

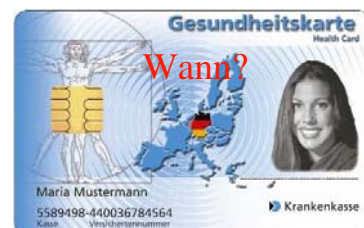
## DICOM-eMail in der Teleradiologie

@GIT-Initiative für Telemedizin

TeleHealthCare 2005 – 09. Mai 2005

## PKI - Grundvoraussetzung für die Telemedizin

- Problem: Weder Gesundheitskarte noch Heilberufsausweis verfügbar
- Public Key Infrastruktur (PKI) wird **jetzt** gebraucht
- HPC und Co. für Kommunikation mit dem Ausland (z.B. Frankreich) nicht geeignet
- PGP weltweit am häufigsten eingesetzte Programm

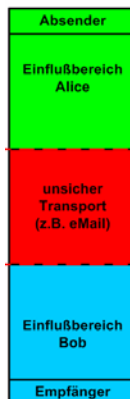


## PGP / GnuPG

- Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen
- für nahezu alle Betriebssysteme verfügbar
- für praktisch alle eMail-Clients verfügbar
- Einsatz der Kryptographie per „Mausklick“
- Zukunftssicher: X.509 und S/MIME werden unterstützt



## Alice schreibt Bob einen Brief ...

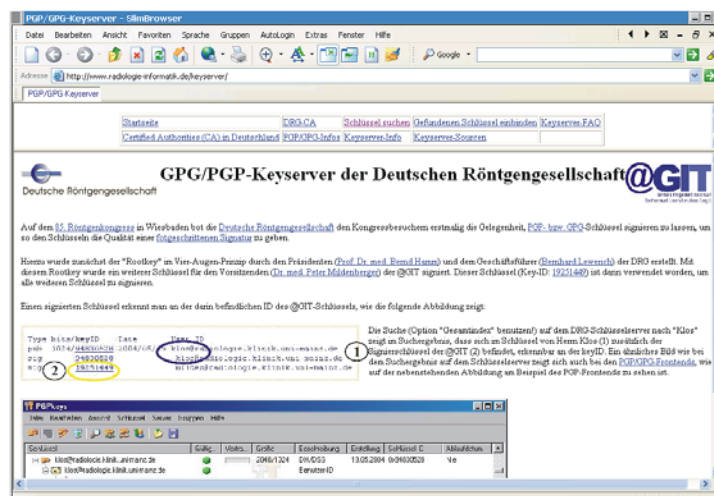


## Öffentliche Schlüssel über DRG-Keyserver erreichbar

- Keyserver stellen die öffentlichen Schlüssel den Kommunikationspartnern zur Verfügung
- Deutsche Röntzengesellschaft (DRG) signiert öffentliche Schlüssel
- D.h. die DRG stellt die Identität von Person und öffentlichen Schlüssel sicher
- Die Schlüssel erhalten so den Wert einer "fortgeschrittenen Signatur" nach dem deutschen Signaturgesetz
- Laut Auskunft von Juristen reicht die fortgeschrittene Signatur für die meisten Telemedizin-Projekte

## Öffentliche Schlüssel auf DRG-Keyserver verfügbar

<http://www.drg.de>



The screenshot shows a web browser window displaying the DRG-Keyserver website. The browser's address bar shows the URL <http://www.radiologie-fomatik.de/keyserv/>. The website header includes the @GIT logo and the text 'GPG/PGP-Keyserver der Deutschen Röntzengesellschaft @GIT'. Below the header, there is a navigation menu with links like 'Statistik', 'DRG-CA', 'Schlüssel suchen', etc. The main content area features a search interface with a search bar and a search button. A search result is displayed, showing a key ID and a QR code. A small window titled 'PGP-Key' is open at the bottom of the browser window, showing details of a key.

## Ergebnisse





- DRG-Signierte Schlüssel
  - Röntgenkongress 2004: 152
  - DICOM-Treffen 2004: 30
  - Röntgenkongress 2005: ?
- Besucher auf der Keyserver-Homepage
  - Januar 2005: 52
  - Februar 2005: 147
  - März 2005: 137
  - April 2005: 409

Und die praktische Anwendung ?

## @GIT Teleradiologie-Initiative



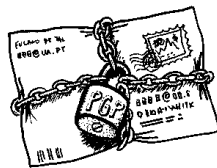
- Gründung 2003 auf dem DICOM-Workshop in Mainz
- Schirmherrschaft:  
Arbeitsgemeinschaft Informationstechnologie   
der Deutschen Röntgengesellschaft (DRG) 

## Anforderungen an eine Lösung

- Integrierbar in
  - existierenden Workflow
  - vorhandene IT-Infrastrukturen
- Kompatibel zu vorhandenen Firewall-Lösungen
- Einfaches Hinzufügen / Ändern neuer / vorhandener Kommunikations-Partner
- Diskussion über verschiedener Möglichkeiten (SSH, SCP, TLS, DICOM, ...)

## Ergebnis

- Nur eMail wird den Anforderungen gerecht



- Insbesondere für den spontanen Aufbau von Ad-Hoc-Verbindungen

**Teleradiologie per DICOM-eMail:**  
Der empfohlene Minimalstandard der DRG

## Warum eMail?

- Gut dokumentierter Standard:
  - SMTP, POP3, IMAP
  - DICOM Suppl. 54  
(MIME-konforme DICOM-Attachments)
  - Diverse RFCs  
(OpenPGP, TLS, ...)
- Nutzung vorhandener Infrastruktur
- Keine Änderungen in Firewall
- Benutzer und Administratoren mit eMail vertraut

## Datenschutz und -sicherheit?

- Ungeschützte Datenübertragung in Deutschland verboten
- Lösung: OpenPGP MIME-Format (RFC 3156)
  - Verschlüsselung und Authentifizierung von eMails
  - Gleichzeitige zip-Kompression möglich
- PGP/GnuPG am weitesten verbreitet
- Vom Bundesamt für Sicherheit (BSI) empfohlen

## Aber...

- Zuordnung der Daten zu einem Patienten?
  - DICOM einfach: Header mit Patienteninformationen
  - Non-DICOM: MIME-konform neues X-Tag eingeführt:  
X-TELEMEDICINE-STUDYID
- Zu übermittelnde Dateien oftmals groß
  - Große Dateien werden in mehreren eMails versendet
  - Zwei X-Tag-Erweiterungen des eMail-Headers:  
X-TELEMEDICINE-PART  
X-TELEMEDICINE-TOTAL
- Unsicheres Protokoll – ist die eMail angekommen ?
  - Nutzung von Notify-Funktionalität

## Aktuelle Erweiterungen der Empfehlung: Status-Codes

- Public Key zur Überprüfung nicht vorhanden
- Public Key nicht mehr gültig
- Signatur fehlerhaft
- Signatur ok, Key nicht vertrauenswürdig
- Korruptes Attachment, Entschlüsselung nicht möglich
- x von n eMails fehlen
- ...

## Zusammenfassung

- Die Initiative der Deutschen Röntgengesellschaft bzw. der @GIT erlaubt **heute** den Einsatz der Telemedizin / -radiologie
- Auch nach Einführung der HPC PGP wertvolles Mittel zur Kommunikation mit Kollegen im Ausland
- Kommunikation mittels eMail heute so selbstverständlich wie telefonieren
- Sicherheitserweiterungen erlauben sicheren Datentransfer per eMail
- Kombination mit DICOM-Standard ideal für die Teleradiologie bei ad-hoc-Verbindungen

## Fragen ?

**Vielen Dank für Ihre  
Aufmerksamkeit !**

