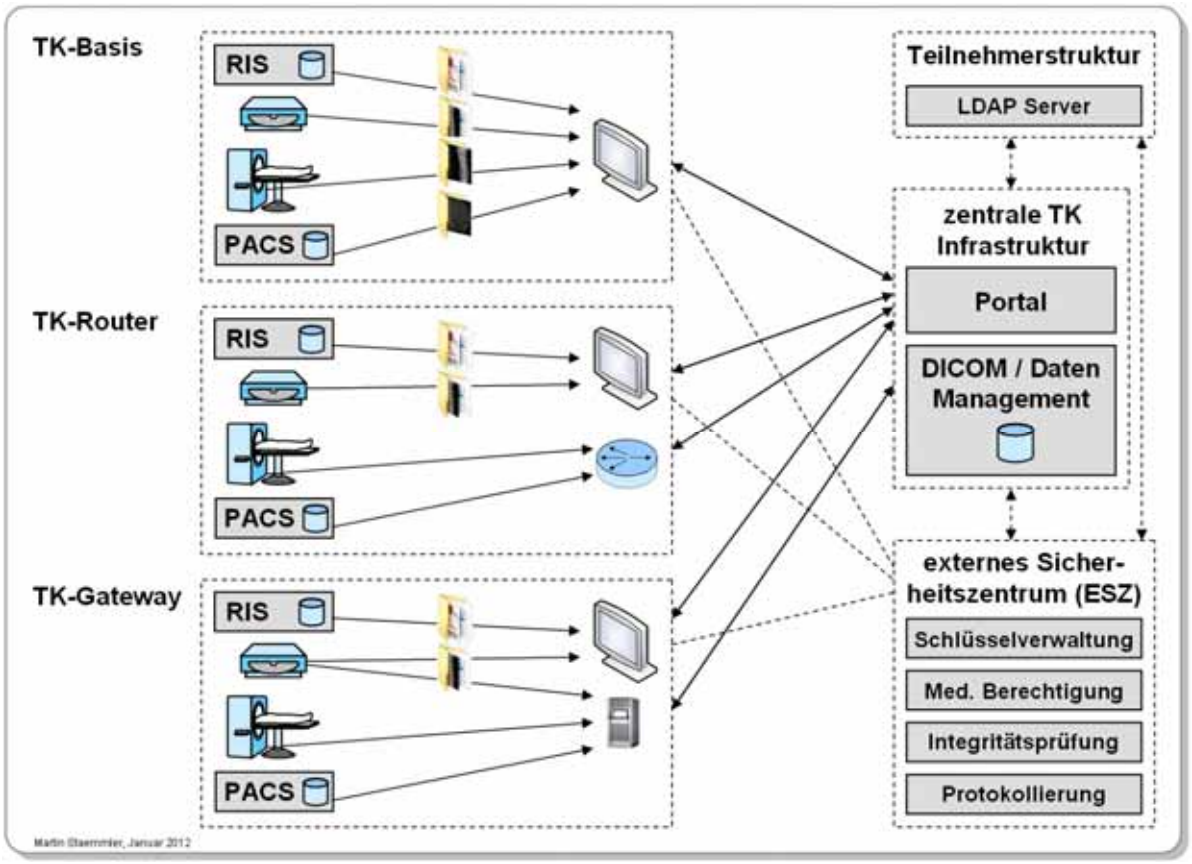

Abbildung 1: Systemarchitektur der Plattform zur Telekoopeeration

Abbildung 1 weist drei Funktionsstufen auf:

- In der Version „TK-Basis“ erfolgt der Zugang rein webbasiert über einen so genannten Web-Viewer, der per download von der zentralen TK-Infrastruktur verfügbar ist. In dieser einfachen Version können Behandlungs- und Bilddaten manuell aus einer Einrichtung über einen upload innerhalb des Web-Viewers für Berechtigte in anderen Einrichtungen bereitgestellt werden.
- Mit der in einer Einrichtung zu installierenden Anwendung „TK-Router“ steht statt der manuellen upload Funktion ein automatisiertes Routing für DICOM-Objekte zur Verfügung, d.h. DICOM-Objekte können direkt von einer Modalität, einem Befundungsarbeitsplatz oder einem PACS an Berechtigte in andere Einrichtungen weitergeleitet werden.
- Die Funktionsstufe „TK-Gateway“ realisiert zusätzlich zum Routing ein „Mini-PACS“ in der jeweiligen Einrichtung, das als temporärer Zwischenspeicher für DICOM-Objekte dienen kann

und somit die Entscheidung zur Übernahme der Daten in das Ermessen der Einrichtung stellt. Technisch gesehen benötigt der „TK-Gateway“ entweder die Installation lokaler Hardware oder eine entsprechende virtuelle Maschine.

Abhängig von der Funktionsstufe bei der empfangenden Einrichtung erhält diese Behandlungs- und Bilddaten durch manuelle Übernahme (TK-Basis) oder durch automatische Bereitstellung (TK-Router und TK-Gateway).
Die Umsetzung dieser Funktionalitäten in einer Systemarchitektur hat einer Vielzahl von Anforderungen und Rahmendingungen zu genügen:

- Die rein webbasierte Version TK-Basis führt ebenso wie die Beantwortung der Frage zur Administrierbarkeit bei der Anzahl von Einrichtungen zu einer Topologie, die auf einer zentralen TK-Infrastruktur aufsetzt. Diese stellt zwar einen möglichen „single-point-of-failure“ dar, dem aber durch entsprechende Redundanz und Virtualisierung begegnet werden kann.
- Personenbezogene Daten dürfen nur berechtigten Personen zur Kenntnis gelangen. Für die Telekooperation sind damit die Einwilligung des Patienten und vor allem der Behandlungszusammenhang eine Voraussetzung. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt eine 2-Faktor Authentifizierung der Nutzer vor, die durch Wissen, Besitz und persönliche Eigenschaften erfolgen kann [1]. Da die Auswertung persönlicher Eigenschaften wie z.B. Fingerabdruck oder Iris-Scan sich in der klinischen Praxis wenig eignet, ist das Wissen um ein Login und Passwort und der Besitz eines Token z.B. für ein „one-time-password“ oder ein Mobiltelefon für eine „mobileTAN“ erforderlich.
- Lediglich berechtigte medizinische Nutzer dürfen für einen Zugriff auf Patientendaten autorisiert werden. Nicht medizinische Nutzer inklusive Mitarbeiter und Administratoren eines Betreibers sind vom Zugriff auszuschließen. Dennoch müssen sie in der Lage sein, ihren Verwaltungsaufgaben in der zentralen TK-Infrastruktur nachgehen können.
- Der Schutz von Einrichtungen durch Firewalls ist in der Regel mit einer vollständigen Sperrung aller Ports verbunden außer denjenigen, die für Standarddienste wie email, SSL basierte Kommunikation oder Webzugriff offen sein müssen. Damit steht für die Telekooperation kein eigener Port zur Verfügung, so dass eine protokollmäßige Kapselung über den http bzw. https Port bzw. den Email Port verwendet werden muss.
- Eine Transportverschlüsselung auf Netzwerkebene stellt mit Protokollen wie SSL oder IPsec heutzutage kein Problem dar. Jedoch muss auf der Anwendungsebene ebenso eine Verschlüsselung erfolgen, damit Mitarbeiter und Administratoren eines Betreibers weder Zugriff auf personenbezogene Daten erhalten noch in der Lage sind Manipulationen, z.B. an einer revisionssicheren Protokollierung, vorzunehmen.
- Diese Sicherstellung der Integrität ist auf die implementierten Anwendungen zu erweitern.

3. Ergebnisse

Die Umsetzung der obigen Anforderungen zeigt die rechte Seite von *Abbildung 1*. Das Portal realisiert den webbasierten Zugang für die drei Funktionsstufen zusammen mit einem Management für Behandlungs- und Bilddaten, die in der zentralen TK-Infrastruktur nur temporär zum Zweck der Telekooperation gehalten werden.

Benutzer erhalten Zugang durch eine 2-Faktor Authentifizierung, die mit Login und Passwort über den LDAP Server und einen Tokendienst erfolgt (*Abbildung 2*). Für eine einfache Handhabung im klinischen Betrieb, kann das Token in einer gesicherten Umgebung wie einer medizinischen Einrichtung, die sich mit einer öffentlichen, statischen IP gegenüber der zentralen TK-Infrastruktur ausweist, ersetzt werden. Für Benutzer in einer klinischen Einrichtung kann damit die Anmeldung mit Login und Passwort ausreichend sein, außerhalb z.B. im Bereitschaftsdienst von zu Hause, ist zusätzlich ein „one-time-password“ oder die Nutzung einer „mobileTAN“ erforderlich.

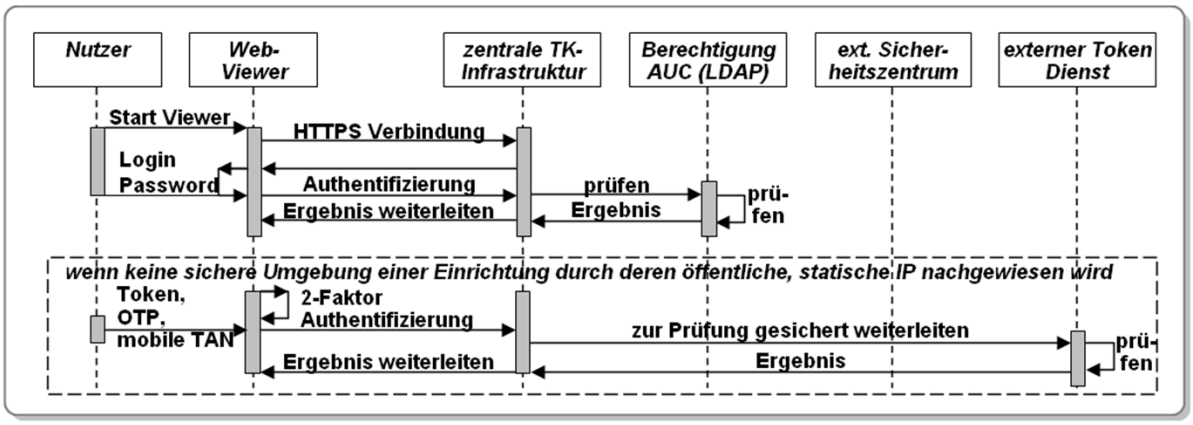

Abbildung 2: Ablauf der Authentifizierung

Generell ist der Zugriff auf Behandlungs- und Bilddaten an ein persönliches Login gekoppelt, ein abteilungsbezogenes Login ist rechtlich nicht zulässig. Für die Umsetzung im klinischen Alltag bildet daher der LDAP Server die Organisationsstrukturen der Einrichtungen im Traumanetz für einen abteilungsbezogenen Versand (z.B. an die Unfallchirurgie einer Einrichtung) ab. Berechtigt für den Zugriff auf diese Informationen ist jedoch nur eine Person, die nachweislich zu dieser unfallchirurgischen Abteilung gehört. Die Pflege dieser Zuordnungen in der Teilnehmerstruktur erfolgt mit gestuften Berechtigungen durch die AUC und durch die Telekooperationsverantwortlichen der Traumzentren.

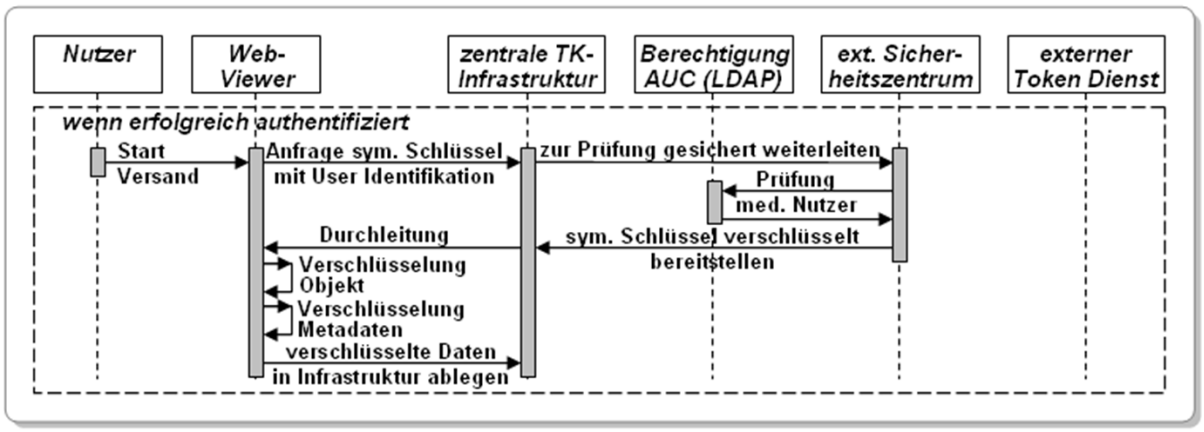

Abbildung 3: Ende-zu-Ende Sicherheit durch symmetrische Verschlüsselung

Ende-zu-Ende Sicherheit ist durch die Verschlüsselung der Datenobjekte beim Versender und die Entschlüsselung beim Empfänger gewährleistet. Aufgrund einer notwendigen abteilungsbezogenen Adressierung – der Diensthabende ist dem Versender nicht bekannt – wird kein „public-private-key“ Verfahren verwendet, sondern ein symmetrisches Verfahren (AES 256).

Um diesen symmetrischen Schlüssel gegen Kompromittierung zu sichern, wird er von einem so genannten externen Sicherheitszentrum (ESZ) erst zur Laufzeit über eine gesicherte Verbindung den Anwendungen (TK-Viewer, TK-Router und TK-Gateway) bereitgestellt und nie in einer Einrichtung abgespeichert (*Abbildung 3*). Um zu verhindern, dass der Betreiber der zentralen TK-Infrastruktur diesen Schlüssel kennt, wird das ESZ durch einen externen, unabhängigen Sicherheitsdienstleister in anderen Rechenzentren redundant betrieben. Der Schlüssel ist mit einem Gültigkeitszeitraum versehen, so dass im Fall einer Kompromittierung ein neuer Schlüssel bereitgestellt werden kann. Ebenso wird im ESZ geprüft, ob es sich um einen medizinischen Nutzer handelt, nur dann erfolgt die Übermittlung des Schlüssels. Da alle Datenobjekte in der zentralen TK-Infrastruktur nur verschlüsselt gehalten werden, müssen zugehörige Metadaten separat

verschlüsselt vorliegen, um eine schnelle Suche anwenderseitig nicht durch den download umfangreicher Datenmengen zu beeinträchtigen.

Die Aufteilung der Hoheitsbereiche zwischen dem Betreiber der zentralen TK-Infrastruktur und dem Sicherheitsdienstleister für das ESZ ermöglichen zudem die revisionssichere Protokollierung und eine Integritätsprüfung im ESZ.

4. Diskussion

Im Gegensatz zu bestehenden Lösungen der Teleradiologie [3, 7-9, 11] verfügt dieser Lösungsansatz über ein gestuftes Vorgehen, das ausgehend von einem einfachen webbasierten Zugang den Ausbau bis zu einem Mini-PACS in der Einrichtung beinhaltet.

Ende-zu-Ende Verschlüsselung ist auf Netzwerkebene ein übliches Vorgehen in VPN-Tunneln oder zwischen aktiven Netzwerkkomponenten [13]. Durch Verwendung von HTTPS in der Telekooperationsplattform wird gleichermaßen ein gesicherter Transport gewährleistet. Gegenüber PKI-basierten Lösungen wie im Projekt Teleimage [9] wird in diesem Vorhaben ein symmetrisches Verschlüsselungsverfahren auf der Anwendungsebene verwendet, dass mit einer Aufteilung in zwei Hoheitsbereiche verbunden ist: (i) Betreiber der zentralen TK-Infrastruktur und (ii) externer Sicherheitsdienstleister. Vorteilhaft ist, dass somit auf eine aufwändige, nutzerbezogene PKI verzichtet werden kann. In Verbindung mit der Abbildung der Organisationsstruktur besteht für die Nutzer die Möglichkeit einer abteilungsbezogenen Adressierung ohne jedoch die Vorgabe einer personenbezogenen Entgegennahme zu verletzen.

Mit der Umsetzung einer 2-Faktor Authentifizierung für Benutzer wird gegenüber bestehenden Netzwerken eine weitergehende Sicherheit erreicht, die auch den Zugang aus ungesicherten Umgebungen beinhaltet.

Während die Mehrzahl von Teleradiologienetzwerken nur DICOM-Objekte überträgt, erlaubt die Telekooperationsplattform die Bereitstellung von Behandlungs- und DICOM Bilddaten. Zusammen mit der Portalfunktion können für die Szenarien notwendige Zusatzinformationen übermittelt werden. Damit verfolgt die Plattform zumindest einen fallbezogenen Ansatz und steht im Wettbewerb wie z.B. zur bundesdeutschen elektronischen Fallakte (eFA)[2], den Infrastrukturdiensten des Cross-Enterprise Document Sharing (XDS) von IHE [4] oder den Mehrwertdiensten der geplanten Telematikinfrastruktur in Deutschland. Alle diese Lösungen erfordern jedoch spezifische Gateways oder Konnektoren in jeder Einrichtung und widersprechen damit dem einfachen, webbasierten Ansatz gemäß TK-Basis.

5. Schlussfolgerung und Ausblick

Die Telekooperationsplattform hat im Herbst 2011 mit zwei Pilotregionen im Saarland und in Schleswig-Holstein mit ca. je 10 Kliniken den Betrieb aufgenommen und zu Beginn des Jahres 2012 wird eine dritte Pilotregion in Bayern starten. Parallel wurde die Konzeption der Systemarchitektur den zuständigen Datenschützern der Bundesländer vorgelegt, von denen bereits eine erste Bestätigung der datenschutzkonformen Umsetzung vorliegt.

Für die Pilotphase hat die AUC eine Vorleistung in Bezug auf die Finanzierung übernommen, grundsätzlich muss der Betrieb jedoch durch Gebühren für die Einrichtungen kostendeckend gestaltet werden. Das Kostenmodell orientiert sich primär an der Größe der Einrichtungen (lokales, regionales, überregionales Traumazentrum) und an der in Anspruch genommenen Funktionalität (TK-Basis, TK-Router, TK-Gateway). Die Verantwortung für den Betrieb liegt jedoch nicht bei der AUC selbst, sondern bei den beteiligten Unternehmen, die in ihrer Rolle als Betreiber für den

Betrieb, die Installationsunterstützung, die Hotline, den Support, die Wartung und die Pflege verantwortlich sind.

Zur Evaluierung der Auswirkungen dieser Telekooperationsplattform auf die Versorgung von Schwerverletzen kann partiell auf die bestehenden Daten des TraumaRegisters [6] zurückgegriffen werden, die bereits heute in jedem Traumanetzwerk erfasst werden.

Vordringliches Ziel für das Jahr 2012 ist es durch die Anbindung möglichst vieler TraumaNetze und damit Traumazentren die Versorgungsqualität der Schwerverletzten zu verbessern. Ebenso soll der Nutzen der zentralen TK-Infrastruktur durch die Unterstützung von Anwendungsszenarien anderer Fachgebiete weiteren Patientengruppen zugute kommen.

6. Literaturangaben

[1] Bundesamt für Sicherheit in der Informationstechnik. M4.133 Geeignete Auswahl von Authentikationsmechanismen, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m04/m04133.html, (letzter Zugriff 25.3.2012)

[2] eFA (elektronische Fallakte) www.fallakte.de (letzter Zugriff 25.3.2012)

[3] Engelmann, U., Münch, H., Schröter, A., Meinzer, HP. Teleradiologie-Konzepte der letzten 10 Jahre am Beispiel von CHILI In: Jäckel (Hrsg.) Telemedizinführer Deutschland 2008. Bad Nauheim: Minerva 242-248, (2007)

[4] IHE Cross Enterprise Document Sharing (XDS), www.ihe.net, (letzter Zugriff 25.3.2012)

[5] Ruchholtz S. Das TraumaNetzwerk der Deutschen Gesellschaft für Unfallchirurgie (DGU), Notfall Rettungsmed 10:420–422 (2007)

[6] Probst C, Richter M, Haasper C, Lefering R, Otte D, Oestern HJ, Krettek C, Hüfner T. Traumaregister der Deutschen Gesellschaft für Unfallchirurgie.Chirurg. 2008 Jul;79(7):650-6 (2008)

[7] reif und möller diagnostic-network ag. www.diagnostic-network-ag.de/index.php (2011)

[8] Staemmler M, Schmidt C, Dräger J, Ehricke HH. Nachhaltige und verlässliche landesweite Telematik-Dienste – organisatorische und technische Umsetzung, in e-Health 2010, medical future verlag, S 163-166, (2009)

[9] Stingl C, Slaming D, Kurmann T. Sichere und webbasierte Verteilung Radiologischer Bilddaten – Das Projekt Teleimage. Tagungsband eHealth 2008, Wien: 55-60 (2008)

[10] SALK. Überregionales Traumazentrum, Salzburg, http://www.salk.at/80_6557.html (letzter Zugriff 25.3.2012)

[11] Weisser G. Praktische Erfahrungen im Teleradiologie-Projekt Rhein-Neckar-Dreieck, apps.drg.de/data/DOWN LOADS/roentgenkongress-2009/Weisser_RK306_Teleradiologie_22mai09.pdf, Deutscher Röntgenkongress (2009)

[12] Weissbuch Schwerverletzen-Versorgung, Deutsche Gesellschaft für Unfallchirurgie e.V., Berlin, http://www.dgu-online.de/pdf/unfallchirurgie/weissbuch/weissbuch.pdf (letzter Zugriff 25.3.2012)

[13] Wozak F, Schabetsberger T, Ammenwerth E. End-to-end Security in telemedical Networks – a Practical Guideline. J. Med. Inf. 2007; 76: 484:490

Corresponding Author
Martin Staemmler
Medizininformatik, Fachbereich ETI, Fachhochschule Stralsund
Zur Schwedenschanze 15, D-18435 Stralsund, Deutschland
Email: martin.staemmler@fh-stralsund.de