Fachhochschule Dortmund
University of Applied Sciences

Ein Embedded System zur Digitalen Signatur nach dem DICOM-Standard

DICOM-Treffen, 05. Juli 2003 in Mainz

B. Schütze, M. Kroll, T. Geisbe, H.-G. Lipinski, T. J. Filler

Fachhochschule Dortmund
University of Applied Sciences

Sie erwartet im Folgenden

- Motivation
- Digitale Signatur
- DICOM-Signer: Konzept
- DICOM-Signer: eingesetzte Software
- DICOM-Signer: Einschränkungen
- Zusammenfassung

Fachhochschule Dortmund
University of Applied Sciences

Motivation

- Schutz der DICOM-Daten bei Übertragung im Netz
- Vorschrift zur digitalen Signatur nach RöV bei elektronischer Speicherung (§ 28 Abs. 5, § 43)
- Supplement 41 Umsetzung des DICOM-Standards

Fachhochschule Dortmund
University of Applied Sciences

Digitale Signatur (1)

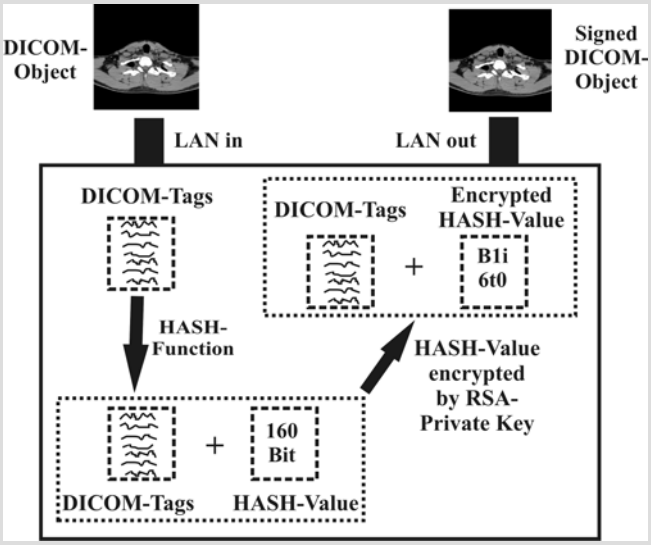
Eine elektronische Signatur wird dazu benutzt, um:

- die Unverfälschtheit eines elektronischen Dokumentes sicher zu überprüfen,
- den Unterzeichner eines elektronischen Dokumentes sicher zu identifizieren,
- sowohl die INTEGRITÄT eines elektronischen Dokumentes als auch die IDENTITÄT seines Unterzeichners über lange Zeiträume zu verifizieren.

Elektronische Signaturen stellen **nicht** die Vertraulichkeit sicher!

Fachhochschule Dortmund
University of Applied Sciences

Digitale Signatur (2)



Fachhochschule Dortmund
University of Applied Sciences

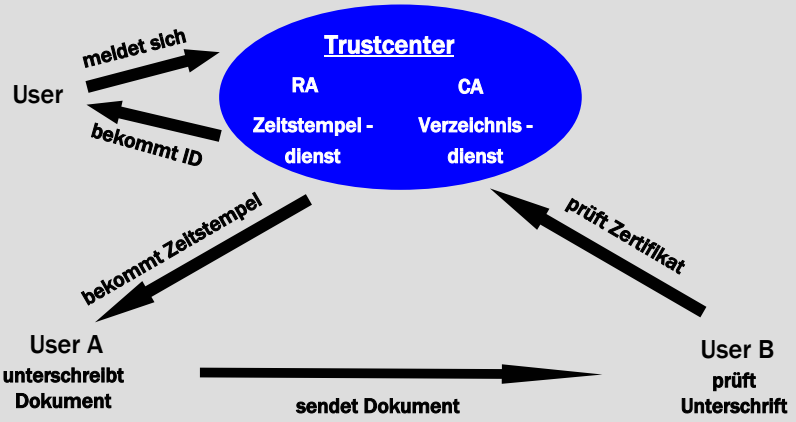
Digitale Signatur (3)

Der DICOM-Standard verwendet:

- Zur HASH-Bildung MD5, RipeMD-160, SHA1
- RSA zwecks Verschlüsselung des Hashwertes
- X.509-Zertifikate, die den Public-Key enthalten und dem DICOM-Objekt hinzugefügt werden

Fachhochschule Dortmund
University of Applied Sciences

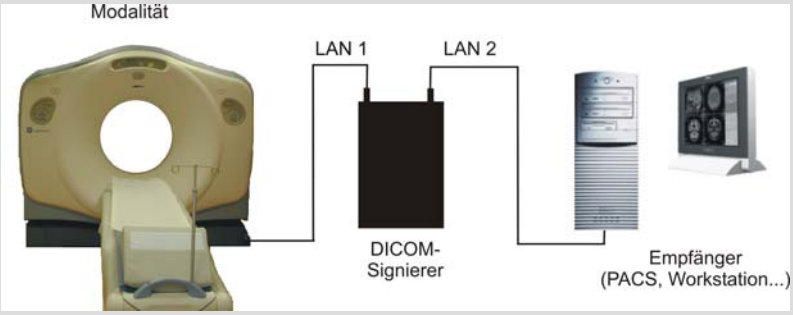
Public-Key-Infrastruktur



Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: Grundidee

- LAN-Port 1
  - Empfang der DICOM-Daten zur Signierung
  - FTP- und Telnet-Server zur Systemkonfiguration
- LAN-Port2
  - Verbindung zum eigentlichen Empfänger



Fachhochschule Dortmund
University of Applied Sciences

Hardware

- Embedded Board
  - Pentium
  - 512MB RAM
  - 2 LAN Schnittstelle
  - 20GB Festplatte
- Gehäuse
  - 20x20x9cm
- Betriebssystem
  - Windows XP Embedded
  - ~100MB HD (komplett)

Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: Software

- Java 2 Standard Edition v1.4.1
- Open Source DICOM Toolkit dcm4che
  - unterstützt das Auslesen der Informationen eines DICOM-Bildes, das Schreiben von DICOM-Bildern und das DICOM-Netzwerk-Protokoll
- Open Source Crypto Package Bouncycastle
  - Unterstützt das Auslesen eines X.509-Zertifikates sowie die Algorithmen RIPEMD160 und RSA

Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: LAN-Software

Netzwerk-Schnittstelle 1 unterstützt

- einen **FTP-Server** für Aktualisierungen
  - des x.509-Zertifikates
  - der Konfigurationsdateien
    - ➔Zu signierende Elemente
    - ➔AE Titles des Sender und des Empfängers
    - ➔Bildeingangs- und Ausgangs-Verzeichnisse
- einen **Telnet-Server** zur System-Administration
  - Auslesen von Logfiles
  - Analyse und (Re-)Konfiguration des Betriebsystems bzw des Signers

Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: Struktur

- **Receiver**
  - Nimmt Bilddaten entgegen und legt sie in ein Verzeichnis ab
- **Signer**
  - Überprüft die Bilddaten
  - Signiert die Bilddaten
  - Legt die signierten Bilddaten in das Ausgangsverzeichnis ab
- **Sender**
  - Verschickt die Bilddaten aus dem Ausgangsverzeichnis zum Empfänger

Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: Umfang

- Der DICOM-Signer unterstützt
  - SOP Class UID
    - ➔CTImageStorage
    - ➔MRImageStorage
- Zur Erzeugung einer Signatur sind zur Zeit folgende DICOM Datentypen erfolgreich getestet
  - AS, AT, CS, DA, DS, DT, IS, OW, PN, SH, TM, UI, US

Fachhochschule Dortmund
University of Applied Sciences

DICOM-Signer: to do

- Erweiterung der DICOM-Funktionalität
- Gründliche Testszenarien
  - Überprüfen aller DICOM Datentypen
  - Verhalten von Betrachtungssoftware
  - Drucken signierter DICOM-Daten
- Portierung nach Red Hat Embedded Linux
- Minimierung des OS auf 64 MB (Flash-Karte)
- Erstellen einer Dokumentation
- Unterstützung weiterer SOP-Klassen

Fachhochschule Dortmund
University of Applied Sciences

Zusammenfassung

- Digitale Daten müssen bei der Übertragung in Netzwerken geschützt werden.
- Nach RöV müssen in der Teleradiologie die zu übertragenden Daten signiert werden.
- Nach RöV elektronisch gespeicherte Daten müssen ebenfalls digital signiert werden.
- Der DICOM-Standard bietet die Möglichkeiten zur digitalen Signatur.
- Auch ältere Modalitäten können mit der hier vorgestellten Lösung um die Möglichkeit der Signierung erweitert werden.

Fachhochschule Dortmund
University of Applied Sciences

Vielen Dank
für Ihre
Aufmerksamkeit!

Kontakt: (schuetze, kroll@medizin-informatik.org)