Einsatz von elektronischen Signaturen in der Langzeitarchivierung

Niels Fromm

AG Elektronisches Publizieren

Gliederung

- Sicherheit
- Rechtliche Grundlagen
- Technische Grundlagen
- Elektronische Signaturen
- Probleme in der Langzeitarchivierung
- Anwendung in der Langzeitarchivierung

Sicherheit

- Digitale Daten sind beliebig veränderbar

- Authentizität
  „Wer hat die Daten gesendet / erstellt?“
- Integrität
  „Wurden die Daten seitdem geändert?“
- Verbindlichkeit
  „Nichtabstreitbarkeit einer Handlung“

Sicherheit

- Lösung:

elektronische Signatur

- Vollständiger Ersatz für Unterschrift auf Papier ?

Rechtliche Grundlagen

- Europäischer Rechtsrahmen: „Signaturrichtlinie“

  „Richtlinie 1999/93/EG des Europäischen Parlamentes und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“

- Umsetzung in deutsches Recht 16.05.2001

  „Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)“

Rechtliche Grundlagen

- einfache elektronische Signatur
  - technologische Offenheit
  - alle Verfahren die der Authentifizierung dienen, auch ohne weitere Sicherheitsmerkmale
  - z.B. eingescannte Unterschrift
- fortgeschrittene elektronische Signatur
  nach Art. 2 Nr. 2:
  - eindeutige Zuordnung zum Unterzeichner
  - ermöglicht Identifizierung des Unterzeichners
  - wird mit Mitteln erstellt, die der Unterzeichner unter alleiniger Kontrolle hat
  - ermöglicht Erkennung von Veränderungen der Daten
  - z.B. „Humboldt-CA“, PGP

Rechtliche Grundlagen

- qualifizierte elektronische Signatur

  Besondere Rechtsfolgen bestehen laut der Signaturrichtlinie (Art. 5 Abs. 1) nur für:
  „fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt werden“
  Das Zertifikat ermöglichst die Identifizierung des Unterzeichners, indem die Signatur einer Person zugeordnet wird. Qualifiziert ist ein Zertifikat nach Art.2 Nr.10 der Signaturrichtlinie dann, wenn es einen bestimmten Mindestinhalt hat (Anhang I der Richtlinie) und von einem Zertifizierungsdiensteanbieter (vertrauenswürdiger Dritter) ausgestellt wird, der die Anforderungen des Anhanges II erfüllt.

- akkreditierte elektronische Signaturen

Technische Grundlagen

- Hash-Algorithmen

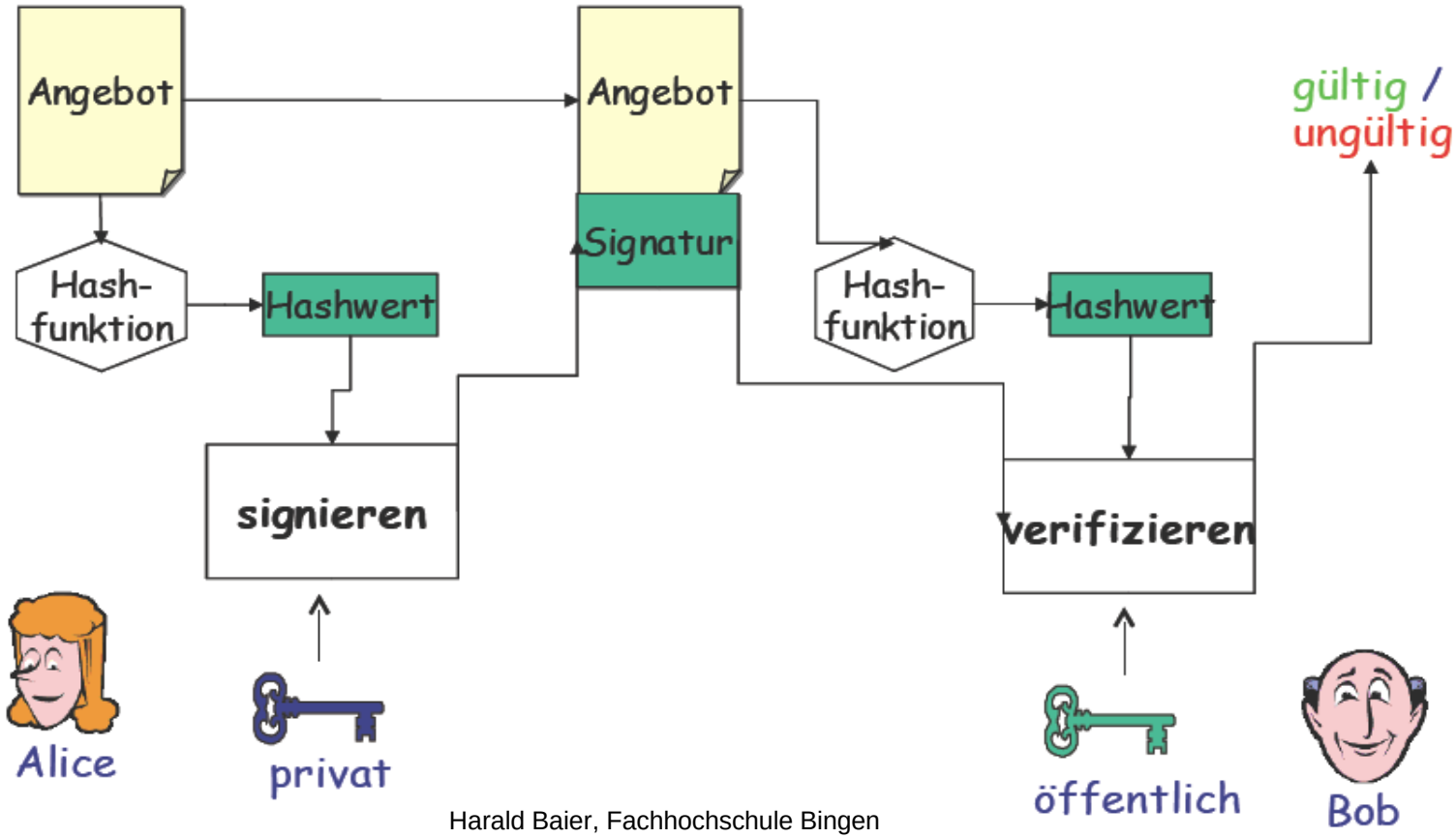
  Das Ziel eines Hashing-Verfahrens ist, aus einer großen Eingabemenge eine kleine Ausgabemenge, den so genannten Hashwert zu erzeugen.

  - Eindeutigkeit
  - Kollision: wenn zwei unterschiedliche Dateien zu einem Hashwert führen
  - SHA-160,SHA-512, RIPEMD-160

- Asymetrische Verschlüsselung

Elektronische Signatur

- Funktionsweise elektronische Signatur



Harald Baier, Fachhochschule Bingen

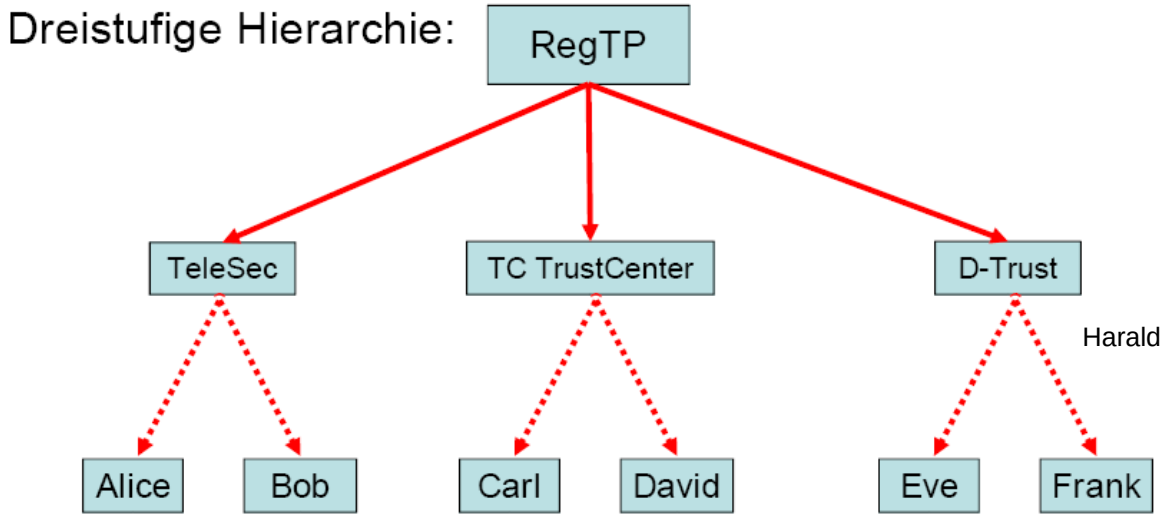
Elektronische Signatur

Problem:

öffentlicher Schlüssel muss authentisch sein

Lösung:

vertrauenswürdiger Dritter signiert öffentlichen Schlüssel
-> Zertifikat



Harald Baier, Hochschule Darmstadt

Probleme bei LZA

- Verlust Sicherungseigenschaften von Hash- und Verschlüsselungsalgorithmen

  - theoretisch: qualifizierte elektronische Signatur Unterschrift gleichgestellt -> unbegrenzt gültig

  - praktisch: Verlust von Beweisbarkeit der elektronischen Signatur (z.B. Zertifikat nur ca. 4 Jahre gültig)

  - Ansatz: langfristige Sicherung des Beweises, das eine Signatur zu einem bestimmten Zeitpunkt gültig war -> Über- oder Neusignatur bzw. Zeitstempelung

Probleme bei LZA

- Konzept für Langzeitarchivierung

  - Interpretierbarkeit von Informationen

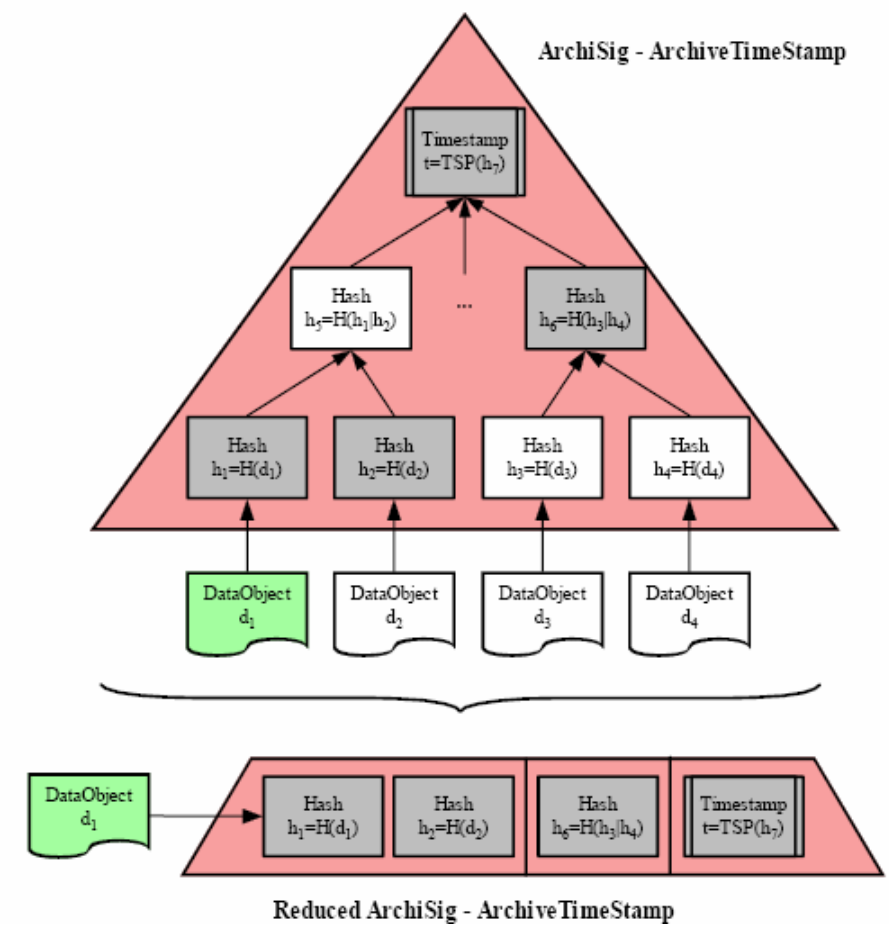
  - kontinuierliche Migration
    -> Veränderung von Daten durch Formatkonversion

Anwendung in LZA

- Projekt Archisafe /Archisig
  www.archisafe.de PTB Braunschweig
- Fokus:
  Erhaltung der Rechtssicherheit (Gültigkeit) einer sehr großen Zahl von Dokumenten / Signaturen
- Archivierte Daten: PDF-Dokument und Metadaten in ARS genanntes XML-Dokument integriert (ArchiSafe Record Keeping Strategy)
- Technologie: Hashbaum

Anwendung in LZA

- Technologie: Hashbaum



Anwendung in LZA

- Projekt Transidoc
  www.transidoc.de
- Fokus: Erhaltung der Rechtssicherheit bei Migration von Dokumenten
- Technologie „Transformationsregeln“
  - genaue Dokumentation, wie ein Dokument in ein anderes Format konvertiert wurde
  - Signatur dieser Regeln

edoc.hu-berlin.de

Daten

- ~ 5000 Publikationen
- ~ 200000 Dateien
- ~ 100 GB Daten
- 5 Kopien in RAID5 Speichersystemen an vier verschiedenen Standorten in Berlin
- 2 Kopien im TSM Backupsystem an zwei verschiedenen Standorten in Berlin

LZA-Strategie

- Konzept der kontinuierlichen Migration
- Hohe Anforderungen an Formatierung des Originals
- Trotzdem noch hoher Aufwand beim Konvertieren nach XML
- Originalformate: MS-Word, PS, Latex
- Präsentationsformate: PDF, HTML
- Archivierungsformat: XML, PS, Latex
- Weitere Formate dann per XSLT-Transformation aus XML

Konzept (1)

Containererstellung / Versionierung

- Ziel: AIP- und DIP-Container, Integritätsprüfung des Archivs oder einzelner Publikation
- Im METS-Format mit allen Metadaten
- Speicherung im Filesystem im Ordner der Publikation
- Referenzierung aller zugehörigen Dateien einer Publikation mit zwei Hashwerten durch zwei unterschiedliche Verfahren
- Versionierung: Erstellung eines neuen Containers bei Veränderung an der Publikation (Arbeitsabläufe, hinzufügen und löschen von Informationen, auslaufen eines Hashverfahrens)

Konzept (2)

Elektronische Signatur

- Ziel: „rechtssichere“ Dokumentation des Zeitpunktes der Annahme (mit bestimmten Inhalt) und aller Veränderungen an der Publikation
- Nur für bestimmte Publikationen
- Signatur jeder neuen Version eines Containers einer Publikation
- „Externe“ Signatur mit Zeitstempel und OCSP-Antwort abgelegt im Filesystem

Offene Fragen

Langzeitsicherung der Signaturen

- Eine Publikation hat mindestens zwei Signaturen (Annahme und nach erfolgter Konvertierung in XML)
- „Beliebig“ viele weitere Container-Versionen und damit Signaturen möglich
- Gesucht: Verfahren zur möglichst automatisierten Langzeitsicherung dieser Signaturen

Vielen Dank für Ihre Aufmerksamkeit