Aufbau einer Public Key Infrastruktur: Der Ansatz für die DRG

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

Telemed 2005 – Telematik im Gesundheitswesen – 08./09. April 2005

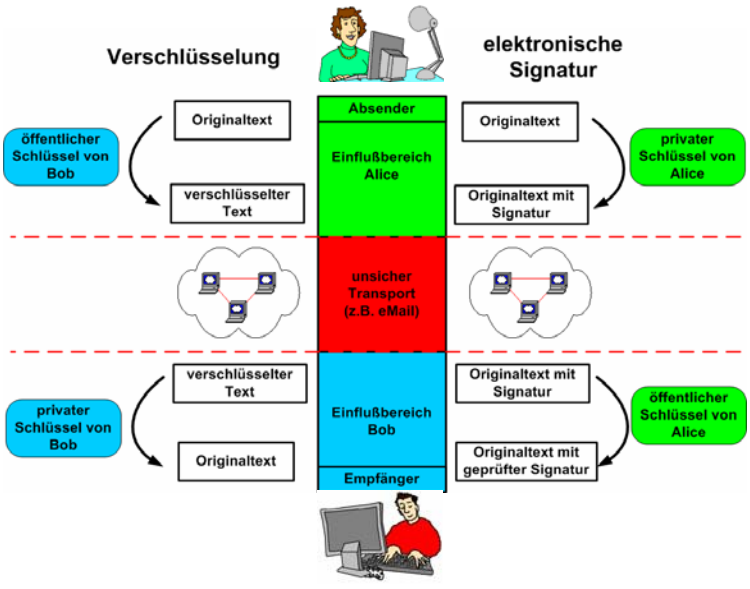
PKI - Grundvoraussetzung für die Telemedizin

- 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 für elektronische Unterschrift und Signatur

- Algorithmen gelten weltweit als sicher
- Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen
- Für nahezu alle Betriebssysteme verfügbar
- Für praktisch alle eMail-Clients verfügbar
- Ermöglicht Kryptographie per „Mausklick“
- Zukunftssicher: X.508 und S/MIME werden unterstützt

Alice schreibt Bob einen Brief …



Keyserver: Vermittlung der öffentlichen Schlüssel

- Deutsche Röntgengesellschaft (DRG) signiert öffentliche Schlüssel
- D.h. die DRG stellt die Identität von Person und öffentlichen Schlüssel sicher
- Öffentliche Schlüssel auf Keyserver verfügbar

  http://www.radiologie-informatik.de/keyserver/
- Keyserver basiert auf Open-Source-Lösung
- „Computer Emergency and Rescue Team“ des Deutschen Forschungsnetzes (DFN-CERT) setzt dieselbe Software für ihren PGP-Keyserver ein

Kontakt / Anfragen

agit-pki@drg.de