The Public Key Infrastructure of the Radiological Society of Germany

B. Schütze[1)], M. Kämmerer[1)], G. Klos[1)], P. Mildenberger[1)]

1) Johannes Gutenberg-University of Mainz - Department of Radiology, Mainz, Germany

Available ...??

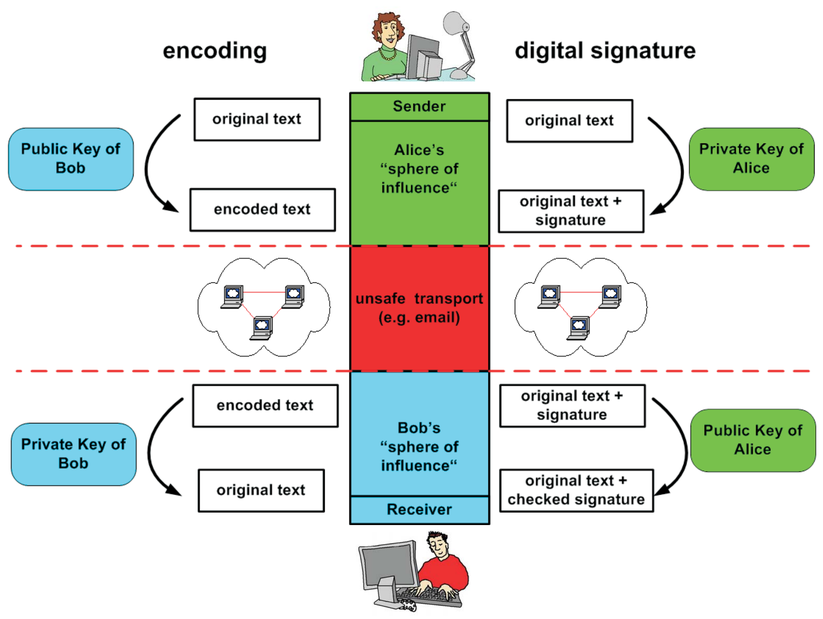
Public Key Infrastructure (PKI): Prerequisite for telemedicine

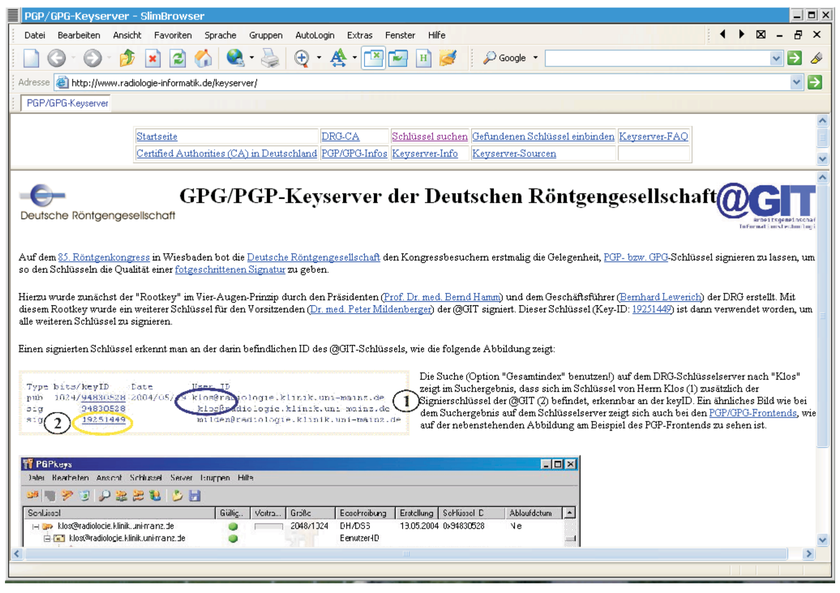
- Problem: Neither German health card nor health professional card available
- HPC and co. not suitable for communication with foreign countries (e.g. France)
- Public Key Infrastruktur (PKI) is needed now
- PGP most frequently used program worldwide

PGP/GnuPG-Characteristic for an digital signature

- Algorithms are regarded worldwide as sure
- Recommended by the Federal Office of Safety in Information Technology (Bundesamt für Sicherheit in der Informationstechnologie, BSI)
- For almost all operating systems available
- For practical all e-mail clients available
- Use of the cryptography "by mouse click"
- X.509 and S/MIME are supported, i.e. the proceedings cooperate also with the German health card and the HPC

Alice sends Bob an e-mail encoded and signed digital with PGP





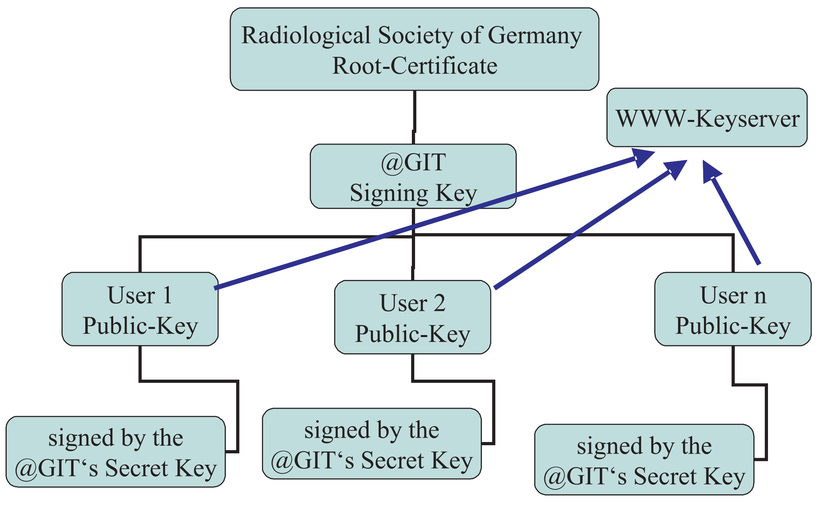
Public keys are available about Keyserver

- Keyserver provide the public keys to the communication partners
- Keyserver for PGP/GnuPG-keys are availably as Open Source projects
- PGP/GnuPG software can look automatically for the needed public keys on the Keyserver
- DRG makes their Keyserver available on the Internet

http://www.drg.de/

Only Keys certified by DRG are on DRG-Keyserver

- Radiological Society of Germany (Deutsche Röntgengesellschaft, DRG) signs public keys
- The DRG guarantees the identity of person and the signed public key
- So the keys get the value of an "advanced signature" according to the German signature law
- According to the information of lawyers the advanced signature suffices for most telemedicine projects



Corresponding Author:
Dr. Bernd Schütze
E-Mail: schuetze@medizin-informatik.org