Elektronische Signaturen im Rahmen der intersektoralen Kommunikation

TELEMED 2015 - 20. Nationales Forum für Gesundheitstelematik und Telemedizin

am 23. und 24. Juni 2015
in der Vertretung des Landes Nordrhein-Westfalen beim Bund
Hiroshimastraße 12 - 16, D-10785 Berlin

Prof. Dr. Paul Schmücker
Hochschule Mannheim, Fakultät für Informatik
Institut für Medizinische Informatik

Inhaltsverzeichnis

1. Einführung

Registratur:
Ort zur Aufbewahrung von Akten, auf die gegebenenfalls nochmals zugegriffen werden muss

Archiv:
Einrichtung zur systematischen Erfassung, Erhaltung und Betreuung von Schriftgut über lange Zeiträume sowie der Raum für dessen Aufbewahrung

Das bedeutet, dass Krankenhäuser Registraturen und keine Archive besitzen.

Digitales Archiv:

Ansammlung von elektronischen Dokumenten und sonstigen elektronischen Objekten auf einem digitalen Speichermedium

Voraussetzung: ordnungsgemäße, revisionssichere und beweiskräftige Aufbewahrung über einen vorgegebenen Zeitraum

Werkzeuge zum Ablegen, Wiederauffinden und Präsentieren von Daten, Dokumenten, Bildern etc. erforderlich; Inhalte verbunden durch Patientenidentifikation

2. Elektronische Signaturen - Stand der Einführung und aktuelle Entwicklungen

- Wie kann ich digital erzeugte Dokumente beweissicher erstellen, weiterleiten und aufbewahren?
- Wie tausche ich Informationen einrichtungsübergreifend beweissicher aus?
- Welchen Anforderungen muss man gerecht werden, um gescannte Dokumente möglichst beweissicher aufzu-bewahren?
- Wie gewährleistet man die IT-Sicherheit?

Beweissicherheit von elektronischen Dokumenten

vier Szenarien im Rahmen der Beweissicherheit von Dokumenten:

A. konventionelle Dokumente
B. digital erzeugte Dokumente ohne Signaturen
C. digital erzeugte und signierte Dokumente
   - Lösung: Integration der digitalen Signatur in das rechner-unterstützte Krankenhausinformationssystem analog Verbundprojekt ArchiSig
   - 02. März 2009: Gründung des Competence Center für die Elektronische Signatur im Gesundheitswesen (CCESigG)
D. Mikrokopien und gescannte Dokumente

Arten von Signaturen

- Signatur: persönliche Bestätigung der Echtheit eines Dokumentes und der in diesem dokumentierten Willensäußerung, Voraussetzungen: Signaturkarte, Kartenleser, Signatur-Software, PIN, Zertifizierungs-diensteanbieter
- Zeitstempel: Bestätigung durch einen Zertifizierungs-diensteanbieter, dass ein digitales Objekt zu einem bestimmten Zeitpunkt ein bestimmtes Aussehen hatte

„Einfache“ elektronische Signaturen
- Ziel: Authentisierung elektronischer Daten (Authentizität)
- Keine technischen Anforderungen

„Fortgeschrittene“ elektronische Signaturen
- Ziel: Änderungen elektronischer Daten erkennen (Integrität)
- Kaum technische Anforderungen

„Qualifizierte“ elektronische Signaturen
- Ziel: Äquivalent zur handschriftlichen Unterschrift
- Zertifizierungsdiensteanbieter (ZDA): Betriebsanzeige
- Technischen Komponenten: Herstellererklärung

„Akkreditierte“ elektronische Signaturen
- Ziel: Höchste Sicherheit
- Zertifizierungsdiensteanbieter (ZDA): Akkreditierung
- Technischen Komponenten: Prüfung und Bestätigung

IT-Report Gesundheitswesen 2011

Elektronische Signaturen in Krankenhäusern

- 5% Einsatz von Signaturen
- 11% Einsatz von elektronischen Signaturen in Vorbereitung
- 25% Einsatz von elektronischen Signaturen geplant
- 41% Einsatz von elektronischen Signaturen nicht geplant
- 18% keine Angabe

Hübner et al. 2012
Hochschule Osnabrück

3. Problemstellungen bei der Einführung digitaler Signaturen

- Kryptographische Algorithmen können mit der Zeit ihre Sicherheitseignung verlieren.
- Zeitlich begrenzte Prüfbarkeit und Verfügbarkeit von qualifizierten Zertifikaten
  - **5 Jahre bei nicht akkreditierten Zertifizierungsdiensteanbietern**
  - **30 Jahre bei akkreditierten Zertifizierungsdiensteanbietern**
- Informationen zur Sicherheitseignung der Algorithmen liegen nicht in digitaler Form vor.
- Transformation in andere Dokumentenformate oder -träger führt zur Ungültigkeit der ursprünglichen Signaturen.

 Elektronisch signierte Dokumente können im Laufe der Zeit an Beweiswert verlieren

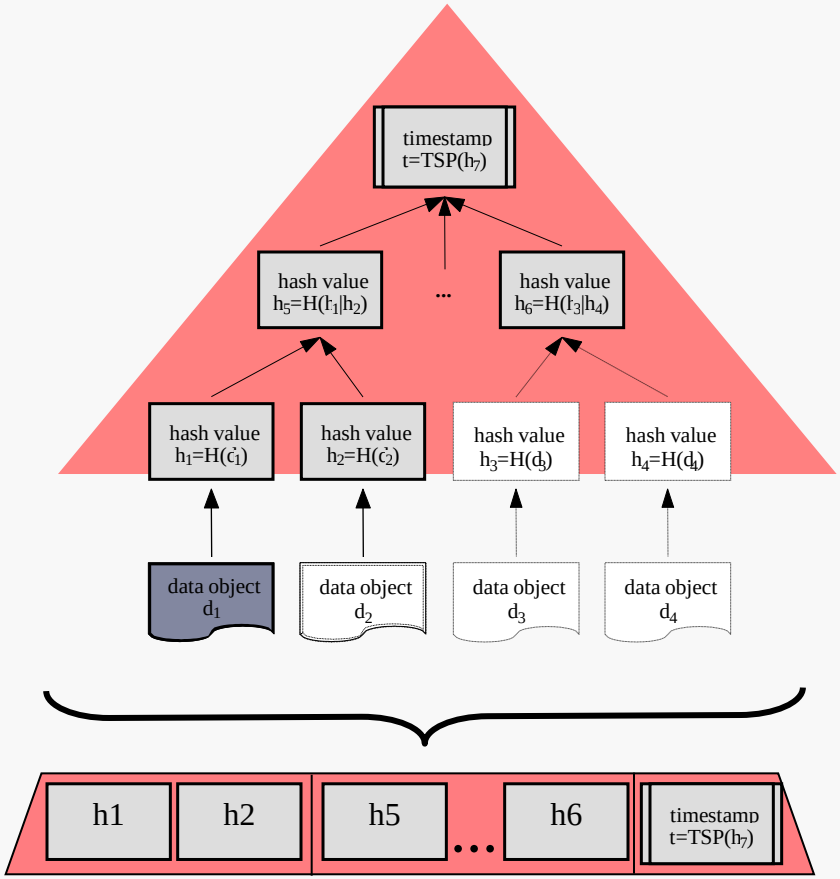
ArchiSig - Archivzeitstempel

Zeitstempel für viele Datenobjekte

- Hashtree (Merkle) + akkreditierter Zeitstempel
- reduzierbar zu Liste = erneute Signatur

Eigenschaften

- signaturgesetzkonform: Zeitstempel mit akkreditierter Signatur
- wirtschaftlich: ein Zeitstempel für viele Datenobjekte
- datenschutzkonform: Löschung von Datenobjekten möglich



Braunschweiger Regeln von CCESigG e.V.

- Verwendung archivgerechter Dateiformate (z.B. PDF/A) und akkreditierter Signaturen und Zeitstempel
- akkreditierte Signatur originär elektronischer Dokumente, für die gesetzliche Regelungen eine Schriftform erfordern
- akkreditierte Signatur für Dokumente zur externen Verwendung und für interne Dokumente mit besonders hohem Beweiswert
- akkreditierter Zeitstempel für die Dokumente externer Einsender
- geeignetes Authentifizierungsverfahren für alle sonstigen Dokumente

BSI TR 03125 - Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur vertrauens-würdigen elektronischen Langzeitspeicherung (TR-VELS)

- Spezifikation und Fortschreibung anwendungsübergreifender Anforderungen für die langfristige, rechts- und revisionssichere Aufbewahrung elektronischer Dokumente
- dafür Auswahl und adäquater Einsatz geeigneter Sicherungsmittel
- Entwicklung einer hersteller- und produktunabhängigen Referenzarchitektur mit Definition sicherheitstechnischer Mindestanforderungen an Systeme, Komponenten und Schnittstellen sowie im Zusammenspiel

4. Rechtssicheres ersetzendes Scannen

Gegenstand: Rechtssicheres ersetzendes Scannen von Papierdokumenten

Autoren: Heino Kuhlemann (Schliersee), Prof. Dr. Paul Schmücker (Mannheim), Dr. Carl Dujat (Erkelenz), Volkmar Eder (Tübingen);

Regelungen für das ersetzende Scannen:
Sozialversicherungen, siehe § 110a Abs. 2 Satz 1 SGB IV
Handelsgesetzbuch, siehe §§ 239 Abs. 4 und 257 Abs. 3 HGB
Röntgenbilder und sonstige Aufzeichnungen, siehe § 28 Abs. 4 RöntgenVO

Regelungen für alle Branchen wünschenswert

ansonsten technische und organisatorische Maßnahmen zur Sicherstellung einer hohen Beweissicherheit von gescannten Dokumenten erforderlich

siehe www.informatik.hs-mannheim.de/aku

Lebenszyklen gescannter Dokumente

Phase 1: Erstellen eines digitalen Dokumentes, Ausdruck, Unterschrift Medienwechsel

Phase 2: Aufbewahrung der konventionellen Dokumente

Phase 3: Scannen, Indexieren, Signieren und Vernichten des Papiers

Phase 4: Aufbewahren der gescannten Dokumente

Phase 5: Vernichten des digitalen Dokuments

Problem: *Vernichtete Papierdokumente können nicht mehr auf Echt- und Unversehrtheit überprüft werden.*

Technische BSI-Richtlinie RESISCAN

Entwicklung einer Technischen Richtlinie RESISCAN zum rechtssicheren dokumentenersetzenden Scannen durch das Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Ziel: Spezifikation der Qualitätsanforderungen an die Scanprozesse für die angestrebte Rechts- und Beweissicherheit sowie Erarbeitung eines Konzeptes und Überprüfung auf Praxistauglichkeit

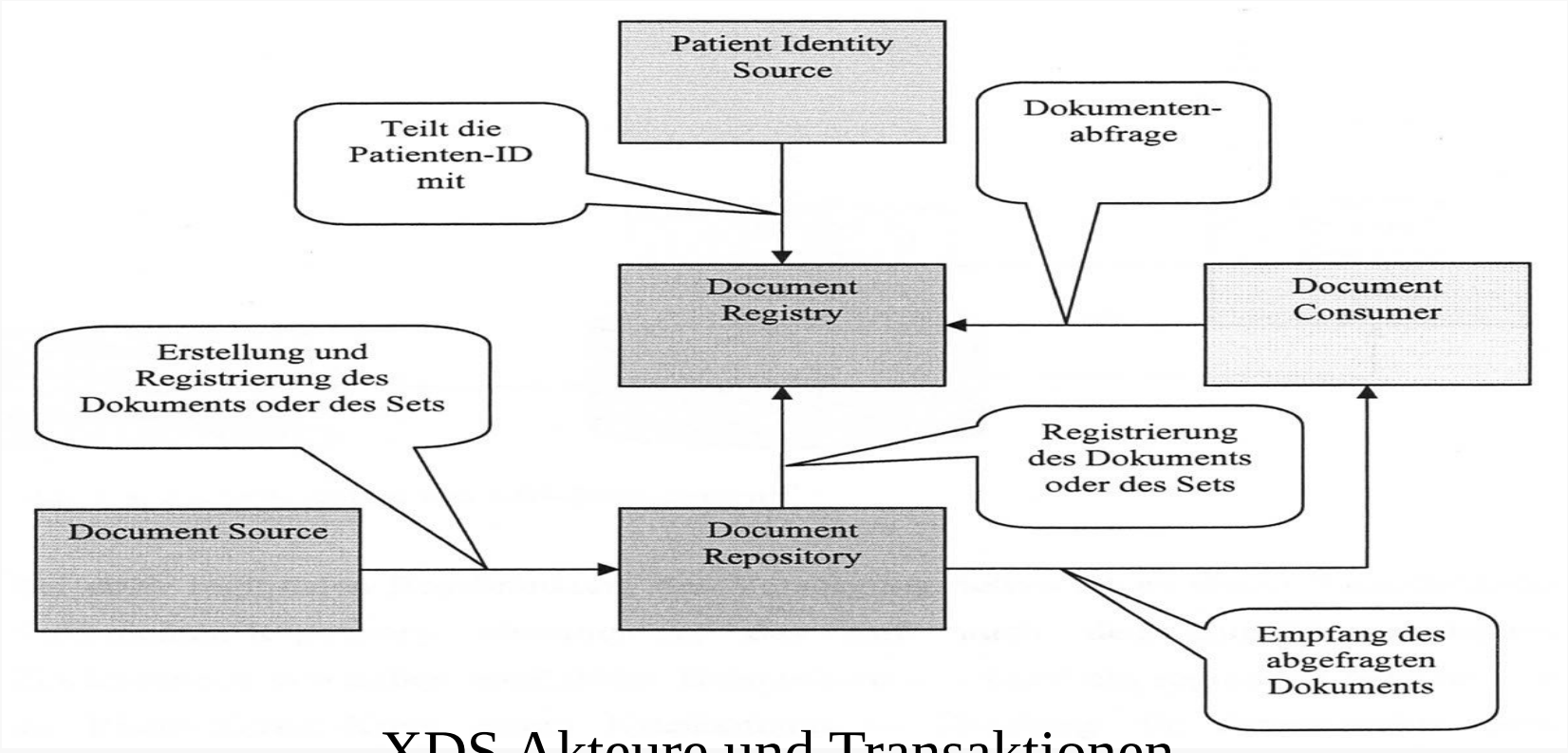
Die rechtliche Zulässigkeit des ersetzenden Scannens ist nicht Gegenstand der Richtlinie.

Veröffentlichung der Technischen BSI-Richtlinie: Februar 2013

5. Innovative elektronische Aktensysteme

ECM-basierte Aktensysteme auf Basis von IHE

- ECM - Enterprise Content Management
  Verwaltung, Aufbewahrung und Bereitstellung aller Informationen einer Einrichtung in einem System; dies können Dokumente, Bilder, Signale, Filme, Töne, Daten etc. sein.
- IHE - Integrating the Healthcare Enterprise
  Initiative zur Standardisierung von Behandlungsprozessen



XDS Akteure und Transaktionen

(XDS – Cross-Enterprise Document Sharing)

6. Zusammenfassung und Ausblick

- beweissichere Lösungen zur elektronischen Archivierung vorhanden bzw. realisierbar
- Beachtung der Grundsätze zur Langzeitsicherung elektronisch signierter Dokumente (VOI, ArchiSig, Braunschweiger Regeln
- Forderung nach ArchiSig-Konformität bei Ausschreibungen
- Voraussetzung: Ausbau der elektronischen Dokumentations- und Signaturverfahren
- Lösung für die Rechtslücke beim ersetzenden Scannen wünschenswert

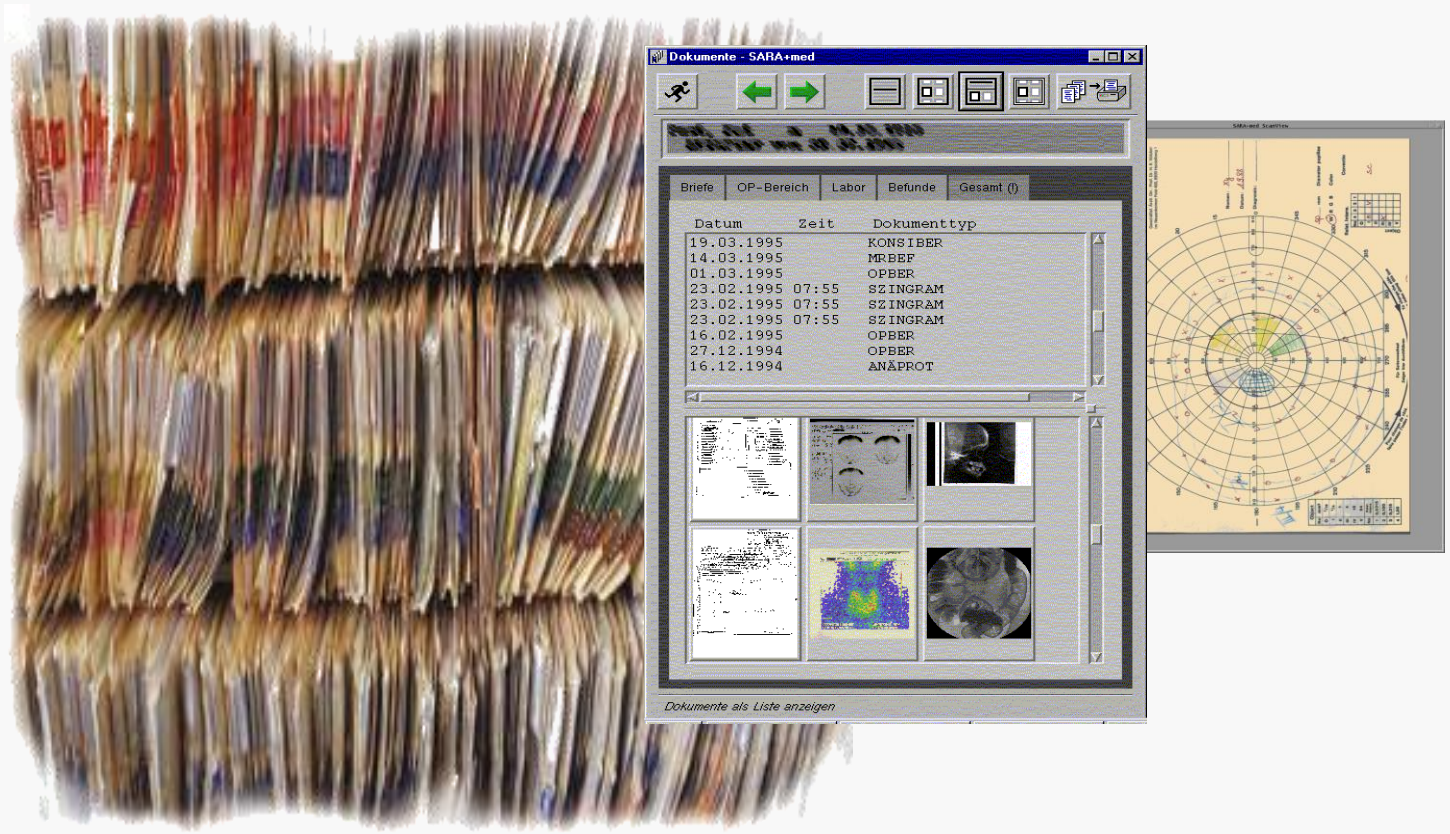
Fazit:

Digitale Archivsysteme sind heutzutage

- **rechtlich sicher realisierbar, abgesehen von der Unsicherheit bei gescanten Dokumenten, und**
- **wertvolle Informationsquellen,**
- **aber inhaltlich nur schwer auswertbar.**

7. Literatur

- Roßnagel, A.; Schmücker, P. (Hrsg.): Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit? Economica, Verlagsgruppe Hüthig Jehle Rehm: Heidelberg, München, Landsberg, Berlin 2005.
- Schmücker, P.; Dujat, C.; Seidel, C.: gmds-Praxisleitfaden „Dokumenten-management, digitale Archivierung und elektronische Signaturen im Gesundheitswesen“. Antares Computer Verlag: Dietzenbach 2012.
- Seidel, C.; Kosock, H.; Brandner, A.; Balfanz, J.; Schmücker, P.: Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens. Hrsg.: Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. (CCESigG), Shaker-Verlag: Aachen 2010.



Vielen Dank für Ihre Aufmerksamkeit!

Notizen:

Notizen: