

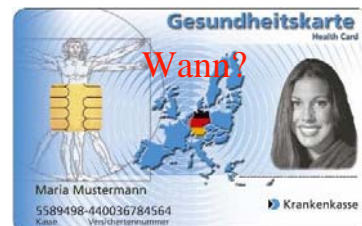
## Aufbau einer Public Key Infrastruktur: Der Ansatz für die DRG

B. Schütze, M. Kämmerer, G. Klos, P. Mildemberger

86. Deutschen Röntgenkongress – 07. 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

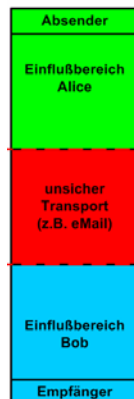


## PGP / GnuPG

- 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 page title is "GPG/PGP-Keyserver der Deutschen Röntzengesellschaft @GIT". The main content area shows search results for a key with ID "192148". The key is listed as:

```

Type: RSA/KEYID Text
pub 1024/192148 2006/1204 DRG02
uid [?] 192148
uid [?] 192148
  
```

Below the search results, there is a table with columns: Name, Mail, Orga, Valid, Date, Country, Expires, Subkey, and Algorithm. The table contains one entry:

Name	Mail	Orga	Valid	Date	Country	Expires	Subkey	Algorithm
192148	192148@drg.de	DRG02	2006/1204	DRG02	13.05.2004	0-2048/0203	Yes	

The website also includes a navigation menu with links like "Statistik", "DRG-CA", "Schlüssel suchen", and "GPG/PGP-Keyserver".

## 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

## Zusammenfassung

- Die Initiative der Deutschen Röntgengesellschaft bzw. der @GIT erlaubt **heute** den Einsatz der Telemedizin
- Ideale Unterstützung vorhandener Telemedizin-Initiativen, z.B. der @GIT Arbeitsgruppe Telemedizin
- Auch nach Einführung der HPC wertvolles Mittel zur Kommunikation mit Kollegen im Ausland
- DRG-signierte öffentliche Schlüssel vom Schlüsselserver im Internet (<http://www.drg.de>) abrufbar

## Wo werden PGP-Schlüssel erstellt?

- Entweder privat
- oder auf dem

**DICOM-Workshop**

**Mainz,  
01./02. Juli 2004**



## Fragen ?

**Vielen Dank für Ihre  
Aufmerksamkeit !**

