TransiDoc
Technologie für sichere Transformation

Dr. Andreas U. Schmidt
Fraunhofer Institut für sichere Informationstechnologie SIT, Darmstadt

TransiDoc

Fraunhofer SIT Institut Sichere Informations-Technologie

Das TransiDoc-Projekt

August 2004 – Juni 2007, Konsortialführung Fraunhofer SIT

Konsortium

Fraunhofer Institut Sichere Informations-Technologie

UniversitätsKlinikum Heidelberg

InterComponentWare

provet – Projektgruppe verfassungsverträgliche Technikgestaltung e.V.

Curiavant Internet GmbH

Fördergeber

Bundesministerium für Wirtschaft und Technologie

DLR

BNotK Bundesnotarkammer (assoziiert)

DATEV (assoziiert)

Primäre Anwendungsbereiche

- **E-Government**:
  Bauverwaltung – Annahme von Bauanträgen
- **Gesundheitswesen**:
  Patientenakten in DMPs, Anonymisierung
- **Langzeitarchivierung**:
  Format- und Versionswechsel sign. Dokumente
- **Elektronische Beglaubigung**:
  Gemäß VerwVerfG, BeurkG

Projekt-Ziele

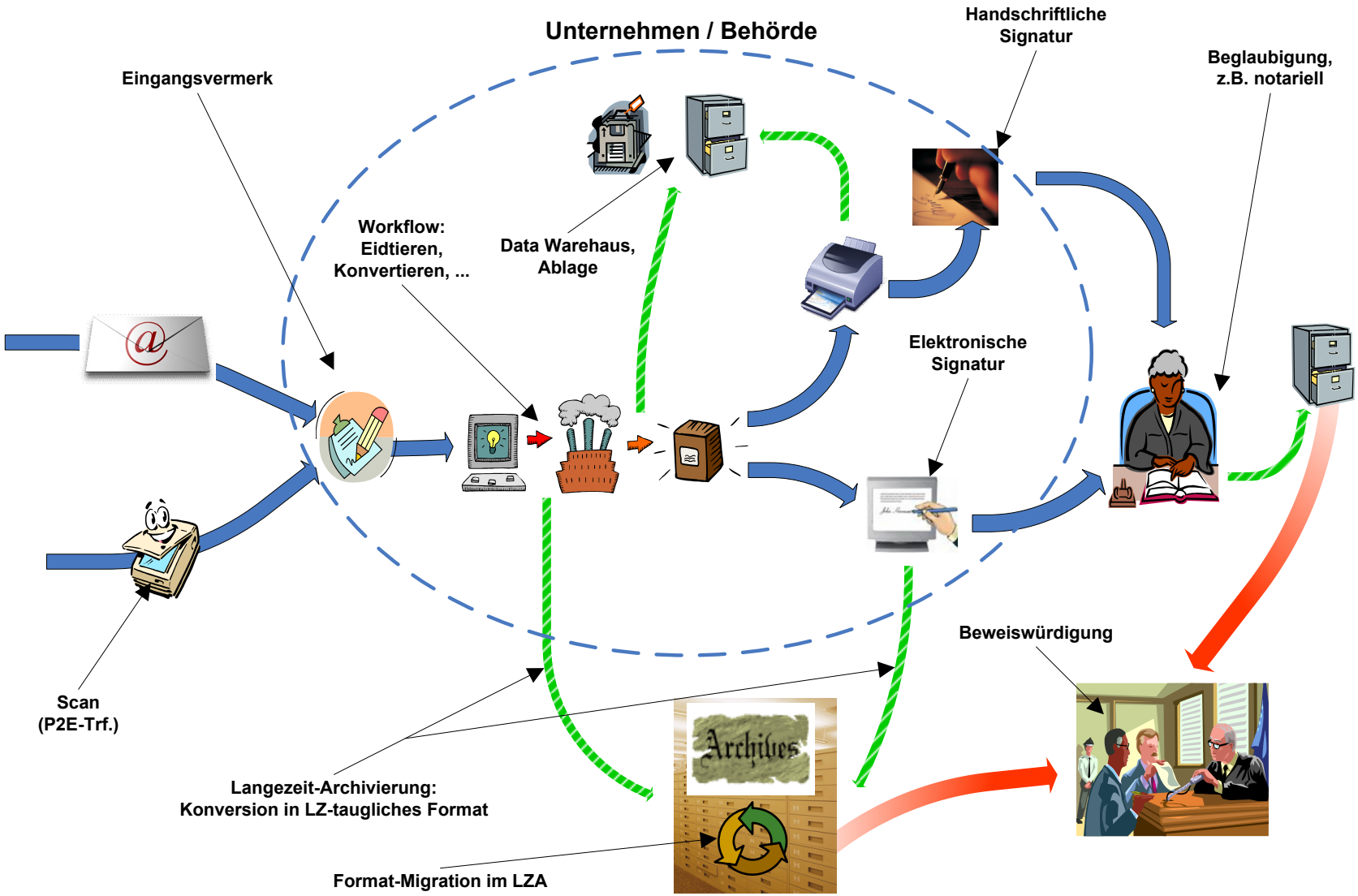
- Serverbasierte **Prototypen/Demonstratoren** für og. Anwendungsbereiche
- Rechtlich haltbare technische *und* organisatorische Methoden - **Guidelines**
- Rechtspraktische Evaluierung – **Simulationsstudie**

www.transidoc.de

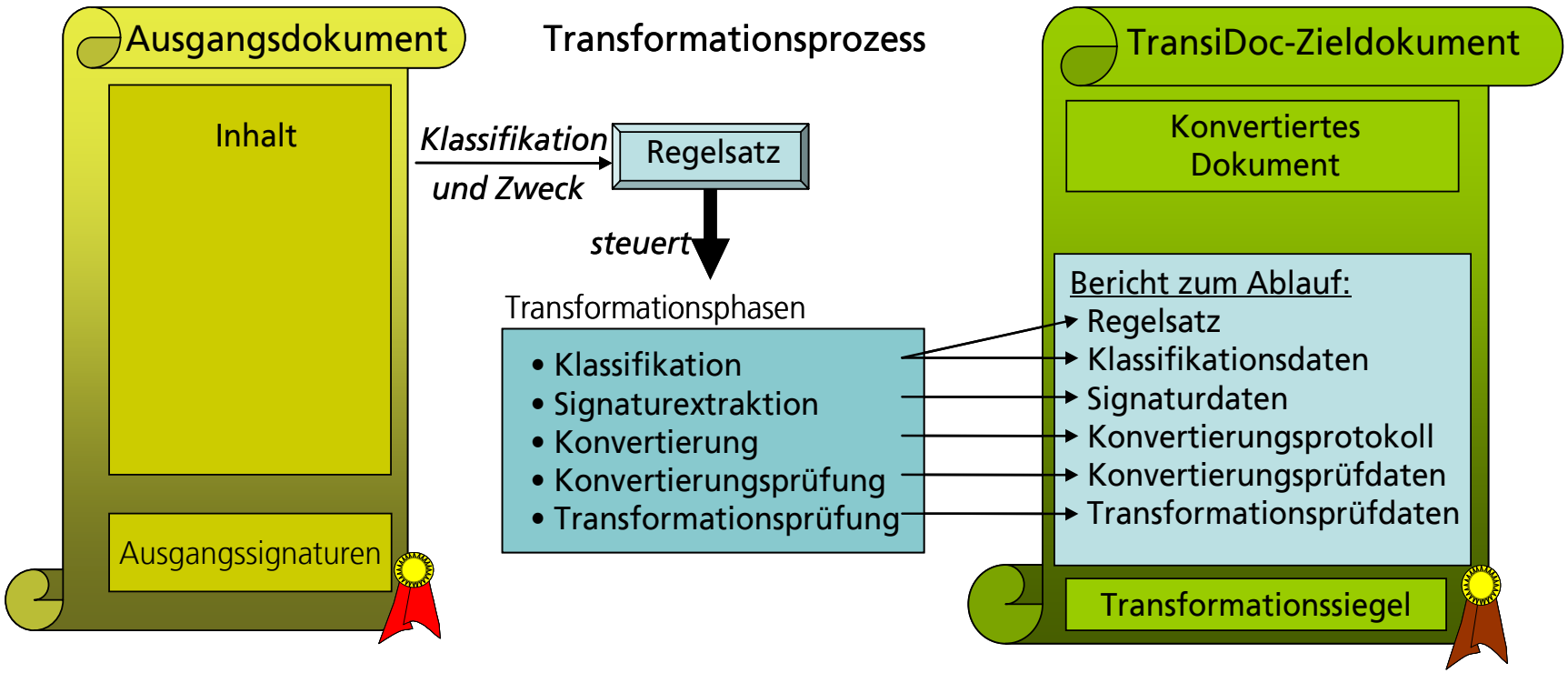
TransiDoc Ausgangspunkte

- Elektronische Signaturen können Beweiskraft verlieren (“altern”) durch die Zunahme von Rechenleistung und mögliche Fortschritte in der Kryptologie oder noch unbekannte Technologien wie Quanten Computer.
  - Elektronisch signierte Dokumente verlieren ihre rechtliche Beweiskraft und damit Bindungswirkung
- Veränderungen an Dokumenten brechen die elektronische Signatur
  - Ständig zunehmende Zahl von anwendungsspezifischen Datenformaten (bereichsspezifisch, siehe z. B. Medizin, HL7 etc.) und Versionen
  - Formatskonversionen zum Erhalt der Lesbarkeit sind unvermeidlich
  - Gefahr von Veränderungen (unwillkürlich oder mit Absicht) oder Verlusten
- Daher muss systematisch Vorsorge getroffen werden für
- die Langzeit-Sicherung **des Beweiswertes** und
- rechtlich **sichere Transformation** signierter Dokumente.

„Transformationen“ in Arbeitsabläufen



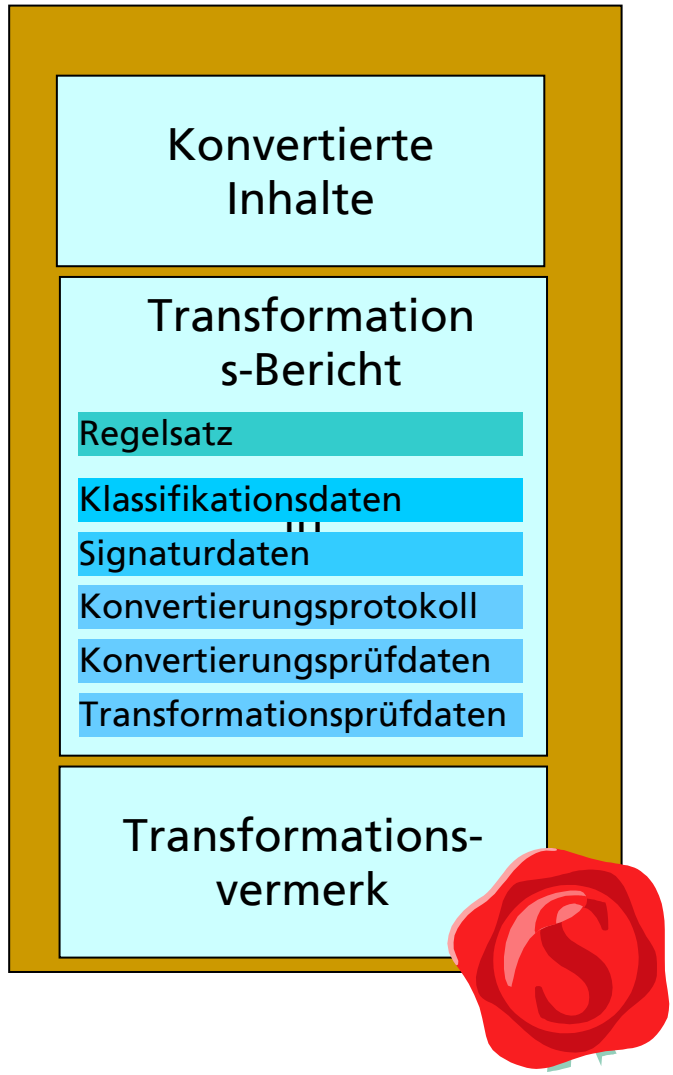
TransiDoc - Transformationsprozess



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

- Das Transformationssiegel bezieht sich auf
  - konvertierte Inhalte
  - Transformationsbericht
  - Transformationsvermerk

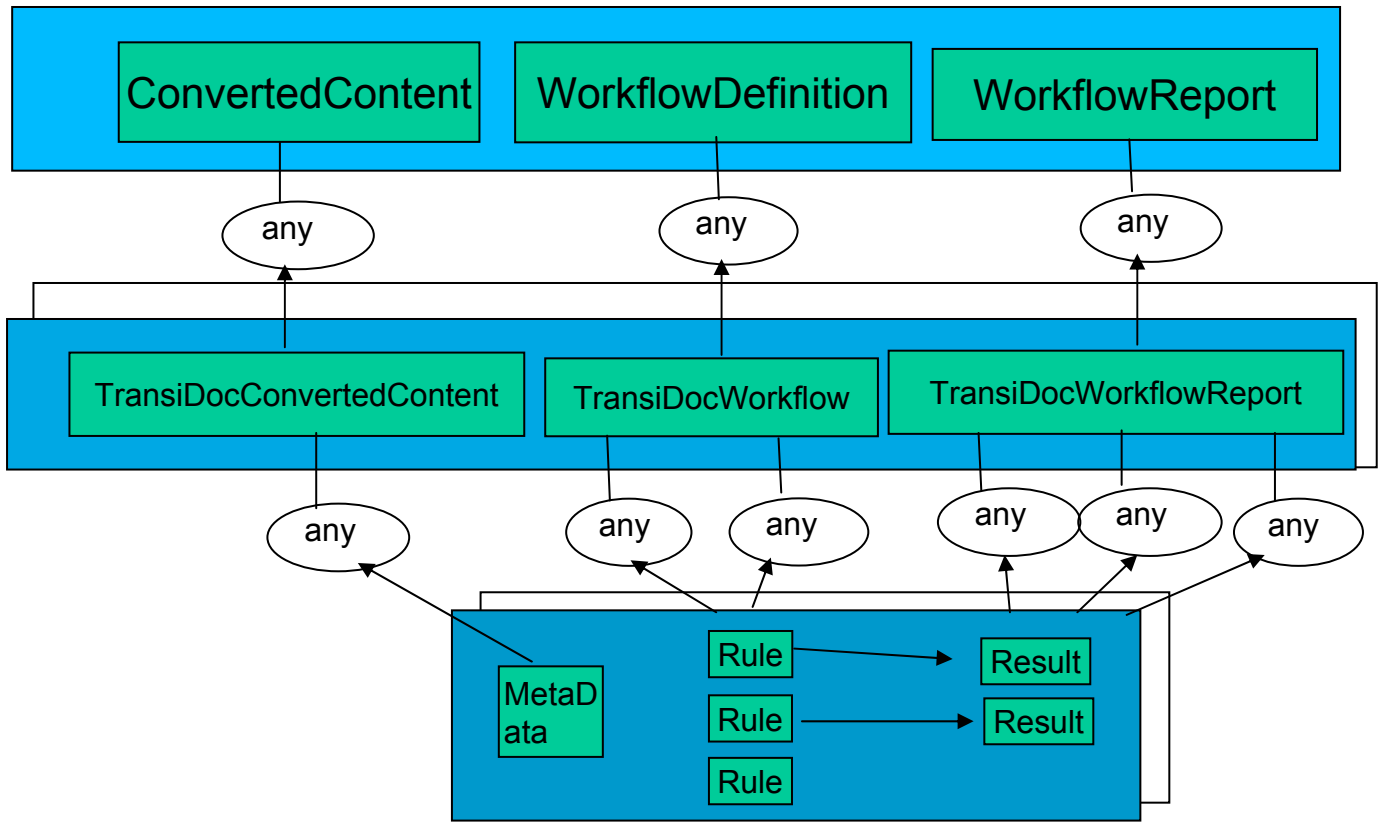


Workflow-orientiertes Datenmodell des Zieldokuments

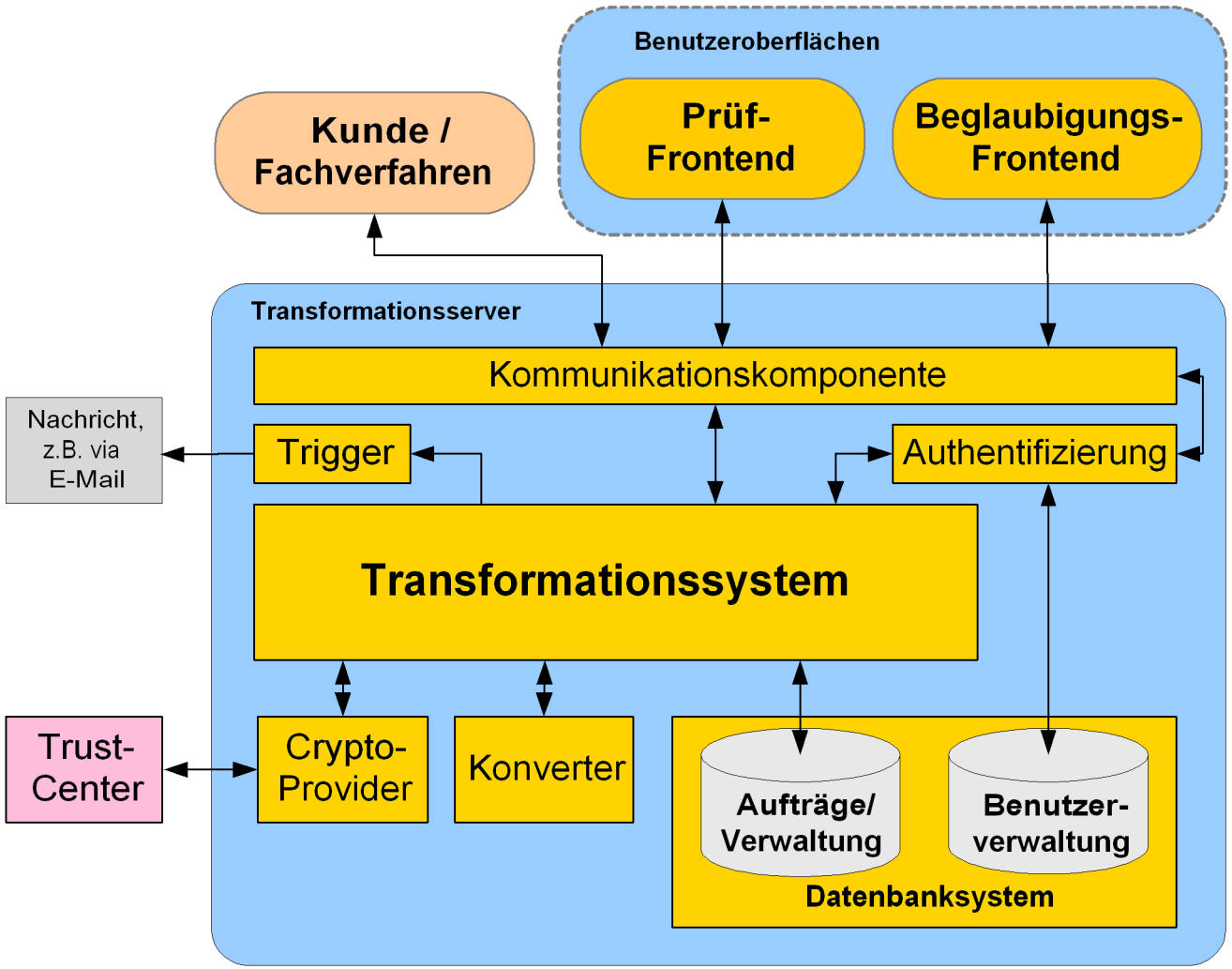
Generische Datenstruktur

Generische TransiDoc Datenstruktur

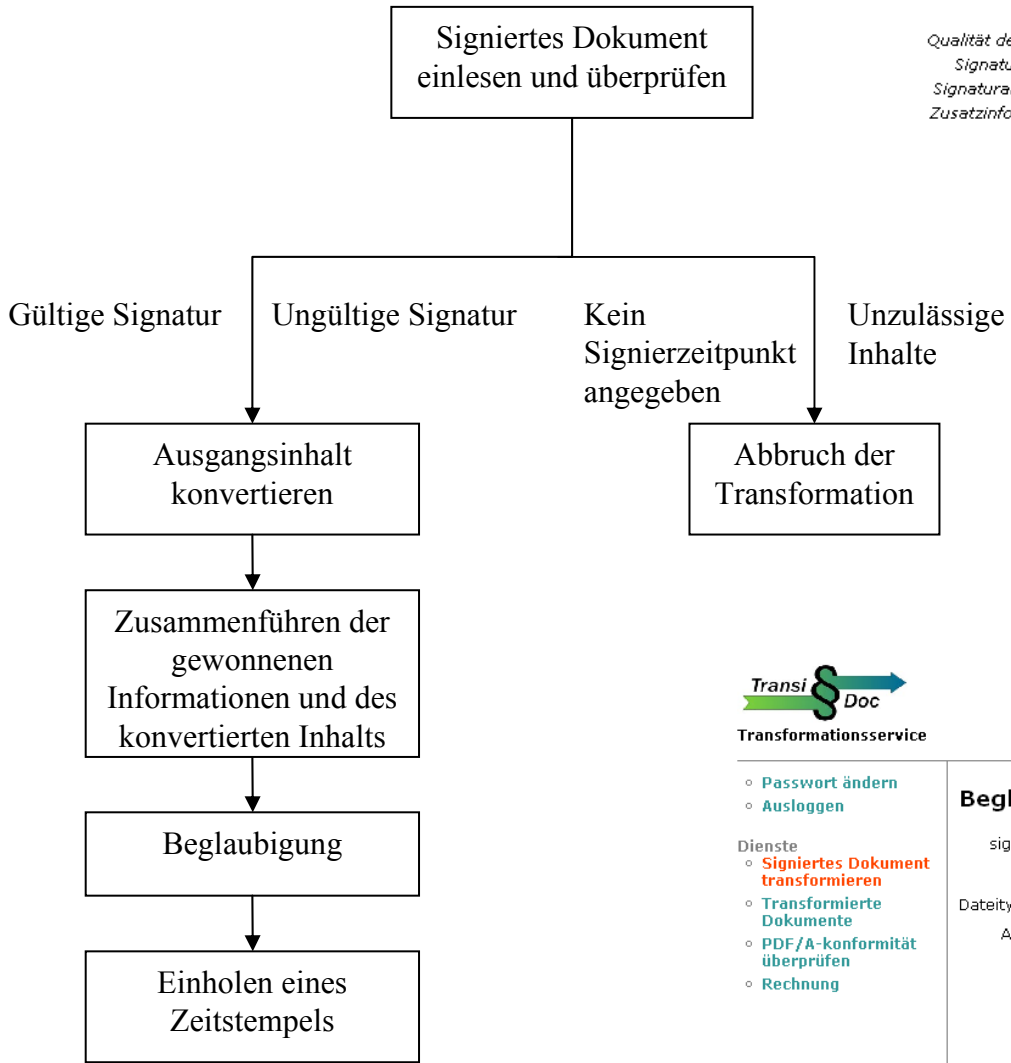
Anwendungs-spezifische Datenstruktur

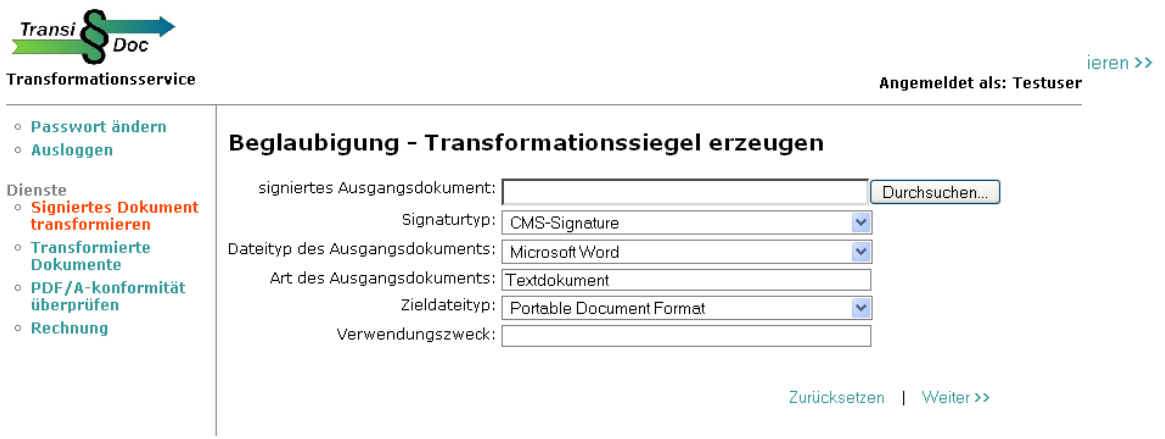


TransiDoc-Referenzarchitektur



Beispielablauf - Beglaubigung





Prüfung mit dem TransiDoc-Verifikationstool

Verifikation des TransiDoc-Zieldokuments

- Verifikation der Signatur
- Prüfen der syntaktischen Korrektheit
- Anzeige
- Prüfergebnisse des Verifikationsservice
- Informationen zum Ausgangsdokument
- Transformationssiegel
- Darstellung des Ablaufs der Transformation
- Gegenüberstellen von Regeln und Ergebnissen

✔ Ihr Dokument ist das Ergebnis einer Transformation

Transformationsphasen:

Klassifikation	**Signaturextraktion**	Konvertierung	Konvertierungsprüfung	Transformationsprüfung

Ablauf und Ergebnis der Phase "Signaturextraktion"

Aufgabe: Prüfung aller Ausgangssignaturen und Erfassen der Signaturdaten

Ausführungszeit: 30.03.2004, 09:14:07 Uhr - 30.03.2004, 09:14:18 Uhr

Manuell durchgeführt von:

Bernhardt Kleefuß

Rolle: Bediensteter des Oberbürgermeisteramts

Adresse: Hauptstr. 27, 77777 Kleinstadt, Deutschland

Verwendete Phasen-Komponenten:

"Transi-Converter-Paper2PDF", Version 2.6

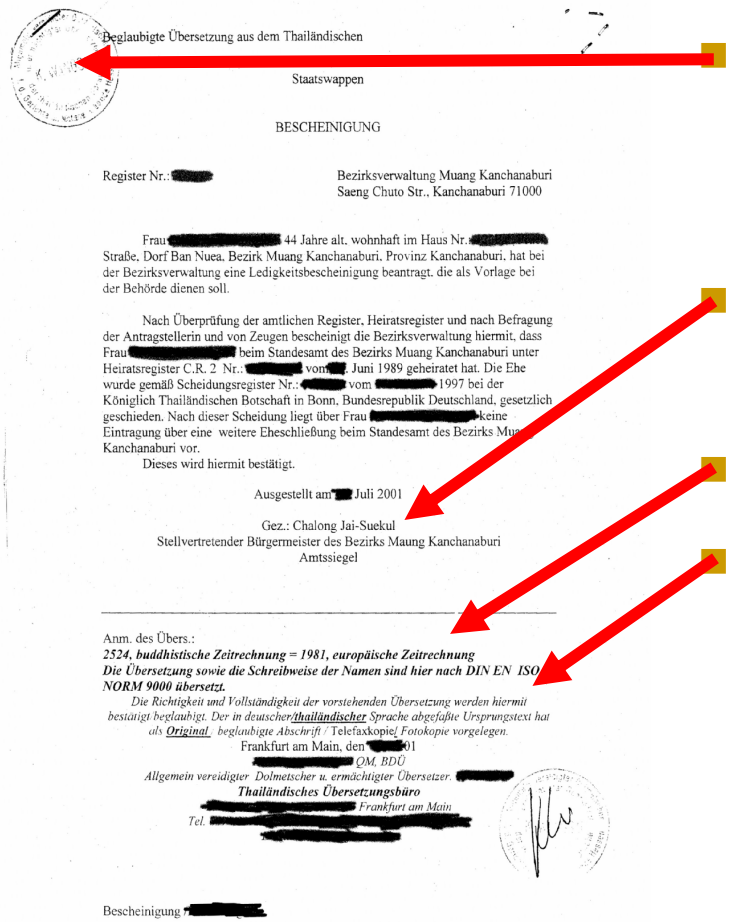
Hersteller: TransiTrust GmbH

Adresse: Hauptstraße 46A, 88888 Großstadt, Deutschland

Einzelergebnisse der Phase:

Bedeutung	Ergebnis	
Ergebnis der Signaturprüfung:	*Qualität der Originalsignatur:*	"Handschriftliche Unterschrift"
Signaturdaten:	*Name des Signierers:*	"Achim Bürgermeister"
	Signaturzeitpunkt:	"20.11.2001, 15:33:00 Uhr Zeit ermittelt von: Datumsangabe im Papierdokument"

Beglaubigte Übersetzungen



Beglaubigte Übersetzung aus dem Thailändischen

Staatswappen

BESCHEINIGUNG

Register Nr.: [redacted]

Bezirksverwaltung Muang Kanchanaburi
Saeng Chuto Str., Kanchanaburi 71000

Frau [redacted] 44 Jahre alt, wohnhaft im Haus Nr. [redacted] Straße, Dorf Ban Nuea, Bezirk Muang Kanchanaburi, Provinz Kanchanaburi, hat bei der Bezirksverwaltung eine Ledigkeitsbescheinigung beantragt, die als Vorlage bei der Behörde dienen soll.

Nach Überprüfung der amtlichen Register, Heiratsregister und nach Befragung der Antragstellerin und von Zeugen bescheinigt die Bezirksverwaltung hiermit, dass Frau [redacted] beim Standesamt des Bezirks Muang Kanchanaburi unter Heiratsregister C.R. 2 Nr. [redacted] vom [redacted] Juni 1989 geheiratet hat. Die Ehe wurde gemäß Scheidungsregister Nr. [redacted] vom [redacted] 1997 bei der Königlich Thailändischen Botschaft in Bonn, Bundesrepublik Deutschland, gesetzlich geschieden. Nach dieser Scheidung liegt über Frau [redacted] keine Eintragung über eine weitere Eheschließung beim Standesamt des Bezirks Muang Kanchanaburi vor.

Dieses wird hiermit bestätigt.

Ausgestellt am [redacted] Juli 2001

Gez.: Chalong Jai-Suekul
Stellvertretender Bürgermeister des Bezirks Maung Kanchanaburi
Amtssiegel

Anm. des Übers.:
2524, buddhistische Zeitrechnung = 1981, europäische Zeitrechnung
Die Übersetzung sowie die Schreibweise der Namen sind hier nach DIN EN ISO NORM 9000 übersetzt.

*Die Richtigkeit und Vollständigkeit der vorstehenden Übersetzung werden hiermit bestätigt beglaubigt. Der in deutscher/**thailändischer** Sprache abgefaßte Ursprungstext hat als **Original**, beglaubigte Abschrift / Telefaxkopie/ Fotokopie vorgelegen.*

Frankfurt am Main, den [redacted]01

[redacted] QM, BDÜ

Allgemein vereidigter Dolmetscher u. ermächtigter Übersetzer. [redacted]

Thailändisches Übersetzungsbüro

[redacted] *Frankfurt am Main*

Tel. [redacted]

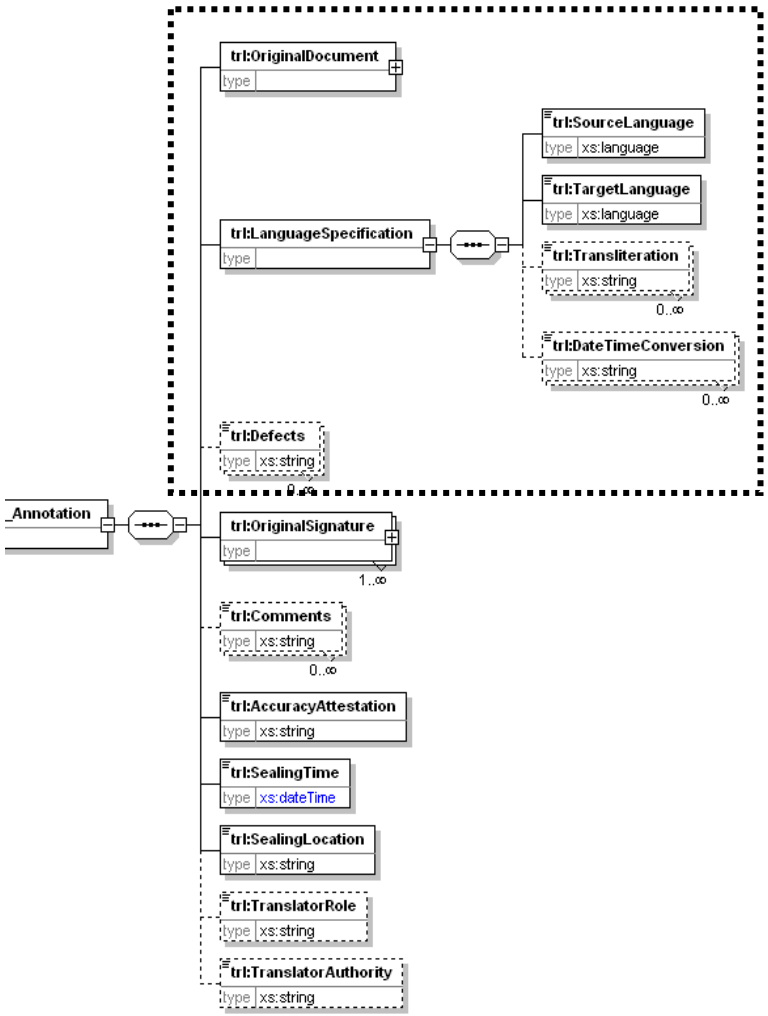
Bescheinigung [redacted]

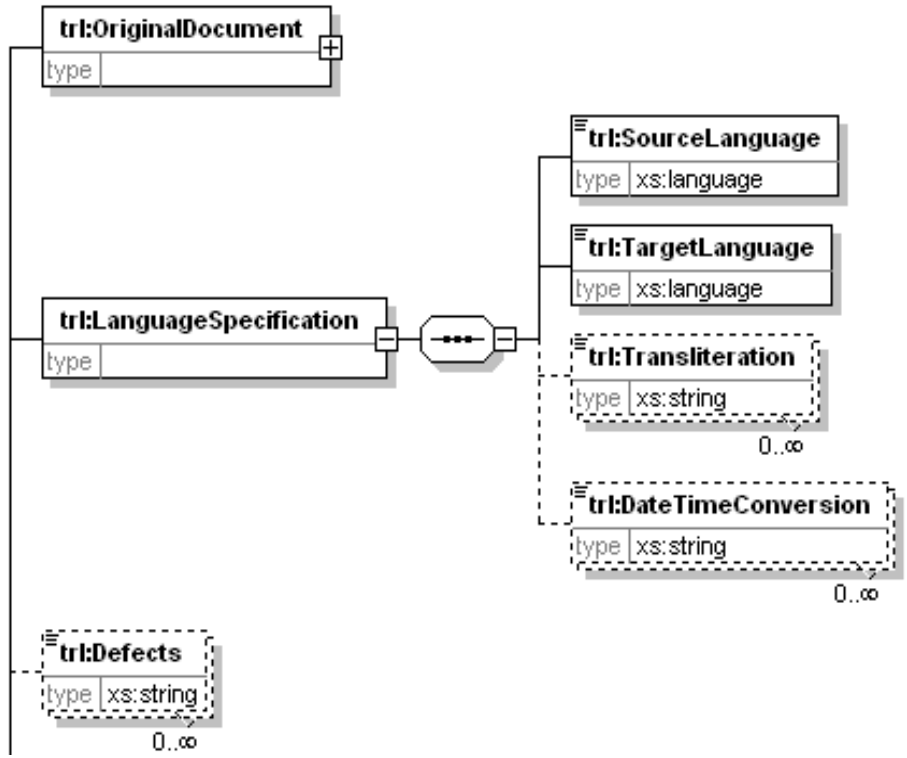
- Ausgangs- und Zieldokument durch Siegel und Heftung verbunden
- Beschreibung handschriftl. Signaturen
- Vermerk des Übersetzers
- Überseter-Unterschrift und -Siegel

Beglaubigte Übersetzungen

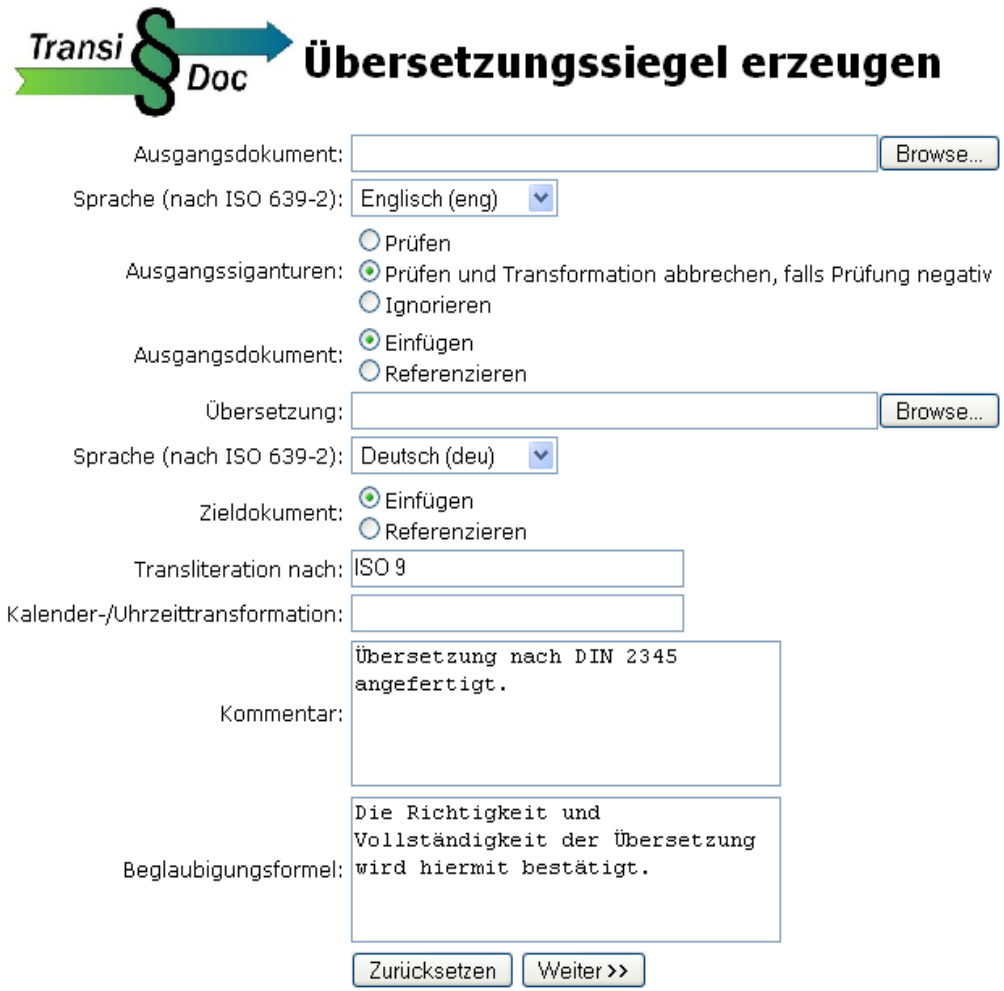
- Durchgeführt z.B. von “beeidigten” Übersetzern, die bei einem Amtsgericht registriert und mit einem speziellen Siegel ausgestattet sind
- Varianten rechtlicher Regelungen in den Bundesländern
- Keine Beschränkungen bzgl. technischer Mittel
- DIN 2345 – Qualitätssicherungsrichtlinien
- Anforderungen bei elektronischen beglaubigten Übersetzungen.
  - Elektronische Signaturen des Originals extrahieren
  - Signierer Identität prüfen, wo möglich – Prüfvermerk
  - Integrität des Ausgangsdokuments
  - Übersetzer-Signatur und – Siegel werden ersetzt durch zwei Charakteristika
    - Elektronische Signatur des Übersetzers
    - Ausweis als Übersetzer, z.B. Attributzertifikat
- **Untrennbare Bindung von Ausgangs- und Zieldokument**

Übersetzungssiegel





TransiDoc – Übersetzungs-Service



- Quell- un Zielsprache gemäß ISO 639-2 codes (z.B. “eng” für English)
  - XML schema type ‘xs:language’ verwendet ISO 639-2
- Standards für die Transliteration von Namen (z.B. ISO 9 für Kyrillisch → Latein)
- Datum und Zeit-Konvertierung
  - ISO 8601 und ISO 2015

Weiterentwicklungen

- Konvertierungsproblem
- Identiät des Ausgangsdokuments
- Attestierung des Transformationssystems

- Generalisierung: Workflow-Systeme
  „Signierte elektronische Laufzettel“ in der Vorgangsbearbeitung

Konvertierung problematischer Formate und Inhalte

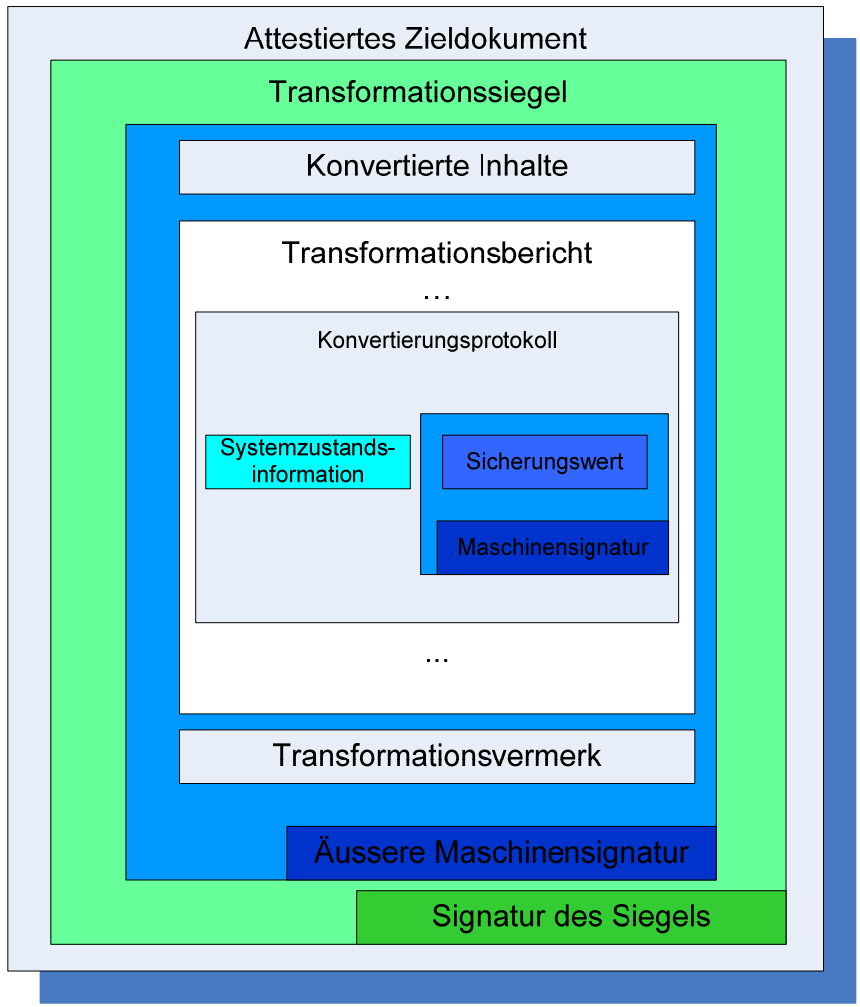
- Konvertierungsproblem
  - Verlustbehaftete Konvertierung bei weniger mächtigen Zielformaten
  - Mehrdeutigkeit bei mächtigeren Zielformaten
  - Gezielte Auslassung / Verfälschung bei Transformationen
  - Analog / verwandt: Präsentationsproblem
- Umgang mit problematischen Inhalten
  - (automatische) Detektion – schwierig, in Abhängigkeit von Komplexität und Offenheit des Ausgangsformats
    - Beispiel: Eliminieren aktiver Inhalte
  - Politiken bei der Transformation: Dokumentation und Default-Methoden
  - Präsentation: Menschliche Prüfer als Fallback; Anzeige in Varianten

Identität des Ausgangsdokuments

- Problem: Mehrere Zieldokumente liegen vor, welches entstammt dem „echten“ Ausgangsdokument?
  - Ausgangsdokument gefälscht oder
  - Transformation gefälscht
- Authentizitätsnachweise über digitale Dokumente ist schwierig, da sie keine Geschichte haben
- Technische Maßnahmun zur Gewinnung von Indizien
  - Hash-Wert des Ausgangsdokuments aufnehmen (TransiDoc-Datenstruktur)
  - Physische Analyse (Papier, Druck, Charakteristika handschriftl Unterschriften)
  - Digitale Wasserzeichen
  - (2D) Barcodes bei E2P-Transformation
  - Dokumenten-Historie mittels Metadaten herstellen

Attestierung des Transformationssystems

- Problematisch: Sichere Aussagen über **Eigenschaften des Transformationssystems**
  - Schlecht gesicherte Systeme
  - Transformation auf verteilten Systemen
  - Transformierer handelt für eigene Zwecke
- **Attestierte Transformation**
  - Sichere Feststellung von System-Eigenschaften und Identität
  - Bindung an das technische System und seine Eigenschaften
  - Bindung an den Transformationsprozess
  - Bindung an das Zieldokument
- Methoden z.B. basierend auf **Trusted Computing**
  - Trusted Boot und Stored Measurement Log
  - Maschinensignatur mit Systemidentität oder Pseudonym



Vertrauenswürdige Siegel für automatisierte Abläufe

- Umgang mit Dokumenten in (räumlich verteilten) Arbeitsabläufen findet auf vielen verschiedenen Plattformen statt
- Nachweis „Wer hat wann was auf welchem Gerät gemacht – und war dieses sicher“ fehlt meist – im Ablauf und für spätere Überprüfung
- Idee
  - Information über den Systemzustand bei Ausführung eines Arbeitsschrittes durch Attestierung
  - Integration der Attestierungsdaten in abgesicherte Datenstrukturen zum Nachweis von Abläufen
  - Grundmodell entsprechend TransiDoc
  - Integration in automatisierte Arbeitsabläufe
  - Integration elektronischer Signaturen, z.B. von Bearbeitern
  - Ergänzung existierender Standards wie BPEL
- Entsprechende Verwendung der TransiDoc-Ergebnisse in EU-FP6-Projekten SERENITY und HYDRA

Details zum Nachlesen

Der TransiDoc-Schlussbericht erscheint in einer ausführlichen Version demnächst im Nomos-Verlag