

# SecTelMed – sichere Kommunikation über öffentliche Leitungen

Aufbau und Entwicklung einer sicheren und frei verfügbaren Telemedizinlösung

M. Kämmerer, G. Klos, P. Mildenerger  
Klinik und Poliklinik für Radiologie des Universitätsklinikums Mainz

Aus dem Bedarf heraus radiologische Bilddaten zur Telekonsultation zwischen der Diakonie Bad Kreuznach und der Uniklinik Mainz auszutauschen entstand das Projekt SecTelMed. Ein wichtiger Punkt war die Integration der bereits vorhandenen IT-Infrastrukturen. Das bedeutet, die Lösung musste sich unproblematisch in bereits vorhandene Strukturen eingliedern lassen. Dies erleichtert die Installation und Administration und ist somit kostengünstig. Sicherheit und Datenschutz sind bei der Kommunikation medizinischer Daten eine Grundvoraussetzung. Um das Rad nicht neu zu erfinden wurde hierfür auf Standardsoftware aus dem Open Source Bereich beziehungsweise auf frei verfügbare Software zurückgegriffen. Dies war auch notwendig, um eine Schnittstelle zum unkomplizierten Datenaustausch mit anderen Telemedizinprojekten zur Verfügung zu stellen.

## 1 Material und Methodik

### 1.1 Programme und Programmbibliotheken

Die verwendeten Programme und Bibliotheken ergeben sich aus den praktischen Notwendigkeiten. Als Datenaustauschplattform wird uns Zugang durch die Netzwerkgruppe der Uniklinik Mainz zu dem bereits bestehenden SSH-Server in der Demilitarisierten Zone (DMZ) gewährt (Abb. 1). Der Zugriff auf den Datenserver erfolgt durch einen SSH-Tunnel gesichert aus dem Internet heraus. Der definierte Durchgang durch die Firewall kommt durch ein Portforwarding über einen VPN-Router zustande. Eine VPN-Verbindung wird nicht aufgebaut. Für die Kommunikation mit diesem Server ist eine SSH-Verbindung notwendig. Die eigentliche Datenübertragung erfolgt durch Secure Copy [1, 2]. Dazu wurden zunächst die freien Implementationen Putty (SSH) und PuttySCP (SCP) [3] verwendet. Aufgrund der schnelleren Übertragungsgeschwindigkeit wurden diese durch die OpenSSH [1] Bibliothek ersetzt. Damit ist zunächst der Datenübertragungsweg gesichert. Für eine ausreichende Datensicherheit, wie sie im Bundesdatenschutzgesetz [4] gefordert wird, ist zusätzlich eine hinreichende Verschlüsselung der Übertragungsdaten notwendig. Wir verwenden hierfür den quasi Standard für Verschlüsselung – Pretty Good Privacy (PGP) in der frei verfügbaren Variante GnuPG aus dem OpenPGP Projekt [5]. Da Bilddaten in großer Anzahl und Größe zu verschicken sind müssen die Daten noch zusammengefasst und verlustfrei komprimiert werden. Dazu werden die Standardbibliotheken tar und bzip2 verwendet. Tar ist ein Archivierungsformat, welches ausschließlich eine gegebene Dateistruktur in einer Datei zusammenfasst (Archivdatei). Die Kompression erfolgt verlustfrei durch den bzip2 Algorithmus [6]. Der Empfang der Bilddaten wird durch StoreSCP aus dem DICOM Toolkit von OFFIS [7] geregelt. Da die telemedizinischen Daten auch wieder in einer anderen DICOM/ PACS Umgebung gespeichert werden, wird nach dem Empfang, getriggert durch Store- SCP, die Patientenidentifikationsnummer (PatientID, Tag 0010:0020 des DICOM Headers) mit einem frei wählbaren Prefix versehen. Als letztes Programm kommt für den Datentransfer noch StoreSCU zum Einsatz. Hiermit können nach erfolgreichem Empfang der DICOM Daten diese wieder in einem gegebenenfalls vorliegenden DICOM-Netzwerk an die entsprechende Arbeitsstation weitergeleitet werden. Damit eine Rückmeldung an den Benutzer erfolgen kann verwenden wir zusätzlich noch eine Email-Bibliothek, welche Emails optional nach erfolgtem Versand/Empfang den Erfolg/Misserfolg an beliebige Email Adressen über einen SMTP-Server verschicken kann.

### 1.2 SecTelMed Control Center

Die oben genannten Programme und Bibliotheken sind in der manuellen Verwendung recht kompliziert zu bedienen, da umfangreiche Kommandozeilenparameter zu übergeben sind. Deswegen werden diese durch unsere Eigenentwicklung SecTelMed als Frontend gesteuert. Die Applikation ist als Serverprogramm zu verstehen das normalerweise im Hintergrund (Backend) arbeitet. Sobald die Konfiguration abgeschlossen ist besteht keine Notwendigkeit mehr mit dem Programm in Interaktion zu treten. Die gesamte Kommunikation mit dem SecTelMed Server findet über jedes beliebige DICOMSend und -Receivefähige Programm sowie die optionalen Bestätigungs-E-mails statt.

#### 1.2.1 Verbindungsverwaltung

Das Control Center verwaltet die zuvor genannten Applikationen und Bibliotheken. Darüber hinaus werden aber auch die notwendigen Kommandozeilenparameter durch das SecTelMed verwaltet. Hierfür kommt zusätzlich die OpenSSL Bibliothek [8] zum Einsatz, um so die notwendigen Login/Passwortkombinationen verschlüsselt ablegen zu können. Diese und andere Einstellungen werden nach den AE-Titeln [Abb. 2. 1] getrennt gespeichert. Weiterhin findet die OpenSSL Bibliothek Verwendung für die Generierung von MD5 und SHA1 Summen zur Integritätsprüfung der verschiedenen von SecTelMed verwendeten Programmteile und der übertragenen Daten.

Die Steuerung des StoreSCP erfolgt über eine durch das Control Center generierte Stapeldatei (Batch) [Abb. 2. 2], die zum Beispiel durch Ablage in dem Autostartverzeichnis automatisch mit dem Anmelden eines Benutzers startet...

## Dokumentinformationen zum Volltext-Download

Ä

Titel:

SecTelMed â€“ sichere Kommunikation Ã¼ber Ã¶ffentliche Leitungen

Artikel ist erschienen in:

Telemedizinführer Deutschland, Ausgabe 2004

Kontakt/Autor(en): M. Kämmerer, G. Klos, P. Mildenberger

Klinik und Poliklinik für Radiologie des Universitätsklinikums Mainz

Seitenzahl:

4,5

Sonstiges

8 Abb., 2 Diagr. Dateityp/-größe: PDF /Ä 2.870 kB Click&Buy-Preis in Euro: kostenlos

Ä

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Ä

Hier gehts zum freien PDF Download...