

Aufbau einer Public Key Infrastruktur - Der DRG-Ansatz

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

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



WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

PGP / GnuPG

- Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen
- Für nahezu alle Betriebssysteme verfügbar
- Für praktisch alle eMail-Clients verfügbar



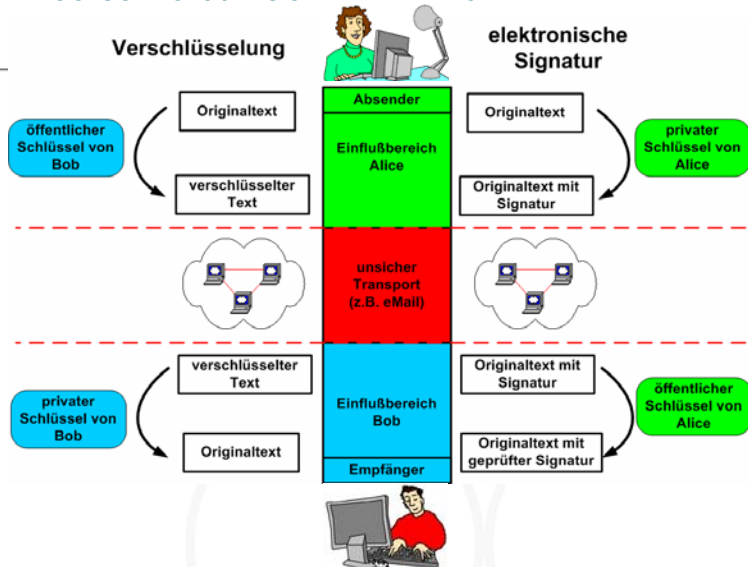
WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

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

WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

Alice schreibt Bob einen Brief ...



WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

PKI-Initiative der DRG

- Deutsche Röntgengesellschaft (DRG) signiert öffentliche Schlüssel
- Zuvor überprüft die DRG die Identität von Person und öffentlichen Schlüssel an Hand Personalausweis
- 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
- Keyserver stellen die öffentlichen Schlüssel den Kommunikationspartnern zur Verfügung

WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

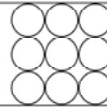
Öffentliche Schlüssel auf DRG-Keyserver verfügbar

The screenshot shows a web browser window displaying the DRG Keyserver website. The address bar shows the URL <http://www.drg.de>, which is highlighted with a blue box. The page content includes the title "GPG/PGP-Keyserver der Deutschen Röntgengesellschaft @GIT" and a table of public keys. The table has columns for Type, Name, Date, and Key ID. The first row shows a key for "Ulrich, Klaus" with a key ID of "0104A/01". The second row shows a key for "Ulrich, Klaus" with a key ID of "0104A/01". The third row shows a key for "Ulrich, Klaus" with a key ID of "0104A/01".

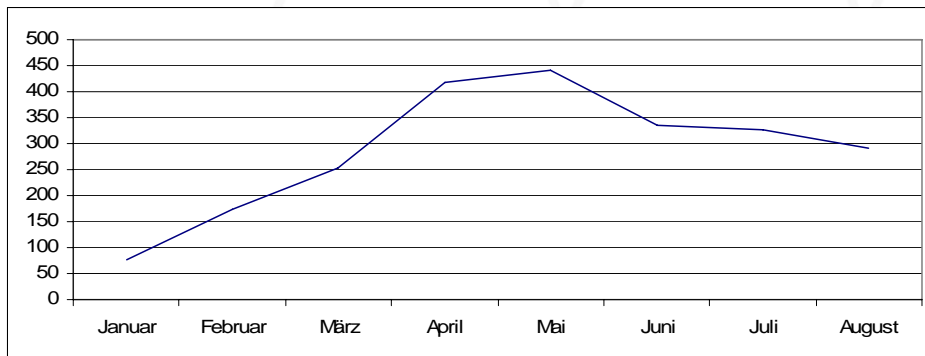
Type	Name	Date	Key ID
pub	Ulrich, Klaus	2004/12/04	0104A/01
pub	Ulrich, Klaus	2004/12/04	0104A/01
pub	Ulrich, Klaus	2004/12/04	0104A/01

WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

Ergebnisse

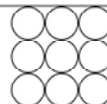


- DRG-signierte Schlüssel > 200
- Besucher auf der Keyserver-Homepage (2005)



WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

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 abrufbar

WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

Wo werden PGP-Schlüssel erstellt?

→ Entweder privat

→ oder auf dem

**Deutschen
Röntgenkongress**

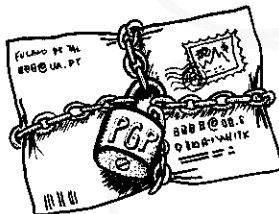
**Berlin,
24.-27. Mai 2006**



WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE

Fragen ?

**Vielen Dank für Ihre
Aufmerksamkeit !**



agit-pki@drg.de

WESTDEUTSCHES HERZZENTRUM ESSEN
KLINIK FÜR THORAX- UND KARDIOVASKULÄRE CHIRURGIE