Anlage 4 **Datenschutzkonzept**

zum TKmed® Teilehmervertrag

Inhaltsverzeichnis

1 Begriffsbestimmungen

- *Account:* Elektronischer Zugang eines *Benutzers* über das Internet mittels gesicherter Verbindung zur *zentralen TK-Infrastruktur* des TKmed® Netzwerks mittels Zugangskennung / Passwort und *Token.*
- *Administrator:* Benutzer der u.a. über Rechte zur Verwaltung und Vergabe von *Account*s verfügt.
- *Auftragnehmer:* CHILI GmbH, Friedrich-Ebert-Str. 2, 69221 Dossenheim auf Grundlage des Rahmenvertrags TKmed® zwischen dieser und der Akademie der Unfallchirurgie GmbH (AUC).
- *Ausbaustufe: TK-Basis, TK-Router* oder *TK-Gateway.*
- *Benutzer:* Allgemeine Bezeichnung für alle Anwender (z. B. *Nutzer* und *Administratoren*), welche, je nach Berechtigung, die zentrale *TK-Infrastruktur* oder die *TK-Komponenten* nutzen.
- *Bilddaten*: Bilddaten von Patienten im DICOM-Standard oder Non-DICOM-Format (z.B. digitale Sonografie-, Röntgen-, CT-, MRT- Bilddatensätze*).*
- *CHILI Viewer:* Java-basierter *Vie*wer, der in einem Web-Browser läuft und u.a. zur Betrachtung und Bearbeitung von *Bilddaten* dient.
- *Daten*: Alle administrativen und medizinischen Behandlungsdaten wie Formulare, *Bilddaten*, Befunde, Labor- und sonstige Untersuchungsergebnisse, einschließlich der Dokumentation zur Telekooperation zwischen *Teilnehmern* in digitaler Form.
- *DICOM*: „Digital Imaging and Communications in Medicine" ist ein offener Standard zum Bilddatenaustausch in der Medizin. Siehe http://medical.nema.org.
- *ESZ*: Externes Sicherheitszentrum, u.a. zur Verwaltung der Schlüssel für die Verschlüsselung der Daten im *TK-Rechenzentrum*.
- *HTTPS:* „HyperText Transfer Protocol Secure", per SSL verschlüsseltes Übertragungsprotokoll im Internet.
- *Infrastruktur-Betreiber:* Die CHILI GmbH gemeinsam mit der pegasus gmbh.
- *Institution = Teilnehmer*
- *LDAP: „*Lightweight Directory Access Protocol", Verzeichnisdienst zur Benutzerverwaltung.
- *Medizinischer Anwender = Nutzer.*
- *Nutzer*: Als Gesellschafter, angestellte oder anderweitig in die Behandlung von Patienten des *Teilnehmers* eingebundene Person mit medizinischer Qualifikation und Funktion (z.B. Arzt oder Physiotherapeut), für die e*in Account* mi*t Nutzer*rechten vergeben ist.
- *PACS*: „Picture Archiving and Communication System", Bildverwaltungssystem in *Institutionen*.
- *Portal*: Gesichertes Portal für die *Teilnehmer* und *Nutzer* zur Interaktion mit der zentralen *TK-Infrastruktur* und zur Administration.
- *Teilnehmer*: Kliniken, (Einzel-)Ärzte oder Physiotherapeuten, Gemeinschaften zwischen diesen (Berufsausübungsgemeinschaften, MVZ etc.), die in der Regel durch ein Institutskennzeichen eines Krankenhauses, eine KV-Zulassung (Abrechnungsnummer) oder als eigenständige wirtschaftliche Einheit charakterisiert sind. Bei Leistungserbringern, die unter einem Institutskennzeichen oder einer KV-Zulassung an mehreren Standorten Einrichtungen betreiben, ist für jeden Standort, der im TKmed® Adressverzeichnis gelistet wird, ein eigener Teilnehmervertrag zu schließen. Die Abbildung eines Standortes als Abteilung eines bestehenden Standortes ist unzulässig.
- *TK-Basis*: *CHILI Viewer* beim *Teilnehmer* zur Darstellung von *Daten* und zum manuellen Hoch- und Herunterladen von *Daten* über die *zentrale TK-Infrastruktur* sowie deren Bereitstellung für berechtigte *Nutzer*.
- *TK-Beauftragter:* Als Ansprechpartner benannter Mitarbeiter des *Teilnehmers* zur Abstimmung zwischen *Auftragnehmer* und *Teilnehmer*.
- *TK-Gateway*: Wie *TK-Basis*, zusätzlich lokales System für automatischen, regelbasierten Versand und Empfang von *Daten* über die *zentrale TK-Infrastruktur* verbunden mit einer lokalen, temporären Zwischenspeicherung der *Daten*. Der *CHILI Viewer* ermöglicht die Nutzung der *TK-Gateway* Funktionen. Das *TK-Gateway* ist eine Serveranwendung und benötigt eine lokale Hardware oder eine virtualisierte Umgebung. Das *TK-Gateway* ist mit Zusatzmodulen auch in der Variante *TK-Gateway Professional* verfügbar.
- *TK-Komponenten*: Alle teilnehmerseitigen Komponenten (z.B. der *CHILI Viewer* für *TK-Basis*, die *TK-Router* Anwendung oder das *TK-Gateway*) mit ihren möglichen Erweiterungen.

- *TK-Rechenzentrum:* Redundante Rechenzentren der pegasus gmbh. Dort werden u.a. die Server und die Datenhaltung für die zentrale TK-Infrastruktur betrieben. Das *Portal* wird ebenso durch diese Rechenzentren zur Verfügung gestellt.
- *TK-Router*: Wie *TK-Basis*, zusätzlich eine lokale Anwendung beim *Teilnehmer* für automatischen Versand und Empfang von *DICOM* Daten über die zentrale *TK-Infrastruktur*.
- *TK-TNW-Beauftragter*: Ansprechpartner in einem *TNW,* der die Aktivitäten der Netzwerk-Krankenhäuser abstimmt und für die Abstimmung zwischen *Auftragnehmer* und *TNW* zuständig ist.
- *TKmed® Direkt*: Ermöglicht den Upload von *Datenobjekten (DICOM und non-DICOM)* an einen *TKmed® Nutzer* durch eine Person, die nicht *TKmed®-Nutzer ist, sich aber zuvor durch die Anforderung eines Links für den Upload registriert hat.*
- *TKmed® Direkt Professional*: Wie *TKmed® Direkt*, jedoch erhält die Person einen Link für den Upload in Form einer persönlichen Einladung von einem TKmed® Nutzer.
- *TNW*: Traumanetzwerk(e): Organisation und zertifizierter Verbund von Krankenhäusern, die als Traumazentren angemeldet oder bereits auditiert sind.
- *Token:* Eine Hardware- oder Softwarekomponente im Besitz eines *Nutzers* für die Zugriffskontrolle des *Account*s.
- *VPN:* Virtual Private Network, ein geschlossenes privates Netz, das über eine öffentliche Netzwerkstruktur betrieben wird.
- *WAF: W*eb Application Firewall.
- *Zentrale TK-Infrastruktur*: Sämtliche Systeme für den Betrieb von TKmed®, die nicht von dem *Teilnehmer* verantwortet werden. Besteht aus dem *TK-Rechenzentrum* und dem *ESZ*.

2 Zusammenfassung

2.1 Medizinische Ausgangslage

Im Jahr 2006 wurde von der Deutschen Gesellschaft für Unfallchirurgie (DGU) das Weißbuch Schwerverletztenversorgung[1] publiziert, in dem einerseits eine abgestufte Strukturqualität und erstmalig auch eine bestimmte Prozessqualität der Schwerverletztenversorgung innerhalb der Krankenhäuser gefordert wurde. Andererseits wurden regionale Zusammenschlüsse von Krankenhäusern (regionale Traumanetzwerke) zur Zusammenarbeit bei der Schwerverletztenversorgung empfohlen. Das Ziel ist eine Steigerung der Qualität der Patientenversorgung und der Patientensicherheit.

Mit Auditierungs- und Zertifizierungsschritten wird ein fester Rahmen für die Schwerverletzenversorgung durch Traumanetzwerke (TNW) gewährleistet. Inzwischen führte diese Initiative der DGU zur Bildung von ca. 55 Traumanetzwerken mit ca. 800 beteiligten unfallchirurgischen Krankenhäusern. Grundlage für deren Kooperation zur Versorgung der Schwerverletzten bildet eine enge und funktionierende Kommunikation zwischen den Krankenhäusern. Diese Kommunikation benötigt den Austausch von Bild- und Behandlungsdaten. Sie ist in einzelnen Traumanetzwerken unterschiedlich ausgeprägt und bisher meist auf das jeweilige TNW oder nur einzelne Teilnehmer davon beschränkt.

2.2 Technische Ausgangslage

Bestehende Lösungen zum Austausch von Bilddaten setzen weitgehend auf den Standard DICOM zur Repräsentation der Bilddaten und zur Kommunikation auf Anwendungsebene. Sie unterscheiden sich jedoch in Bezug auf die verwendete Topologie und die Kommunikation auf der Netzwerkebene. Eine reine Punkt-zu-Punkt[2] („peer-to-peer") Kommunikation ist i. d. R. nur für wenige direkte Verbindungen zwischen Institutionen geeignet, wenn gezielt jede Netzwerkverbindung eingerichtet werden muss (z.B. VPN-Tunnel). Eine skalierbare Lösung bietet DICOM-E-Mail[3], da bei jeder Institution die Pflege der E-Mail-Adressen der miteinander kooperierenden Partner einfach möglich ist. Eine Alternative zu „peer-to-peer" ist eine zentralistische Topologie („hub-to-spoke"), die über einen zentralen Knoten die DICOM-Objekte zwischen den Institutionen vermittelt und damit von den partnerspezifischen Verbindungseigenschaften und Protokollen abstrahiert.

Die bestehenden Lösungen zum Bilddatenaustausch sind meist regional ausgeprägt und sind teilweise durch einzelne Institutionen einer Region dominiert. Ein bundesweites Angebot besteht derzeit nicht.

Für den Austausch von Behandlungsdaten stellt sich die Situation ohne einen Standard wie DICOM weitaus problematischer dar. Einige Modellvorhaben nutzen regional- oder konzernbezogene Insellösungen. Die Verzögerungen bei der Einführung einer bundesweiten Telematikinfrastruktur haben zudem integrative und übergreifende Ansätze verhindert, so dass ein einfacher Dokumentenaustausch mit zumeist unstrukturiertem Inhalt die primäre Grundlage heutiger Lösungsansätze bildet.

2.3 Vorgehen

Das Gesamtprojekt zur Entwicklung von TKmed® setzt auf den Teleradiologie Produkten der Firma CHILI GmbH aus Heidelberg auf, die spezifisch für die Anforderungen für die TKmed® und zur Gewährleistung des Datenschutzes in Bezug auf Autorisierung und Authentifizierung durch Leistungen der Firma pegasus gmbh aus Regenstauf ergänzt werden. Die beabsichtigte Lösung setzt auf einer zentralen Infrastruktur im Sinne von „hub-and-spoke" (s.o.) auf und bietet den Institutionen einen Zugang per HTTPS. Zusätzlich wird eine Anbindung von bestehenden Netzwerken auf Basis des DICOM-E-Mail-Protokolls und von VPN-Verbindungen über eine Umverschlüsselung unterstützt.

---

[1] DGU Weißbuch, Erläuterung: dgu-online.de/weissbuch; Download: dgu-online.de/wb-download.
[2] Punkt-zu-Punkt, Vernetzungsform in der jeder Teilnehmer mit jedem verbunden ist. Die Anzahl der notwendigen Verbindungen steigt überproportional zur Anzahl der Teilnehmer.
[3] DICOM-E-Mail, DICOM Standard und Empfehlung der Deutschen Röntgengesellschaft zur Datenübertragung auf E-Mail-Basis insb. von DICOM-Daten zwischen Netzwerkteilnehmern. Bei DICOM-E-Mail können die Daten verschlüsselt werden.

Im Rahmen des Gesamtprojekts übernimmt pegasus gmbh zusammen mit CHILI GmbH die Verantwortung für den Betrieb der zentralen TK-Infrastruktur.

2.4 Zielsetzung

Die geplante bundesweite Telekommunikationslösung TKmed® soll mit ihren Anwendungen die Kooperation für Traumanetzwerke und auch einzelne Teilnehmer in verschiedenen Szenarien unterstützen. Darüber hinaus soll TKmed® als fachdisziplinübergreifende und offene Plattform auch explizit von nicht unfallchirurgischen Abteilungen genutzt werden können.

3 Fachliches Konzept

Die fachlichen Anforderungen von Seiten des Medizinischen Anwenders lassen sich in vier wesentliche Szenarien einteilen.

3.1 Szenario „zweite Meinung"

Gerade bei Schwerverletzten wird häufig die Konsultation mit einem externen Fachkollegen gesucht. Diese so genannte „zweite Meinung" („second opinion") oder auch Expertenkonsultation helfen dem Arzt vor Ort in seiner Entscheidung und Optimierung der Weiterbehandlung. Voraussetzung für eine weiterführende Konsultation ist die Zurverfügungstellung aller relevanten Untersuchungsergebnisse (vorliegende Befunde und Bilddaten) und eine Qualifizierung der mit der Konsultation verbundenen Fragestellung (z.B. über einen Anruf, einen Freitext, ein Formular, eine Fallanmeldung) für den externen Fachkollegen. Wünschenswert ist in manchen Fällen zudem eine Synchronisation der Anwendungen bei der Betrachtung von Bilddaten, d.h. beide Fachkollegen sehen den gleichen Satz von Bilddaten und jegliche Benutzerinteraktion wird an den jeweils anderen propagiert.

Technisch erfordert dieses Szenario meist eine zeitnahe Übertragung der vorliegenden Daten in Befundungsqualität (ohne diagnostisch verlustbehaftete Kompression) sowohl für Bilddaten im DICOM-Format als auch für weitere Daten in anderen Formaten. Zudem soll die Übertragung bidirektional möglich sein, um die „zweite Meinung" zu dokumentieren und an den Anfragenden übermitteln zu können. Eine Übernahme der Daten in IT-Systeme des externen Fachkollegen ist in der Regel nicht zwingend erforderlich. Eine temporäre Zwischenspeicherung auf der zentralen TK-Infrastruktur kann für Rückfragen hilfreich sein.

3.2 Szenario „Verlegung"

Von den ca. 35000 Schwerverletzten pro Jahr werden ca. 25% zur weiteren Behandlung in eine andere Institution verlegt. Das Vorgehen bei einer Verlegungsentscheidung ist dem Szenario „zweite Meinung" sehr ähnlich. Eine Verlegung erfordert jedoch zwingend die Übernahme aller übermittelten relevanten Bild- und Behandlungsdaten in die Dokumentation auf Seiten der anderen Institution, beinhaltet aber ggf. keine schnelle Rückmeldung.

Aus technischer Sicht gelten grundsätzlich die gleichen Anforderungen wie bei der „zweiten Meinung". Zusätzlich soll jedoch gewährleistet sein, dass die Bilddaten und Behandlungsdaten in der anderen Institution für die Übernahme in deren Dokumentationssysteme (z.B. PACS, RIS[4], KIS[5], DMS[6]) geeignet bereitgestellt werden.

3.3 Szenario „Teleradiologie nach RöV"

Unter „Teleradiologie nach Röntgenverordnung (RöV)" versteht man die bildgebende Untersuchung eines Menschen mit Röntgenstrahlen unter der Verantwortung eines so genannten Teleradiologen, der sich nicht am Ort der Durchführung der Untersuchung befindet. Ziel ist es u.a. notwendige radiologische Untersuchungen auch außerhalb üblicher Dienstzeiten durchführen zu können.

Aus technischer Sicht ist dieses Szenario mit dem der „Verlegung" in vielen Punkten vergleichbar. Allerdings enthalten die RöV und die DIN die Vorgabe einer maximalen Dauer von 15 Min. zur Übertragung eines typischen Bilddatensatzes (oft mehrere 100 Bilder) und stellen damit weitreichende Anforderungen an die Übertragungsbandbreite. Ebenso ist durch arbeitstägliche Prüfung die Verfügbarkeit und durch monatliche Kontrollen die Qualität der Übertragungseinrichtungen nachzuweisen. TKmed® kann für die Teleradiologie nach RöV genutzt werden. Eine Teleradiologie nach RöV wird grundsätzlich zwischen jeweils zwei bestimmten Teilnehmern (wobei ein Teilnehmer durchaus

[4] RIS, „RadiologieInformationsSystem" Radiologisches Verwaltungssystem in Krankenhäusern
[5] KIS, „KrankenhausInformationsSystem" Verwaltungssystem in Krankenhäusern
[6] DMS, „DokumentenManagementSystem" Datenbankgestützte Verwaltung elektronischer Dokumente

an mehreren Verbindungen teilnehmen kann) abgenommen. Für die Teleradiologie nach RöV sind eine Abnahme nach DIN 6868-159, eine Genehmigung und eine nachfolgende Qualitätssicherung erforderlich.

3.4 Szenario „Einbindung externer Kooperationspartner"

Externe Kooperationspartner sind z.B. Rehabilitationskliniken, niedergelassene Ärzte oder Physiotherapeuten, die an der Behandlung beteiligt sind. Im Gegensatz zu den übrigen Szenarien benötigen sie meist nur eine Teilmenge der vorliegenden Bild- und Behandlungsdaten, um eine weitere Therapie kompetent durchführen zu können. Die Auswahl dieser Teildatenmenge ist nicht Bestandteil dieses Konzepts, da sie durch die behandelnden Ärzte erfolgt. Lediglich die Übernahme und Bereitstellung dieser Teildatenmenge für einen Versand an den externen Kooperationspartner sollen durch TKmed® ermöglicht werden.

Dieses Szenario entspricht weitgehend dem der „Verlegung", allerdings mit anderen Zeitvorgaben, da es sich um eine länger andauernde Weiterbehandlung handelt.

3.5 Szenario „Ad hoc Kommunikation"

Im Gegensatz zu den vorigen Szenarien erlaubt das Szenario „Ad hoc Kommunikation" auch für Personen, die nicht zum Nutzerkreis eines TKmed® Teilnehmers gehören, zum Beispiel Patienten oder an der Behandlung eines Patienten beteiligten Personen, den Versand von Datenobjekten an einen TKmed® Nutzer, sofern dieser Nutzer seinen Account für TKmed® Direkt bzw. TKmed® Direkt Professional frei geschaltet hat. Diese „ad hoc Kommunikation" ist unidirektional, selbst eine nachträgliche Einsichtnahme der versandten Datenobjekte durch den Versender ist nicht möglich, da dieser sich gegenüber TKmed® nicht eindeutig authentifizieren kann (er ist im Teilnehmerverzeichnis nicht als Nutzer geführt).

3.6 Funktionales Stufenkonzept

Grundlage der Umsetzung bildet die zentrale TK-Infrastruktur, die für alle an der TKmed® angemeldeten Teilnehmer als Plattform bereitsteht. Grundsätzlich stehen für die Anbindung einer Institution an die zentrale TK-Infrastruktur mehrere Protokolle (insb. HTTP/HTTPS, VPN Tunnel) zur Verfügung.

Die Funktionalität dieser Plattform ergibt sich aus den folgenden Ausbaustufen:

- TK-Basis
- TK-Router
- TK-Gateway

TK-Basis erlaubt die manuelle Übernahme von DICOM-Objekten und Non-DICOM-Objekten (Datei-Upload und –Download, Texteingabe, formularbasierte Eingabe) und den Versand an einen definierten Empfänger über die zentrale TK-Infrastruktur (Abbildung 1). Der Empfänger erhält über die zentrale TK-Infrastruktur Zugriff auf die bereitgestellten Daten und kann diese bei Bedarf manuell übernehmen. TK-Basis ist als reine Webanwendung dadurch gekennzeichnet, dass auf Seiten der Teilnehmer keine Hardware installiert werden muss. Notwendige Software wird per Download bereitgestellt. Der Zugang zur Infrastruktur erfordert eine Authentifizierung und Autorisierung der Benutzer.

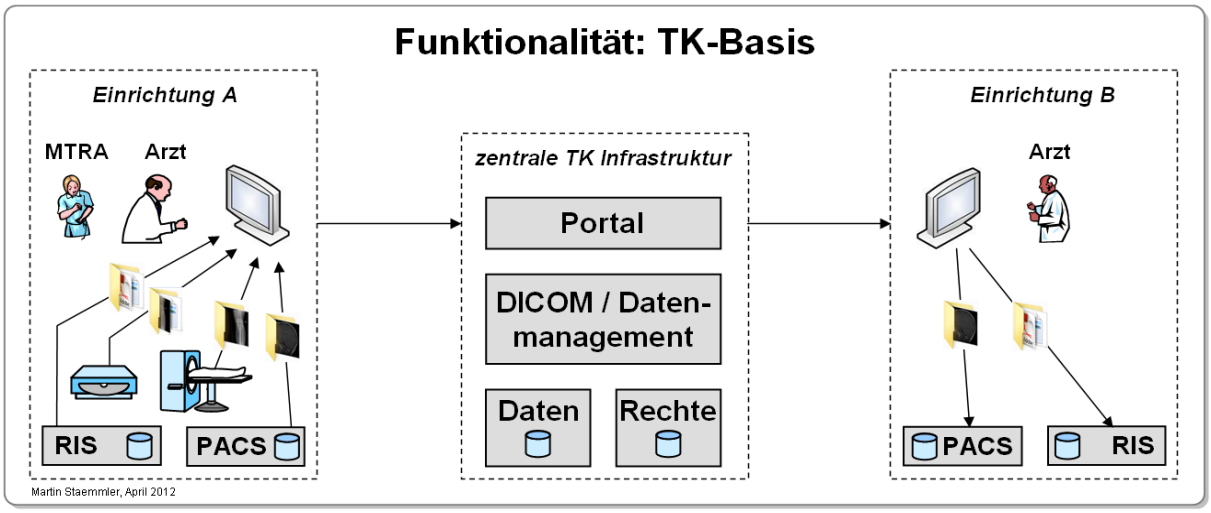

Abbildung 1: Darstellung TK-Basis

TK-Router oder TK-Gateway sehen jeweils eine Komponente in unterschiedlichem Funktionsumfang bei dem jeweiligen Teilnehmer vor (Abbildung 2 und Abbildung 3). TK-Router oder TK-Gateway erlauben eine automatisierte Übernahme von DICOM-Objekten und unterstützen dabei klinische Arbeitsabläufe. Ein TK-Gateway realisiert zudem eine lokale, temporäre Zwischenspeicherung der Daten und vereinfacht damit das institutionseigene Datenmanagement z.B. in Bezug auf Patientenzuordnungen.

Ebenso kann ein Teilnehmer, der mit TK-Router oder TK-Gateway arbeitet, problemlos mit einem anderen Teilnehmer, der TK-Basis verwendet, kommunizieren, allerdings ohne einen durchgängig automatisierten Arbeitsablauf.

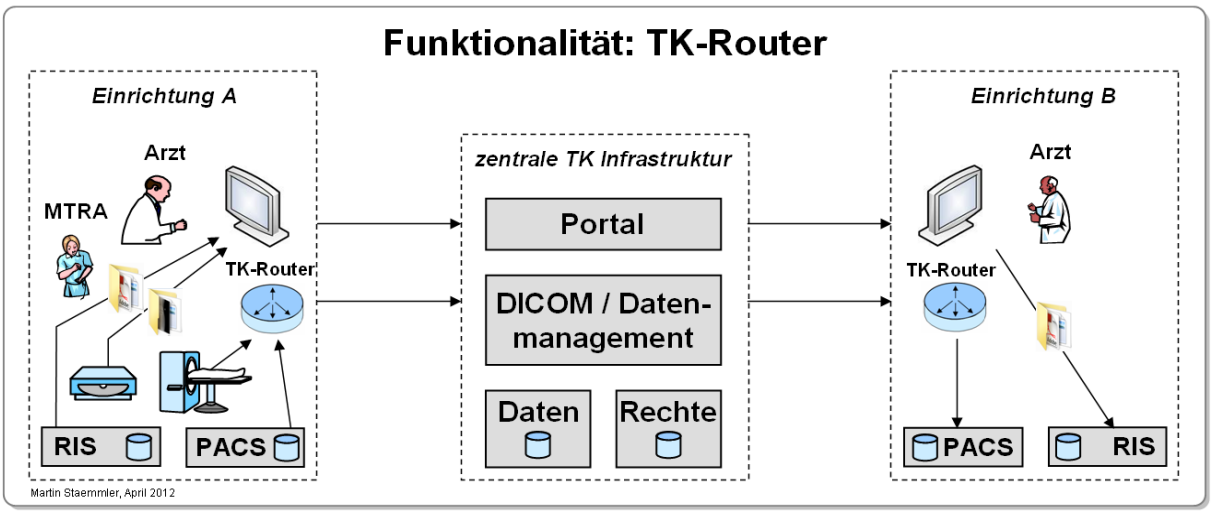

Abbildung 2: Darstellung TK-Router

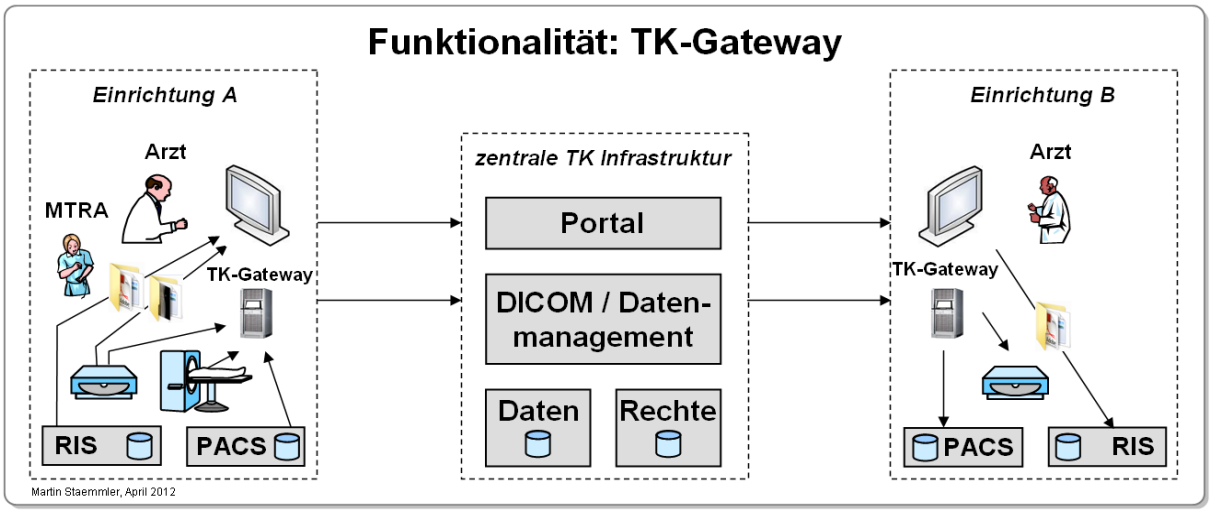

Abbildung 3: Darstellung TK-Gateway

Während TK-Basis, TK-Router und TK-Gateway einen bidirektionalen Austausch von Datenobjekten für Nutzer von TKmed® vorsehen, erlauben TKmed® Direkt und TKmed® Direkt Professional den unidirektionalen Versand von Datenobjekten an TKmed® Nutzer durch Personen, die nicht TKmed® Nutzer sind. TKmed® Nutzer können in ihrem Nutzerprofil ihre Adresse für den Empfang von TKmed® Direkt bzw. TKmed® Direkt Professional frei schalten.
TKmed® Direkt erlaubt den Versand durch vorab nicht bekannte Personen in einem zweistufigen Vorgehen (Beantragung eines Links, Nutzung des per E-Mail erhaltenen Links für den Upload), während TKmed® Direkt Professional eine Einladung (Versand eines personengebundenen Links für den Upload) an mögliche Versender voraussetzt.

4 Technische Beschreibung

Dieses Kapitel stellt die Gesamtstruktur zur Umsetzung der fachlichen Szenarien vor. Ausgehend von einem Gesamtüberblick wird auf die einzelnen Teilbereiche wie TK-Rechenzentrum, Anbindung der Teilnehmer sowie Sicherheitsmechanismen eingegangen.

4.1 Gesamtstruktur

Abbildung 4 zeigt die technische Struktur für den Versand und Empfang der Daten. Hier sind die Teilnehmer dargestellt, welche auf die zentrale TK-Infrastruktur zugreifen bzw. Daten übermitteln oder erhalten. Dies erfolgt je nach Ausbaustufe über die entsprechende TK-Komponente (CHILI Viewer (TK-Basis), die TK-Router Anwendung oder das TK-Gateway).

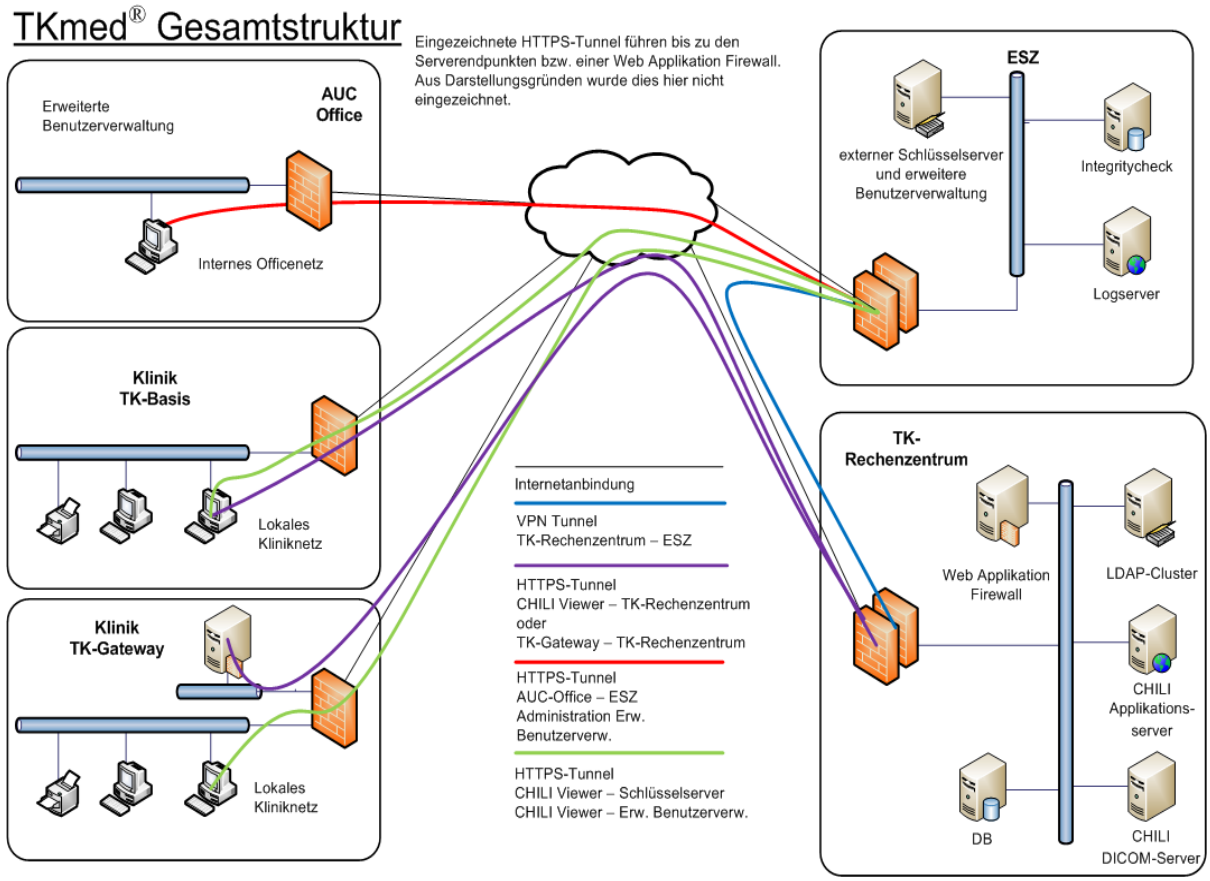

Abbildung 4: Übersicht der Gesamtstruktur

4.2 Aufbau der zentralen TK-Infrastruktur

Die zentrale TK-Infrastruktur besteht aus dem TK-Rechenzentrum sowie dem Externen Sicherheits-Zentrum (ESZ). Die Daten liegen im TK-Rechenzentrum nur in verschlüsselter Form vor (siehe Kapitel 5.8). Um bestmöglichen Datenschutz zu gewährleisten, wurde eine Trennung von verschlüsselten Daten und den Schlüsseln selbst realisiert. Die Schlüsselverwaltung wird in das ESZ (siehe Kapitel 4.2.2) ausgelagert und ist somit vom Betreiber des Rechenzentrums abgetrennt. Eine Ver- und Entschlüsselung von Daten ist nur auf der Teilnehmerseite (also nur bei Sender und Empfänger) möglich, da die TK-Komponenten nur dann die Schlüssel erhalten, wenn berechtigte Medizinische und Nicht-Medizinische Anwender angemeldet sind (siehe Kapitel 5.4.2, 5.4.8). Um auf Teilnehmerseite die Schlüssel zur Ver- bzw. Entschlüsselung abfragen zu können, muss eine Verbindung ausgehend von den TK-Komponenten in das ESZ bestehen. Zur Vereinfachung des IP-Routings ist das ESZ per VPN an das TK-Rechenzentrum

angeschlossen, d.h. auf Netzwerkebene werden die verschlüsselten Anfragen der TK-Komponenten über das TK-Rechenzentrum („Single Point of Entry") in das ESZ weitergeleitet.

Folgende zusätzliche Datenschutzmerkmale werden umgesetzt:

1. **Übertragung der Log-Information** in ein externes revisionssicheres System (im ESZ), um eine Manipulation des Logs zu unterbinden. Integrierte Agents gewährleisten eine Zwischenspeicherung der Log-Informationen der Anwendungen, falls die Verbindung zum zentralen Logserver unterbrochen ist. Ist die Verbindung wiederhergestellt, so werden die zwischenzeitlich angefallenen Log-Informationen nachträglich übermittelt. Die lokalen Logs bleiben zur besseren Administrierbarkeit auf den ursprünglichen Systemen erhalten.
2. **Übertragung des Ergebnisses des Integritätschecks** (Authentifizierung der Applikationen) aus dem TK-Rechenzentrum in das ESZ, um eine Manipulation der verwendeten Anwendungen zu erkennen.
3. **Auslagerung eines Teils der Benutzerverwaltung in das ESZ**, um eine Manipulation der Zugriffsrechte zu verhindern. Die Rolle Medizinischer Anwender (siehe Kapitel 5.4.3) kann nur durch einen ESZ-Institutions-Administrator verändert werden. Mit den Rechten eines TKmed®-Administrators besteht keine Möglichkeit die Rolle des Medizinischen Anwenders anzulegen.

4.2.1 TK-Rechenzentrum

Das TK-Rechenzentrum ist in zwei räumlich getrennten Rechenzentren der pegasus gmbh untergebracht und besteht aus folgenden Komponenten:

- CHILI DICOM-Server, u.a. zum Routing von Bild-/DICOM-Daten
- CHILI Applikationsserver zur Bereitstellung des CHILI Viewers
- CHILI DB-Server, Datenbankserver für den CHILI DICOM-Server und CHILI Applikations-server
- Datenbankserver für Auswertung und Logging, z.B. von Transportstatistiken und sicher-heitsrelevanten Logs (die Logs liegen zusätzlich im ESZ, siehe Kapitel 5.6)
- Portalserver für TKmed® (Benutzerverwaltung, Auswertung usw.)
- LDAP Cluster (Windows 2008 AD)
- Firewall Cluster
- Web Applikation Firewall
- VMware Servercluster
- Storagesystem
- Loginserver für Portal
- Token-Loginserver für Portal
- Tokenserver (Verwaltung der Hardware- und Softwaretoken (siehe Kap.5.1.1))

Die beiden Rechenzentren sind durch Zugangskontrollmechanismen und Videoüberwachung gegen unbefugten Zutritt abgesichert.

Für die Weiterentwicklung und Tests stehen separate TK-Infrastrukturen zur Verfügung, so dass die Produktivumgebung nicht beeinträchtigt werden kann.

Alle Server und Komponenten innerhalb des TK-Rechenzentrums sind zeitlich synchronisiert. Zum Einsatz kommt hierbei NTP[7] nach RFC[8] 958. Dieses Protokoll übernimmt die gesetzliche Uhrzeit in Deutschland der Physikalisch - Technischen Bundesanstalt (PTB) in Braunschweig. Über NTP wird dann das Zeitsignal an allen Servern und Systemen innerhalb der beiden Rechenzentren synchronisiert.

[7] NTP, Network Time Protokoll, Norm zur Synchronisierung von EDV-Systemen über das Internet
[8] RFC, Request for Comments, Internationale Empfehlungen für Datenprotokolle usw. zum Betrieb des Internets.

4.2.2 Externes Sicherheitszentrum (ESZ)

Das ESZ wird von Beauftragten der AUC administriert und überwacht. Die Administratoren des Infrastruktur-Betreibers haben keinen direkten Zugriff auf die Systeme und die dort gelagerten Daten. Durch und im Rahmen der Auslagerung des ESZ auf einen externen Dienstleister wird gewährleistet, dass weder AUC noch CHILI oder pegasus Zugriff auf Schlüssel nehmen oder deren Herausgabe verlangen können. Dadurch wird ausgeschlossen, dass die in Abschnitt 2.3 genannten Beteiligten oder andere Dritte sich Einblick in die übermittelten medizinische Daten beschaffen können.

Das System ist wie folgt aufgebaut:

- Alle notwendigen Dienste werden innerhalb zweier VMware ESXi-Server betrieben.
- Auf dem Server VMware-ESX-1 werden folgende Instanzen betrieben:
  - Logserver: Windows Server 2008 mit der zentralen Logging Software (siehe Kapitel 5.6).
  - Key-Server-1: SLES 11 mit der erweiterten Benutzerverwaltung und der Schlüsselverwaltung (siehe Kapitel 5.4.8).
- Auf dem Server VMware-ESX-2 werden folgende Instanzen betrieben:
  - Integritätscheck-Server Windows Server 2008 mit der Integritätscheck Anwendung (siehe Kapitel 5.7).
  - Key-Server-2: SLES 11 Backupsystem mit der erweiterten Benutzerverwaltung und der Schlüsselverwaltung (siehe Kapitel 5.4.8).
- Zusätzlich wird vor den beiden VMware Servern eine Firewall inkl. VPN betrieben. Diese stellt sicher, dass auf das System nur von berechtigten IP-Adressen aus zugegriffen werden kann.

Um die Verfügbarkeit der KEY-Server sicherzustellen, wird folgendes Verfahren verwendet:

4. Die Datenbank auf dem Key-Server-1 wird fortlaufend zum Key-Server-2 repliziert.
5. Die TK-Komponenten versuchen (Nr. 5 im Ablaufplan Kapitel 5.2) zuerst den Key-Server-1 zur erreichen.
6. Steht der Key-Server-1 nicht zur Verfügung, so versucht die TK-Komponente den Key-Server-2 zu erreichen.
   1. Solange der Key-Server-1 nicht zur Verfügung steht, wird das System in einen „Read-Only Mode" versetzt. Dies bedeutet, dass sich zwar weiterhin Benutzer am System anmelden können aber in dieser Zeit keine Änderungen an der ESZ Datenbank gemacht werden können (Neuanlage von Benutzern, ändern des Flags „Medizinischer Anwender", usw.). Diese Maßnahme stellt sicher, dass bei Rückführung zum Key-Server-1 keine Datenbank Inkonsistenzen entstehen können.
   2. Steht der Key-Server-1 wieder zur Verfügung, so ist das System wieder komplett einsatzfähig und der „Read Only Mode" wird aufgehoben. Etwaige neue Logbucheinträge werden im Laufe der folgenden Nacht vom Key-Server-2 an den Key-Server-1 übertragen, um die Nachvollziehbarkeit der Anmeldevorgänge zu gewährleisten.

4.3 Teilnehmer-Strukturen und Ausbaustufen

4.3.1 Anbindung TK-Basis

Einzelne Clients erhalten mittels Web-Browser Zugriff auf die zentrale TK-Infrastruktur. Diese Option wird hauptsächlich kleinen Institutionen zur Verfügung gestellt und für die Anbindung von niedergelassenen Ärzten und Physiotherapeuten genutzt, um diesen Zugriff auf an sie adressierte Bilddaten zu geben. Der Zugriff erfolgt über eine SSL verschlüsselte Verbindung über das Internet. Hierfür wird auf der Seite des Apache Webservers auf Open SSL zurückgegriffen. An dem CHILI Viewer melden sich die Medizinischen Anwender mittels der weiter unten beschrieben Authentifizierung an (siehe Kapitel 5.1-5.1.2). Die Zugangs- und Berechtigungsdaten werden auf dem in Kapitel 5.2 erwähnten LDAP-Server gespeichert.

4.3.2 Anbindung TK-Router

Die Anbindung des TK-Routers erfolgt wahlweise innerhalb des Krankenhaus/Institutions-Netzwerkes oder innerhalb einer DMZ[9] hinter der institutionseigenen Firewall. Die Auswahl, ob ein TK-Router innerhalb des Krankenhaus/Institutions-Netzwerkes oder innerhalb einer DMZ betrieben wird obliegt der EDV-Administration der jeweiligen Institution und deren Sicherheitsrichtlinien. Der TK-Router ist eine Java-Applikation, welche auf einem von der Institution bereitgestellten Windows System (Windows XP – Windows 2008 Server) betrieben wird.

Die Datenübertragung vom TK-Router innerhalb der Institution zur zentralen TK-Infrastruktur erfolgt mittels SSL verschlüsselten HTTPS Verbindungen über die Internetanbindung der jeweiligen Institution.

Der TK-Router beinhaltet die Funktionalität von TK-Basis und zusätzlich die Möglichkeit des automatischen Versands der Bilddaten zum zentralen Server sowie des automatischen Empfangs der Daten mit Weiterleitung der Daten in die eigene PACS-Umgebung der Institution. Der CHILI Viewer (TK-Basis) steht den Medizinischen Anwendern ebenfalls zur Verfügung.

4.3.3 Anbindung TK-Gateway

Die Anbindung des TK-Gateways erfolgt wahlweise innerhalb des Krankenhaus/Institutions-Netzwerkes oder innerhalb einer DMZ hinter der institutionseigenen Firewall. Die Auswahl, ob ein Gateway innerhalb des Institutions-Netzwerkes oder innerhalb einer DMZ betrieben wird obliegt der EDV-Administration der jeweiligen Institution und deren Sicherheitsrichtlinien.

Die Datenübertragung vom Gateway innerhalb der Institution zur zentralen TK-Infrastruktur erfolgt mittels SSL verschlüsselten HTTPS Verbindungen über die Internetanbindung der Institution.

Das TK-Gateway ist eine Serveranwendung und benötigt lokale Hardware oder eine virtualisierte Umgebung.

Das TK-Gateway beinhaltet die Funktionalität von TK-Router und zusätzlich die Möglichkeit des automatischen Versands der Bilddaten zum zentralen Server und des automatischen Empfangs der Daten mit Weiterleitung der Daten in die eigene PACS-Umgebung der Institution. Die Verarbeitungsregeln können hier flexibel eingestellt werden. Darüber hinaus ist eine Anbindung weiterer Abteilungen oder die Nutzung als "Mini-PACS" möglich. Der CHILI Viewer (TK-Basis) steht den Benutzern ebenfalls zur Verfügung.

4.3.4 Anbindung TKmed® Direkt / TKmed® Direkt Professional

Beliebigen Personen (Patienten, behandelnde Ärzte, etc.) ist es möglich, Datenobjekte an Nutzer des TKmed® Netzwerks zu senden, sofern diese eine Freigabe für den Empfang durch TKmed® Direkt bzw. TKmed® Direkt Professional erteilt haben. Als Versandziele stehen nur diese durch die TKmed® Nutzer freigegebenen Ziele zur Verfügung. Der Versand erfolgt verschlüsselt mit einem Einmalschlüssel über den Webbrowser.

TKmed® Direkt beinhaltet einen zweistufigen Ansatz. Zunächst beantragt eine beliebige Person für ein bestimmtes Versandziel einen Link für den Upload, den er an seine angegebene E-Mail-Adresse geschickt bekommt. Mit diesem Link kann der Upload von Datenobjekten erfolgen.

TKmed® Direkt Professional basiert auf einer Einladung (personalisierte E-Mail) an eine ausgewählte Person, die einen Upload Link enthält. Dieser steht dann der jeweiligen Person für eine definierte Zahl von Uploads und einen definierten Zeitraum zur Verfügung.

5 Informationssicherheit und Datenschutz

Das Datenschutzkonzept TKmed® führt ein Konzept fort, das von den Firmen CHILI GmbH und pegasus gmbh erarbeitet wurde. Die umfangreichen Weiterentwicklungen des Datenschutzkonzeptes, zum Beispiel zur Zwei–Faktor-Authentifizierung und zur Treuhänder-Funktion für die Schlüssel mit dem ESZ,

[9] DMZ, Demilitarisierte Zone, Abgeschotteter Bereich an einer Firewall zur Trennung vom internen Netzwerk

wurden von dem Projektteam TKmed® der AUC, vor allem von deren Beratern Prof. Dr. Staemmler, PD Dr. Walz und PD Dr. Weisser, in Zusammenarbeit mit den Firmen bis zum vorliegenden Stand betrieben.

5.1 Authentifizierung

Die Authentifizierung der Benutzer wird grundsätzlich über Besitz und Wissen geregelt. Jeder Benutzer benötigt einen Benutzernamen (E-Mail-Adresse) und ein ihm bekanntes Passwort, welches vergeben oder durch den Benutzer festgelegt wurde. Für die Kennwörter gelten die Richtlinien wie unter Kapitel 5.4.1 aufgeführt. Es stehen zwei Möglichkeiten zur Authentifizierung bereit.

5.1.1 Authentifizierung per Token und Login

Die Authentifizierung des Benutzers erfolgt zusätzlich zum Passwort per OTP-Token[10] (One Time Password). Dieses muss der Benutzer zusätzlich zur Eingabe des Benutzernamens und Passworts in der Applikation eingeben.

Als Tokenserver kommt das Produkt LINOTP (http://lsexperts.de/linotp.html) der Firma LSE Leading Security Experts GmbH aus Weiterstadt zum Einsatz.

Als Token können wahlweise Hardware-Token des Herstellers SafeNet (Schlüsselanhänger, z.B.: www.safenet-inc.com/etoken-pass/) oder sogenannte Soft-Tokens, die einer Smartphone App für iPhone, Android usw. entsprechen (z.B. code.google.com/p/google-authenticator/) oder mobile TAN zur Verfügung gestellt werden. Die Auswahl des zu verwendenden Tokens ist dem Benutzer freigestellt.

Dieses Verfahren findet z. B. Anwendung bei kleinen Institutionen, welche über dynamische IP-Adressen an das Internet angebunden sind, bei niedergelassenen Ärzten und Physiotherapeuten oder bei Ärzten in der Rufbereitschaft.

5.1.2 Authentifizierung per IP-Adresse und Login

In Institutionen, die anhand einer statischen IP-Adresse einwandfrei zuzuordnen sind, kann das Loginverfahren per Benutzername/Passwort durchgeführt werden. Der Benutzer kann sich mit Benutzername und Passwort also nur über eine der zentralen TK-Infrastruktur bekannten IP-Adresse anmelden.

5.1.3 Instanzentrennung vor der Authentifizierung

Um die Sicherheit der zentralen TK-Infrastruktur und des Web-Browsers nicht zu gefährden, wird der Authentifizierungsprozess auf zwei vorgelagerten Servern durchgeführt.

Es steht jeweils ein eigener Loginserver für die Authentifizierung per Token und per IP-Adresse zur Verfügung.

Der entsprechende erste Server stellt nur die Login-Maske für die Authentifizierung zur Verfügung. Diese Login-Maske wird durch eine zusätzliche Web Application Firewall (WAF, siehe Kapitel 5.5) abgesichert.

Nach erfolgter Authentifizierung wird mittels eines Tickets der angemeldete Benutzer an den Portalserver weitergeleitet. Dieser stellt allgemeine Informationen und den Zugang für berechtigte Benutzer zur Benutzerverwaltung zur Verfügung.

Über einen Link auf dem Portalserver kann der Benutzer zum CHILI Applikationsserver mittels Ticket weitergereicht werden. Dort ist keine weitere Authentifizierung mehr erforderlich.

Dieses Verfahren stellt sicher, dass nicht angemeldete Benutzer nur Zugriff auf den Login-Server haben und Angriffsversuche auf Anwendungsebene (Portal und CHILI Applikations-Server, CHILI Viewer) nicht ermöglicht werden.

[10] OTP-Token, Software oder Hardware zum Erzeugen von Einmalkennwörtern, die nur für einen begrenzten Zeitraum gültig sind

5.2 Authentifizierungsschritte der TK-Komponenten

Die einzelnen Schritte für die Authentifizierung der TK-Komponenten sind in Abbildung 5 für den CHILI Viewer (TK-Basis) dargestellt, gelten aber ebenso für TK-Router und TK-Gateway.

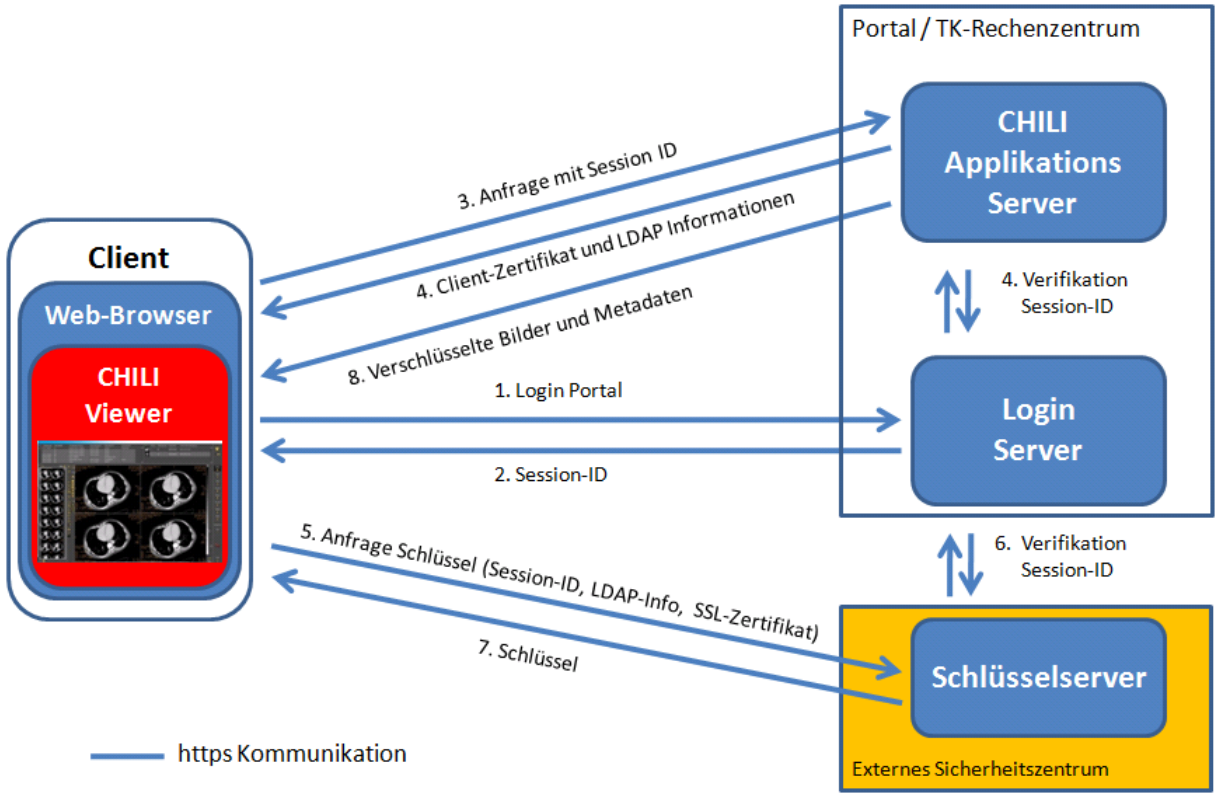

Abbildung 5: Authentifizierung CHILI Viewer

Die Schritte werden im Folgenden erläutert:

1. Die jeweilige TK-Komponente meldet sich zunächst am Loginserver an. TK-Router und TK-Gateway melden sich am Loginserver mit institutionsspezifischen Logindaten automatisch an der zentralen TK-Infrastruktur an. Die Logindaten sind auf dem TK-Router und TK-Gateway jeweils verschlüsselt abgelegt.
2. Nach erfolgter Anmeldung wird vom Loginserver eine Session-ID zur TK-Komponente übertragen. Die Session-ID wird aus verschlüsselten Benutzerinformationen und Timestamp generiert.
3. Diese Session-ID wird anschließend von der TK-Komponente an den CHILI Applikationsserver gesendet.
4. Der CHILI Applikationsserver verifiziert die Session-ID am Loginserver und liefert bei Erfolg Daten zum Benutzer (LDAP-Daten) und für jeden Schlüsselserver jeweils ein SSL Client-Zertifikat zurück an die TK-Komponente. Die Client-Zertifikate erhält der CHILI Applikationsserver seinerseits vom Loginserver, sofern die Session-ID gültig war.
5. Die TK-Komponente kann mit der Kombination aus Session-ID, LDAP-Benutzerdaten und Client-Zertifikat beim Schlüsselserver die Schlüssel anfragen.
6. Der Schlüsselserver prüft diese Informationen. Die Session-ID wird am Loginserver ausgewertet, um eine Zuordnung der Berechtigung im Schlüsselserver im Sinne eines SSO (Single Sign On) zu unterstützen.
7. War diese Prüfung erfolgreich, so werden die Schlüssel an die TK-Komponente ausgeliefert.
8. Anschließend kann die TK-Komponente die verschlüsselten Bild- und Metadaten, die sie vom CHILI Applikationsserver per Download erhält, entschlüsseln bzw. für den Upload verschlüsseln (siehe

Kapitel 5.8.2). Die Daten, die während der Authentifizierung zwischen der TK-Komponente und dem CHILI Applikationsserver bzw. Schlüsselserver übertragen werden, sind zusätzlich zur SSL-Verschlüsselung nochmals mit einem pre-shared Key (AES 128) verschlüsselt, der fest in die Anwendungen einkompiliert ist.

5.3 Authentifizierungsschritte für TKmed® Direkt / TKmed® Direkt Professional

Die Authentifizierungsschritte im Rahmen des Uploads von Datenobjekten mittels TKmed® Direkt bzw. TKmed® Direkt Professional sind in Abbildung 6 dargestellt.

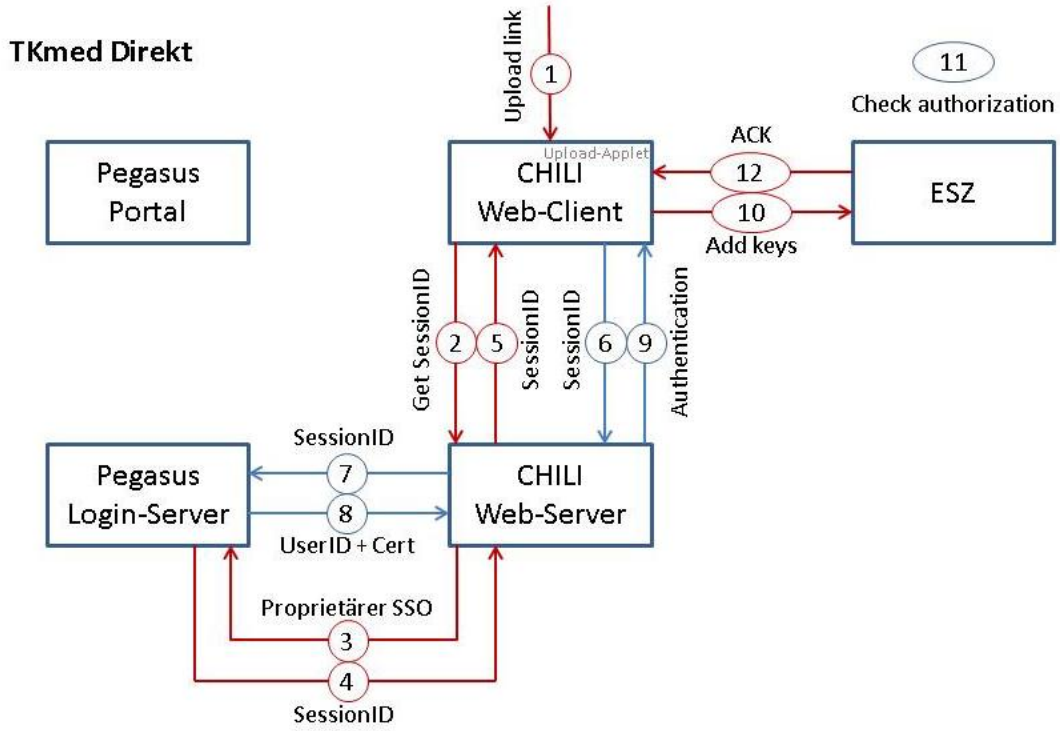

Abbildung 6: TKmed® Direkt Workflow

1. Der Person, die kein Nutzer von TKmed® ist, liegt, durch eine an sie gerichtete E-Mail oder eine persönliche Einladung, ein Link für den Upload vor. Mit diesem Link wird der CHILI Web-Client aufgerufen.

2-5. Über ein SSO-Verfahren wird mit Hilfe des CHILI Web-Servers eine gültige SessionID erstellt.

6-9. Mit Hilfe dieser SessionID wird ein festgelegter Standardnutzer für den Upload am Login-Server angemeldet. Dieser hat ausschließlich das Recht Datenobjekte an die TKmed® Infrastruktur zu versenden und Schlüssel im ESZ hinzuzufügen.

10-12. Datenobjekte werden vor dem Upload mit einem Einmalschlüssel verschlüsselt, welcher zusammen mit einer ID im ESZ abgelegt wird. Anschließend werden die verschlüsselten Bilddaten zusammen mit der ID über den CHILI Web-Server in die TKmed® Infrastruktur hochgeladen. Die ID dient bei dem Zugriff auf diese Datenobjekte durch den berechtigten TKmed® Nutzer zur Bereitstellung des zugehörigen Schlüssels durch das ESZ.

5.4 Benutzerverwaltung

Für das Portal und für das ESZ sind unterschiedliche Benutzer notwendig. Ihnen sind jeweils bestimmte Rollen zugeordnet. Allen Benutzern wird ein personalisierter Account zugeteilt. Folgende Arten von Benutzern existieren:

Benutzer: Allgemeine Bezeichnung für alle Anwender, welche das System benutzen.

- Portalbenutzer und
- ESZ-Benutzer

Portalbenutzer: Alle Anwender, die Dienste des TK-Rechenzentrums nutzen, z.B. das Portal oder den CHILI Viewer. Folgende Rollen existieren (siehe Kapitel 5.4.2), wobei einem Portalbenutzer mehrere Rollen zugeordnet sein können:

- TKmed®-Administrator,
- TNW-Administrator,
- AUC-TKmed®-Administrator,
- Institutions-Administrator,
- Medizinischer Anwender und
- Nicht-Medizinischer Anwender

ESZ-Benutzer: Alle Anwender, welche administrativen Zugriff zum ESZ haben. Folgende Rollen existieren (siehe Kapitel 5.4.2):

- ESZ-Administrator,
- ESZ-AUC-TKmed®-Administrator und
- ESZ-Institutions-Administrator

Die ESZ-Benutzer werden ausschließlich über eine separate Datenbank im ESZ verwaltet. Ebenso werden die Attribute „Medizinischer Anwender" und „Institutions-Administrator" nur im ESZ gepflegt. Im ESZ findet zudem, genau wie im LDAP des TK-Rechenzentrums (s.u.), eine Zuordnung von Portalbenutzern zu Institutionen statt. Diese Zuordnung stellt sicher, dass Mitarbeiter des Infrastruktur-Betreibers sich selbst keine Rollen geben können, die zum Zugriff auf Daten berechtigen (siehe Kapitel 5.4.8).

Die Portalbenutzer werden über einen im TK-Rechenzentrum betriebenen LDAP-Server verwaltet. Über Gruppenzugehörigkeiten können Portalbenutzer je einer Institution sowie einzelnen Abteilungen innerhalb der Institutionen zugeordnet werden. Durch das unter Kapitel 5.4.8 beschriebene Verfahren ist sichergestellt, dass die teilnehmenden Personen tatsächlich Medizinische Anwender sind und dass die TKmed®-Administratoren sich selbst nicht die Rolle eines Medizinischen Anwenders, eines Nicht-Medizinischen Anwenders oder eines Institutions-Administrators zuteilen können.

Beim Versenden eines Datensatzes muss der Medizinische Anwender aus der versendenden Institution die Ziel-Institution inkl. Abteilung (z.B. Uniklinik Regensburg / Unfallchirurgie) auswählen, die für die Weiterbehandlung zuständig ist. Beim Eintreffen der Daten in der Ziel-Institution wird allen Medizinischen Anwendern, welche Mitglied der adressierten Abteilung sind, eine Zugriffsmöglichkeit auf die Daten des Patienten gewährt. Ebenso ist eine direkte Adressierung an einen bestimmten Medizinischen Anwender möglich. Medizinische Anwender aus anderen Abteilungen der gleichen Institution haben keinen Zugriff.

Der LDAP-Server selbst ist ein Windows 2008 basiertes Active Directory. Administrative Zugangsdaten zu diesem Active Directory besitzen ausschließlich drei Administratoren der Infrastruktur-Betreiber, die durch den Auftragnehmer schriftlich festgelegt wurden. Diese Mitarbeiter wurden für die Bedienung des Systems technisch geschult. Darüber hinaus wurde für diese Mitarbeiter eine Unterweisung in den Bereichen Datenschutz und Awareness durch einen externen Datenschutzbeauftragten (RA Baron von Hohenhau, Fachanwalt für IT-Recht, Regensburg) durchgeführt. Verschwiegenheits- und Verpflichtungserklärungen dieser Personen liegen vor.

Die Verwaltung der Portalbenutzer- und ESZ-Benutzerverwaltung nutzt ein SSL-gesichertes Webinterface.

5.4.1 Kennwortrichtlinien

Folgende Kennwortrichtlinien gelten für alle Benutzer.

Kennwortlänge:	Mind. 8 Zeichen
Komplexität:	Mind. ein Großbuchstabe Mind. ein Kleinbuchstabe Mind. eine Zahl Sonderzeichen sind möglich

5.4.2 Funktionale Rollen

Innerhalb von TKmed® existieren sechs funktionale Rollen für das Portal, sowie drei funktionale Rollen für das ESZ, die im Folgenden beschrieben werden. Die Rechte der einzelnen Rollen sind in Tabelle 1 und Tabelle 2 gelistet und in Abbildung 7 im Überblick dargestellt:

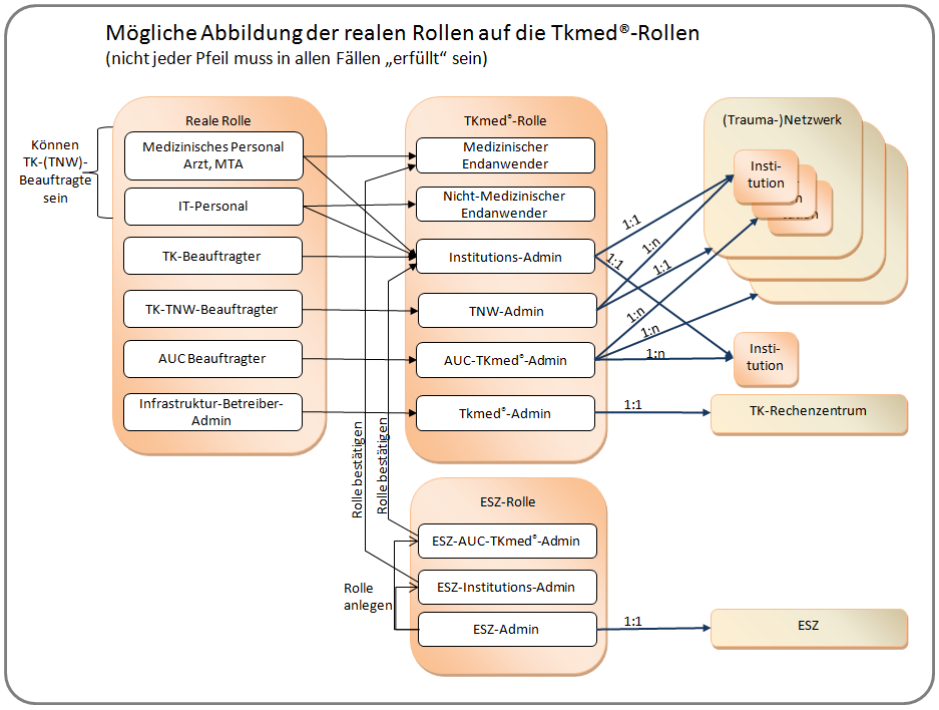

Abbildung 7: Rollenkonzept

Portalbenutzer:

TKmed®-Administrator:

Der TKmed®-Administrator hat das Recht zur Systemadministration im Portal und kann Rollen wie die des TNW-Administrators und Institutions-Administrators gemäß Tabelle 1 anlegen. Diese Rolle übernehmen ausschließlich die Administratoren des Infrastruktur-Betreibers. Diese Rolle beinhaltet damit auch die Administration des LDAP-Servers.

Die betroffenen Personen erhalten die Rolle nur nach schriftlicher Festlegung durch die Geschäftsführung des Auftragnehmers.

AUC-TKmed®-Administrator:

Der AUC-TKmed®-Administrator hat das Recht die Versand-Statistiken[11] aller Teilnehmer unabhängig von ihrer TNW-Zugehörigkeit bzw. auch von nicht TNW-Teilnehmern einzusehen. Darüber hinaus hat er eingeschränkten Zugriff auf die Portalbenutzer (siehe Tabelle 1). Diese Rolle erhalten ausschließlich Beauftragte der AUC. Daher darf sie auch nur von TKmed®-Administratoren auf Anweisung der AUC angelegt werden. Personen, welche die Rolle AUC-TKmed®-Administrator Rolle innehaben, können zusätzlich im ESZ durch den ESZ-Administrator die Rolle ESZ-AUC-TKmed®-Administrator erhalten. Dies ist nötig um Institutions-Administratoren im ESZ bestätigen zu können (siehe Kapitel 5.4.8). AUC-TKmed®-Administratoren werden datenschutzrechtlich unterwiesen und zur Geheimhaltung verpflichtet. Als Vorlage für die schriftlichen Erklärungen dienen die im Anhang angefügten entsprechenden Dokumente im Kapitel 6.

TNW-Administrator:

Der TNW-Administrator hat das Recht, die Versand-Statistiken[11] aller Teilnehmer des ihm zugeordneten TNW einzusehen. Darüber hinaus hat er eingeschränkten administrativen Zugriff auf die Portalbenutzer in seinem TNW (siehe Tabelle 1). Diese Rolle erhalten TK-TNW-Beauftragte eines TNW oder Beauftragte anderer Netze wie z.B. Schlaganfall-Netze, sofern der Teilnehmer zu einem solchen Netz und nicht zu einem TNW gehört. Diese Rolle kann ausschließlich von TKmed®-Administratoren auf Anweisung der AUC angelegt werden. Die Personen werden datenschutzrechtlich unterwiesen und zur Geheimhaltung verpflichtet. Als Vorlage für die schriftlichen Erklärungen dienen die im Anhang angefügten entsprechenden Dokumente im Kapitel 6.

Institutions-Administrator:

Institutions-Administratoren verwalten die Medizinischen Anwender in ihrer eigenen Institution. Diese Rolle kann ausschließlich von TKmed®-Administratoren auf Anweisung der Institution (Vertragspartner für die Teilnahme an TKmed®) angelegt werden. Zusätzlich muss der Institutions-Administrator im ESZ durch einen ESZ-AUC-TKmed®-Administrator bestätigt werden. Anschließend erhält die Person, welche die Rolle Institutions-Administrator wahrnimmt, auch die Rolle ESZ-Institutions-Administrator. Dies ist nötig, um Medizinische Anwender im ESZ bestätigen zu können (siehe Kapitel 5.4.8). Es dürfen nicht mehr als drei Institutions-Administratoren pro Institution angelegt werden.

Medizinischer Anwender:

Medizinisches Personal, das von Institutions-Administratoren angelegt wird. Benutzer, die diese Rolle innehaben, dürfen Daten betrachten, senden und empfangen, sofern sie im ESZ als Medizinischer Anwender bestätigt wurden (siehe 5.4.8) und im LDAP den entsprechenden Gruppen zugeordnet sind. Die Bestätigung als Medizinischer Anwender erfolgt im ESZ durch einen ESZ-Institutions-Administrator. Solange keine Bestätigung erfolgt, ist der Benutzer als Nicht-Medizinischer Anwender eingestuft.

Ein Medizinischer Anwender kann einer oder mehreren Abteilungen innerhalb seiner Institution zugeordnet sein. Für jede Abteilung kann ein Versandziel (entspricht einem im TKmed® eindeutigen AET für die Abteilung einer Institution) eingerichtet werden, das jedoch kein Login erlaubt.

Nicht-Medizinischer Anwender:

Personal, das von TKmed®-Administratoren oder von Institutions-Administratoren angelegt wird. Benutzer, die diese Rolle innehaben, dürfen Daten über eine sogenannte „Uploader-Anwendung", die eine stark limitierte Version des CHILI Viewers darstellt, hochladen und senden, aber keine Daten empfangen oder ansehen.

TKmed® Direkt Standardnutzer:

Diese Rolle enthält ausschließlich die Berechtigung Datenobjekte (Bilddaten und Dokumente) an dafür frei geschaltete TKmed® Nutzer zu versenden.

TKmed® Direkt Professional Anwender:

Entspricht einem Medizinischen Anwender, kann jedoch zusätzlich Zuweiser im Rahmen von TKmed® Direkt Professional einladen.

[11] Bei diesen Statistiken werden z.B. die Anzahl übertragener Bilder und die Versanddauer angezeigt, es sind keine Patientendaten einzusehen.

Tabelle 1: Darstellung der Rechte für die verschiedenen Rollen der Portalnutzer

	TKmed®-Admin	AUC-TKmed®-Admin	TNW-Admin	Institutions-Admin	Med. Anwender	Nicht-Med. Anwender	TKmed® Direkt Professional Anwender
Anlegen/Erstellen von:							
Nicht-Medizinischen Anwendern	Nein	Nein	Nein	Ja	Nein	Nein	Nein
Medizinischen Anwendern	Nein	Nein	Nein	Ja	Nein	Nein	Nein
Institutions-Administratoren	Ja	Nein	Ja	Nein	Nein	Nein	Nein
TNW-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AUC-TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TKmed® Direkt Professional Einladungen	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Löschen von:							
Nicht-Medizinischen Anwendern	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Medizinischen Anwendern	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Institutions-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TNW-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AUC-TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Ändern:							
Zuordnung der medizinischen Fachabteilung	Ja	Nein	Nein	Ja	Nein	Nein	Nein
eigenes Kennwort	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Sichtbarkeit von Anwendern/Abteilungen des eigenen Instituts im TKmed® Direkt Versandbaum	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Einladungs-Konfiguration TKmed® Direkt	Nein	Nein	Nein	Ja	Nein	Nein	Nein

Einladungs-Verwaltung TKmed® Direkt	Nein	Nein	Nein	Ja	Nein	Nein	Nein

Rücksetzen des Kennwortes von:							
Nicht-Medizinischen Anwendern	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Medizinischen Anwendern	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Institutions-Administratoren	Ja	Nein	Ja	Nein	Nein	Nein	Nein
TNW-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Sperren/Entsperren des Kontos von:							
Nicht-Medizinischen Anwenden	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Medizinischen Anwendern	Ja	Nein	Nein	Ja	Nein	Nein	Nein
Institutions-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TNW-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein
TKmed®-Administratoren	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Medizinische Bilddaten / Dokumente:							
Betrachten	Nein	Nein	Nein	Nein	Ja	Nein	Ja
Versenden	Nein	Nein	Nein	Nein	Ja	Ja	Ja
Löschen	Nein	Nein	Nein	Nein	Ja	Nein	Ja
Import per CD-ROM	Nein	Nein	Nein	Nein	Ja	Ja	Ja

Ansicht Versand-Statistik für:							
Nicht-Medizinischen Anwendern selbst	Ja	Ja	Ja	Ja	Nein	Nein	Nein
Medizinischen Anwender selbst	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Institution	Ja	Ja	Ja	Ja	Nein	Nein	Nein
TNW	Ja	Ja	Ja	Nein	Nein	Nein	Nein
TKmed® gesamt	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ansicht Benutzerliste:							
Institution	Ja	Ja	Ja	Ja	Nein	Nein	Nein
TNW	Ja	Ja	Ja	Nein	Nein	Nein	Nein
TKmed® gesamt	Ja	Ja	Nein	Nein	Nein	Nein	Nein

ESZ-Benutzer:

ESZ-Administrator:

Der ESZ-Administrator kann weitere ESZ-Benutzer anlegen und Schlüssel ändern. Die Rolle ESZ-Administrator übernehmen ausschließlich Beauftragte der AUC. Die betroffenen Personen erhalten die Rolle nur nach schriftlicher Festlegung durch die AUC. Die Personen werden datenschutzrechtlich unterwiesen und zu Geheimhaltung (insbesondere im Bereich der Schlüsselverwaltung) verpflichtet. Als Vorlage für die schriftlichen Erklärungen dienen die im Anhang angefügten entsprechenden Dokumente im Kapitel 6.

ESZ-AUC-TKmed®-Administrator:

Der ESZ-AUC-TKmed®-Administrator hat das Recht für einen Portalbenutzer die Rolle Institutions-Administrator zu bestätigen oder wieder zu entziehen. Die Rolle ESZ-AUC-TKmed®-Administrator wird ausschließlich durch Beauftragte der AUC wahrgenommen, und setzt die Rolle AUC-TKmed®-Administrator voraus.

ESZ-Institutions-Administrator:

Der ESZ-Institutions-Administrator hat das Recht für einen Portalbenutzer die Rolle Medizinischer Anwender zu bestätigen oder wieder zu entziehen. Die Rolle ESZ-Institutions-Administrator setzt die Rolle Institutions-Administrator voraus.

Tabelle 2: Darstellung der Rechte für die administrativen Rollen im ESZ

	ESZ-Admin	ESZ-AUC-TKmed®-Admin	ESZ-Institut.-Admin
Anlegen von:			
ESZ-Administratoren im „Vier Augen Prinzip"	Ja	Nein	Nein
ESZ-AUC-TKmed®-Administrator	Ja	Nein	Nein
ESZ-Institutions-Administrator	Ja	Nein	Nein
Ändern:			
Des eigenen Kennwortes	Ja	Ja	Ja
Der Schlüssel im ESZ im „Vier Augen Prinzip"	Ja	Nein	Nein
Bestätigen/Entziehen der Rolle Institutions-Administrator	Nein	Ja	Nein
Bestätigen/Entziehen der Rolle Medizinischer Anwender	Nein	Nein	Ja
Rücksetzen des Kennwortes von:			
ESZ-Administratoren	Ja	Nein	Nein
AUC TKmed®-Administratoren	Ja	Nein	Nein
Institutions-Administratoren	Ja	Nein	Nein

5.4.3 Portalbenutzerverwaltung: Medizinische Anwender anlegen

Das Anlegen der Portalbenutzer erfolgt über die administrativen Funktionen des Portals. Zur Anlage eines Portalbenutzers werden folgende Daten erhoben:

- Name, Vorname
- Titel
- E-Mail-Adresse
- Alternativer Anmeldename

- Geburtsdatum
- Mobilfunknummer (für Benachrichtigungen)
- Krankenhaus oder Praxis
- Zugehörigkeit zu einer oder mehreren medizinischen Fachabteilungen

Die Vergabe des Kennwortes erfolgt wie unter Kapitel 5.4.4 beschrieben.

Die Bestätigung eines Medizinischen Anwenders im ESZ erfolgt wie unter Kapitel 5.4.8 beschrieben.

5.4.4 Portalbenutzerverwaltung: Kennwort-Rücksetzung

In den administrativen Funktionen des Portals haben die Portalbenutzer die Möglichkeit, ihr eigenes Kennwort durch folgenden Ablauf zurück zu setzen.

1. Der Portalbenutzer aktiviert die Schaltfläche „Kennwort zurücksetzen".
2. Das System bittet um die Eingabe der E-Mail-Adresse.
3. Gehört die E-Mail-Adresse zu einem bekannten Portalbenutzer, so wird an diese E-Mail-Adresse ein Aktivierungslink gesendet. Ungültige E-Mail-Adressen führen zu einer Fehlermeldung.
4. Der Portalbenutzer betätigt den Aktivierungslink in der ihm zugesandten E-Mail.
5. Daraufhin erhält der Portalbenutzer eine SMS mit einem Code zur Eingabe in dem TKmed® Webinterface zur endgültigen Bestätigung.
6. Das System fordert den Portalbenutzer auf, ein neues Kennwort zu vergeben.
7. Das Login kann erfolgreich durchgeführt werden.

TKmed®-Administratoren haben die Möglichkeit, den Rücksetzvorgang für beliebige Portalbenutzer zu starten (Ziffer 1-3). Institutions-Administratoren haben nur das Recht, den Vorgang für Portalbenutzer der eigenen Institution zu starten (Ziffer 1-3). Die Verifizierung (Ziffer 4-7) muss durch den Portalbenutzer selbst erfolgen. So ist sichergestellt, dass kein Administrator die Kennwörter anderer Portalbenutzer im System kennt.

5.4.5 Portalbenutzerverwaltung: Verlust eines Tokens

Bei Verlust eines Tokens hat der Portalbenutzer dies den TKmed®-Administratoren unverzüglich zu melden. Diese sperren das Token mit sofortiger Wirkung in der Portalbenutzerverwaltung und weisen dem Portalbenutzer ein neues Token zu.

5.4.6 Portalbenutzerverwaltung: Protokollierung

Alle in den administrativen Funktionen des Portals getätigten Aktionen werden protokolliert (siehe Kapitel 5.6).

Somit ist sichergestellt, dass jede Aktion innerhalb der Benutzerverwaltung nachvollziehbar ist (Client-IP, Benutzername, Aktion, Datum/Uhrzeit).

Innerhalb des Windows Active Directory werden ebenfalls alle Aktionen in der Benutzerverwaltung protokolliert, um ein direktes Eingreifen in den LDAP-Server mit Active Directory Verwaltungstools außerhalb der administrativen Funktionen des Portals zu dokumentieren.

Zugriff auf die Logs haben ausschließlich TKmed®-Administratoren; auf Nachfrage werden die Logs auch Beauftragten der AUC bereitgestellt.

5.4.7 Portalbenutzerzugriffe: Protokollierung

Um die Umsetzung der Datenschutzrichtlinien kontrollieren zu können, werden alle Zugriffe auf Daten innerhalb des Portals und des CHILI Viewers protokolliert. Dabei werden folgende Attribute erfasst:

- Benutzername
- IP-Adresse der Zugriffsstation
- verschlüsselte Patientendaten (Datenbank-ID)
- Anzahl und Größe der versendeten Daten
- versendende Institution
- empfangende Institution
- Übertragungszeit für einen Versand
- Zeitpunkt des Zugriffs auf Bilddaten sowie die Zeit bis zur Anzeige im CHILI Viewer (Bildladezeit)

Der Zugriff auf die Protokolle ist TKmed®-Administratoren vorbehalten. Auf Nachfrage oder im Rahmen statistischer Auswertungen erhalten Beauftragte der AUC die Protokolldaten oder Auszüge daraus. Institutions-Administratoren haben Zugriff auf die ihrer Institution zugeordneten Protokolle. Medizinische Anwender können im CHILI Viewer über eine Statusübersicht einsehen, welche ihrer Daten versendet wurden. Eine Einsicht in die von der eigenen Abteilung versendeten Daten soll möglich sein, jedoch ohne Angabe des Versenders.

5.4.8 Erweiterte Benutzerverwaltung im ESZ

Im ausgelagerten ESZ wird die erweiterte Benutzerverwaltung betrieben. Diese beinhaltet folgende Funktionen:

Wird in der Portalbenutzerverwaltung ein neuer Portalbenutzer angelegt oder dessen Rechte bzw. Rollen verändert, so wird per Scriptaufruf eine Information an die ESZ-Benutzerverwaltung gesendet. Diese beinhaltet folgende Attribute:

- Institutions- bzw. Teilnehmernummer
- Name der Institution
- Benutzer-ID
- Titel
- Vorname Benutzer
- Nachname Benutzer
- LDAP Benutzer-DN
- Benutzerstatus „aktiv / inaktiv"
- Medizinischer Anwender „Ja / Nein".
- Institutions-Administrator „Ja / Nein"

Durch das Script wird der Portalbenutzer in der internen Datenbank des ESZ angelegt.

Um zu verhindern, dass TKmed®-Administratoren sich selbst die Rollen Medizinischer Anwender, Nicht-Medizinischer Anwender oder Institutions-Administrator zuweisen können, gelten die Berechtigungen wie in Tabelle 1 und Tabelle 2 beschrieben. Daraus ergibt sich folgende Vorgehensweise:

1. Anlage Institutions-Administrator:
   1.1. Der TKmed®-Administrator legt den Institutions-Administrator im Portal an.
   1.2. Per Script werden die oben genannten Attribute an das ESZ übertragen und die Rolle Institutions-Administrator angefordert.
   1.3. Der ESZ-AUC-TKmed®-Administrator bestätigt die Rolle Institutions-Administrator.
   1.4. Der neue Institutions-Administrator erhält eine E-Mail zur Bestätigung. Diese E-Mail enthält einen Link in das Portal.
   1.5. Er führt den Link aus und vergibt dabei sein Kennwort und akzeptiert die dort aufgeführte Verschwiegenheitserklärung. Danach wird die Rolle per Script freigeschaltet.

2. Anlage Medizinischer Anwender
   2.1. Der Institutions-Administrator legt den Medizinischen Anwender im Portal an.
   2.2. Per Script werden die oben genannten Attribute an das ESZ übertragen und die Rolle Medizinischer Anwender angefordert.
   2.3. Der ESZ-Institutions-Administrator (gleiche Person wie der Institutions-Administrator) bestätigt die Rolle Medizinischer Anwender. Die Bereitstellung der Schlüssel im ESZ wird durch diese Freigabe gesteuert.
   2.4. Der neue Medizinische Anwender erhält eine E-Mail zur Bestätigung. Diese E-Mail enthält einen Link in das Portal.
   2.5. Er führt den Link aus und vergibt dabei sein Kennwort und akzeptiert die dort aufgeführte Verschwiegenheitserklärung. Danach wird die Rolle per Script freigeschaltet.
3. Anlage Nicht-Medizinischer Anwender
   3.1. Der Institutions-Administrator legt den Nicht-Medizinischen Anwender im Portal an.
   3.2. Per Script werden die oben genannten Attribute an das ESZ übertragen und die Rolle Nicht-Medizinischer Anwender angefordert.
   3.3. Der neue Nicht-Medizinische Anwender erhält eine E-Mail zur Bestätigung. Diese E-Mail enthält einen Link in das Portal.
   3.4. Er führt den Link aus und vergibt dabei sein Kennwort und akzeptiert die dort aufgeführte Verschwiegenheitserklärung. Danach wird die Rolle per Script freigeschaltet.

Für jede der Rollen Medizinischer Anwender, Nicht-Medizinischer Anwender, Institutions-Administrator wird abgespeichert, welcher Institution diese zugeordnet sind. Dies wird entsprechend beim Zugriff auf Daten geprüft. Institutions-Administratoren können nur für Ihre Institution Anwender anlegen.

Werden für die Rollen Institutions-Administrator und Medizinischer Anwender die Institutionsnummer oder der Institutionsname geändert, so muss eine erneute Bestätigung im ESZ erfolgen.

5.4.9 Nutzerverwaltung im Rahmen von TKmed® Direkt und TKmed® Direkt Professional

Für TKmed® Direkt und TKmed® Direkt Professional gibt es keine Benutzer. Für den Upload gibt es ein SSO Verfahren mit Zertifikaten zum Abgleich zwischen Portal und TKmed® Direkt.

Der TKmed® Upload Benutzer hat ausschließlich das Recht Datenobjekte und Schlüssel in die zentrale Infrastruktur hochzuladen. Er kann sich nicht einloggen, um Bilder oder Schlüssel abzurufen.

5.5 Web Application Firewall (WAF)

Zusätzlich zu den genannten Maßnahmen dient eine WAF zum Schutz der Webserver nach außen. Hier kommt eine Softwarelösung, welche auf einen Apache-Webserver mit „mod_security" und „mod_proxy", aufbaut, zum Einsatz.

5.6 Zentrale Logbuchfunktion

Die Server der zentralen TK-Infrastruktur generieren verschieden Logs, die auf den Servern selbst abgelegt werden.

Tabelle 3: Liste der Server-Logs

	Server	Ursprung des Logs	Art des Logs
1	Zentraler LDAP-Cluster	Betriebssystem	MS Eventdatenbank
2	Zentraler LDAP-Cluster	LDAP-Server	MS Eventdatenbank

3	Loginserver	Betriebssystem	Lokale Datei via Syslog
4	Loginserver	Applikationen (Apache, PHP usw.)	Lokale Datei via Syslog
5	Loginserver	Applikationen (Loginportal)	SQL-Datenbank
6	Token-Loginserver	Betriebssystem	Lokale Datei via Syslog
7	Token-Loginserver	Applikationen (Apache, PHP usw.)	Lokale Datei via Syslog
8	Token-Loginserver	Applikationen (Loginportal)	SQL-Datenbank
9	Portalserver	Betriebssystem	Lokale Datei via Syslog
10	Portalserver	Applikationen (Apache, PHP usw.)	Lokale Datei via Syslog
11	Portalserver	Applikationen (Loginportal)	SQL-Datenbank
12	DB-Portalserver	Betriebssystem	Lokale Datei via Syslog
13	DB-Portalserver	Applikationen (Apache, PG usw.)	Lokale Datei via Syslog
14	Tokenserver	Betriebssystem	Lokale Datei via Syslog
15	Tokenserver	Applikationen (Apache, PHP usw.)	Lokale Datei via Syslog
16	Tokenserver	Applikationen (Loginportal)	SQL-Datenbank
17	CHILI Applikationsserver	Betriebssystem	Lokale Datei via Syslog
18	CHILI Applikationsserver	Applikationen (Apache, usw.)	Lokale Datei via Syslog
19	CHILI Applikationsserver	Applikationen (CHILI Komponenten)	SQL-Datenbank, lokale Dateien
20	CHILI DICOM-Server	Betriebssystem	Lokale Datei via Syslog
21	CHILI DICOM-Server	Applikationen (Apache, usw.)	Lokale Datei via Syslog
22	CHILI DICOM-Server	Applikationen (CHILI Komponenten)	SQL-Datenbank, lokale Dateien
23	CHILI DB-Server	Betriebssystem	Lokale Datei via Syslog
24	CHILI DB-Server	Applikationen (Apache, usw.)	Lokale Datei via Syslog
25	CHILI DB-Server	Applikationen (CHILI Komponenten)	SQL-Datenbank, lokale Dateien

Die aufgeführten Logs werden mit einer speziellen Software (http://www.tripwire.com/_log-center/) außerhalb des TK-Rechenzentrums im ESZ revisionssicher gespeichert (siehe Kapitel 4.2).

Der Transfer der Logs erfolgt über einen am jeweiligen Server installierten Agent. Dieser sammelt das Log am Server ein und überträgt es verschlüsselt an den Tripwire Server im ESZ.

Bei nicht Erreichbarkeit des Tripewire Servers im ESZ werden die gesammelten Logs zwischengespeichert und nach Wiederherstellung nachträglich übertragen.

5.7 Integritätscheck der Applikationen

Alle relevanten Dateien (Betriebssystem und alle in diesem Dokument beschriebenen Anwendungen) auf den Servern der zentralen TK-Infrastruktur werden durch einen Integritätscheck abgesichert. Dieser Prozess erstellt für jede Datei einen Hash über Dateiinhalt, Dateigröße, Dateiänderungsdatum usw. (http://www.tripwire.com/file-integrity-monitoring/). Die Hashwerte werden im ESZ abgelegt. Jegliche Dateiänderung wird durch einen Agenten erfasst und führt zur Neuberechnung des Hashwerts. Durch Vergleich der Hashwerte können Veränderungen festgestellt werden, die einen Alarm auslösen und die TKmed®- Administratoren informieren. Bei geplanten Dateiänderungen (Softwareupdates, Konfigurationsänderungen usw.) wird dieser Vorgang ebenfalls durchgeführt und vom Administrator innerhalb der Überwachungssoftware bestätigt.

5.8 Verschlüsselung

Innerhalb der zentralen TK-Infrastruktur liegen alle Daten ausschließlich verschlüsselt vor (nicht pseudonymisiert). Die Funktionsweise der Verschlüsselung in Verbindung mit dem ESZ ist im Folgenden dargestellt.

5.8.1 Schlüsselverwaltung im ESZ

Alle in diesem Kapitel beschriebenen Schlüssel sind im ESZ abgelegt. Die Verwaltung obliegt alleine den ESZ-Administratoren. Über einen gesicherten Zugang zu einem Webinterface können diese Schlüssel angepasst werden. Änderungen der Schlüssel werden mit einer Historienfunktion protokolliert, so dass bei Bedarf auch noch auf die vorherigen Schlüssel zugegriffen werden kann. Eine Änderung der Schlüssel ist nur im „Vier Augen Prinzip" möglich. Die Eingabe der neuen Schlüssel ist zweigeteilt. Die erste Hälfte

eines neuen Schlüssels ist von einem ESZ-Administrator einzugeben. Danach muss die zweite Hälfte des Schlüssels durch einen zweiten ESZ-Administrator eingegeben werden. Erst danach ist der neue Schlüssel vollständig und gültig.

Es sind zwei symmetrische Schlüssel vorgesehen:

- SymKeyData (AES 128) für Medizinische Daten, z.B DICOM- Objekte/Dateien (inkl. der Header/Metadaten), Befunde usw., die direkt im Dateisystem gespeichert werden.
- SymKeyDB (AES 128) für Datenbankmetainformation, d.h. extrahierte Header/Metadaten aus den DICOM-Objekten/Daten.

Beide Schlüssel haben immer einen gemeinsamen Gültigkeitszeitraum, so dass mehrere Schlüssel gleichzeitig auf dem Schlüsselserver existieren können.

5.8.2 Konzept Datenverschlüsselung Patientendaten

Upload von Daten

- Die TK-Komponente extrahiert aus den hochzuladenden Daten für das Datenmanagement notwendige Informationen (Patientenname, Studiendatum, usw.), im folgenden Metadaten genannt.
- Aus dem Bild wird ein Vorschau-Icon (Thumbnail) berechnet.
- Mit Hilfe von SymKeyData werden die Bild- und Behandlungsdaten und die Vorschau-Icons komplett symmetrisch verschlüsselt.
- Personenbezogene Daten innerhalb der Metadaten werden mit dem SymKeyDB verschlüsselt (siehe Kapitel 5.8.3).
- Verschlüsselte Bild- und Behandlungsdaten, Vorschau-Icons und Metadaten werden über gesicherte Leitungen zur zentralen TK-Infrastruktur übertragen.
- Empfangene Daten werden dort gespeichert.
- Die Metadaten werden verwendet, um die Daten in der Datenbank zu organisieren. Verschlüsselte Daten bleiben verschlüsselt.
- Die Aufbewahrungsfristen sind in Kapitel 5.9.3 beschrieben.

Betrachten von Daten

- Nach erfolgreicher Anmeldung (siehe Kapitel 5.2) erfolgt der Zugriff auf die Datenbank.
- Hierbei stehen alle unverschlüsselten Metadaten zur Suche zur Verfügung. Verschlüsselte Metadaten müssen erst zum Client übertragen werden, wo sie mit dem SymKeyDB entschlüsselt und angezeigt werden.
- Die verschlüsselten Daten werden zum Client übertragen und dort mit dem SymKeyData entschlüsselt und angezeigt.
- Für die unverschlüsselten Daten greifen die Berechtigungen.

5.8.3 Verschlüsselung der extrahierten Metadaten aus DICOM-Objekten/Dateien

Für die Verwaltung der Daten auf dem CHILI Applikationsserver werden die folgenden Datenbankfelder benötigt. Mit einem „X" in der Spalte „verschlüsselt" gekennzeichnete Felder werden mit SymKeyDB verschlüsselt, gesichert übertragen und in der Datenbank verschlüsselt gespeichert.

Prinzipiell kann frei ausgewählt werden, welche Datenbankfelder verschlüsselt werden. Die aufgeführte Auswahl stellt den aktuellen Stand in der Abstimmung der am Datenschutzkonzept beteiligten Gruppen dar. Eine spätere Verschlüsselung einzelner Felder ist nachträglich möglich. Eine Zurücknahme der Verschlüsselung einzelner Felder jedoch nicht. Die Änderung der Schlüssel ist möglich (siehe Kapitel 5.8.1).

Aus Datenschutzgründen sollen nur die Felder unverschlüsselt bleiben, die für das Datenmanagement benötigt werden, aus Performance- und Handhabungsgründen soll die Anzahl der verschlüsselten Felder

beschränkt werden. Aus dieser Abwägung ergibt sich folgendes für die Verschlüsselung einzelner Felder mit SymKeyDB:

Patientenbezogene Felder:

Feldname	Bedeutung	verschlüsselt
name	Name/Vorname	X
id	Patienten-ID	X
birthdate	Geburtsdatum	X
birthtime	Geburtszeit	X
sex	Geschlecht	X

Studienbezogene Felder:

Feldname	Bedeutung	verschlüsselt
instanceuid	DICOM Studien Instance-UID	
id	Studien-ID	X
studydate	Aufnahmedatum der Studie	
studytime	Aufnahmezeit der Studie	
modality	Modalität	
manufacturer	Hersteller der Modalität	
referingphysician	Anfordernder Arzt	X
description	Studienbeschreibung	
manufacturersmodelname	Typ/Modell der Modalität	
importtime	Zeitpunkt des ersten Imports	
chilisenderid	CHILI-interne ID, wird nicht gefüllt	
accessionnumber	Accessionnummer, i.a. vom RIS generiert	
institutionname	Institution, in der die Bilder erstellt wurden	X
performingphysician	Für Untersuchung verantwortlicher Arzt	X
reportingphysician	Arzt, der die Bilder befundet hat	X

Serien-bezogene Datenfelder:

Feldname	Bedeutung	verschlüsselt
instanceuid	DICOM Serien Instance-UID	
number	Seriennummer innerhalb der Studie	
acquisition	Nummer des Aufnahmevorgangs der Modalität	
echonumber	Verwendete Echonummer	
temporalposition	Zeitliche Reihenfolge	
seriesdate	Aufnahmedatum der Serie	
seriestime	Aufnahmezeit der Serie	
description	Serienbeschreibung	
contrast	Kontrastmittel	
bodypartexamined	Aufgenommenes Körperteil	X
scanningsequence	Typ der aufgenommenen Daten	
frameofreferenceuid	UID des verwendeten Koordinatensystems	

Bild-bezogene Datenfelder:

Feldname	Bedeutung	verschlüsselt
instanceuid	DICOM-Bild Instance-UID	
imagetype	Typ des Bildes (Localizer, …)	
number	Bildnnummer innerhalb der Serie	
imagedate	Aufnahmedatum des Bildes	

imagetime	Zeitpunkt der Bilderstellung	
slicelocation	Schichtposition	
rows	Höhe des Bildes in Bildpunkten	
columns	Breite des Bildes in Bildpunkten	
bitsallocated	Anzahl Bits, die für die Werte eines Bildpunkts belegt werden	
window_center	Mittelpunkt des Grauwertfensters	
window_width	Breite des Grauwertfenster	

Anmerkung zur Begründung für die Auswahl der Felder:

- „studydate", „studytime", „importtime" werden unterschiedlich interpretiert und gefüllt, studydate und studytime sind für alle darunter liegenden Serien identisch und dienen als Zuordnungsmerkmal.
- Nicht gelistete DICOM-Header/Metadaten werden auch nicht in der Datenbank gespeichert und sind somit durch die Verschlüsselung der DICOM-Dateien mittels SymKeyData geschützt (siehe 5.8.4).

5.8.4 Verschlüsselung der DICOM-Bilddaten

Die im DICOM-Objekt enthaltenen Bilddaten, inklusive der enthaltenen Metadaten, werden mit dem SymKeyData vor einem Versand verschlüsselt. Sie liegen in der zentralen TK-Infrastruktur ausschließlich verschlüsselt vor.

5.8.5 Verschlüsselung der Vorschau-Icons (Thumbnails)

Der Viewer zeigt zur besseren Orientierung in den Bild-Serien zu den jeweiligen Bildern sogenannte Vorschau-Icons an. Dies sind verkleinerte Darstellungen des eigentlichen Bildes. Diese werden, wie die Bilddaten, mit dem SymKeyData verschlüsselt. Sie liegen in der zentralen TK-Infrastruktur ausschließlich verschlüsselt vor.

5.8.6 Kompromittierung und notwendige Umschlüsselung

Da bei TKmed® Daten nur kurzfristig gespeichert werden (siehe Kapitel 5.9.3), werden bei einer Kompromittierung des SymKeyDB oder des SymKeyData alle mit diesen Schlüsseln verschlüsselten Daten gelöscht. Es werden neue Schlüssel generiert und eingesetzt. Weiterhin benötigte Daten müssen erneut versendet werden.

5.8.7 Konzept Datenverschlüsselung auf physikalischer Ebene

Innerhalb der zentralen TK-Infrastruktur wird keine Verschlüsselung auf physikalischer Ebene (Festplattenverschlüsselung etc.) angewendet, da die Daten seitens der Anwendungen bereits verschlüsselt abgespeichert werden. Das LDAP-Cluster nutzt seine eigene Verschlüsselung, z.B. für Passwörter.

Innerhalb der TK-Gateways in den Institutionen werden die Daten nicht verschlüsselt, da sie sich auf gesichertem hoheitlichem Gebiet der Institutionen (z.B. der Krankenhäuser) befinden und somit allen anderen institutionsinternen Systemen gleichgestellt sind. TKmed®-Administratoren haben keinen Zugriff auf die TK-Gateways.

5.8.8 Verschlüsselung Kommunikation und Netzwerk

Alle Verbindungen zwischen den beteiligten Systemen über das Internet sind verschlüsselt. Die Teilbereiche sind im Folgenden dargestellt.

Verbindung TK-Komponenten zur zentralen TK-Infrastruktur:

Für die Verbindungen

- TK-Basis zum TK-Rechenzentrum
- TK-Router und TK-Gateway zum TK-Rechenzentrum
- TK-Basis zum ESZ
- TK-Router und TK-Gateway zum ESZ
- TKmed® Direkt und TKmed® Direkt Professional

gilt, dass die Kommunikation mittels HTTPS erfolgt, welche ein gesichertes Zertifikat aus einem Trustcenter verwendet. Der Aussteller des Zertifikates ist die Firma THAWTE, Südafrika (www.thawte.com).

Folgende Zertifikatseinstellungen werden dabei verwendet:

- Zertifikatslaufzeit: 3 Jahre
- Schlüssellänge: RSA 2048 bit
- Signaturalgorithmus: sha1RSA
- Signaturhashalgorithmus: sha1

Verbindung TK-Rechenzentrum zum ESZ:

Die Kommunikation erfolgt innerhalb eines VPN-Tunnels auf IPsec-Basis (gemäß RFC 4301) mit folgenden Parametern:

Phase 1:	Encryption:	AES 256
	Hash Methode:	sha1
	Diffie-Hellman Group:	2
	Timeout:	28800 sec.
Phase 2:	Encryption:	AES 256
	Hash Methode:	sha1
	Diffie-Hellman Group:	2
	Timeout:	3600 sec.
Identify:	Shared Passphrase:	mind. 12 Stellen
	Mode:	Mainmode

5.8.9 Verschlüsselung bei TKmed® Direkt / TKmed® Direkt Professional

Für TKmed® Direkt wird ein Einwegschlüsselverfahren verwendet.

Pro Upload wird ein neuer Schlüssel erzeugt mit welchem die Daten verschlüsselt werden. Die verschlüsselten Daten werden zusammen mit einer ID in das TKmed® Netzwerk hochgeladen. Der Schlüssel wird zusammen mit der ID im ESZ gespeichert.

Zum Entschlüsseln werden die passenden Schlüssel bei vorliegender Berechtigung anhand der ID aus dem ESZ geholt, um die Daten wieder zu entschlüsseln.

5.9 Weitere Datenschutzaspekte

5.9.1 Patienteneinwilligung

Im Teilnehmervertrag ist festgehalten, dass die Teilnehmer dafür Sorge tragen müssen, dass die Zustimmung der Patienten zum Daten-Transfer den gesetzlichen Bestimmungen (gemäß §4a BDSG) entspricht und regelhaft vorliegt.

Für TKmed® Direkt, das auch von Patienten zum Upload von Datenobjekten verwendet werden kann, ergibt sich die Einwilligung des Patienten durch den vorgenommenen Versand. Für TKmed® Direkt Professional hat der Versender, in der Regel ein behandelnder Arzt dafür zu sorgen, dass die Zustimmung des Patienten zum Versand den gesetzlichen Bestimmungen (gemäß §4a BDSG) entspricht und regelhaft vorliegt. Zusätzlich beinhaltet in TKmed® Direkt und TKmed® Direkt Professional einen Hinweis auf die datenschutzrechtliche Relevanz beim Versand.

5.9.2 Langzeitarchivierung

Eine Langzeitarchivierung ist nicht Gegenstand des TKmed®, es handelt sich vielmehr um eine zeitlich begrenzte Zwischenspeicherung (siehe Kapitel 5.9.3). Die medizinische Dokumentationspflicht obliegt den Teilnehmern gemäß Teilnehmervertrag.

5.9.3 Aufbewahrungsfrist der Daten in der zentralen TK-Infrastruktur

Innerhalb der zentralen TK-Infrastruktur werden die Daten nur für einen begrenzten Zeitraum vorgehalten. Bei den unter Kapitel 3 beschriebenen Szenarien werden die Daten nach einem Zeitraum von 14 Tagen automatisch und unwiederbringlich gelöscht.

Innerhalb der TK-Gateways können die Daten in den Institutionen für einen längeren Zeitraum gespeichert werden. Die Festlegung des Zeitraumes obliegt der Institution selbst.

5.9.4 Fernwartung

Fernwartungsarbeiten an den TK-Komponenten (z.B. via VPN-Verbindung zu einem Teilnehmer) werden nur von autorisierten Mitarbeitern der Infrastruktur-Betreiber durchgeführt. Diese Mitarbeiter sind auf das Datengeheimnis (§ 5 Bundesdatenschutzgesetz, siehe auch Kapitel 6.4) verpflichtet. Weitere Details können Anlage 6 „Fernwartung" des Teilnehmervertrages entnommen werden.

5.9.5 Allgemeine Datenschutzaspekte des Infrastruktur-Betreibers

Neben den oben speziell ausgeführten Punkten erfüllen die Infrastruktur-Betreiber auch die weiteren Datenschutzaspekte eines IT-Dienstleiters. Diese Verfahren werden durch den Datenschutzbeauftragten festgelegt und kontrolliert:

- Datenschutzmanagement/Regelung der Verantwortlichkeiten im Bereich Datenschutz
- Erstellung eines Datenschutzkonzeptes
- Prüfung rechtlicher Rahmenbedingungen bei der Verarbeitung personenbezogener Daten
- Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten
- Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
- Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten
- Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten
- Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten
- Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten
- Dokumentation der datenschutzrechtlichen Zulässigkeit
- Aufrechterhaltung des Datenschutzes im laufenden Betrieb
- Datenschutzaspekte bei der Protokollierung
- Datenschutzgerechte Löschung/Vernichtung

6 Anlagen

Die hier aufgeführten Erklärungen gelten für die Mitarbeiter der Infrastruktur Betreiber. In den Formulierungen wird exemplarisch die CHILI GmbH genannt.

6.1 Erklärung zum Umgang mit der EDV

Erklärung zum Umgang mit Anlagen der elektronischen Datenverarbeitung
Der Mitarbeiter erhält Zugang zu einem PC mit Internetanschluss. Die Benutzung des Internet-Zuganges unterliegt folgenden Bestimmungen:

1. Schutz der Datenverarbeitungsanlagen vor Viren

1.1 Jeder Rechner ist mit einem Virenschutzprogramm ausgestattet. Der Mitarbeiter muss fremde Programme und externe Datenträger wie z. B. Disketten, CD-ROMs, DVDs und andere Medien vor jeder Nutzung auf Rechnern der CHILI GmbH durch diese Schutzprogramme auf Viren und andere schädliche Programme überprüfen lassen. Nur durch den dauernden Einsatz aktueller Virenschutzprogramme kann ein ausreichendes Schutzniveau gegen Computer-Viren sichergestellt werden.

1.2 Ergeben sich Hinweise auf Viren muss der Mitarbeiter die EDV-Abteilung und seinen Vorgesetzten informieren und darf die betreffenden Programme in keinem Fall nutzen.

2. Nutzung von Internetdiensten

2.1 Untersagt ist der Umgang mit Daten pornographischen, politisch radikalen oder rechtswidrigen Inhalts. Die CHILI GmbH weist den Mitarbeiter ausdrücklich darauf hin, dass die Nutzung einiger dieser Inhalte bei Strafe verboten ist.

2.2 Nicht gestattet sind ferner

- die Bereitstellung interaktiver Programme im Internet
- das Ausführen von Dateien
- online-shopping oder
- das Herunterladen sowie das Filesharing von Spielen, Unterhaltungsmedien usw.

Etwas anderes gilt nur, wenn dies zur Ausübung der arbeitsvertraglichen Pflichten des Mitarbeiters erforderlich ist.

2.3 Die CHILI GmbH ist berechtigt, jede Nutzung von Internet und E-Mail zu speichern, um die Einhaltung der obigen Bestimmungen anhand der gespeicherten Daten zu überprüfen.

Bei Verstößen gegen das Verbot der privaten Nutzung des betrieblichen Internet- bzw. E-Mail-Anschlusses während der Arbeitszeit behält sich die CHILI GmbH rechtliche Maßnahmen bis hin zur Kündigung des Arbeitsverhältnisses vor.

2.4 Wegen der erheblichen Gefährdung durch Computer-Viren ist es dem Mitarbeiter generell untersagt Computerprogramme aus dem Internet auf die Rechner der CHILI GmbH zu übertragen (herunterzuladen). Etwas anderes gilt nur, wenn dies zur Ausübung der arbeitsvertraglichen Pflichten des Mitarbeiters erforderlich ist.

3. <u>Sicherung von Daten für die betriebliche Nutzung</u>

Eine Datensicherung der lokalen Massenspeicher am einzelnen Arbeitsplatz wird von der CHILI GmbH nicht durchgeführt. Deshalb dürfen Daten für die betriebliche Nutzung nicht ungesichert auf den lokalen Laufwerken gespeichert werden, sondern sind ohne Ausnahme in einem der Netzwerke zu speichern.

6.2 Verpflichtungserklärung

Auf die vorstehenden Inhalte zum Umgang mit Anlagen der elektronischen Datenverarbeitung wurde der Mitarbeiter heute hingewiesen. Die aufgeführten Pflichten des Mitarbeiters stellen einen wichtigen Teil des Arbeitsverhältnisses dar. Der Mitarbeiter verpflichtet sich hiermit ausdrücklich zur Einhaltung dieser Pflichten. Pflichtverletzungen durch den Mitarbeiter können Schadenersatzansprüche sowie arbeitsrechtliche Konsequenzen bis hin zur Kündigung des Arbeitsverhältnisses nach sich ziehen.

Unterschrift CHILI Geschäftsleitung und Mitarbeiter

6.3 Merkblatt für Datensicherheit und Datenschutz

Merkblatt für Datensicherheit und Datenschutz

Neben den bereits bestehenden gesetzlichen Vorschriften (z. B. BetrVG, HGB) und den Geheimhaltungsvorschriften für unseren Betrieb gelten für Sie aufgrund Ihrer Tätigkeit im Bereich der Datenverarbeitung auch die Bestimmungen des Bundesdatenschutzgesetzes, insbesondere § 5. Danach ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen. Der Schutz personenbezogener Daten gemäß BDSG erstreckt sich auf alle in Dateien (z. B. EDV-Dateien, Mikrofilm-Dateien, Karteien u. ä.) gespeicherten personenbezogenen Daten sowie auf Akten und Aktensammlungen, die Dateicharakter haben. Dazu gehören auch die Ein- und Ausgabeformulare der Datenverarbeitung. Bei der Verarbeitung von Daten des Rechnungswesens sind die jeweils geltenden Grundsätze ordnungsgemäßer Datenverarbeitung im Sinne der ordnungsmäßigen Buchführung gemäß AO und HGB zu beachten. Bitte melden Sie sofort Mängel auf den Gebieten der Datensicherheit und des Datenschutzes sowie der Ordnungsmäßigkeit der Datenverarbeitung. Sie helfen damit nicht nur der CHILI GmbH, sondern sichern damit auch ihren Arbeitsplatz, ganz abgesehen von der rechtlichen Verpflichtung.

Unterschrift CHILI Geschäftsleitung und Mitarbeiter

6.4 Verpflichtungserklärung im Sinne des BDSG

Verpflichtungserklärung nach § 5 Bundesdatenschutzgesetz (BDSG)

Aufgrund Ihrer Aufgabenstellung bei der CHILI GmbH gilt für Sie das Datengeheimnis nach § 5 Bundesdatenschutzgesetz (BDSG). Danach ist es Ihnen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.
Gemäß § 5 BDSG sind Sie verpflichtet das Datengeheimnis zu wahren. Diese Verpflichtung besteht auch über das Ende Ihrer Tätigkeit in unserem Unternehmen hinaus.
Wir weisen Sie darauf hin, dass Verstöße gegen das Datengeheimnis nach den §§ 43 und 44 BDSG und anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden können. Abschriften der genannten Vorschriften des BDSG (§§ 5, 43 und 44) sind beigefügt.
Ihre sich ggf. aus dem Arbeits- bzw. Dienstvertrag und der Arbeitsordnung ergebende allgemeine Geheimhaltungsverpflichtung wird durch diese Erklärung nicht berührt.

Über die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes wurde ich unterrichtet. Die sich daraus ergebenden Verhaltensweisen wurden mir mitgeteilt. Meine Verpflichtung auf das Datengeheimnis nach § 5 BDSG habe ich hiermit zur Kenntnis genommen.
Anlagen: §§ 5, 43 und 44 BDSG

Unterschrift CHILI Geschäftsleitung und Mitarbeiter

6.5 Verschwiegenheitserklärung Mitarbeiter

Verpflichtung zur Verschwiegenheit

1. Verschwiegenheit bei Geschäfts- und Betriebsgeheimnissen des Arbeitgebers und Kunden des Arbeitgebers

Der Mitarbeiter wird über alle betrieblichen Angelegenheiten, die ihm im Rahmen oder aus Anlass seiner Tätigkeit beim Arbeitgeber oder bei Kunden des Arbeitgebers bekannt geworden sind, Stillschweigen bewahren.

Zur Wahrung der Verschwiegenheitspflicht gehört auch, dass alle vorkommenden Vorgänge unter Verschluss zu halten sind, soweit dies möglich ist, und dafür Sorge getragen wird, dass unbefugten Personen ein Einblick in Unterlagen unmöglich gemacht wird. Zur Wahrung der Verschwiegenheitspflicht gehört weiter, dass Geschäfts- und Betriebsgeheimnisse des Arbeitsgebers wie auch der Kunden des Arbeitgebers nicht für eigene Zwecke in irgendeiner Weise verwertet werden.

Die Verschwiegenheitspflicht erstreckt sich nicht nur auf fremde Geheimnisse, sondern auf alles, was in Ausübung oder bei Gelegenheit der Tätigkeit beim Arbeitgeber oder bei Kunden des Arbeitgebers anvertraut wurde oder bekannt geworden ist. Dabei muss jeder Anschein einer Verletzung der Verschwiegenheit vermieden werden. Die Verschwiegenheitspflicht erstreckt sich auch auf alle internen Büroverhältnisse, sowie die bekannt gewordenen oder werdenden persönlichen wirtschaftlichen und steuerlichen Verhältnisse von anderen Mitarbeitern, Kunden oder Mitgliedern bzw. Mandanten von Kunden.

Die Verschwiegenheitspflicht besteht nicht nur gegenüber Fremden, sondern auch gegenüber den Familienangehörigen, gegenüber Arbeitskollegen, sowie eine Mitteilung nicht aus dienstlichen Gründen erforderlich ist und auch gegenüber denjenigen, die von der betreffenden Tatsache bereits Kenntnis erlangt haben. Die Verschwiegenheitspflicht besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

2. Besondere berufliche Verschwiegenheit bei Kunden der steuerberatenden und medizinischen Berufe

Mein Arbeitgeber, die CHILI GmbH, hat mich ausdrücklich über die besondere berufliche Verschwiegenheit und die damit verbundene außerordentliche Vertraulichkeit der steuerberatenden und medizinischen Berufe gem. den einschlägigen Bestimmungen des Steuerberatungsgesetzes und der ärztlichen Schweigepflicht belehrt und auf diese verpflichtet.

Verstöße gegen die vorgenannten Bestimmungen können arbeitsrechtliche Folgen bis hin zur fristlosen Kündigung nach sich ziehen.

Unterschrift CHILI Geschäftsleitung und Mitarbeiter

7 Referenzen

An dem Datenschutzkonzept der TKmed® haben folgende Personen und Firmen mitgewirkt und zeichnen verantwortlich (s. a. Kapitel 4):

Person	Funktion im TKmed® Projekt	Institution / Unternehmen
Christian Bohn	Zusätzliche Entwicklung der Verschlüsselungskomponenten	CHILI GmbH Dossenheim / Heidelberg
Tobias Christian	Projektdurchführung	CHILI GmbH Dossenheim / Heidelberg
Dr. Uwe Engelmann	Projektentwicklung Bereitstellung der Softwarekomponenten	CHILI GmbH Dossenheim / Heidelberg
Dr. med. Antonio Ernstberger	Projektentwicklung und -management	Unfallchirurgie, Universitätsklinikum Regensburg,
Dr. med. Alexander Leis	Projektentwicklung	Unfallchirurgie, Universitätsklinikum Regensburg,
Dr. Heiko Münch	Projektentwicklung Zusätzliche Entwicklung der Verschlüsselungskomponenten	CHILI GmbH Dossenheim / Heidelberg
Barbara Rimmler	Projektdurchführung	CHILI GmbH Dossenheim / Heidelberg
Prof. Dr. Martin Staemmler	Projektentwicklung und -management	Medizininformatik, Fachhochschule Stralsund
Prof. Dr. med. Johannes Sturm	Projektleitung	AUC - Akademie der Unfallchirurgie GmbH
Florian Schwind	Zusätzliche Entwicklung der Verschlüsselungskomponenten	CHILI GmbH Dossenheim / Heidelberg
PD Dr. med. Michael Walz	Projektentwicklung und -management	Ärztliche Stelle für Qualitätssicherung in der Radiologie, TÜV SÜD Life Service GmbH
Robert Weininger	Projektentwicklung Bereitstellung der zentralen TK-Infrastruktur	pegasus gmbh Regenstauf
Thorsten Weires	Projektdurchführung	CHILI GmbH Dossenheim / Heidelberg
PD Dr. med. Gerald Weisser	Projektentwicklung und -management	Informationstechnik und Qualitätssicherung, Institut für Klinische Radiologie und Nuklearmedizin, Universitätsmedizin Mannheim