Aufbau einer Public Key Infrastruktur - der Ansatz für die DRG

B. Schütze, G. Klos, M. Kämmerer

Überblick

- Fragestellung / Motivation
- Warum PGP?
- Abgrenzung zur HPC
- Zusammenfassung

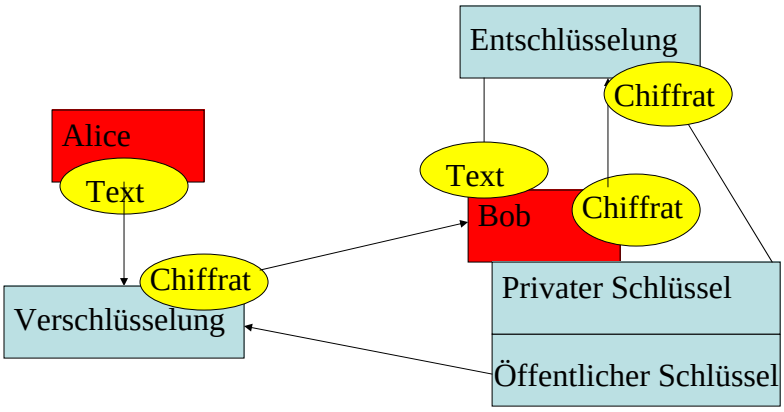
Fragestellung / Motivation

- Einsatz telematischer Methoden kann die Patientenversorgung verbessern
- Technische Mittel zur elektronischen Datenübertragung in weitem Umfeld vorhanden
- Es fehlen jedoch das Mittel zur „sicheren“ Übertragung entsprechend den gesetzlichen Vorschriften: eine Public-Key-Infrastruktur

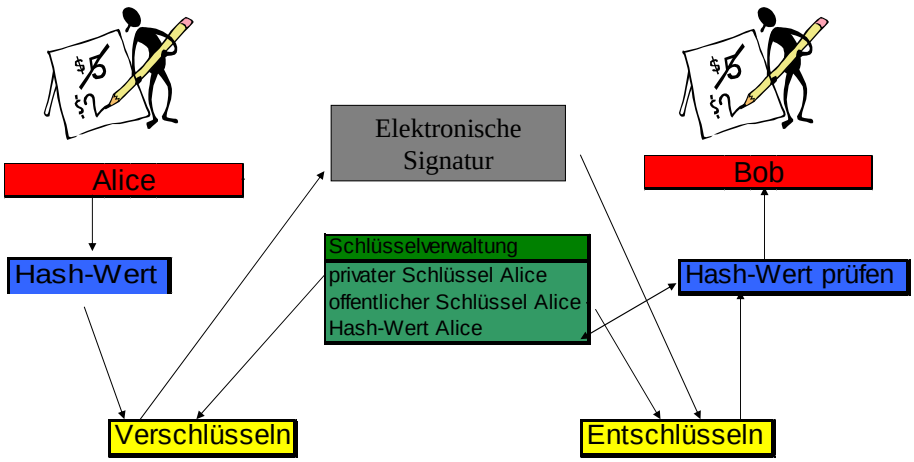
Warum PGP?

- PGP ist das weltweit am meisten genutzte Programm zur Verschlüsselung und zum Einsatz der elektronischen Signatur
- PGP nutzt als sicher anerkannte kryptographische Algorithmen
- PGP liegt als Open-Source vor und der Source-Code wurde von vielen Kryptologen untersucht
- PGP bietet die Mittel zum Aufbau einer PKI

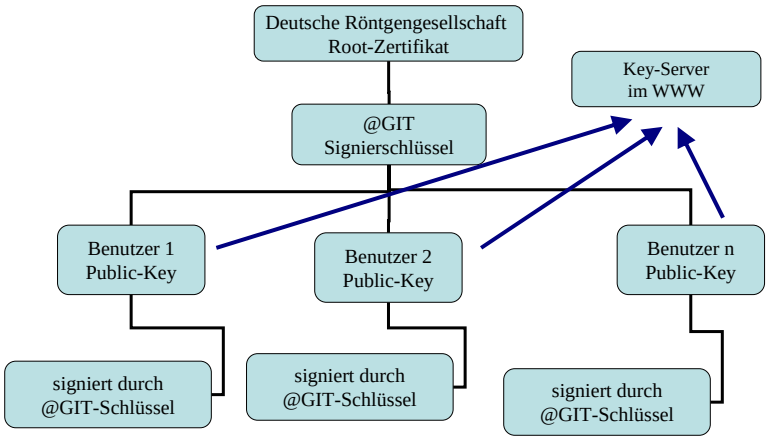
Verschlüsselung mit PGP



Signatur mit PGP



Erstellung einer PKI



Schlüsselerzeugung

- Entweder privat oder
- auf dem Stand der @GIT
- anschließend auf öffentlichen Keyserver abrufbar unter

http://www.tele-x-standard.de

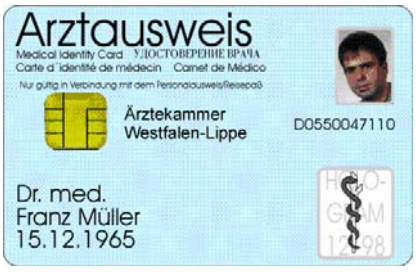
Anforderungen an eine Fortgeschrittene Signatur

1. die Signatur ist „ausschließlich dem Signaturschlüssel-Inhaber zugeordnet“,
2. sie wurde „mit Mitteln erzeugt“, „die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann“,
3. „die Identifizierung des Signaturschlüssel-Inhabers“ ist möglich und
4. die „Daten, auf die sie sich beziehen“, sind „so verknüpft..., dass eine nachträgliche Veränderung der Daten erkannt werden kann“

   ☞ D.h. die Schlüssel können zur Telemedizin verwendet werden !

Nur eine Interimslösung?

- Gute Lösung bis zur Einführung der HPC
- Nach Einführung der HPC immer noch wertvoll für die Kommunikation mit dem Ausland



- Wer kauft sich im Ausland einen deutsche HPC?
- Wer kauft sich ein entsprechendes Lesegerät?

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 (wann?) wertvolles Mittel zur Kommunikation mit Kollegen im Ausland
- DRG-signierte öffentliche Schlüssel vom Schlüsselserver im Internet abrufbar

Fragen?

Vielen Dank
für Ihre
Aufmerksamkeit!