UniversitätsKlinikum Heidelberg

Der ArchiSig-Prototyp –

6 Jahre Erfahrung mit der Integration der Elektronischen Signatur in ein rechnerunterstütztes Klinikuminformationssystem

conhIT 2010 – Satellitenveranstaltung GMDS/BVMI
Berlin, 19.4.2010

Antje Brandner
Sektion Medizinische Informationssysteme
Zentrum für Informations- und Medizintechnik (ZIM)

Agenda

- Problemstellung
- Historie: Projekt ArchiSig
  - Ausgangsproblematik
  - Konzepte
- ArchiSig-Prototyp
  - Systemarchitektur
  - Signaturintegration in i.s.h.med
  - Evaluationen
- Betrieb des Prototyps
  - Erfahrungen und Erkenntnisse

Problemstellung

- Immense Datenvolumina (ca. 6-7 Mio. neue Dokumente pro Jahr, aktuell ca. 11 Mio. Seiten)
- Unterschriftsrelevanz von ca. 60%
- Aufbewahrungsfristen von 30 Jahren und mehr
- Zunehmend elektronisch erzeugte Dokumente
- Begrenzte Beweiskraft elektronischer Dokumente
- Konventionelle und elektronische Archivierung

Bieten elektronische Signaturen Rechtssicherheit bei der elektronischen Archivierung?

Projekt „ArchiSig“

- Projekt: ArchiSig - Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente
- Programm: VERNET – Sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen
- Projektförderung: Bundesministerium für Wirtschaft und Technologie (BMWi)
- Projektlaufzeit: Juli 2001 - Dezember 2003
- Konsortium: Interdisziplinäres Team aus Wissenschaft, Industrie und Anwendern

Universitätsklinikum Heidelberg | Fraunhofer Gesellschaft Darmstadt | Universität Kassel | Niedersächsische Staatskanzlei | IXOS Software AG Grasbrunn / München | SECUDE Sicherheitstechnologie Informationssysteme, Darmstadt | DATEV eG Nürnberg | PERGIS Systemhaus GmbH Ludwigshafen

Probleme der Langzeitsicherheit el. Signaturen

- Sicherung der Authentizität
  - Zeitlich begrenzte Prüfbarkeit der Zertifikate
  - Dokumentation, Gültigkeitsabfragen und Sperrlisten nicht mehr verfügbar
    - Nach 5 Jahren bei qualifizierten ZDA (bei Einstellung der Zertifizierungsdienste früher)
    - Nach 30 Jahren bei akkreditierten ZDA

  Rechtzeitige Einholung und Speicherung notwendiger Verifikationsdaten
- Sicherung der Integrität
  - Nachlassende Sicherheit der Verschlüsselungs-Algorithmen oder deren Parameter
  - Nachlassende Sicherheit der Hash-Algorithmen

  Signaturerneuerung = Erzeugung erneuter Signaturen

Einholung und Speicherung von Verifikationsdaten

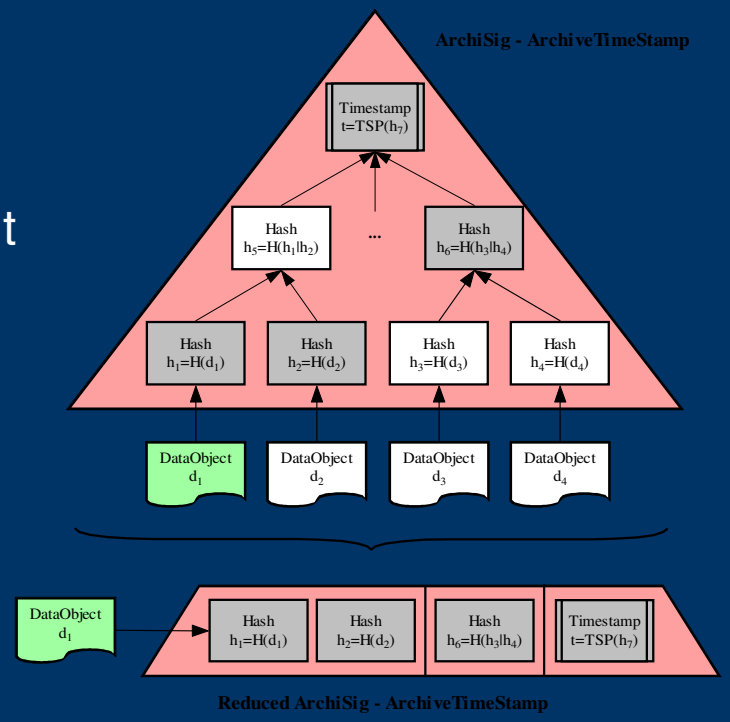
- Welche Verifikationsdaten?
  - Qualifizierte Zertifikate des Benutzers, des ZDAs und der Wurzelinstanz
  - Qualifizierter Zeitstempel mit Zertifikaten als Nachweis des Signaturzeitpunktes
  - Gültigkeitsabfrage zum Benutzerzertifikat mit Zertifikaten
- Einholung der Verifikationsdaten vor der Archivierung des signierten Dokumentes
- Speicherung der Verifikationsdaten im signierten Dokument selbst
  - Ständige Verfügbarkeit
  - Langfristige Sicherung durch Signaturerneuerung

Anforderungen an die Signaturerneuerungen

- Rechtliche Anforderungen
  - Erneute Signatur ist ein Sicherungsmittel und keine Willenserklärung
  - Sicherheitseignung der Algorithmen gemäß Veröffentlichungen der BNetzA
  - Rechtzeitige Signaturerneuerung mit sicheren Algorithmen
  - Signaturerneuerung durch qualifizierten Zeitstempel mit qualifizierter elektronischer Signatur
  - Erneuerung der Signaturen bei sicherem Hash-Algorithmus ausreichend
  - Erneute Signatur muss alle Signaturen und kann viele Dokumente umfassen
- Anwendungsorientierte Anforderungen
  - Effizienz und Wirtschaftlichkeit
  - Allgemeine, formatunabhängige Anwendbarkeit
  - Datenschutzkonformität

Konzept zur Signaturerneuerung (I)

- Signaturerneuerung durch Archivzeitstempel
  - Archivzeitstempel für viele Dokumente = Hashwertbaum (Merkle) + Zeitstempel mit qualifizierter Signatur
  - Reduzierter Archivzeitstempel = Erneute Signatur
  - Zentrale Speicherung und Erneuerung
  - Anforderung bei Verifikation des signierten Dokumentes



Konzept zur Signaturerneuerung (II)

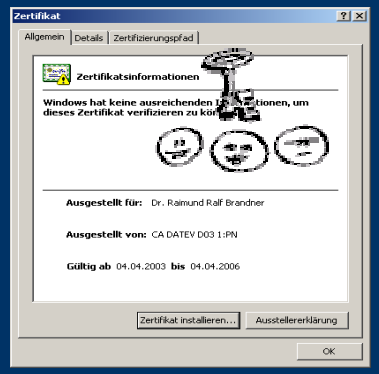
- Initiale Archivzeitstempelung
  - Erzeugung von Hashwerten bei der Archivierung der Dokumente und Bildung eines Archivzeitstempels
  - Bewertung der Sicherheitseignung kryptographischer Algorithmen durch das Archivsystem ist gegeben
- Zeitstempel-Erneuerung
  - Notwendig bevor kryptographische Algorithmen im Zeitstempel unsicher werden
  - Für betroffene Archivzeitstempel Zeitstempel hashen und erneuten Archivzeitstempel bilden
  - Kein Zugriff auf die archivierten Dokumente selbst
- Hashbaum-Erneuerung
  - Notwendig bevor Hash-Algorithmus im Hashwertbaum unsicher wird
  - Für betroffene Archivzeitstempel archivierte Dokumente und reduzierte Archivzeitstempel hashen und erneuten Archivzeitstempel bilden

Agenda

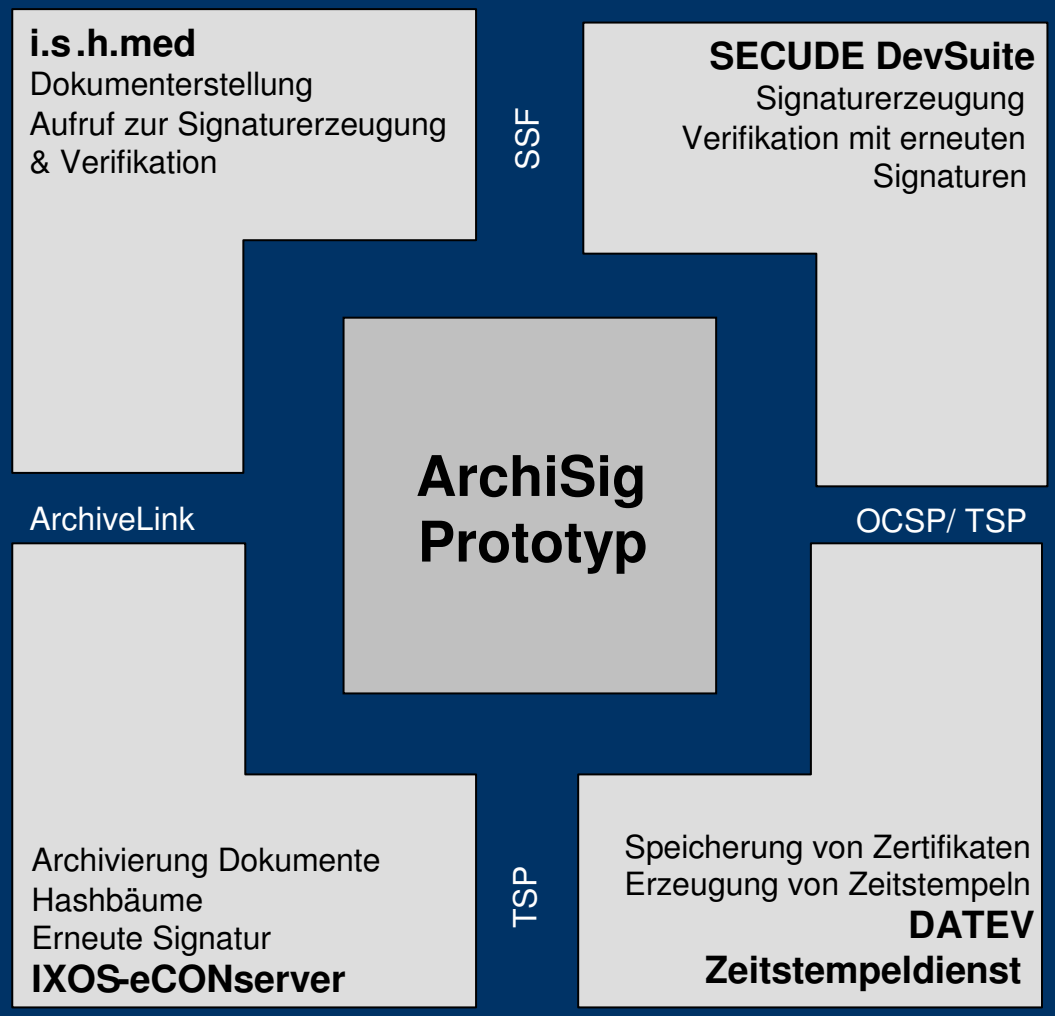
- Problemstellung
- Historie: Projekt ArchiSig
  - Ausgangsproblematik
  - Konzepte
- ArchiSig-Prototyp
  - Systemarchitektur
  - Signaturintegration in i.s.h.med
  - Evaluationen
- Betrieb des Prototyps
  - Erfahrungen und Erkenntnisse

Public Key Infrastruktur (PKI)

- Zertifizierungsdiensteanbieter (ZDA)
  - Ausstellung von Zertifikaten
    - Identifizierung und Registrierung
    - Namensgebung und Zertifizierung
    - Verzeichnisdienst und Sperrdienst
  - Ausstellung von Zeitstempeln
- Signaturerstellungseinheiten
  - Sichere Speicherung und Anwendung des privaten Schlüssels
  - z.B. Smartcard
- Signaturanwendungskomponenten
  - Daten der Signaturerzeugung oder -verifikation zuführen
  - Signaturen oder Zertifikate überprüfen sowie Prüfergebnisse anzeigen

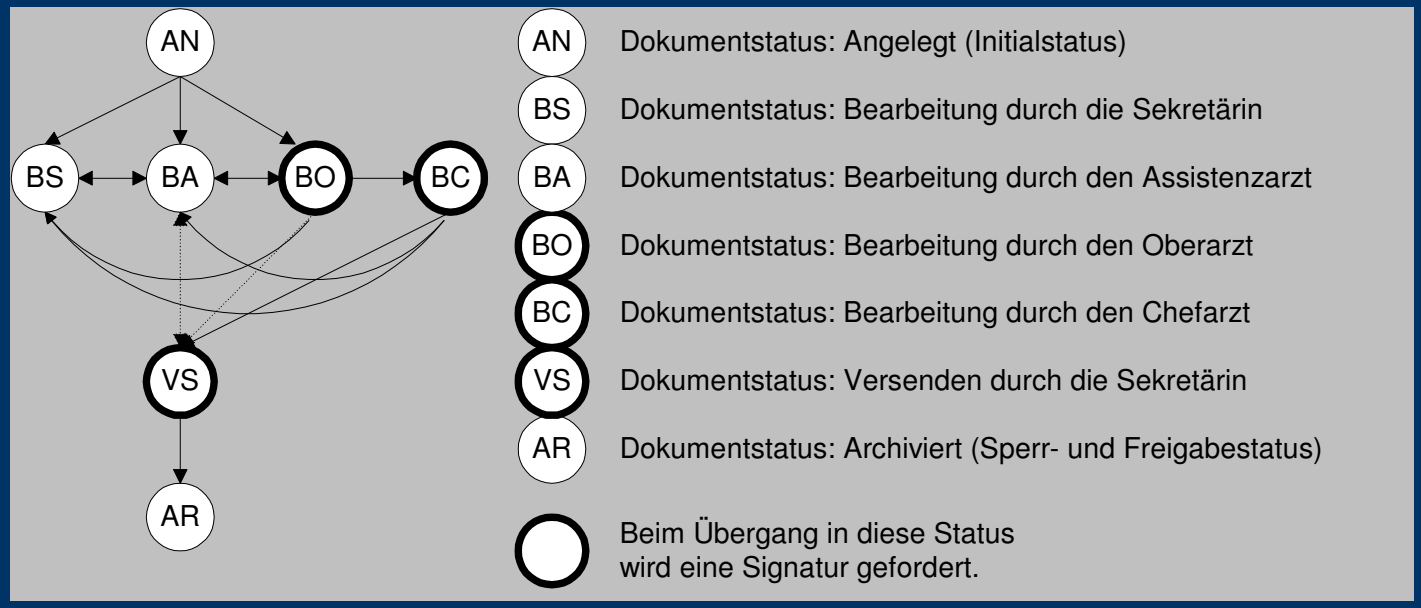


Systemarchitektur des ArchiSig-Prototyps



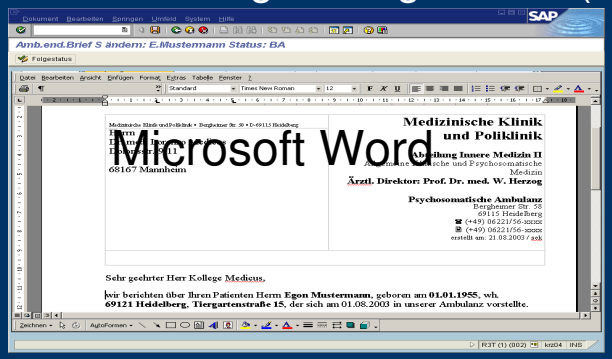
Signaturintegration in i.s.h.med (I)

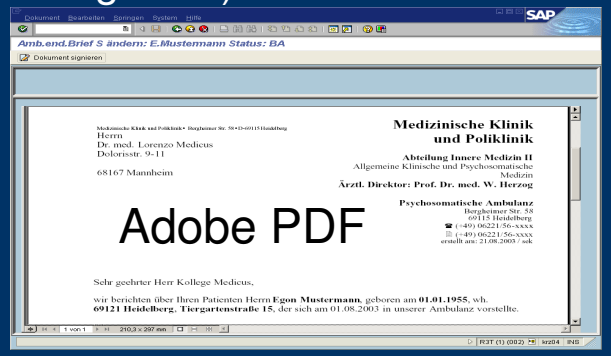
- Anwendungsszenario Arztbriefschreibung
  - Narrativer Text (Word-Container)
  - Zugriff über Sichttyp Dokumente des klinischen Arbeitsplatzes
  - Dokumentselektion über Dokumentstatus, Organisationseinheit, Dokumenttyp und Dokumentdatum



Signaturintegration in i.s.h.med (II)

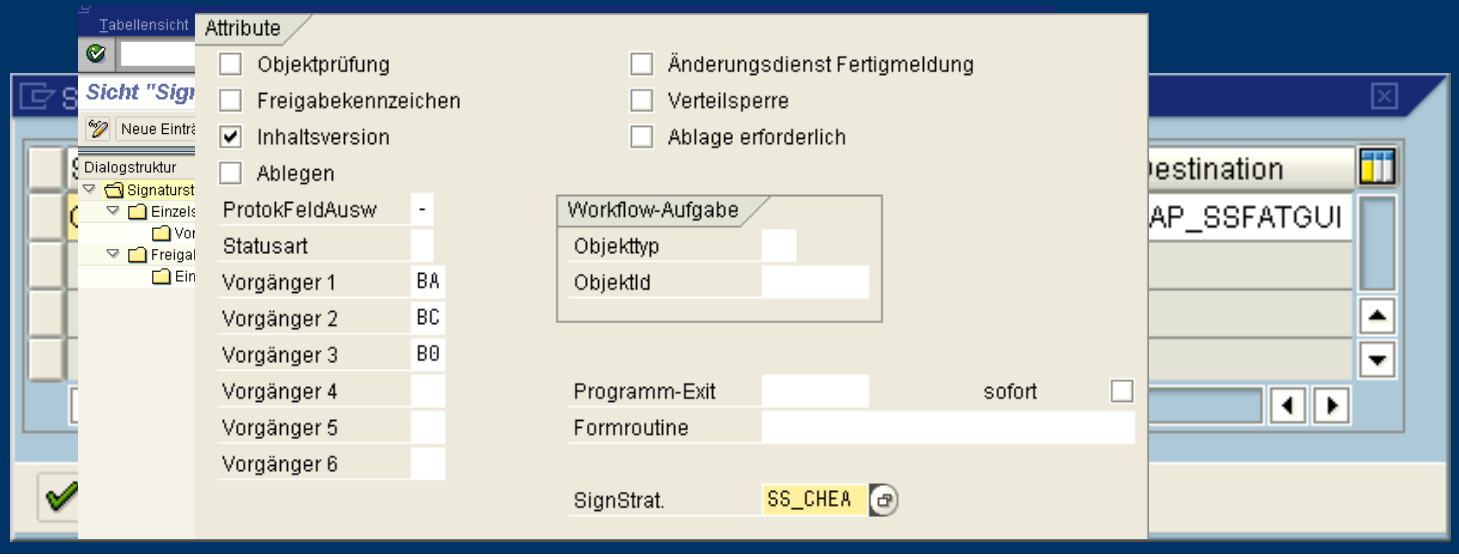
- Erweitertes Dokumentenmanagement
  - Signaturerzeugung beim Dokumentstatus-Übergang
  - Source-Dokument (Word, PD)
    - Änderungen
    - Copy&Paste
    - Gewohntes Look&Feel
  - Zusätzliches Signatur-Dokument (PDF)
    - Eindeutige Präsentation über lange Zeiträume
    - Konvertierung aus Source-Dokument vor der ersten Signatur
    - Visualisierung der Signaturen (Namen, Prüfergebnis)





Signaturintegration in i.s.h.med (III)

- Customizing
  - Benutzerverwaltung:
    - Zuordnung Benutzername – Zertifikatsinhaber, Signaturerstellungseinheit
  - Definition von Signaturstrategien:
    - Aufforderung zur Einzelsignatur
    - Überprüfung geforderter (Mehrfach-) Signaturen
  - Definition der Dokumentart (Dokumentstatus)
    - Zuordnung Dokumentstatus – Signaturstrategie



Signatur der Arztbriefe in i.s.h.med

Dokument Bearbeiten Springen System Hilfe

Amb.end.Brief S E.Mustermann Stat

Folgestatus

Name: Assistenzarzt Organisation: Universitaetsklinikum Heidelberg Org.einheit: Testbenutzer Signiert am: 09-09-2003 18:15:29

Medizinische Klinik und Poliklinik • Bergheimer Str. 58 • D-69115 Heidelberg

Herrn
Dr. med. Lorenzo Medicus
Dolorisstr. 9-11

68167 Mannheim

Folgestatus

Abkz	Statustext	SA	Frg
AR	Archiviert	A	X
BS	Bearb.Sekretärin		

Sehr geehrter Herr Kollege Medicus,

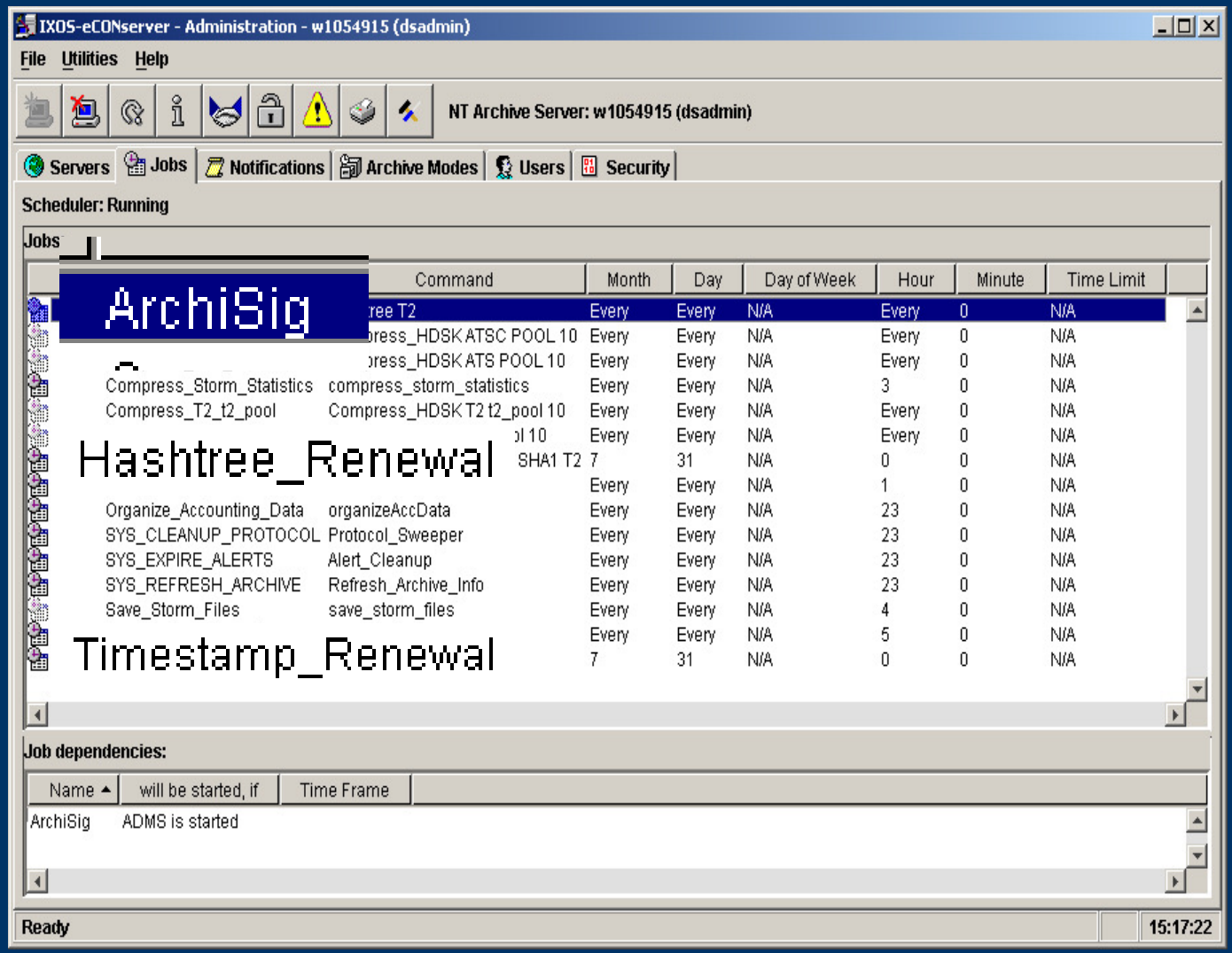
wir berichten über Ihren Patienten Herrn **Egon Mustermann**, geboren am **01.01.1955**, wh. **69121 Heidelberg**, **Tiergartenstraße 15**, der sich am 01.08.2003 in unserer Ambulanz vorstellte.

Diagnosen:

1 von 1 210,3 x 297 mm

R3T (1) (002) krz04 INS

Signaturerneuerung im eCONserver



Evaluation zur Rechtssicherheit

- Simulationsstudie zur Rechtssicherheit der ArchiSig-Konzepte
  - Sachverständige Testpersonen (Unabhängige Anwälte, Richter und Sachverständige)
  - erprobten Prototyptechnik (Signierte Dokumente, ArchiSig-Archivsystem, Secude-Viewer)
  - anhand 12 nachgestellter Fälle (Simulierte elektronische Akten, simulierte Prozesse)
  - an ihren Arbeitsplätzen (Vorbereitung der Verhandlung per Mail, echte Verhandlung)
  - unter wissenschaftlicher Beobachtung (Protokolle, Interviews, Beobachtung, Aktenauswertung)

ArchiSig-Dokumente erhalten den Anscheinsbeweis des § 292a ZPO für die Echtheit des Dokuments (mittlerweile gilt 371 ZPO)

Sonst freie Beweiswürdigung mit Hilfe von Indizien – unterschiedliche Ergebnisse, keine Rechtssicherheit

Evaluation zur Wirtschaftlichkeit

- Universitätsklinikum Heidelberg
  - 7.000.000 Dokumente pro Jahr
  - 60% sind unterschriftsrelevant: 4.200.000 Dokumente
- Staatskanzlei Niedersachen
  - 200.000.000 Dokumente pro Jahr
  - 1 % unterschrifts-relevant: 2.000.000 Dokumente
- Signaturerneuerung nach herkömmlichen Konzepten
  - Heidelberg: **4.200.000 Dok. * 0,30 € = 1.260.000 €**
  - Niedersachsen: **2.000.000 Dok. * 0,30 € = 600.000 €**
- Signaturerneuerung nach ArchiSig-Konzept
  - Heidelberg (1 ZS pro 1.000 Dok.:) **4.200 * 0,30 € = 1.260 €**
  - Niedersachsen (1x pro Tag) **360 Zeitstempel * 0,30 € = 108 €**

Evaluation zur Anwendbarkeit in der klinischen Routine

- Interventionsstudie zur Anwendbarkeit des Prototypen im Rahmen der Arztbriefschreibung
  - Assistenz-, Ober- und Chefärzte der Medizinischen Universitätsklinik Heidelberg
  - signierten seit August 2003 (zunächst geplant bis September 2003)
  - vorläufige und endgültige Arztbriefe
  - in 2 stationären und 2 ambulanten Bereichen
- Datenanalysen und Benutzerbefragungen zeigten:

  Vollständig elektronische Arztbriefschreibung mit Signatur verkürzt die mittlere Erstellungsdauer von 37 auf 16 Tage bei endgültigen Briefen

  Benutzerzufriedenheit und Weiterführung des Prototyps

Agenda

- Problemstellung
- Historie: Projekt ArchiSig
  - Ausgangsproblematik
  - Konzepte
- ArchiSig-Prototyp
  - Systemarchitektur
  - Signaturintegration in i.s.h.med
  - Evaluationen
- Betrieb des Prototyps
  - Erfahrungen und Erkenntnisse

Weiterführung des Prototyps

- die Ärzte:
  - „die Organisationsunterstützung hilft uns, wir machen weiter“
  - „wenn der HBA kommt müssen wir ja eh signieren“
- die IT:
  - „bis der HBA mit qualifizierten elektronischen Signaturen kommt“
  - „bis wir eine Lösung in Standardprodukten haben“
- der Software-Hersteller:
  - „wir arbeiten an einer Lösung“

Prototyp: Umfang / in Zahlen

- Erweiterung auf 5 stationäre und 5 ambulante Bereiche
- Insgesamt 14.000 elektronisch signierte Briefe:
  - ca. 10.000 endgültige Arztbriefe (mit 3 Signaturen)
  - über 4.000 vorläufige Arztbriefe (mit 1 Signatur)
- Zertifikate wurden für 81 Mitarbeiter ausgestellt
  - Für 22 Mitarbeiter wurden 2 oder mehr Zertifikate ausgestellt, davon waren
    - 10 neue Zertifikate wegen Ablauf des 1. Zertifikats
    - 2 Namenswechsel
    - 10 aufgrund neuer Mitarbeiterausweise (Verlust der Karte, Defekt)

Betrieb des Prototyps

- Problematische Release- und Patchwechsel von IS*H und i.s.h.med
  - Programmierung nutze Komponenten der SAP-Basis, Standardmodifikationen in IS*H und i.s.h.med waren notwendig
- Probleme bei Updates genutzter Komponenten
  - z.B. auseinanderlaufende Versionen von Acrobat + Reader, neue Treiber für Lesegeräte
  - Umstellung von Windows 2000 auf XP
- Support der Firmen, Lizenzen…

Ende des ArchiSig-Prototyps

- Gründe für die Einstellung des Prototyps:
  - Genutzte Algorithmen wurden unsicher:
    - Signaturalgorithmus: RSA 1024 (geeignet bis Ende 3/2008)
    - Hashalgorithmus: SHA-1
  - Die Chips auf den Mitarbeiterausweisen unterstützten keine 2048 Bit Schlüssel
  - Die Software zum Ausstellen der Zertifikate konnte nicht mit neuen Chips umgehen
  - Anpassungen in der Software und ggf. auch bei der Hardware (Lesegeräte) wären dazu gekommen

Ende des ArchiSig-Prototyps

- Sollte man nicht auf „richtige“, d.h. qualifizierte Zertifikate, umsteigen?
  - Zur Erinnerung: die selbst erstellte PKI war für einen Test-Zeitraum des Prototyps über 6-8 Wochen gedacht
  - Wie ändert sich die Organisation, wenn die Zertifikate nicht mehr selbst erstellt werden?
  - Braucht dann noch jeder Arzt eine qualifizierte Signaturkarte?
  - Gibt es noch weitere organisatorische Änderungen?
- Sollte man dann nicht auf ein im Standard unterstütztes Produkt umsteigen?
  - Das war dort noch nicht enthalten: ggf. im übernächsten Enhancement-Package?
- Wie weit ist die Umsetzung der Signaturerneuerung im neuen Archivsystem?

Ende des ArchiSig-Prototyps

Ein neues Projekt…

Resümee

- Elektronische Dokumente können durch qualifizierte elektronische Signaturen rechtssicher, effizient und kostengünstig archiviert werden
- Umsetzung der Konzepte in Standardprodukten
  - Signaturerneuerung in Archivsystemen
  - Signaturerzeugung im KIS ?
- Aufbau der PKI ?
- Aktivitäten des CCESigG
  - Empfehlungen: welche Dokumente sollten mittels elektronischer Signaturen gesichert werden
  - Wie kann die Einbindung in klinische Prozesse aussehen?

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
antje.brandner@med.uni-heidelberg.de