Grundkonzepte rechtssicherer Transformationen signierter Dokumente

Stefanie Fischer Dieskau (provet, Kassel),
Thomas Kunz, Andreas U. Schmidt,
Ursula Viebeg (Fraunhofer SIT, Darmstadt)

QSIG 2005 – Regensburg, 6. April 2005

Fraunhofer Institut Sichere Informations-Technologie

Inhalt

- Begriffsgerüst für sichere Transformationen
- Beispielszenarien:
  - Annahme von Bauanträgen
  - Anonymisierung von Patientenakten
  - Elektronische Poststelle
- Phasenmodell
- Datenkonzepte: Transformationsakte und -siegel
- Grundsätzliche Sicherheitsanforderungen
- Komplexes Beispiel: Amtliche Beglaubigung
- Ein Problem: Authentisierung der Beglaubigerrolle

Warum brauchen wir ein abstraktes Begriffsgerüst

- Problemstellung
  - Viele Anwendungskontexte, insbesondere der rechtliche, besitzen eigene vorbelegte Begriffssysteme
- Ziele
  - Eigenes Begriffsgerüst für „Sichere Transformationen“
  - Flexibel und anwendbar für die meisten Anwendungskontexte

Grundlegende Begriffe (1)

- Eine Transformation ist ein Prozess, bei dem ein **Ausgangsdokument** in ein **Zieldokument** umgewandelt wird.

- Der **Zweck** einer Transformation ist, ein *Zieldokument* mit einer bestimmten *Bedeutung* zu erhalten.

Grundlegende Begriffe (2): Zweck

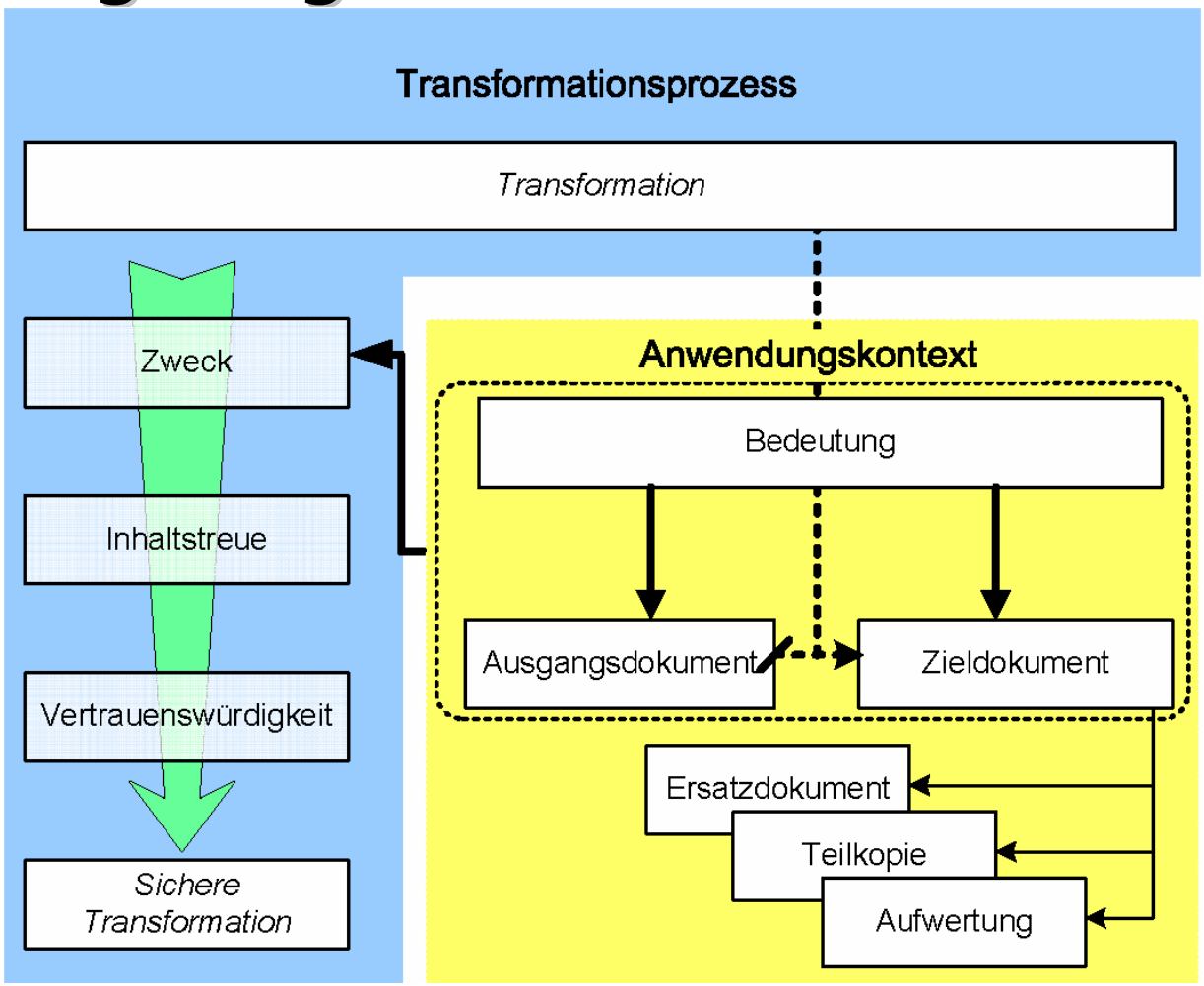
Wichtige Spezialfälle:

- **Ersatzdokument** (gleiche Bedeutung)
  - Beglaubigte Abschrift
- **Teilkopie** (eingeschränkter Bedeutungsumfang)
  - Anonymisierung aus Datenschutzgründen
  - Auszug aus öffentlichem Register
- **Aufwertung** (umfassendere Bedeutung)
  - Verwendung eines anderen Zeichensatzes für Sehbehinderte

Grundlegende Begriffe (3)

- **Inhaltstreue** sind die überprüfbaren Eigenschaften einer Transformation, die sie den *Zweck* erfüllen lässt, z.B. Farberhalt.
- **Vertrauenswürdigkeit** bedeutet, dass nachträglich verifizierbar ist, welche Transformation durchgeführt wurde, dass die *Inhaltstreue* überprüft wurde und dass das Prüfergebnis vermerkt wurde und zurechenbar ist.
- Eine **sichere Transformation** liegt dann vor, wenn das Zieldokument die durch den Zweck der Transformation bestimmte Art der Inhaltstreue zum Ausgangsdokument aufweist und dies in einer *vertrauenswürdigen* Form vermerkt wurde.

Begriffsgerüst für sichere Transformationen



Eine sichere Transformation wird gewährleistet durch die Vertrauenswürdigkeit der Inhalts-Treue für eine bestimmten Zweck.

Der Zweck ist die Transformation eines Ausgangsdokuments mit einer bestimmten Bedeutung in ein Zieldokument mit einer bestimmten Bedeutung.

Elektronische Erfassung eines Bauantrages

- Zweck: Ersatzdokument erstellen (P→E)
- Bauantrag:
  - Textdokumente, Zeichnungen, Bilder
- Transformation:
  - Klassifikation per Augenschein anhand vom Typ
  - Vordefinierter Regelsatz pro Typ
  - Transformationsakte = Logbuch über viele Bauanträge
  - Konvertierung: Einscannen der kompletten Dokumente
  - Prüfungen per Augenschein auf vollständige Erfassung
  - Transformationssiegel = elektronische Signatur

Anonymisierung von medizinischen Dokumenten

- Zweck: Teilkopie erstellen (E→E)
  - entpersonalisierte Fassung
  - Erhalt der Zuordnung zum Signierer (Arzt)
- Medizinisches Dokument:
  - Arztbrief
- Transformation:
  - Signaturextraktion:
    - Signaturprüfung muss Signierer als Arzt ausweisen
    - Fortgeschrittene Signatur kann reichen, spezielle rechtliche Regelungen fehlen – evtl. in speziellen Fällen qualifizierte Signatur (Haftung)
    - Signaturdaten: signierender Arzt, Zertifikatausssteller
  - Konvertierung + Prüfung
    - Automatisch möglich bei einem XML-Dokument

Elektronische Poststelle

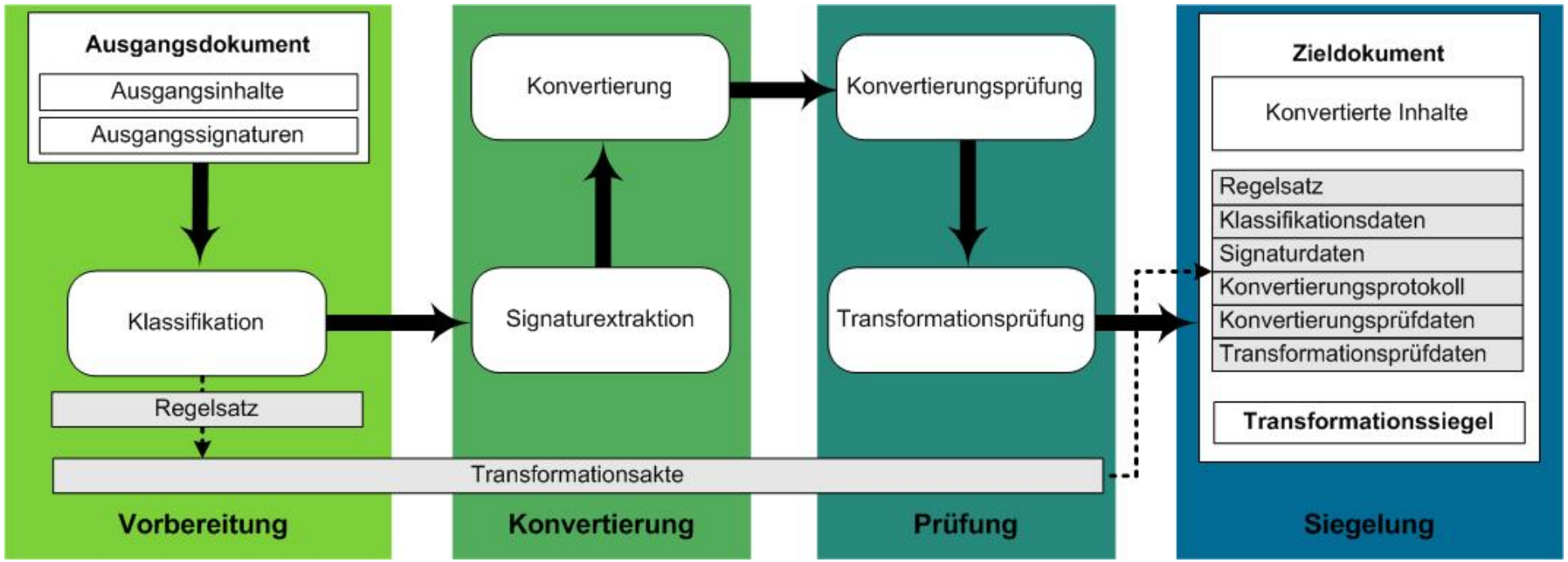
- Umsetzung vieler Formate auf wenige
- Zweck: Ersatzdokument erstellen (E→ E)
- Transformation:
  - Klassifikation automatisch anhand von Dokumentenformat
  - Person nur bei unbekanntem Format erforderlich
  - Vordefinierter Regelsatz pro Format
  - Signaturextraktion:
    - Organisationseigene Signatur-Prüfpolitik
    - Signaturdaten auch Sperrinformationen
  - Klassifikation bestimmt die Konvertierungskomponente
  - Prüfungen: Stichproben per Augenschein möglich
  - Transformationssiegel: elektronische Signatur

Anforderungen an eine sichere Transformation

- Erreichen der gewünschten (Zweck) Inhaltstreue
  - ⇨ Festlegen des Zwecks
  - ⇨ Bestimmen des Ausgangsdokuments
  - ⇨ Prüfen der Inhaltstreue
- Nachträglich prüfbar
  - ⇨ Protokollieren des Ablaufs und der Prüfergebnisse
- Vertrauenswürdig
  - ⇨ Nachprüfbar Festhalten, wer Prüfung durchgeführt hat

➢ Mehrere Phasen,
da reine Konvertierung nicht ausreicht

Phasen einer sicheren Transformation



Vorteile des Phasenmodells

- Umfasst Vielzahl von Transformationsabläufen
  - Verteilte Komponenten (räumlich)
  - Eine monolithische Komponente
- Unabhängig vom Automatisierungsgrad
  - Komplett oder teil-automatisierter Ablauf
  - Vollständig von Personen durchgeführter Ablauf
- Anwendbar für alle drei Transformationsarten
  - P→E, E→E, E→P
- Umsetzbar in den meisten Anwendungskontexten

Klassifikation des Ausgangsdokuments

- Abhängig vom Anwendungskontext und Zweck
- Erfolgt anhand von Eigenschaften, wie
  - Dokumententyp (Arztbrief, Bauzeichnung)
  - Dokumentenformat (Word, PDF)
- Klassifikationsergebnis und Zweck bestimmen:
  - Was gehört zur Inhaltstreue
  - Wie soll Inhaltstreue erreicht und geprüft werden
  - Wie soll Prüfergebnis vertrauenswürdig bestätigt werden

➔**Regelsatz** für einen sicheren Transformationsprozess

Konzept des Regelsatzes

- Bestimmt praktische Umsetzung der Phasen für einen konkreten Anwendungsfall
- Definiert:
  - Sicherheitseigenschaften
  - Organisatorische, technische Regeln
  - Regeln zum Prozessablauf
- Flexibles Konzept
  - Umsetzbar für verschiedenste Anwendungsbereiche
  - Verweis auf bestehende Regelwerke möglich / sinnvoll
  - Definition von Profilen möglich

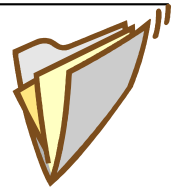
Beispiele für Regeln des Regelsatzes

- Einsatzumgebung entspr. BSI-Grundschutzhandbuch
- Formatvorschriften für Ausgangsdokument
- Prüfpolitik für elektronische Signatur
- einzusetzende Komponenten und deren Parametrisierung
- ob Phase durchgeführt wird
- Grad der Automatisierbarkeit, d.h. wann ist Eingreifen einer Person notwendig
- Art des Transformationssiegels
  - Unterschrift/en
  - (Qualifizierte) elektronische Signatur
  - Siegel

Sicherheitsanforderungen

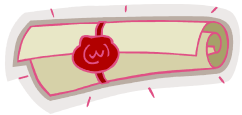
- Gewährleistung der Integrität und evtl. Authentizität aller Daten
- Sicherstellung der korrekten Zuordnung der Daten zueinander, z.B.
  - Regelsatz zu den einzelnen Phasen
  - Transformationsakte zu den konvertierten Daten
- Zurechenbarkeit des Transformationssiegels
  - Wer ist Ersteller?
  - Worauf bezieht es sich?

Konzept der Transformationsakte



- enthält Ablaufprotokolle und Prüfergebnisse
- ermöglicht
  - korrekte Zuordnung der Daten zueinander, durch
    - Daten direkt in der Transformationsakte
    - Verweis auf externe Quellen
    - Hashwert zum Integritätsnachweis
  - Prüfung der Zuordnung der Daten
  - Nachvollziehbarkeit der Transformation
- Flexibles Konzept
  - konkrete Umsetzung anwendungsabhängig

Konzept des Transformationssiegels



Das Transformationssiegel garantiert

- die Eigenschaften einer sicheren Transformation
  - nachträgliche Überprüfbarkeit der Transformation
  - dem Zweck entsprechende Inhaltstreue zwischen Ausgangs- und Zieldokument
  - Zurechenbarkeit und Vertrauenswürdigkeit der Transformation durch Signatur
- die gewünschte Verwendbarkeit des Zieldokuments unabhängig vom Vorliegen des Ausgangsdokuments

Amtliche Beglaubigung (1)

- Szenario basierend auf § 33 VwVfG
  - Formattransformation (E→E) in einer Behörde
  - qualifiziert elektronisch signiertes Ausgangsdokument
- Transformation:
  - Zweck: „zur Vorlage bei Behörde XY“
  - Klassifikation: Bezeichnung des Dokuments
  - Signaturextraktion
    - Prüfen der qualifizierten elektronischen Signatur
    - Signaturdaten
      - Inhaber der Signatur
      - Zeitpunkt der Signaturerstellung
      - Zertifikat + Daten
    - Abbruch des Prozesses bei
      - Fehlschlagen der Integritätsprüfung
      - Signaturersteller kann nicht ausgewiesen werden

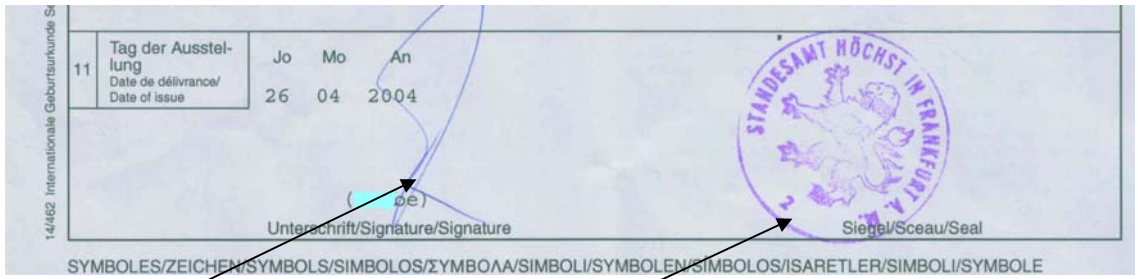
Amtliche Beglaubigung (2)

Transformationssiegel ≈ Beglaubigungsvermerk:

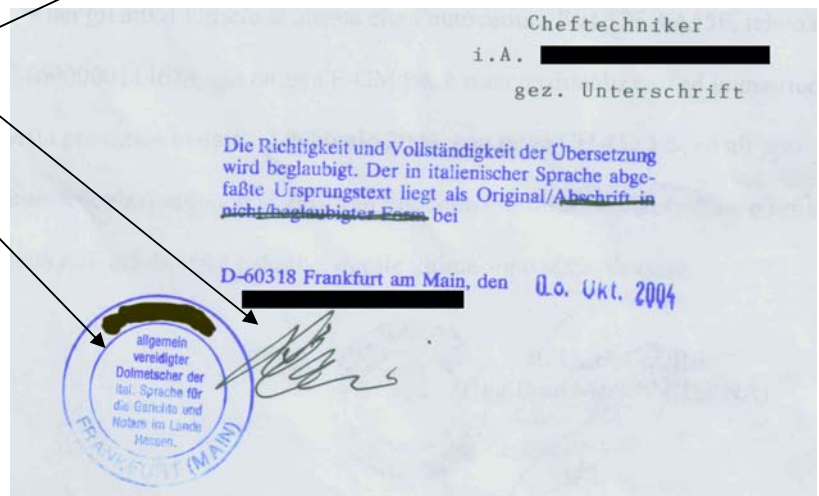
- Bezeichnung des Ausgangsdokuments
- Signaturdaten
- Ort der Beglaubigung
- Zeitpunkt der Beglaubigung
- Name des beglaubigenden Bediensteten
- Bezeichnung der beglaubigenden Behörde
- Feststellung der Übereinstimmung (Inhaltstreue)
- Zweck der Transformation
- Dauerhaft überprüfbare qualifizierte Signatur des zuständigen Bediensteten

Problem: Authentisierung der Beglaubigerrolle

Jede Beglaubigung, ob amtlich, öffentlich oder Privat trägt zwei Authentisierungsmerkmale



- Die Unterschrift authentisiert die Person des Beglaubigers
- Der Rundstemepel oder das Siegel authentisiert seine/ihre Rolle als Beglaubiger



Sichere elektronische Abbildung des 'Papier-Verfahrens':
Für die Sicherung der elektronischen Beglaubigung reicht die Signatur des Beglaubigers nicht aus – ihre positive Verifikation könnte einen falschen Eindruck von Authentizität erwecken, wenn z.B. die Beglaubigerrolle revoziert wurde.

Gesetzliche Vorgaben?

Zu amtlichen Beglaubigungen heißt es (§33 Abs. 5 VwVfG)

"die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel nach Absatz 3 Satz 2 Nr. 4 werden durch ***eine*** dauerhaft überprüfbare qualifizierte elektronische Signatur ersetzt.“

Bei amtlichen Beglaubigungen vielleicht ausreichend (innerbehördliches Vertrauen).

Jedoch: Reicht ***ein*** Authentisierungsmerkmal bei öffentlichen, notariellen und anderen Beglaubigungen?

Authentisierung der Beglaubigerrolle

- Nahe liegende Lösung: Attribut-Zertifikate
- Organisatorische/Institutionelle Probleme
  - Dauerhafter Zugriff durch autorisierte Stelle
  - Sichere Möglichkeit zur Revokation
  - Heterogenität und Dezentralität der Siegel/Rundstempel herausgebenden Stellen
  - Träger der Infrastruktur??