

# TKmed – eine praxisorientierte Lösung zur Telekooperation für die Versorgung von Schwerverletzten

## TKmed – a pragmatic approach for telecooperation for trauma care

M. STAEMMLER<sup>a</sup>, M. WALZ<sup>b</sup>, G. WEISSER<sup>c</sup>, U. ENGELMANN<sup>d</sup>,  
A. ERNSTBERGER<sup>e</sup>, U. SCHMUCKER<sup>f</sup>, J. STURM<sup>f</sup>

<sup>a</sup> *Medizininformatik, Fachbereich ETI, Fachhochschule Stralsund*

<sup>b</sup> *Ärztliche Stelle für Qualitätssicherung in der Radiologie Hessen, TÜV SÜD Life, Service GmbH, Frankfurt*

<sup>c</sup> *Radiologie und Geschäftsfeld Informationstechnologie und Qualitätssicherung, Universitätsmedizin Mannheim*

<sup>d</sup> *CHILI GmbH, Heidelberg*

<sup>e</sup> *Abteilung für Unfallchirurgie, Universitätsklinikum Regensburg*

<sup>f</sup> *Akademie der Unfallchirurgie GmbH, München*

**Zusammenfassung.** Telekooperation unterstützt die Versorgung von Schwerverletzten durch den Austausch von Behandlungs- und Bilddaten im Rahmen einer Notfallkonsultation, einer zweiten Meinung, einer Verlegung, der Rehabilitation oder in der Nachbehandlung. Die TKmed-Lösung ist datenschutzkonform durch eine 2-Faktor Authentifizierung (Besitz und Wissen) sowie eine Ende-zu-Ende Sicherheit auf Basis einer symmetrischen Verschlüsselung (mit der Trennung zwischen dem IT-Betrieb und der Bereitstellung des Schlüssels durch ein externes Sicherheitszentrum) gewährleistet. Versandpartner können auf Abteilungsebene ausgewählt werden, dabei erhalten nur Personen Zugriff, die gemäß einer Abfrage in einem Organisationsverzeichnis (LDAP) zu dieser Abteilung gehören. TKmed ist im Routinebetrieb und wird derzeit von 50 Einrichtungen genutzt.

**Abstract.** Telecooperation is used to support care of trauma patients by facilitating a mutual exchange of treatment and image data in use-cases such as emergency consultation, second-opinion, transfer, rehabilitation and out-patient after-care. The TKmed approach complies with data protection legislation, namely by providing two-factor authentication using ownership and knowledge as well as end-to-end security based on a symmetric encryption (using separation of concern for the IT infrastructure provider and trusted services for the provisioning of the symmetric key at runtime). Telecooperation partners may be chosen at departmental level but only individuals of that department, as a result of checking the organizational assignments maintained by LDAP services, are granted access. The TKmed platform is in routine operation and currently used by 50 trauma centers.

**Keywords.** Telecooperation, authentication, end-to-end-security, trauma

## **1. Einleitung**

Eine hochwertige Versorgung von Schwerverletzten erfordert die einrichtungsübergreifende Kooperation aller Beteiligten. Typische Anwendungsfälle („use cases“) betreffen die „zweite Meinung“, „Abklärung einer Verlegungsindikation“, „Tele-radiologie nach RöV“, „Rehabilitation“, „Physiotherapie“ oder „ambulante Nachbehandlung“. Die Deutsche Gesellschaft für Unfallchirurgie (DGU) hat mit dem Aufbau von ca. 55 Traumanetzen in Deutschland (ca. 800 Traumazentren) die organisatorische Grundlage für eine umfassende Kooperation gelegt [1]. Die lokalen, regionalen und überregionalen Traumazentren in jedem Traumanetz gewährleisten durch ihre Zertifizierung die Struktur- und Prozessqualität gemäß den Vorgaben des Weißbuchs Schwerverletztenversorgung [2]. Dieses beinhaltet auch die Unterstützung der Kooperation durch den Austausch von Bild- und Behandlungsdaten. Eine Analyse in den Traumanetzen zeigte jedoch, dass die Vernetzung zwischen den Traumazentren eines Traumanetzes sehr unterschiedlich und vielfach nicht für alle Traumazentren realisiert war [3]. Zudem gab es kaum die Möglichkeit zum Datenaustausch zwischen den unterschiedlichen Traumanetzen, z. B. im Rahmen der zweiten Meinung oder zur Begutachtung. Diese Situation war für die Akademie der Unfallchirurgie (AUC) der Anlass, eine bundesweite Plattform zum Datenaustausch zu konzipieren, rasch umzusetzen und die Organisation des Betriebs zu unterstützen. Die beteiligten Traumanetze und Traumazentren können damit auf eine Dienstleistung zurückgreifen und müssen nicht selbst als Entwickler bzw. Betreiber aktiv werden. Zudem gewährleistet dieser bundesweite Ansatz eine Traumanetz übergreifende Kooperation.

Ziel dieses Beitrags ist es, die grundlegenden Konzepte dieser Plattform zur Telekooperation in der Medizin (TKmed), den Weg zur Umsetzung und die ersten Ergebnisse zur Nutzung vorzustellen. Dabei berücksichtigt die Konzeption nicht nur die Anforderungen der Nutzer, sondern auch umfänglich die Vorgaben des Datenschutzes.

## **2. Methoden**

### *2.1 Anforderungen*

Zur Erarbeitung der Anforderungen wurde eine interdisziplinäre Arbeitsgruppe bestehend aus Unfallchirurgen, Radiologen und Fachleuten aus der Telemedizin etabliert. Sie erstellte in einem Zeitraum von sechs Monaten in mehreren Treffen funktionale und nicht-funktionale Anforderungen (Tabelle 1).

Sie bildeten die Grundlage für die Erstellung eines Lastenhefts für die „Telekooperation in Traumanetzwerken“, das bereits Vorgaben zur Systemarchitektur und zur Realisierung von Funktionsstufen enthielt:

- Die Verwaltung eines solchen Netzes mit einer hohen Anzahl von Traumazentren erfordert eine zentrale Infrastruktur, da der Abgleich zwischen

dezentral betriebenen Infrastrukturen (z. B. per Traumanetz) mit einem großen Aufwand verbunden wäre und dem Ziel einer bundesweiten Lösung widerspräche. Diese zentrale Infrastruktur sollte zudem einen gesicherten Datenaustausch zwischen den Traumazentren ermöglichen.

- Für die Nutzer sollten drei Funktionsstufen bereitstehen, die einen rein web-basierten Zugang mit manueller Interaktion bis zu einem Gateway mit automatischer Weiterleitung („routing“) für den Transfer von DICOM Objekten umfassen. Für den Transfer von non-DICOM Objekten sollte ein Portal bereitstehen.

Das Lastenheft bildete die Grundlage für die Ausschreibung und die Bewertung der eingegangenen Angebote durch die Mitglieder der interdisziplinären Arbeitsgruppe. Die nachfolgenden Verhandlungen mit Anbietern beinhalteten sowohl eine Demonstration der bereits vorliegenden Produkte als auch eine Klärung offener Punkte in einem iterativen Vorgehen, das nach vier Monaten mit einem Zuschlag für die Bietergemeinschaft (CHILI GmbH, Dossenheim und pegasus GmbH, Regenstauf) abgeschlossen werden konnte. In diesem Zeitraum wurden zudem konkrete Lösungswege für die Umsetzung der Anforderungen erarbeitet.

Funktionale Anforderungen	
F1	Anwendungsfälle: zweite Meinung, Abklärung Verlegungsindikation, TR nach RöV, Rehabilitation, Physiotherapie oder ambulante Nachbehandlung
F2	Aufgabenangemessene Funktionsstufen
F3	Übermittlung von Bild- / Behandlungsdaten (DICOM / non-DICOM Objekte)
F4	Unterstützung medizinischer Vorgänge (Anfrage, Antwort, Dokumentation)
F5	Einfache Integrierbarkeit mit Bestandsstrukturen, ‚Push‘ oder ‚Pull‘ Interaktion
F6	Ortsunabhängiger Benutzerzugang, Adressierung (Abteilung, Einzelperson)
F7	Konferenz – Synchronisation der Bildbetrachtung zwischen Einrichtungen
Nicht-funktionale Anforderungen	
N1	Intuitive Bedienbarkeit
N2	Datenschutz (Authentifizierung, Rollenkonzept für Zugriffe, Ende-zu-Ende Sicherheit, keine Langzeitspeicherung von Bild- oder Behandlungsdaten)
N3	Kurze Übertragungszeiten (z. B. Zeitvorgaben für TR nach RöV)
N4	Betrieb, Verfügbarkeit, Wartbarkeit, Skalierbarkeit, Protokollierung (Audit)
N5	Offenheit (andere med. Fachdisziplinen, Integration mit Bestandsnetzen, etc.)

**Tabelle 1.** Anforderungen

## 2.2 Systemarchitektur

Für den Nutzer stehen drei Funktionsstufen zur Verfügung (Abbildung 1), welche die Anforderungen F1, F2, F3 und F5 für DICOM-Objekte abdecken:

- In der Version „TK-Basis“ erfolgt der Zugang rein webbasiert über eine Web-Viewer Anwendung, die per download von der zentralen TK-Infrastruktur verfügbar ist. In dieser einfachen Version können Behandlungs-

und Bilddaten manuell aus einer Einrichtung per upload innerhalb des Web-Viewers für Berechtigte in anderen Einrichtungen bereitgestellt werden. TK-Basis ist für die gelegentliche Nutzung z. B. zum Bildversand im Bereitschaftsdienst eines lokalen Traumazentrums oder zum Bildempfang für eine Praxis vorgesehen.

- Die in einem Traumazentrum zu installierende Anwendung „TK-Router“ stellt 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. TK-Router erlaubt einen komfortablen, regelmäßigen Versand.
- 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 des Traumazentrums stellt. TK-Gateway ist eine Lösung für die tägliche Nutzung und stellt Optionen zur Integration mit Krankenhausinformationssystemen bzw. Bestandsnetzen bereit. Technisch gesehen benötigt „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), d. h. die Funktionsstufen sind beliebig miteinander kombinierbar.

Bei Nutzung des Web-Viewers in Verbindung mit der zentralen Infrastruktur können die Viewer von zwei Nutzern für eine Telekonferenz synchronisiert werden (Anforderung F7), um sicherzustellen, dass für beide die gleiche Darstellung vorliegt.

## TKmed – eine praxisorientierte Lösung zur Telekooperation für die Versorgung von Schwerverletzten

M. Staemmler, M. Walz, G. Weisser, U. Engelmann, A. Ernstberger, U. Schmucker, J. Sturm

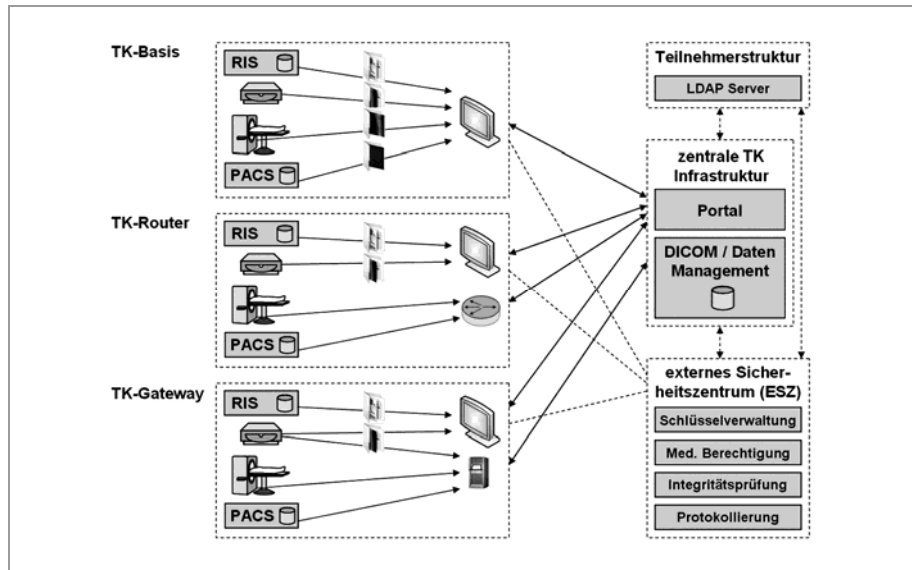


Abbildung 1. Systemarchitektur

Die Übermittlung von non-DICOM Objekten ist sowohl über den Web-Viewer als auch das Portal möglich und erfüllt damit die Anforderung F3. Allerdings benötigen non-DICOM Objekte stets einen Bezug zu einem DICOM Objekt. Zum einen kann dieser Bezug bereits zu einem vorhandenen DICOM Objekt vorliegen (z. B. im Rahmen einer Konsilanfrage) oder der Benutzer kann diesen selbst herstellen, indem relevante Angaben (Patientenstamm- und Studiendaten) erfasst werden. Der Bezug stellt eine Klammer für typische medizinische Vorgänge gemäß Anforderung F4 dar, indem eine Anfrage des Versenders und die Antwort des Empfängers (z. B. Befund) an das DICOM-Objekt gebunden und dokumentiert werden. Beim Versand besteht zudem die Möglichkeit, einen Betreff und eine kurze Nachricht für den Empfänger einzugeben. Portal und Web-Viewer sind intuitiv nutzbar (Anforderung N1), indem sie z. B. Benutzer durch die Freigabe von Funktionen durch den Prozess des Versands oder Empfangs leiten oder durch Hilfetexte bei Elementen der Benutzeroberfläche unterstützen.

### 2.3 Maßnahmen zum Datenschutz

Die Systemarchitektur (Abbildung 1) weist zusätzlich zu den bereits beschriebenen Komponenten die Verwaltung der Teilnehmerstruktur und das sogenannte externe Sicherheitszentrum (ESZ) auf, die beide zur Umsetzung der Anforderungen des Datenschutzes dienen.

Generell ist für den Zugang zu Telekooperation eine korrekte Authentifizierung des Nutzers notwendig, die entsprechend den Vorgaben des Bundesamts für Sicher-

heit in der Informationstechnik (BSI) zwei Bedingungen der drei Vorgaben Wissen, Besitz oder persönliche Merkmale erfüllen muss [4]. Da persönliche Merkmale wie z. B. Fingerabdruck in der klinischen Praxis wenig geeignet sind, wurde für diese 2-Faktor Authentifizierung das Wissen um ein Login und Passwort sowie den Besitz eines Tokens, z. B. für die Generierung eines „one-time-passwords“ oder einer „mobileTAN“ (Mobiltelefon als Token) gewählt. Für eine einfache Handhabung im klinischen Betrieb (Abbildung 2), kann jedoch das Token in einer gesicherten Umgebung wie einer medizinischen Einrichtung, die sich mit einer öffentlichen, statischen IP gegenüber der zentralen TK-Infrastruktur ausweist, entfallen, so dass Login und Passwort ausreichend sind. In einer unsicheren Umgebung (mobil, im Bereitschaftsdienst von zu Hause) wird das Token benötigt. Damit ist ein ubiquitärer Zugang gewährleistet (Anforderung F6).

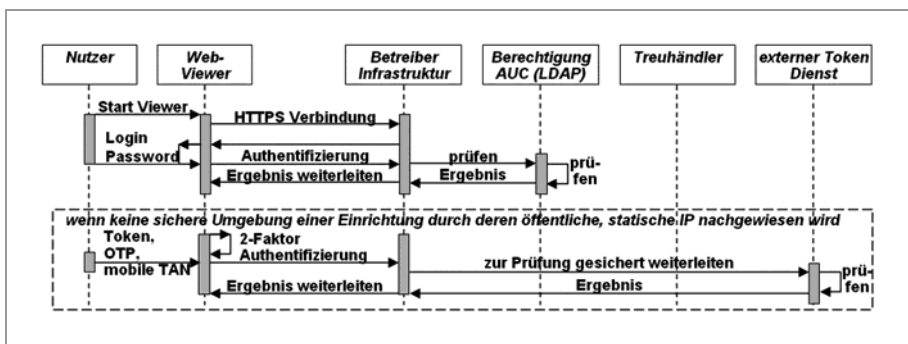


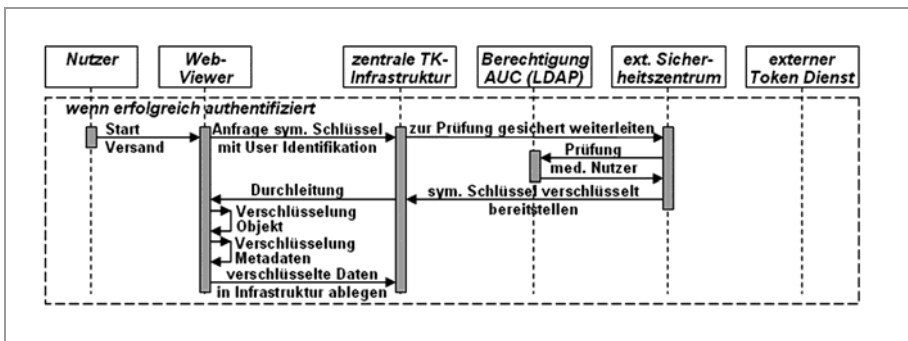
Abbildung 2. 2-Faktor Authentifizierung

Weiterhin sieht Anforderung F6 eine personen- oder abteilungsbezogene Adressierung beim Versand vor, da in der Regel beim Versender nicht bekannt ist, wer der diensthabende Arzt beim Empfänger ist. Ein allgemeines abteilungsbezogenes Zugriffsrecht ist jedoch datenschutzrechtlich unzulässig. Für die Umsetzung im klinischen Alltag bildet daher der LDAP Server die Organisationsstrukturen der Traumazentren mit ihren Abteilungen und berechtigten Personen ab. Berechtigt zum Zugriff auf Bild- und Behandlungsdaten ist nur eine Person, die nachweislich zu der adressierten Abteilung gehört. Die Pflege dieser Zuordnungen in der Teilnehmerstruktur erfolgt durch die Telekooperationsverantwortlichen der Traumazentren.

Grundsätzlich beinhaltet jegliche Kommunikation auf der Transportebene eine verschlüsselte Übermittlung per HTTPS. Damit entfallen spezifische Konfigurationen wie z. B. für VPN oder gar DICOM SCP Dienste in der Firewall eines Traumazentrums.

Alle patientenbezogenen Daten werden zudem durch die Verschlüsselung der Datenobjekte beim Versender und die Entschlüsselung beim Empfänger auf Anwendungsebene zur Gewährleistung einer Ende-zu-Ende Sicherheit geschützt. Aufgrund der abteilungsbezogenen Adressierung kann jedoch nur ein symmetrisches Ver-

fahren (z. B. AES 256) verwendet werden. Um diesen symmetrischen Schlüssel gegen Kompromittierung zu sichern, wird er im 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 separat betrieben. Der Schlüssel ist mit einem Gültigkeitszeitraum versehen, so dass im Fall einer Kompromittierung ein neuer Schlüssel bereitgestellt werden kann. Zudem wird im ESZ die Rolle „medizinischer Benutzer“ gepflegt. Nur für Nutzer, die diese Rolle innehaben, wird der Schlüssel an die Anwendung übermittelt. Da alle Datenobjekte in der zentralen TK-Infrastruktur nur verschlüsselt vorliegen, müssen zugehörige relevante Metadaten separat verschlüsselt bereitgestellt werden, um eine schnelle Suche anwenderseitig nicht durch den download umfangreiche Datenmengen zu beeinträchtigen.



**Abbildung 3.** Bereitstellung des symmetrischen Schlüssels zur Laufzeit

Durch die Aufteilung der Hoheitsbereiche zwischen dem Betreiber der zentralen TK-Infrastruktur und dem Sicherheitsdienstleister für das ESZ kann im ESZ die reversionssichere Protokollierung der Benutzeraktivitäten und die Integritätsprüfung der Anwendungen vorgenommen werden (Anforderung N4).

## 2.4 Vereinbarungen für den Betrieb

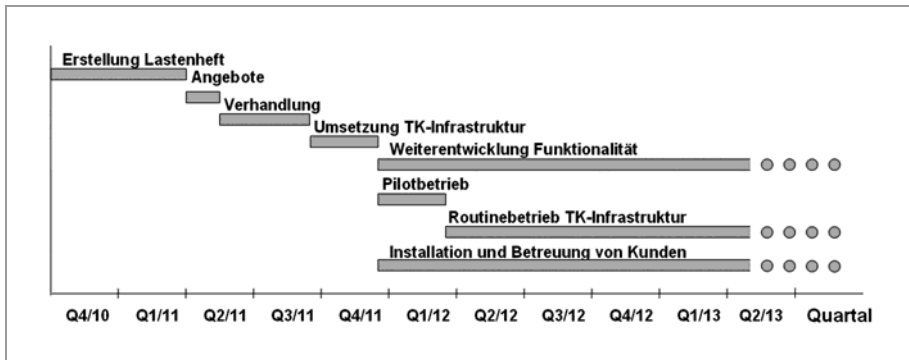
Der Betrieb der TK-Infrastruktur und des ESZ obliegt zwei unabhängigen, örtlich getrennten Providern, die diese Komponenten redundant in je zwei Rechenzentren bereitstellen. Sowohl die TK-Infrastruktur als auch das ESZ stellen einen „single-point-of-failure“ dar. Durch kontinuierliche Spiegelung zwischen den jeweiligen Rechenzentren wird ein Ausfall eines Teilsystems oder einer Komponente durch Gewährleistung einer Hochverfügbarkeit kompensiert.

Neben dem technischen Betrieb sind vertragliche Vereinbarungen notwendig. Die Akademie der Unfallchirurgie (AUC) hat mit einem Rahmenvertrag den An-

bieter (CHILI GmbH als Generalunternehmer) mit der Umsetzung und dem Betrieb des Telekooperationsnetzwerks TKmed beauftragt. Der Rahmenvertrag verpflichtet die AUC den Betrieb des ESZ mit einem separaten Betreiber sicherzustellen. GleichermäÙen sichert der Anbieter den Betrieb der zentralen TK-Infrastruktur gemäÙ der vereinbarten SLAs („service level agreements“) zu (Anforderung N3 und N4). Zwischen einem Teilnehmer und dem Anbieter wird jeweils ein Teilnehmervertrag geschlossen, der den Umfang der Dienstleistung, aber auch die notwendigen datenschutzrechtlichen Aspekte (z. B. Datenverarbeitung im Auftrag) umfasst.

### 3. Ergebnisse

Abbildung 4 stellt den zeitlichen Ablauf des Projekts TKmed dar. Aufgrund vorliegender Produkte und Erfahrungen des Anbieters konnten in einer relativ kurzen Umsetzungsphase die TKmed-spezifischen Eigenschaften (symmetrische Ende-zu-Ende Verschlüsselung, zentrale Verwaltung der Organisationsstruktur, Funktionsstufen und die organisatorische Trennung zwischen Betrieb der zentralen TK-Infrastruktur und dem ESZ) realisiert werden.



**Abbildung 4.** zeitlicher Verlauf der Umsetzung

Am Pilotbetrieb haben drei Traumanetze (Schleswig-Holstein, Saarland) mit je ca. 10 Kliniken erfolgreich teilgenommen. Seit Frühjahr 2012 steht TKmed für den Routinebetrieb zur Verfügung, so dass zum Frühjahr 2013 bereits 50 Kliniken TKmed für die Telekooperation verwenden. Abbildung 5 zeigt die Entwicklung der Nutzung seit Beginn des Pilotbetriebs mit wachsender Versandanzahl und Datenvolumen für den Zeitraum von November 2011 bis März 2013.



### TKmed – eine praxisorientierte Lösung zur Telekooperation für die Versorgung von Schwerverletzten

M. Staemmler, M. Walz, G. Weisser, U. Engelmann, A. Ernstberger, U. Schmucker, J. Sturm

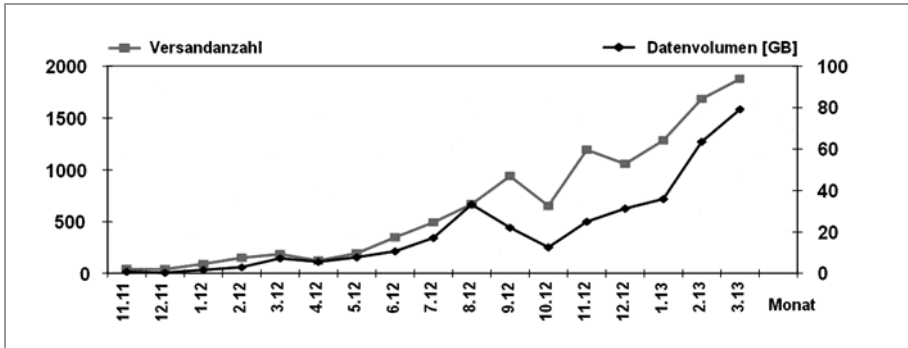


Abbildung 5. Entwicklung der Nutzung über den Zeitraum vom Nov. 2011 bis März 2013

Analysiert man die Versandaktivität der beteiligten Kliniken in dem Zeitraum vom November 2011 bis März 2013 so zeigt sich nur bei ca. 40 % der Teilnehmer eine aktive Rolle als Versender (Abbildung 6). Allerdings ist bei dieser Aussage zu berücksichtigen, dass einerseits in dem betrachteten Zeitraum erst nach und nach die Anbindung der Traumazentren erfolgt ist und andererseits regionale und überregionale Traumazentren primär als Empfänger agieren.

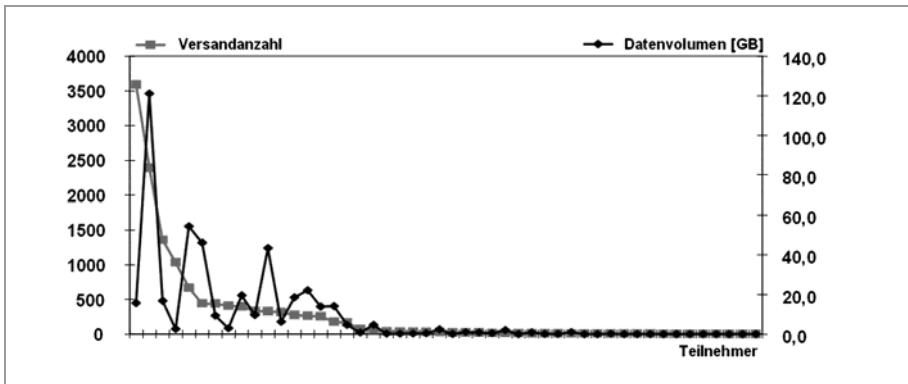
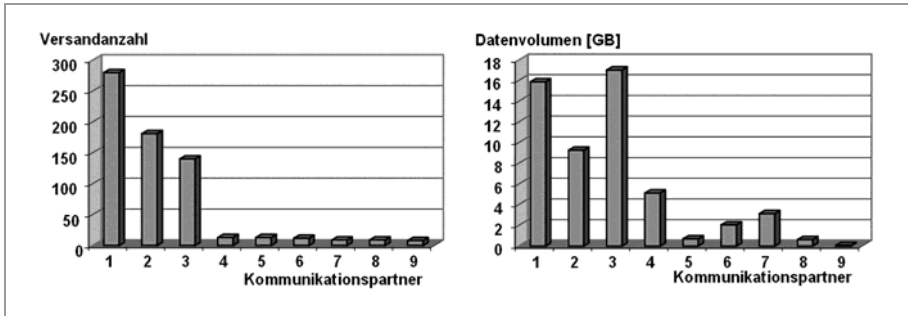


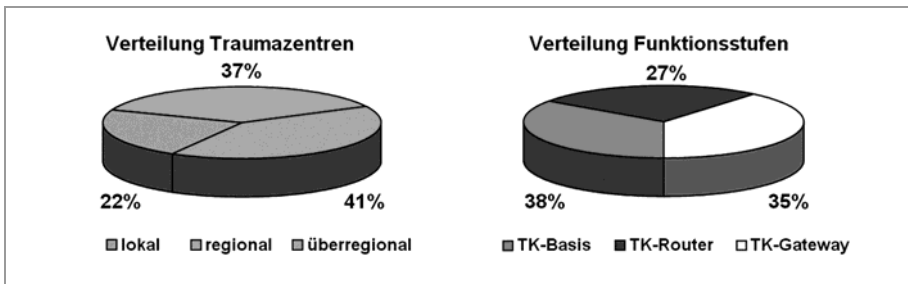
Abbildung 6. Versandanzahl und Datenvolumen im Zeitraum vom Nov. 2011 bis März 2013



**Abbildung 7.** Versandaktivität in einem Traumanetz über den Zeitraum vom Nov. 2011 bis März 2013

Traumanetze sind ein Zusammenschluss von lokalen, regionalen und überregionalen Traumazentren, um in hoher Qualität und Verfügbarkeit eine kooperative Versorgung von Schwerverletzten zu gewährleisten. Dies dokumentiert die Verteilung der Versandaktivität auf die Traumazentren eines Traumanetzes (Abbildung 7), die eine aktive Beteiligung aller Traumazentren zeigt. Erste Analysen weisen daraufhin, dass etwa 10 % des Datentransfers ein Traumazentrum außerhalb des eigenen Traumanetzes betreffen (z. B. zur Konsultation überregionaler Spezialisten).

Die Verteilung zwischen den drei Typen von Traumazentren zeigt Abbildung 7, linke Seite, mit einem hohen Anteil an regionalen und überregionalen Traumazentren. Die Traumazentren nutzen für ihre Kooperation alle drei TKmed-Funktionsstufen, dabei werden TK-Router und TK-Gateway erwartungsgemäß aufgrund ihrer Routing Funktionalität bevorzugt.



**Abbildung 7.** Verteilung der Traumazentren und genutzter Funktionsstufen

Insgesamt dokumentiert diese erste Auswertung der Nutzung, dass das bundesweite Angebot für die Telekooperation mittels TKmed dem Bedarf der Kliniken entspricht und von diesen gut nachgefragt wird.

TKmed stellt sich zudem als offenes Telekooperationsnetzwerk dar. Über ein TK-Gateway besteht nicht nur die Möglichkeit, Einrichtungen in bestehende Netzen

(z. B. bei Klinikkonzernen) anzubinden, sondern auch für eine Einrichtung eine DICOM-E-Mail Funktionalität zu unterstützen.

#### **4. Diskussion**

Im Gegensatz zu bestehenden Lösungen der Teleradiologie [5-9] verfügt TKmed 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 [10], chipkartenbasiert für Personen [11] oder mit PKI-Infrastrukturen [12]. Alle diese Lösungen sind mit einem erhöhten organisatorischen Aufwand oder Kosten verbunden. Im Gegensatz dazu führt die Verwendung eines symmetrischen Verschlüsselungsverfahrens auf der Anwendungsebene zu einem deutlich geringeren Aufwand, auch unter Berücksichtigung der Aufteilung in zwei Hoheitsbereiche: (i) Betreiber der zentralen TK-Infrastruktur und (ii) externer Sicherheitsdienstleister. Zudem gewährleistet es - in Verbindung mit der Abbildung der Organisationsstruktur - für die Nutzer die Möglichkeit einer abteilungsbezogenen Adressierung ohne jedoch die Vorgabe einer personenbezogenen Entgegennahme zu verletzen

Die Umsetzung einer 2-Faktor Authentifizierung für Benutzer von TKmed entspricht den Vorgaben zur Authentifizierung [4,11]; sie ist jedoch heutzutage in einer Vielzahl bestehender anderer Netze noch nicht entsprechend realisiert.

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. Die Bindung an ein DICOM-Objekt unterstützt typische Konsultationsprozesse. Im Vergleich zu aktenbezogenen Lösungen, wie z. B. die bundesdeutsche elektronische Fallakte (eFA) [14, 15], den Infrastrukturdiensten des Cross-Enterprise Document Sharing (XDS) von IHE [16] bzw. der IHE-D Cookbook Initiative [17] oder den Mehrwertdiensten der geplanten Telematikinfrastruktur in Deutschland, benötigt TKmed keine a priori Vergabe von Zugriffsrechten oder einen übergreifenden Master Patient Index. Ebenso erfordert die Anbindung mit TK-Basis im Vergleich zu IHE XDS keine spezifische HW/SW in der jeweiligen Einrichtung. Dies ist sicherlich ein Grund, warum TKmed in relativ kurzer Zeit umgesetzt werden konnte. Andererseits wird die Kooperation zwischen Traumazentren und anderen medizinischen Einrichtungen mittelfristig eine akten- bzw. patientenbezogene Zuordnung erfordern, insbesondere mit der Verfügbarkeit von IHE-basierten Lösungen und Schnittstellen zu Praxis- und Krankenhausinformationssystemen. Die zukünftige Weiterentwicklung von TKmed wird diesen Aspekt berücksichtigen.

## Referenzen

- [1] Ruchholtz S. Das TraumaNetzwerk der Deutschen Gesellschaft für Unfallchirurgie (DGU), Notfall Rettungsmed 10:420–422 (2007).
- [2] Deutsche Gesellschaft für Unfallchirurgie, Weißbuch Schwerverletztenversorgung, 2.Auflage, (2012)
- [3] Ernstberger A, Walz M, Staemmler M, Sturm J, Weisser G. Stand der Teleradiologienutzung in Traumanetzwerken in 2011. RöFo [184], 82. 2012.
- [4] Bundesamt für Sicherheit in der Informationstechnik. M4.133 Geeignete Auswahl von Authentifikationsmechanismen, <https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m04/m04133.html>, (letzter Zugriff 20.5.2013).
- [5] 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).
- [6] reif und möller diagnostic-network ag. [www.diagnostic-network-ag.de/index.php](http://www.diagnostic-network-ag.de/index.php) (2011).
- [7] Staemmler M, Schmidt C, Dräger J, Ehrlicke HH. Nachhaltige und verlässliche landesweite Telematik-Dienste – organisatorische und technische Umsetzung, in e-Health 2010, medical future verlag, S 163-166, (2009).
- [8] Stingl C, Slamang D, Kurmann T. Sichere und webbasierte Verteilung Radiologischer Bilddaten – Das Projekt Teleimage. Tagungsband eHealth 2008, Wien: 55-60 (2008).
- [9] Weisser G. Praktische Erfahrungen im Teleradiologie-Projekt Rhein-Neckar-Dreieck, [apps.drg.de/ data/DOWNLOADS/roentgenkongress-2009/Weisser\\_RK306\\_Teleradiologie\\_22mai09. pdf](http://apps.drg.de/data/DOWNLOADS/roentgenkongress-2009/Weisser_RK306_Teleradiologie_22mai09.pdf), Deutscher Röntgenkongress (2009).
- [10] Wozak F, Schabetsberger T, Ammenwerth E. End-to-end Security in telemedical Networks – a Practical Guideline. J. Med. Inf. 2007; 76: 484-490.
- [11] Alkhateeb A, Singer H, Yakami M, Takahashi T. An End-to-End Secure Patient Information Access Card System, Method Inform Med. 2000; 39: 70-72.
- [12] Kurmann T, Slamang D, Stingl C, Roessl K. Teleimage: An Integrated Approach for Secure and Webbased Exchange of Medical Images and Reports, IFMBE Proceedings 22, Springer, pp. 970-973, 2008.
- [13] Burr, WE, Dodson DF, Newton EM, Perlner RA, Polk WT, Gupta S, Nabbus EA. Electronic Authentication Guideline, National Institute of Standards and Technology, Publication 800-63-1. 2011
- [14] eFA (elektronische Fallakte) [www.fallakte.de](http://www.fallakte.de) (letzter Zugriff 15.5.2013).
- [15] EFA v.2.0, [wiki.hl7.de/index.php/cdaefa:EFA\\_Spezifikation\\_v2.0](http://wiki.hl7.de/index.php/cdaefa:EFA_Spezifikation_v2.0) (letzter Zugriff 15.5.2013).
- [16] IHE Cross Enterprise Document Sharing (XDS), [www.ihe.net](http://www.ihe.net), (letzter Zugriff 15.5.2013).  
IHE Deutschland Cookbook, [wiki.hl7.de/index.php/IHE\\_DE\\_Cookbook](http://wiki.hl7.de/index.php/IHE_DE_Cookbook) (letzter Zugriff 15.5.2013).