# SICHERE UND WEBBASIERTE VERTEILUNG RADIOLOGISCHER DATEN – DAS PROJEKT TELEIMAGE

Stingl C[1], Slamanig D[1], Kurmann T[1,2]

***Kurzfassung***

*Radiologische Institute spielen eine zentrale Rolle bei einer Vielzahl von medizinischen Behandlungen. Dabei entsteht im Regelfall digitales Bildmaterial, das durch den Radiologen befundet und im Anschluss an den zuweisenden Arzt bzw. einen weiteren Facharzt übermittelt wird. Die Dauer für diesen Workflow kann durch einen durchgängigen Einsatz von IKT erheblich reduziert und folglich die Qualität des Behandlungsprozesses gesteigert werden. Dabei sind jedoch geltende rechtliche Rahmenbedingungen und Standards zu beachten und bei der Umsetzung einer konkreten Lösung zu berücksichtigen. Im Rahmen des Forschungsprojektes Teleimage, das von der Fachhochschule Kärnten in Kooperation mit der Siemens AG Österreich durchgeführt wurde, ist der radiologische Workflow vollständig digital umgesetzt worden. Dabei wurde ein Sicherheitskonzept entwickelt und implementiert, das die Anforderungen des österreichischen Datenschutzgesetzes und des Gesundheitstelematikgesetzes erfüllt und darüber hinaus gesetzeskonforme Signaturen für digitale Befunde ermöglicht. Über dieses System können radiologische Institute, zuweisende Ärzte und Patienten Bild- und Befundmaterial webbasiert verwalten und austauschen, sodass ausschließlich autorisierte Personen diese Informationen einsehen können. In diesem Zusammenhang bedeutet „autorisiert", dass eine Person ausschließlich dann auf Daten zugreifen kann, wenn diese Person explizit eine Freigabe von einer berechtigten Person erhalten hat. Dies wird mit Hilfe von kryptographischen Token realisiert die auf den Standardverfahren AES (Advanced Encryption Standard) und RSA basieren. Bei der Entwicklung des Systems wurde ein spezieller Fokus darauf gelegt, dass das System weitestgehend ohne Benutzerinteraktion alle freigegebenen Studien eines Benutzers vollautomatisch herunterlädt und zur für weitere Informationssysteme zur Verfügung stellt.*

## 1. Einleitung

Das Ziel des Forschungsprojektes Teleimage war die Digitalisierung und Optimierung der konventionellen postalischen Übermittlung von radiologischen Bildern und Befunden zwischen zuweisenden Ärzten und Radiologen. Das Hauptaugenmerk lag dabei auf der Entwicklung und Implementierung eines Sicherheitskonzeptes gemäß der in Österreich geltenden gesetzlichen Rahmenbedingungen. Dabei gewährleistet das Sicherheitskonzept, dass die medizinischen Daten sowohl während der Übermittlung, als auch im Archivierungssystem ausschließlich in verschlüsselter Form vorliegen, wobei die Daten während des gesamten Prozesses nie umgeschlüsselt werden und folglich

[1] Studienbereich Medizinische Informationstechnik, Fachhochschule Kärnten, Klagenfurt, Österreich
[2] Siemens AG Österreich, Medical Solutions, Graz, Österreich

ausschließlich auf dem Client des zuweisenden Arztes bzw. Radiologen im Klartext vorliegen. Darüber hinaus wird durch die Verwendung eines Web-Browsers ein zeit- und ortsunabhängiger Zugriff auf patientenbezogene medizinische Daten ermöglicht. Der Zugriff auf den Inhalt medizinischer Dokumente (Studien, Befunde) wird ausschließlich jenen Benutzern ermöglicht, die eine Freigabe auf dieses Dokument besitzen. Eine Freigabe ist ein kryptographisches Token, durch den berechtigte Benutzer den Inhalt eines verschlüsselten Dokuments einsehen können. Dies gilt einerseits für Ärzte, die im Behandlungsprozess des Patienten involviert sind und andererseits für den Patienten selbst, der sein radiologisches Bildmaterial und die zugehörigen Befunde über das Internet einsehen kann.

Medizinische Daten sind sensible Daten, da sie Informationen hinsichtlich des physischen und psychischen Zustandes einer Person beinhalten. Daraus ergibt sich u.a. die Notwendigkeit des Schutzes dieser Daten bei der Übermittlung über eine öffentlich zugängliche Infrastruktur (z.B. Internet). Um die Verteilung medizinischer Daten in Übereinstimmung mit gesetzlichen Forderungen zu realisieren, sind in Österreich zwei Gesetze speziell zu berücksichtigen: das Datenschutzgesetz 2000 und das Gesundheitstelematikgesetz. Im Sinne des Datenschutzgesetzes hat „jedermann den Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten“ [1]. Weiters unterscheidet das Gesetz zwischen personenbezogenen Daten, indirekt personenbezogenen und sensiblen Daten (z.B. medizinische Daten), die einem besonders schutzwürdigen Interesse unterliegen. Die gesetzliche Grundlage für den sicheren Austausch von personenbezogenen medizinischen Daten in Österreich bildet das Gesundheitsreformgesetz und im Speziellen der Artikel 10 (Gesundheitstelematikgesetz). Demzufolge darf der Austausch medizinischer Daten nur dann erfolgen, wenn „Identität und Rolle der Empfänger oder Gesundheitsdiensteanbieter, die ein eingeräumtes Zugriffsrecht auf Gesundheitsdaten in Anspruch nehmen wollen, nachgewiesen sind“. Um den Anforderungen hinsichtlich der Vertraulichkeit gerecht zu werden, haben „Gesundheitsdiensteanbieter beim elektronischen Gesundheitsdatenaustausch über ein Medium, das nicht ihrem ausschließlichen Zugriff unterliegt, von ihnen verschiedene Dritte von der Kenntnisnahme von Gesundheitsdaten durch inhaltliche Verschlüsselung der Daten auszuschließen“. Die Verschlüsselung hat dabei auf dem Computer des Senders zu erfolgen und die Entschlüsselung auf dem des Empfängers. Bezüglich der Integrität fordert das Bundesgesetz die „Verwendung elektronischer Signaturen, sowie deren Nachweis bzw. Prüfung.“ Die erwähnten gesetzlichen Forderungen waren somit die Basis für die Entwicklung eines integrierten Sicherheitskonzepts bei Teleimage.

## 2. Architektur

Der folgende Abschnitt behandelt zunächst den konventionellen radiologischen Workflow und widmet sich danach dem vollautomatisierten Workflow der in *Teleimage* realisiert wurde. Zusätzlich zu den erwähnten Sicherheitseigenschaften des Systems folgt eine detaillierte Beschreibung des entwickelten und implementierten Sicherheitskonzepts.

Um den konventionellen Workflow optimieren und kritische Erfolgsfaktoren identifizieren zu können, ist eine genaue Analyse des Prozesses notwendig. Der konventionelle Workflow betrachtet Patienten, die wegen einer radiologischen Untersuchung von einem zuweisenden Arzt an einen Radiologen überwiesen werden. Im ersten Schritt der radiologischen Untersuchung (siehe *Abbildung 1*) werden mit Hilfe einer Modalität (z.B. CT, MRT) radiologische Bilder erstellt. Daraufhin wird dieses Bildmaterial über ein DICOM Netzwerk [3] im radiologischen Institut an eine Befundkonsole übermittelt und von einem Radiologen befundet. Nach dem Ausdruck des befundrelevanten Bildmaterials wird dieses zusammen mit dem dazugehörigen Befund postalisch oder durch den Patienten an den zuweisenden Arzt übermittelt. Die gravierendsten Nachteile dieses konventionel-

len Workflows sind einerseits der administrative und finanzielle Mehraufwand der Radiologen (z.B. Filmausdrucke) und andererseits die benötigte Zeit für postalische Übermittlungen.

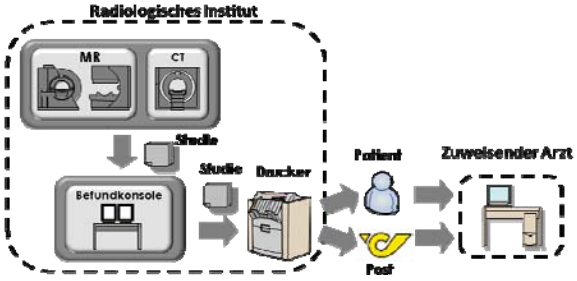


**Abbildung 1. Konventioneller Workflow radiologischer Untersuchungen**

## 2. 1. Digitaler Workflow

Aufgrund dieser Ausgangssituation lag die Zielsetzung bei *Teleimage* auf der digitalen Abbildung, Implementierung und Optimierung des obigen Workflows. *Teleimage* stellt eine webbasierte und vollautomatisierte Bild- und Befundverteilung dar und ermöglicht für alle am Behandlungsprozess beteiligten Gesundheitsdiensteanbieter einen orts- und zeitunabhängigen Zugriff auf medizinische Daten. Ferner wird dabei die Vertraulichkeit und Integrität dieser Daten garantiert. Bei den zuvor genannten Aspekten wurde speziell auf die Konformität mit den oben erwähnten österreichischen Gesetzen geachtet. Durch die Digitalisierung des Workflows werden sowohl die Kosten, als auch die für den integrierten Behandlungsprozess benötigte Zeit reduziert und dies führt letztendlich zu einer Steigerung der Qualität und Effizienz dieses Prozesses. Der beim Einsatz von *Teleimage* (siehe *Abbildung 2*) resultierende Worflow vermeidet in den meisten Fällen den Bildausdruck und die darauf folgende postalische Übermittlung.

Nach der Befundung wird das Bildmaterial via DICOM – Netzwerk [3] an den Teleimage-Client übermittelt. In diesem Prozessschritt werden relevante Parameter aus dem DICOM – Header ausgelesen, um einerseits die Identifikation einer Studie innerhalb des Systems zu ermöglichen und andererseits die initiale Freigabe für den Radiologen, den zuweisenden Arzt und optional für die Administratoren des Systems zu erstellen. Aufgrund der Erfahrungswerte wird initial keine Freigabe für Patienten erstellt.

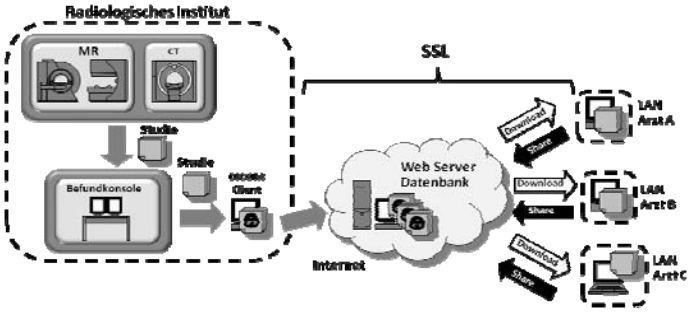


**Abbildung 2. Bildverteilung bei Teleimage**

Zur Erstellung einer gesetzeskonformen digitalen Signatur bietet sich das das Produkt trustDesk Professional der Firma IT Solution und kann bei Bedarf nahtlos in *Teleimage* integriert werden. Dabei wird eine sogenannte pdf-Signatur erstellt und in weiterer Folge wird dieses Dokument digital übermittelt. Jedoch muss an dieser Stelle erwähnt werden, dass die Akzeptanz und Notwendig-

keit von Seiten der Ärzteschaft zu diesem Zeitpunkt noch als gering eingestuft werden muss. Wie im vorhergehenden Abschnitt erwähnt, repräsentiert eine Freigabe ein kryptographisches Token, das einem berechtigten Benutzer den Zugriff auf den Inhalt einer verschlüsselten Studie ermöglicht. Die Metadaten der Studie werden auf dem Teleimage-Client verarbeitet und nach dem Upload der Studie in das Archivierungssystem (Datenbank) integriert. Vor dem Upload der Studie auf den Webserver wird diese zunächst verschlüsselt und durch den „Radiologen" automatisch signiert. Im nächsten Schritt wird eine SSL Verbindung zwischen dem Teleimage-Client und dem Webserver aufgebaut. Diese garantiert die Vertraulichkeit während der Benutzerauthentifikation und der Archivierung der Studie. Mit Hilfe eines Java Applets verwaltet ein Benutzer seine Studien und kann weitere Freigaben für andere Benutzer erstellen. Der Download von Studien kann entweder vollautomatisiert oder manuell durchgeführt werden. Beim Automatischen Modus werden alle für einen Benutzer freigegebenen Studien automatisch auf dessen Client heruntergeladen, durch den DICOM-Viewer betrachtet und in das Praxisinformationssystem integriert werden. Dieser Modus bietet den Vorteil, dass die Interaktionen durch den Benutzer deutlich reduziert und die Applikation somit im Hintergrund betrieben werden kann. Im zweiten, dem manuellen Modus, kann der Benutzer manuell Studien für den Download selektieren und diesen Prozess manuell initiieren. In beiden Fällen erfolgt vor dem Download einer Studie die Verifikation der zugehörigen digitalen Signatur. In Übereinstimmung mit den gesetzlichen Rahmenbedingungen werden einem Benutzer nur jene Studien zur Verfügung gestellt, deren digitale Signatur erfolgreich verifiziert werden kann.

## 2. 2. Software Architektur

Der Client der *Teleimage* Anwendung ist als Java Applet realisiert und ermöglicht neben administrativen Aufgaben und statistischen Analysen die Verwaltung von Studien und Freigaben. Aufgrund der verwendeten Technologien erreichen wir sowohl eine Plattform- als auch eine Browserunabhängigkeit. Sämtliche kryptographischen Operationen (entschlüsseln, verschlüsseln, Erstellung kryptographischer Token, etc.) erfolgen durch das Applet, also auf der Seite des Clients. Die Business-Logic des Servers basiert auf der Java Servlet Technologie und realisiert u.a. den Zugriff auf die Datenhaltungsschicht (Datenbank). Aufgrund der gewählten Architektur können keine Probleme durch eventuelle Portrestriktionen (z.B. Firewalls) entstehen. Das Management der Studien erfolgt auf Basis des Web-based Distributed Authoring and Versioning (WebDAV) Protokolls. Dieses Protokoll stellt eine Erweiterungen des HTTP Protokolls dar und erlaubt den Benutzern das gemeinsame Bearbeiten und Verwalten von Dateien auf Webservern. Durch die Verwendung des WebDAV Protokolls für den Datentransfer kann die Kommunikation auf dem HTTP Port erfolgen.

## 2. 3. Sicherheitskonzept

Die Bindung einer Benutzeridentität an einen öffentlichen Schlüssel wird mittels X.509 Zertifikaten und einer Public Key Infrastruktur (PKI) realisiert. Das bedeutet, dass für jeden Benutzer ein Zertifikat ausgestellt wird, das den signierten öffentlichen Schlüssel des Benutzers beinhaltet. Das Benutzerzertifikat des Benutzers A, das den öffentlichen Schlüssel $PK_A$ enthält, sowie der mit einem Passworts verschlüsselte zugehörige private Schlüssel $SK_A$ werden serverseitig verwaltet. Für die Implementierung der PKI wurde eine hierarchische Architektur gewählt, die unter dem Rootzertifikat, Benutzerzertifikate und ein Zertifikat zum Signieren des Applets beinhaltet. Da das Java Applet Zugriff auf lokale Ressourcen benötigt, wird es digital signiert. Damit kann das Einschleusen von schadhaftem Code vermieden werden.

Anhand der oben beschriebenen Gesetze ist die alleinige Übertragungsverschlüsselung mittels SSL/TLS nicht ausreichend, da die Integrität auf Applikationsebene nicht gewährleistet werden

kann. Deswegen wurde speziell für dieses Projekt ein integriertes Sicherheitskonzept entwickelt und implementiert. Wie bereits erwähnt, ist der Zugriff auf medizinische Daten bei *Teleimage* auf Basis eines Freigabenkonzeptes realisiert. Grundsätzlich bietet der Public Key Cryptography Standard #7 (PKCS#7) [4], der in vielen Produkten integriert ist, standardisierte Formate um ein Konzept für die Vergabe von Freigaben realisieren zu können. Diese Variante ist jedoch für die spätere Erstellung zusätzlicher Freigaben extrem ineffizient und wurde deshalb für dieses Projekt modifiziert.

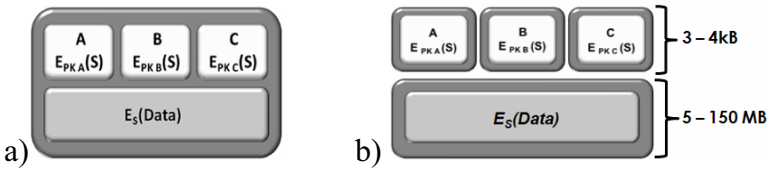


**Abbildung 3. PKCS#7 und die gesplittete Variante des Standards im Überblick**

Ein in PCSK#7 verschlüsselter Klartext (z.B. Studie) ist das Resultat einer symmetrischen Verschlüsselung z.B. AES (Advanced Encryption Standard) der Studie und einer Menge von kryptographischen Tokens, realisiert mittels asymmetrischer Verschlüsselung (z.B. RSA-OAEP). Für jeden Benutzer der eine Freigabe erhält, wird ein kryptographisches Token erstellt. In der modifizierten Implementierung des Verschlüsselungsformates werden die symmetrisch verschlüsselten Daten von den Tokens getrennt. Diese gesplittete Variante des PKCS#7 (siehe *Abbildung 3b*) bietet erstens die Stärken von PKCS#7 und zweitens eine sehr schnelle und flexible Methode zur Erstellung zusätzlicher Tokens für Studien. Die initialen Freigaben, die für den Radiologen, den zuweisenden Arzt sowie optional für Administratoren des Systems werden im Archivierungssystem hinterlegt. Der entscheidende Vorteil dieses Formats wird offensichtlich, wenn zu einem späteren Zeitpunkt (z.B. für das Einholen einer Zweitmeinung) eine zusätzliche Freigabe erstellt werden soll. In diesem Szenario muss lediglich das entsprechende Token (3-4kB) auf den Client transferiert, ein neues Token erstellt und in das Archivierungssystem übermittelt werden. Bei Verwendung des standardisierten Formats müsste anstelle von weniger als 5 kB die gesamte verschlüsselte Studie inklusive Tokens (5-150MB) auf den Client transferiert werden. Neben der Geheimhaltung der Daten spielt auch die Integrität der Daten auf Applikationsebene eine zentrale Rolle. Dies wird durch den Einsatz digitaler Signaturen erreicht, wobei einem Benutzer nur jene Studien zur Verfügung gestellt werden, deren digitale Signatur erfolgreich verifiziert werden konnte.

## 3. Ergebnisse und Ausblick

Das Projekt Teleimage ist seit August 2007 im Echtbetrieb und ist Teil des medizinischen Portfolios der Siemens AG Österreich. Es wird mit Stand Februar 2008 von radiologischen Instituten in den Bundesländern Steiermark, Burgenland und Wien eingesetzt und Institute in weiteren Bundesländern sollen in naher Zukunft folgen. In den radiologischen Instituten konnte eine signifikante Reduktion der Kosten (Filmmaterial, Druckkosten, Entsorgung, etc.) erzielt werden und zudem konnten administrative Tätigkeiten reduziert werden. Im vollautomatisierten Modus bietet das System eine sehr effiziente Methode zur Verteilung von radiologischem Bildmaterial und Befunden. Aus der Sicht des Patienten und des zuweisenden Arztes kann festgehalten werden, dass durch die elektronische Übermittlung die Bild- und Befunddaten für die weitere Behandlung schnellstmöglich zur Verfügung stehen. *Tabelle 1* illustriert die zuvor genannte Zeitersparnis anhand eines Beispiels.

**Tabelle 1. Workflows im Vergleich**

| | Konventioneller Workflow | *Teleimage* Workflow |
|---|---|---|
| **Untersuchung** | 30 min | 30 min |
| **Befundung** | 15 min | 15 min |
| **Ausdruck** | 10 min | |
| **Postzustellung** | 1 - 2 days | |
| **Studien Upload** | | 40 min [1] |
| **Studien Download** | | 23 min [2] |
| | **~ 1 - 2 day** | **1 h 48 min** |

1 ... Upload - Geschwindigkeit 512 kb/s
2 ... Download - Geschwindigkeit 1Mb/s

Im Echtbetrieb werden pro Tag durchschnittlich 50 bis 100 Untersuchungen pro radiologisches Institut durchgeführt. Bei der Betrachtung eines Instituts und einer durchschnittlichen Anzahl von 50 Studien pro Tag reduziert *Teleimage* die Filmkosten von bis zu 3.000€ pro Monat, wobei zusätzliche Kostenersparnisse aus administrativen Tätigkeiten und Druckern bislang nicht evaluiert wurden. Eine Hochrechnung für ein gesamtes Jahr impliziert ein Einsparungspotential von etwa 40.000€ pro radiologischem Institut.

Es sei hier jedoch noch einmal erwähnt, dass das Hauptaugenmerk dieses Forschungsprojektes auf der Implementierung eines integrierten und gesetzeskonformen Sicherheitskonzeptes lag. Ein wesentlicher Aspekt in der weiteren Entwicklung sind einerseits CDA basierte radiologische Befunde, die derzeit in Österreich gerade entwickelt werden und andererseits die Integration der eCard sowohl zur Befundsignatur, zur Authentifizierung am System und zur Weitergabe von Berechtigungen. Weitere Ziele sind das System als Document-Repository im Sinne der ELGA Strategie zu betreiben und die Kompatibilität bezüglich IHE in den Bereichen IT – Infrastruktur und Radiologie.

## 4. Literatur

[1] Bundesgesetz über den Schutz personenbezogener Daten - Datenschutzgesetz 2000, http://www.dsk.gv.at/dsg2000d.htm

[2] Gesundheitsreformgesetz 2005, http://www.bmgf.gv.at

[3] DICOM, Digital Imaging and Communications in Medicine, American College of Radiology and National Electrical Manufacturers Association, 1992

[4] PKCS#7, Cryptographic Message Syntax Standard, RSA Laboratories, 1993.

[5] A. MENEZES, P. VAN OORSCHOT, S. VANSTONE, Handbook of Applied Cryptography, CRC Press, 1996.

[6] C. STINGL, D. SLAMANIG, et al. Realisierung eines sicheren zentralen Datenrepositories, DACH Security 2006, pp. 32-45, IT Verlag, 2006

[7] T. KURMANN, D. SLAMANIG, AND C. STINGL. Gesetzeskonforme und webbasierte Bildverteilung. Proceedings of BMT 2007, Aachen, Germany, 2007.

[8] T. KURMANN, D. SLAMANIG, C. STINGL, AND K. ROESSL. Secure web-based distribution of medical images and findings based on the Austrian eHealth strategy. 21st International Congress of the European Federation for Medical Informatics (MIE 2008), Göteborg, Sweden, May 2008.