Revisions- und Rechtssicherheit beim Umgang mit elektronisch signierten Dokumenten

Andreas U. Schmidt

Fraunhofer-Institut für sichere Informationstechnologie SIT, Darmstadt

Unternehmensweites Vertragsmanagement

16 & 17 Oktober 2006

Köln

Fraunhofer Institut Sichere Informations-Technologie

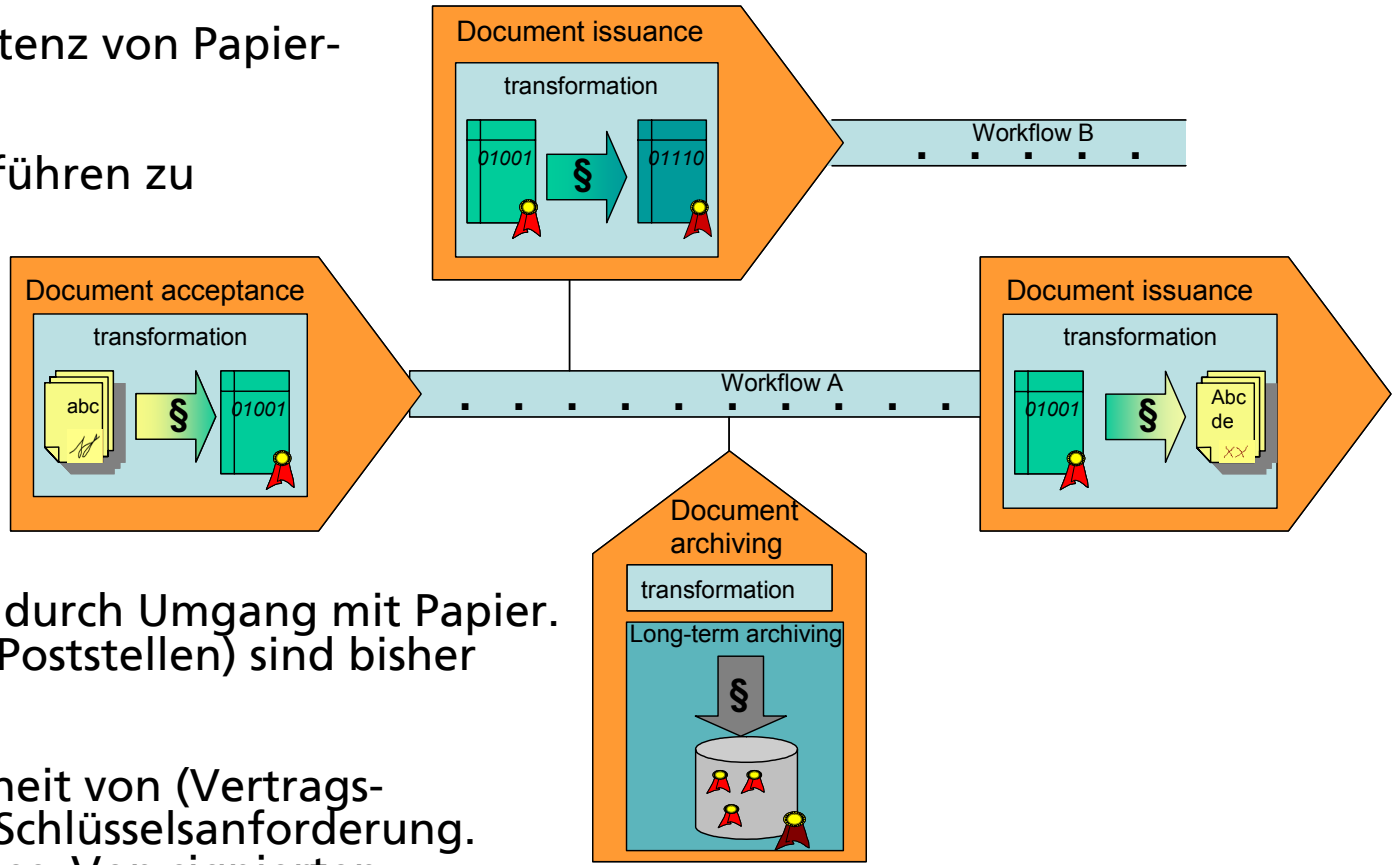
Outline

1. Ausgangspunkt – zentrale Problemstellungen
2. Archivierung elektronisch signierter Dokumente
3. Transformationen von Dokumenten
4. Beglaubigte Übersetzungen elektronisch signierter Dokumente

1.1 Schnittstellen für elektronisch signierte Dokumente in Geschäftsprozessen

Der Ist-Zustand ist nicht befriedigend

- Vorherrschender Zustand: Koexistenz von Papier- und elektronischen Versionen
- Hohe rechtliche Anforderungen führen zu
  - parallele Aktenführung in elektr. und Papierform.
  - Out-of-band Prozesse und Medienbrüche



3 zentrale Schnittpunkte

- **Dokumenteneingang**. Dominiert durch Umgang mit Papier. Nur-elektronische Prozesse (elektr. Poststellen) sind bisher isolierte Efforts

- **Archivierung**. Langfristige Sicherheit von (Vertrags-)Dokumenten ist eine existenzielle Schlüsselsanforderung. Elektronische Aufbewahrung – insbes. Von signierten Dokuemnten – ein Schlüsselproblem.

- **Dokumentenausgang.** Lesbarkeit von Datenformaten und Verifizierbarkeit von Signaturen ist nicht universell garantiert. Vieles bleibt noch bei Papier-Post

1.2 Anforderungen an organisatorische Regelungen und Infrastruktur (aus Konsultationen in der EU [Collaborative Working Environments])

Some infrastructure components should be developed and bound to existing workflow processes

Signature interoperability An interoperability platform for digital signatures is needed that allows the verification, and creation of digital signatures within various technical and collaboration environments, as well as the integration of a multitude of public-key infrastructures (PKI).

Secure transformation of signed documents between data formats is essential. Means for a secure conversion between physical, e.g. paper, and digital representation are needed. Changing the digital document format leads to the problem that the original electronic signature breaks (similar problem for digitised paper documents). One needs means to preserve the probative force of digitally/handwritten signed documents even after transformation/conversion.

Long-term archiving (LTA) can rest on established and ongoing scientific research and existing standards (IETF/LTANS). The integration to a comprehensive document longevity support platform is an important novel requirement for collaboration infrastructures

Legal guidelines and legally sound methodologies. The requirements for document processing stem from the legal background governing the specific application sector, e.g., compulsory periods of record-keeping. Specific rules still cause practical problems with electronically signed docs. Existing legal requirements for document processing in different application areas and international collaboration have to be respected. A legally sound deployment methodology for the organisation of comprehensive inter-organisational workflows and signed document processing is desirable.

1.3 Einige rechtliche Regelungen und Anwendungsfelder

- §6 SigG, §17 SigV: Langzeit-Dokumente sind neu zu signieren!
- GDPdU (§ 14 Abs. 4 UStG: rechtliche Anforderung für Archivierung)
- §33 Verwaltungsverfahrensgesetz, Beurkundungsgesetz regeln amtliche (Behörden) und öffentliche (Notare) Beglaubigungen in elektronischer Form
- Justizkommunikationsgesetz, erlaubt elektronische Aktenführung und Kommunikation bei der Justiz
- Emissionshandel, erfolgt elektronisch, mit qualifizierter elektronische Signatur
- Medizin HBA, Patientenakte

Globales Bild:
Rechts-Berufe, Medizin und Verwaltung als Türöffner für die elektronische Signatur

Der Sicherheitskanon (CIA – Confidentiality, Integrity, Availability)

Langzeit – Vertraulichkeit
langfristig sichere Verschlüsselung

Langzeit – Integrität
Hash- und Signatur-Algorithmen

Langzeit – Verfügbarkeit
Datenformate altern und werden unleserlich

2.1 Risiken für die Langzeitaufbewahrung elektr. Signierter Dokumente

1) Elektronische Signaturen können Beweiskraft verlieren (“altern”) durch die Zunahme von Rechenleistung und mögliche Fortschritte in der Kryptologieoder noch unbekannte Technologien wie Quanten Computer.

- Elektronisch signierte Dokumente verlieren ihre rechtliche Beweiskraft und damit Bindungswirkung

2) 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.

2.2 Die Horrorvision: Signaturen ohne Wert

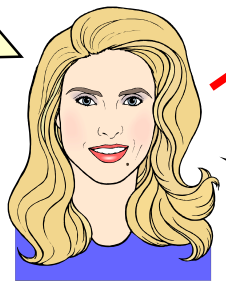
6 Sie sagt bestimmt die Wahrheit, aber ohne Beweis sind mir die Hände gebunden.

5 Der Vertrag hat damit seinen Beweiswert verloren.

3 Stimmt.
Klägerin, sind Sie ihrer Pflicht zur Erneuerung digitaler Signaturen
gemäß §6 SigG und $17 SigV
nachgekommen?

1 Ich habe mein Ladenlokal
für 20 Jahre gemietet.
Den Vertrag hat der Beklagte digital signiert.
Jetzt soll ich ausziehen, weil ein Konkurrent bereit ist, die doppelte Miete zu zahlen.

2 Ein derartiger Vertrag existiert nicht!
Und überhaupt:
Die digitale Signatur basiert auf RSA mit 256 Bits und auch noch MD4 – so etwas bricht heute jeder PDA.



4 Signaturerneuerung??
?
Nein.

2.3 Lösungskonzept für das Alterungsproblem – ArchiSig/ArchiSoft

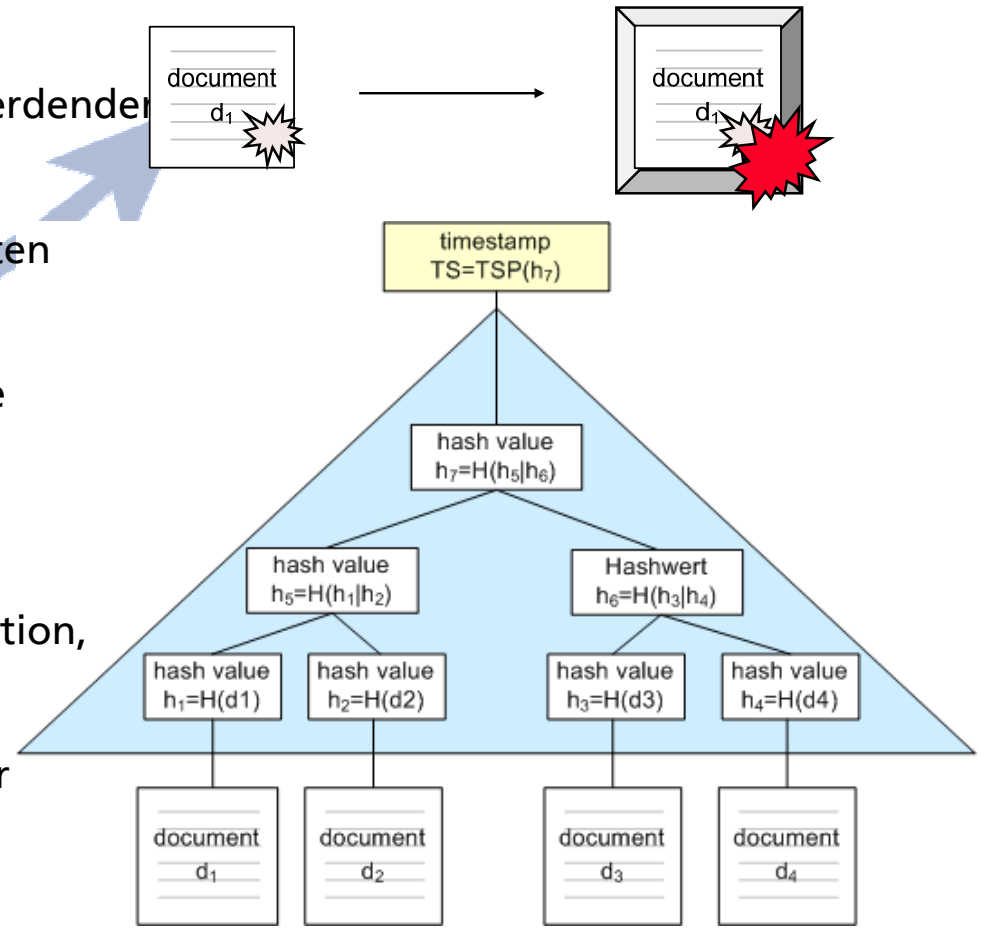
Konzept der Signaturerneuerung

Durch Zeitstempel (und optimiert durch Hash-Bäume)

• Erneuerung und Zeitstempelung bei z. B. schwächer werdender Hash-algorithmen

• jedes Dokument wird gesichert durch einen so genannten evidence record (Verifikationsdaten, Zertifikatsketten)

• effektiv für große Dokumentenmengen und durch eine vollautomatisierte Prozedur



Organisatorischer Hintergrund:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen:

Jährliche Bekanntgabe der Algorithmen und zugehöriger Parameter, wie Schlüssellänge

geeignet für qualifizierte elektronische Signaturen nach Signaturgesetz (SigG) und Signaturverordnung (SigV)

Prognosezeitraum: 6 Jahre (Beispiele vom Januar 2005: Public-Key-Verfahren: RSA Schlüssellänge mindestens 1024, empfohlen 2048, Hashalgorithmen: RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512)

- Hash-Werte berechnen und Zeitstempel einholen
- Erneuerungszeitpunkte festlegen
- Sicherheitseignung von Algorithmen einholen und auswerten
- erzeugen und managen der evidence records
- Zugriff auf evidence records und Verifikation

Beispieleinbindung in ein existierendes DMS:

Geeignet für größere Organisationen

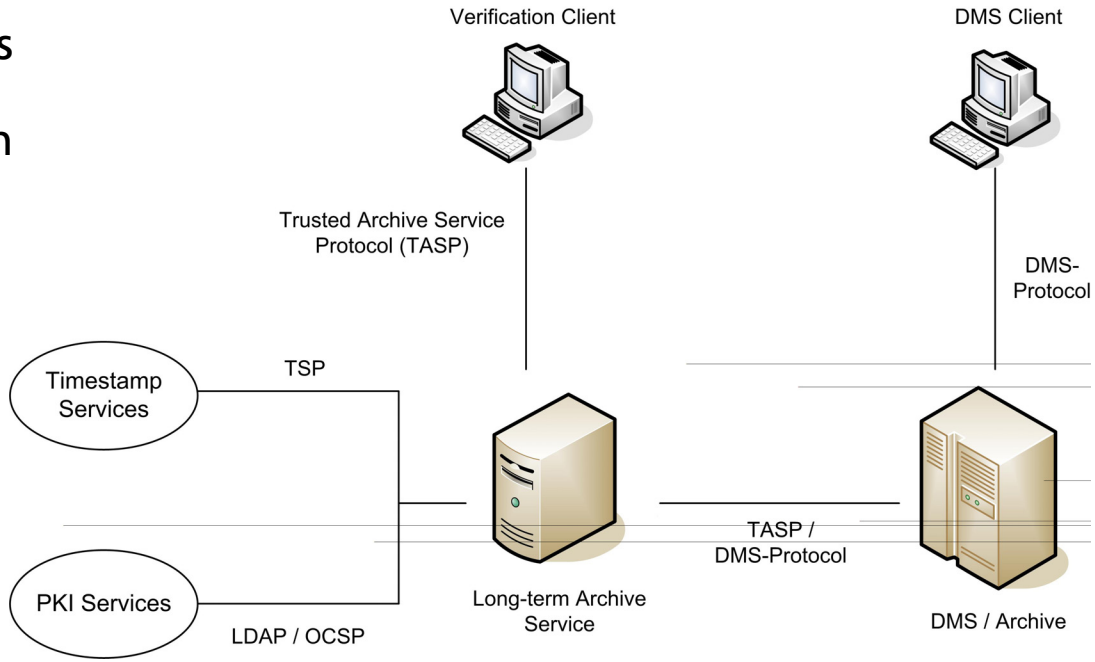
LTA unabhängig von DMS

DMS spricht den LTA an

LTA holt Dokumente vom DMS

LTA arbeitet im Hintergrund weit gehend ohne Benutzer-Interaktion

Alternativ: Remote LTA service



Der Sicherheitskanon (CIA – Confidentiality, Integrity, Availability)

Langzeit – Vertraulichkeit
langfristig sichere Verschlüsselung

Langzeit – Integrität
Hash- und Signatur-Algorithmen

Langzeit – Verfügbarkeit
Datenformate altern und werden unleserlich

3.1 TransiDoc – Rechtssichere Transformation signierter Dokumente

August 2004 – April 2007, Konsortialführung: Fraunhofer SIT

Konsortium

Fraunhofer Institut Sichere Informat Technologie

UniversitätsKlinikum Heidelberg

Inter Component Ware®

provet
Projektgruppe verfassungsverträgliche Technikgestaltung e.V.

Curiavant Internet GmbH

Fördergeber

Bundesministerium für Wirtschaft und Arbeit

DLR
PT Multimedia

BNotK
BUNDESNOTARKAMMER
(assoziiert)

DATEV
(assoziiert)

Primäre Anwendungsbereiche

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

Projekt-Ziele

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

www.transidoc.de

3.2 Grundsätzliches

Oberster Grundsatz: **Reduzierung von Transformationen**

- durch organisatorische Maßnahmen, wie
- Verwendung von standardisierten, stabilen, akzeptierten Formaten

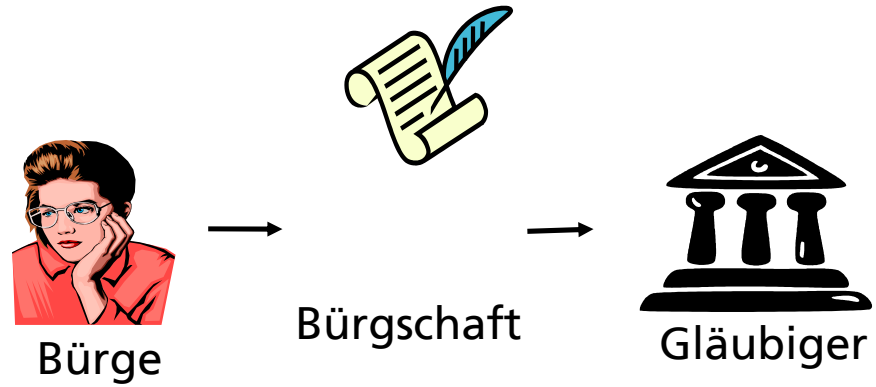
Anforderungen an die Transformation signierter Dokumente

- Vergleichbarer Beweiswert zwischen Ausgangs- und Zieldokument
- Möglichkeit auf das Ausgangsdokument zu verzichten

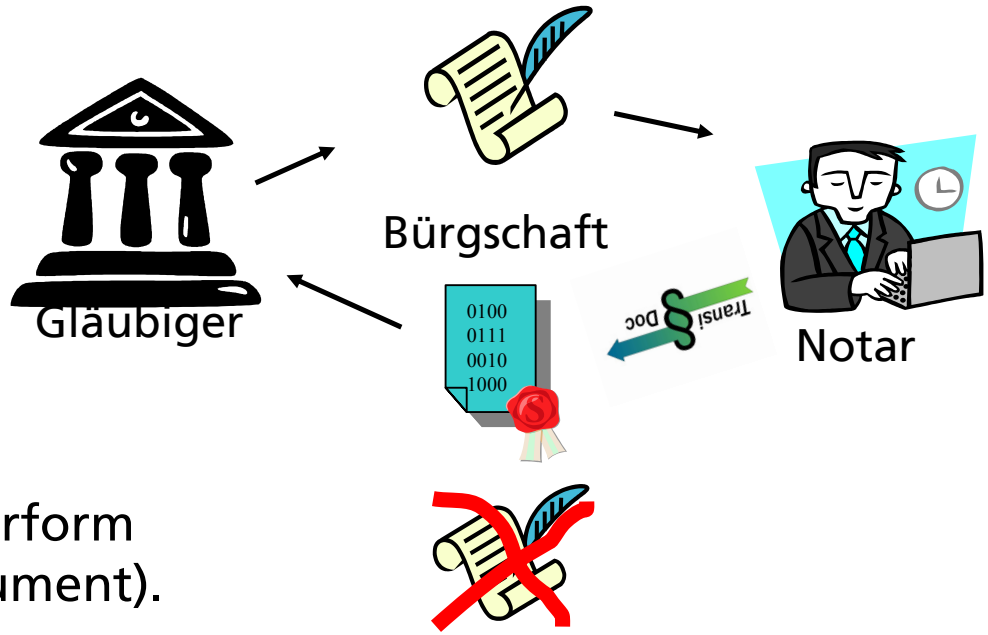
Die Einhaltung der Grundsätze ist eine notwendige Voraussetzung zur Erfüllung der Anforderungen

3.3 Anwendungsszenario: Bürgschaft 1/2

Schritt 1:
Ausstellen einer Bürgschaft = einseitiger Vertrag gegenüber dem Gläubiger (Bank)



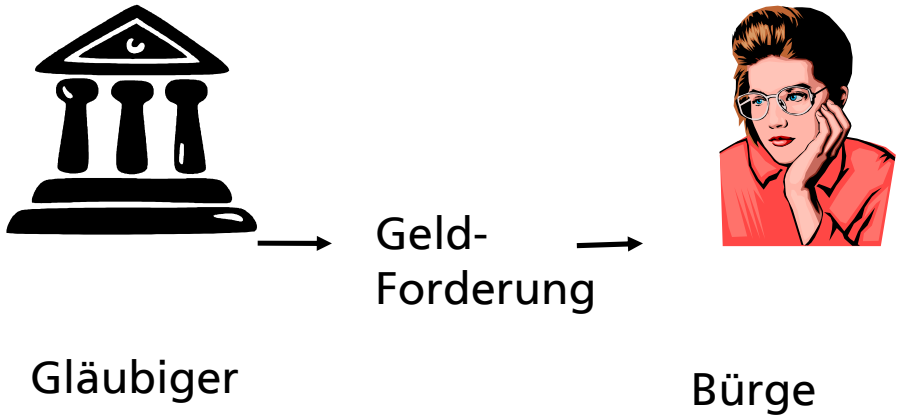
Schritt 2:
Notarielle Beglaubigung der digitalisierten Fassung der Bürgschaft gemäß BeUrkG



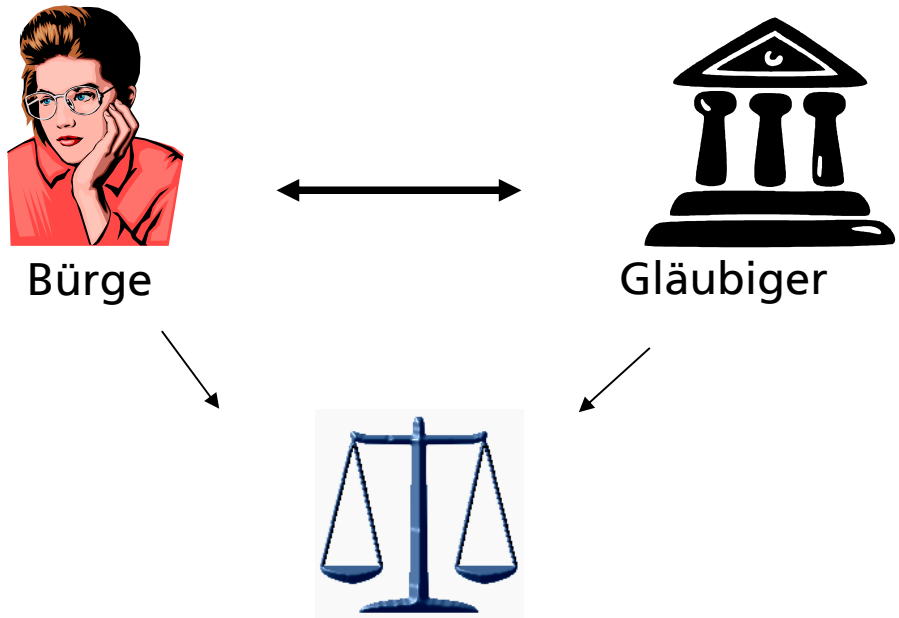
Schritt 3:
Gläubiger vernichtet die Papierform der Bürgschaft (Ausgangsdokument).

3.4 Anwendungsszenario: Bürgschaft 2/2

Schritt 4:
Hauptschuldner ist zahlungsunfähig.
Der Gläubiger verlangt Geld vom Bürgen.



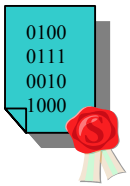
Schritt 5:
Bürge lehnt Forderung ab und widerspricht der Höhe der Bürgschaft.
Gläubiger besteht auf Zahlung.



Schritt 6:
Der Gläubiger zieht vor Gericht.

3.5 Ziel: Das transformierte Dokument reicht als Beweis

Gläubiger

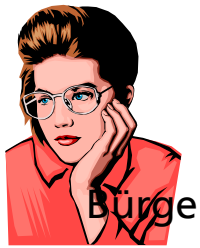


Aha, das elektronische Dokument ist das Ergebnis einer Transformation.
Das Ausgangsdokument liegt nicht mehr vor.

Wurde die Transformation ordnungsgemäß durchgeführt?

Die Prüfung hat ergeben, dass die **TransiDoc Grundsätze** eingehalten wurden.

Das transformierte Dokument reicht daher bei der Beweisführung aus. Das Ausgangsdokument ist nicht notwendig.



Bürge

„Ohne das Original der Bürgschaft hat die Bank keinen Beweis.“

3.6 Nachträgliche Prüfungen einer Transformation

Ich muss erkennen können, dass es sich um ein transformiertes Dokument handelt.

Das Dokument ist als transformiertes Dokument erkennbar.

Welche Transformation ist durchgeführt worden?

Die durchgeführte Transformation inkl. der eingesetzten Geräte und Software sind protokolliert.

Wer hat das Ausgangsdokument signiert / unterschrieben? Welche Prüfungen wurden durchgeführt?

Name, Adresse und eingescannte Unterschrift des Bürgen sind protokolliert.

Wer hat die Transformation durchgeführt, wer ist verantwortlich für die Transformation?

Elektronische Signatur und Zertifikat weisen den Transformierer aus.

Ist die Person berechtigt / autorisiert, diese Transformation durchzuführen?

Ja, das Attributzertifikat weist den Transformierer als Notar aus.

3.7 Grundsätze ordnungsgemäßer Transformationen 1/3

Anstreben einer automatisierbaren Lösung

- **Effizienz, Wirtschaftlichkeit, Vermeidung menschlicher Fehler**
- **Erforderliche menschliche Eingriffe absichern**

Übereinstimmung der Inhalte

Anwendungskontext bestimmt Kriterien für Übereinstimmung:

- z.B. Farbtiefe, Maßstabtreue, Fehler wie ungültige Signaturen
- Gezielte Veränderungen wie Anonymisieren, Dokumentenauszüge

Sicherung der Urheberschaft

- **Elektronische Signaturen verifizieren und Ergebnis festhalten**
- **Korrekte Aufnahme der handschriftlichen Unterschrift/Siegel**

3.8 Grundsätze ordnungsgemäßer Transformationen 2/3

Wahrung der Datenintegrität

- **Betrifft Ausgangs- und Zieldokument, Protokolle, Prüfergebnisse**

Zurechenbarkeit der Transformation

- **Prüfbare Zuordnung zum Verantwortlichen**
- **Durch elektronische Signatur bzw. Unterschrift**

Durchführung der Transformation nur durch Berechtigte

- **Nachträgliche Prüfbarkeit der Berechtigung**
- **Durch Attributzertifikate bzw. Siegel**

3.9 Grundsätze ordnungsgemäßer Transformationen 3/3

Gewährleistung des Daten- und Geheimnisschutzes

- **Schutz des Transformationsprozesses gegen unberechtigten Zugriff**
- **Abwägen zwischen Datensparsamkeit und Beweissicherheit**

Verwendbarkeit und Verkehrsfähigkeit des Zieldokuments

- **Langfristig stabiles, standardisiertes Zielformat**
- **Verwendbarkeit des Zieldokuments ohne Ausgangsdokument**

Nachvollziehbarkeit der Transformation

- **Protokolle des Transformationsverlaufs, inklusive:**
- **Eingesetzte Systeme, Parameter, Prüfergebnisse, Prüfvorgaben**

Zuverlässigkeit des transformierenden Systems

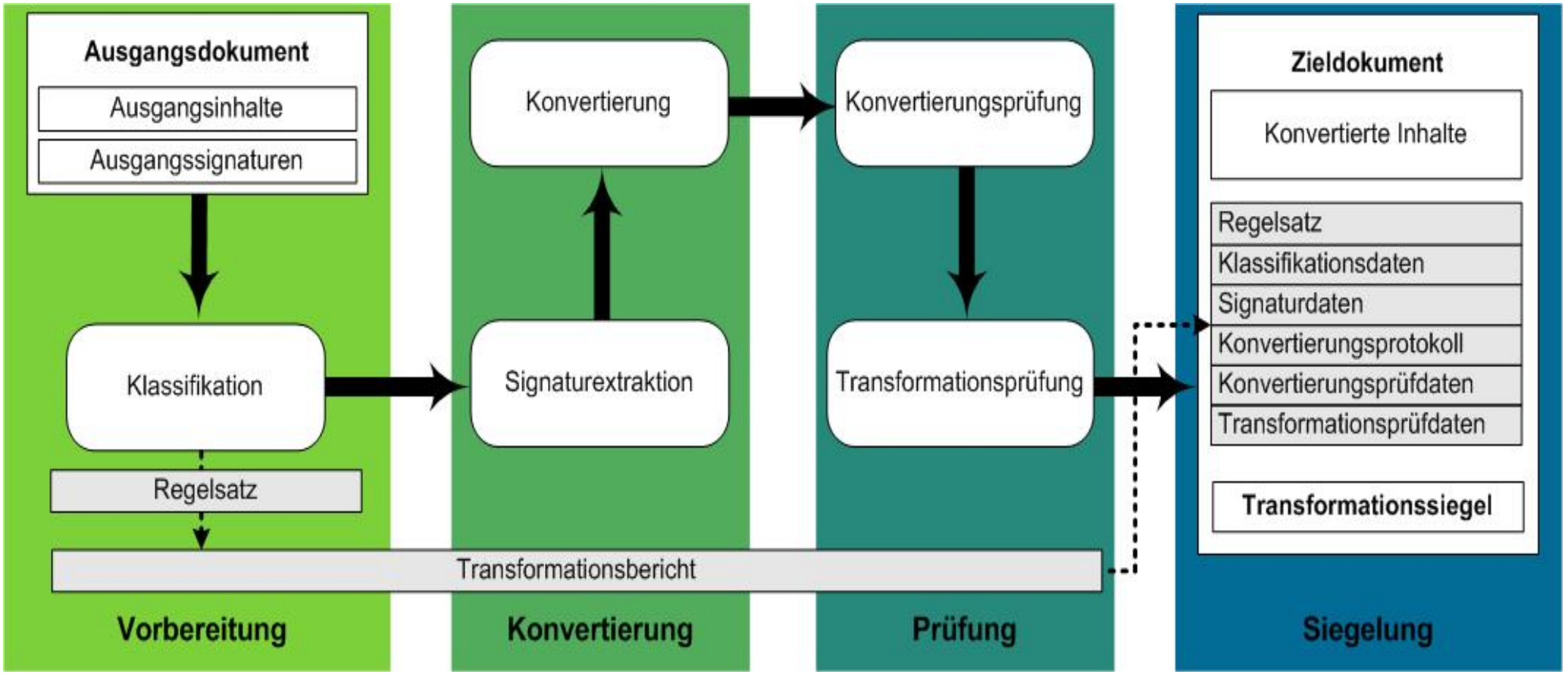
3.10 Ziele und Aufgaben des Transformationsprozesses

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

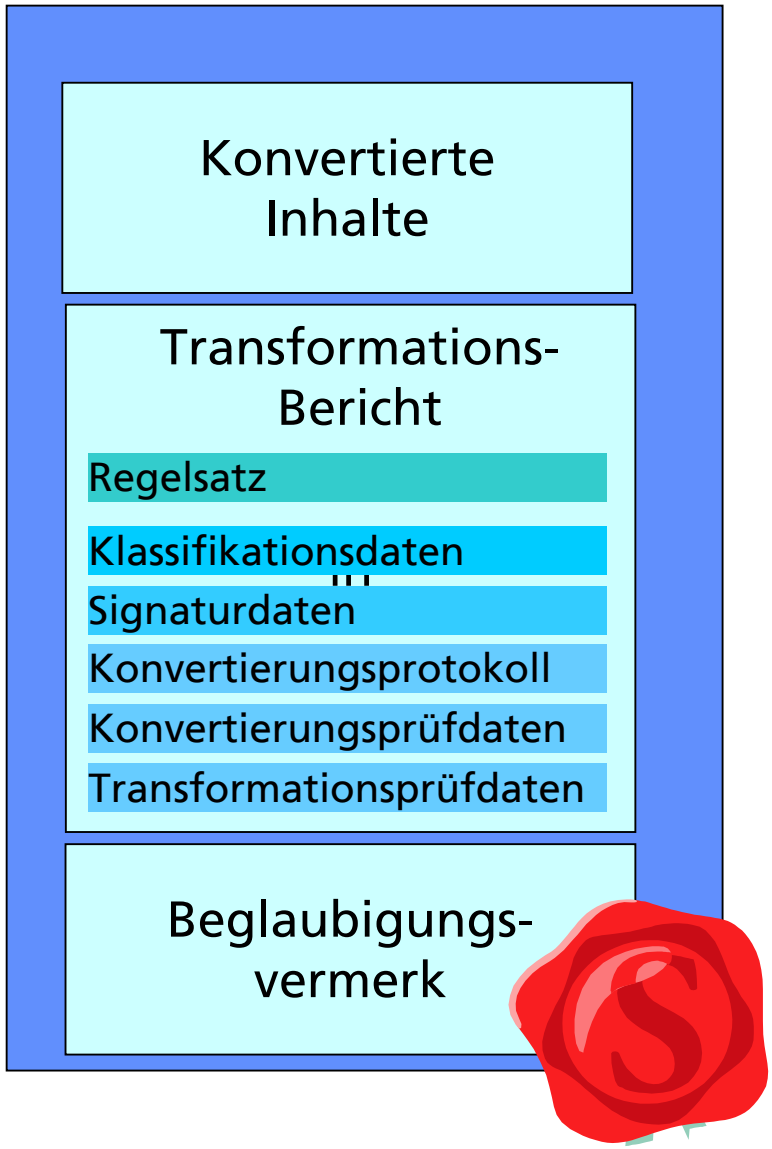
3.11 Phasen einer sicheren Transformation



3.12 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
- Beglaubigungsvermerk

3.13 Struktur des Beglaubigungsvermerks

§ 33 Abs. 4 Nr. 3 und 4 VwVfG für die amtliche Beglaubigung
§ 39a BeurkG für die öffentliche Beglaubigung

- Bezeichnung des Ausgangsdokuments
- Signaturdaten aus Signaturextraktion
- Verwendungszweck des Zieldokuments
- Feststellung der Übereinstimmung
- Zeitpunkt der Beglaubigung
- Ort der Beglaubigung
- Autorisation des Beglaubigers

  - **Rolle des Beglaubigers (z.B. Notar, ermächtigter Übersetzer)**
  - **Verantwortliche Stelle, die dem Beglaubiger bestätigt, dass er in dieser Rolle agieren darf (z.B. BNotK, Amtsgericht).**

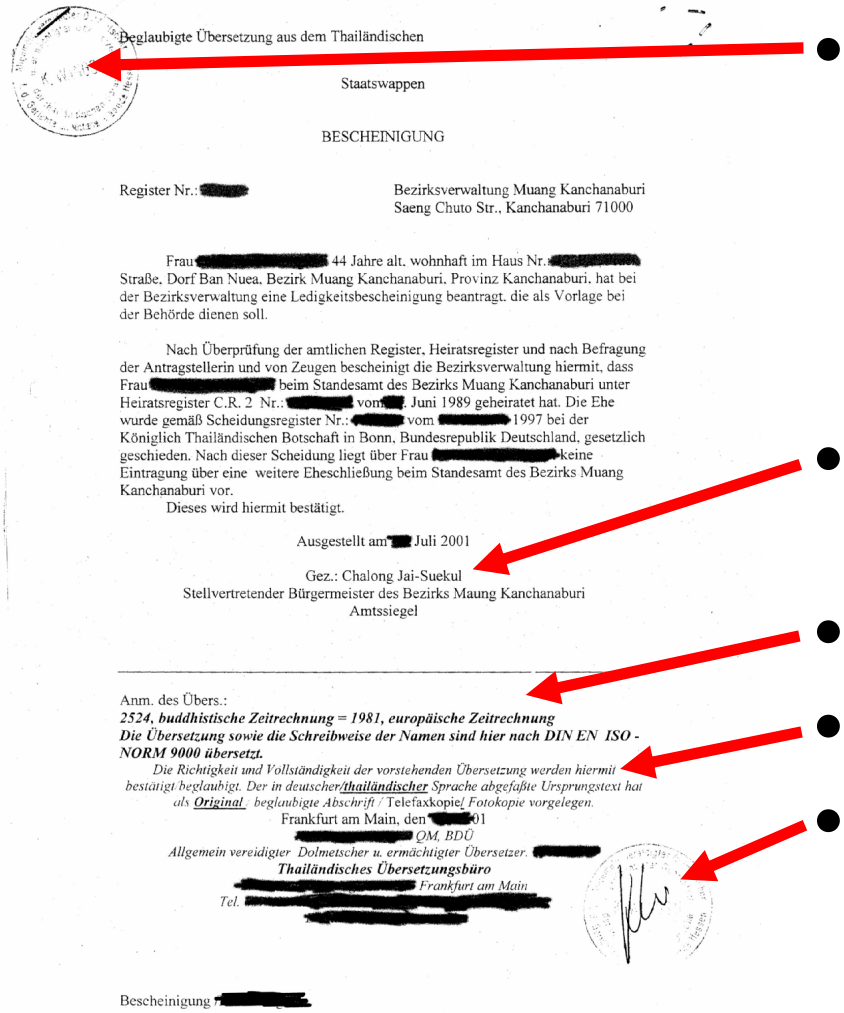
4.1 Beglaubigte Übersetzungen – Ein (vielleicht gar nicht so) exotisches Beispiel

Diplomarbeit von **Jan Piechalski** an der TU Darmstadt

4.2 Authorised Translations under German Law

- Performed by a professional translator, sworn, registered with a judicial circuit corresponding to the location of his office, and equipped with a special seal
- Legal regulations concerning authorising of translators vary within Germany between federal states
- No legal restrictions to the way authorised translations are created

4.3 Authorised Translations – Standards (1/2)



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

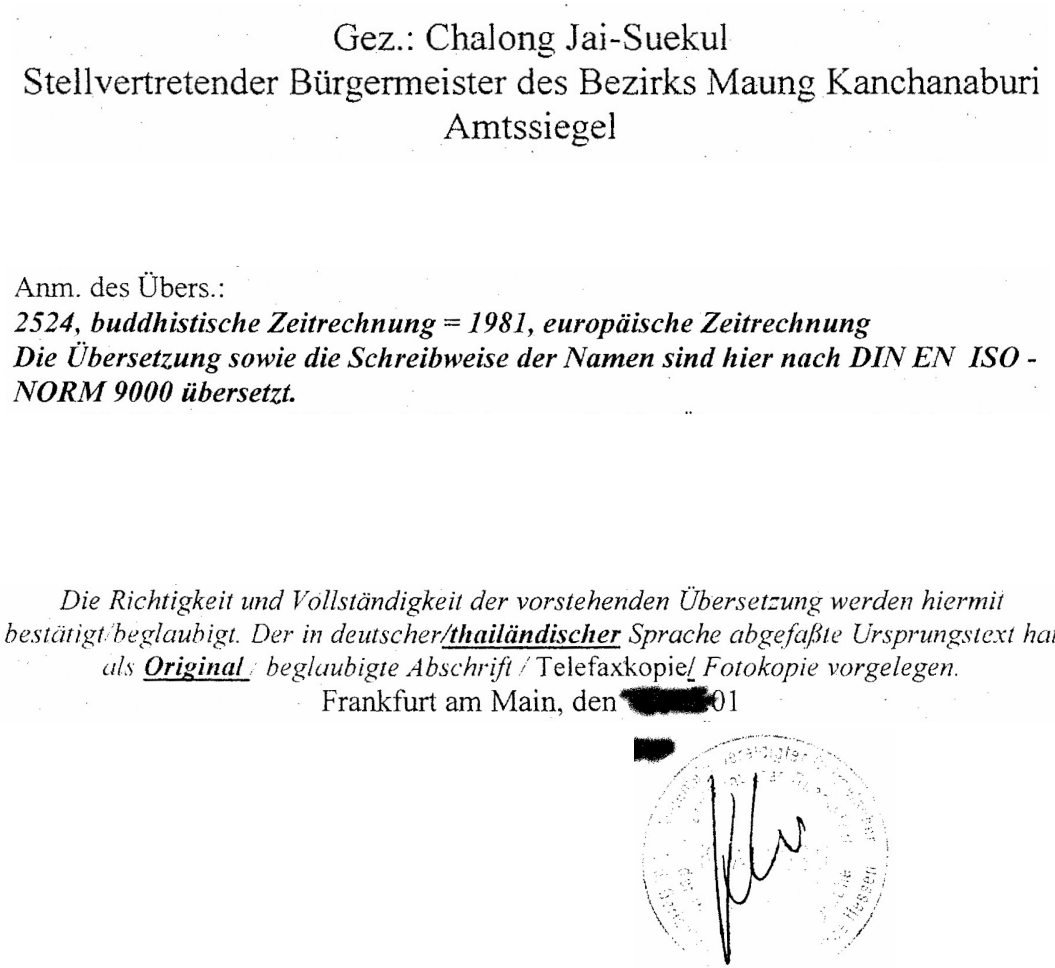
Gez.: Chalong Jai-Suekul
Stellvertretender Bürgermeister des Bezirks Maung Kanchanaburi
Amtssiegel

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]

- The source document and the target document are bound together by stapling the source with the target and stamping the seal over the staple
- Description of handwritten signatures
- Annotation
- "Certificate of accuracy"
- Stamp of the seal and signature

4.4 Authorised Translations – Standards (2/2)



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]

- Handwritten signatures in the source document should be described in the target document, if inevitable as "illegible"
- Annotations made by the translator (e.g. defects in the source document, transliterations of names or calendar transformations having been applied)
- "Certificate of accuracy" consisting of a statement like "I hereby certify the completeness and accuracy of the translation", place, date, stamp of the seal and signature (two authentication characteristics)

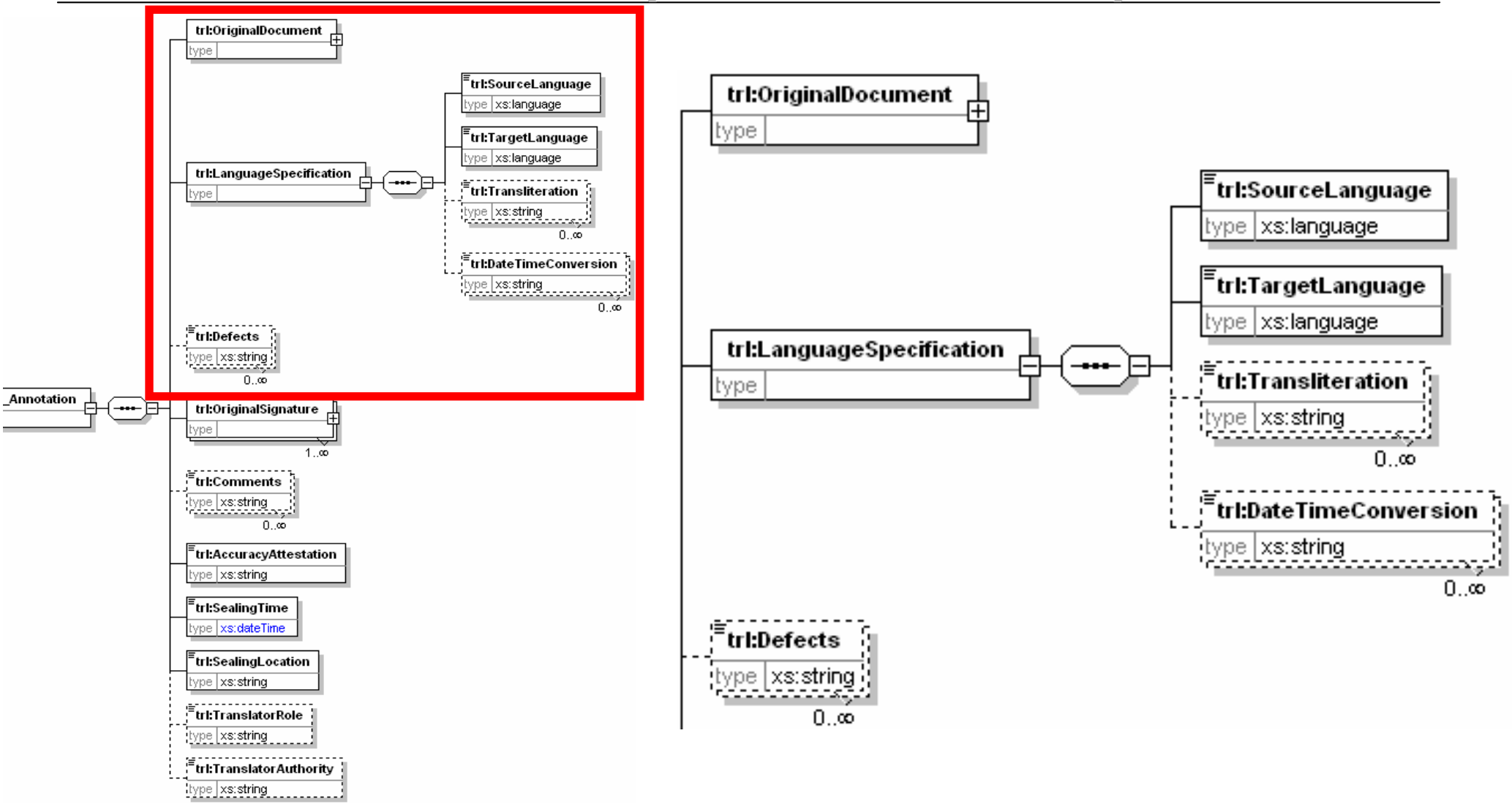
4.5 Requirements for Electronic Translations

- Electronic signatures in the original document: signature extraction instead of a simple description
  - Signer's identity
  - Integrity of the source
- Two authentication characteristics replacing signature and seal
  - Electronic signature
  - Attribute certificate
- **Binding inseparably source and target document by inserting the entire source document into the annotation of the target**

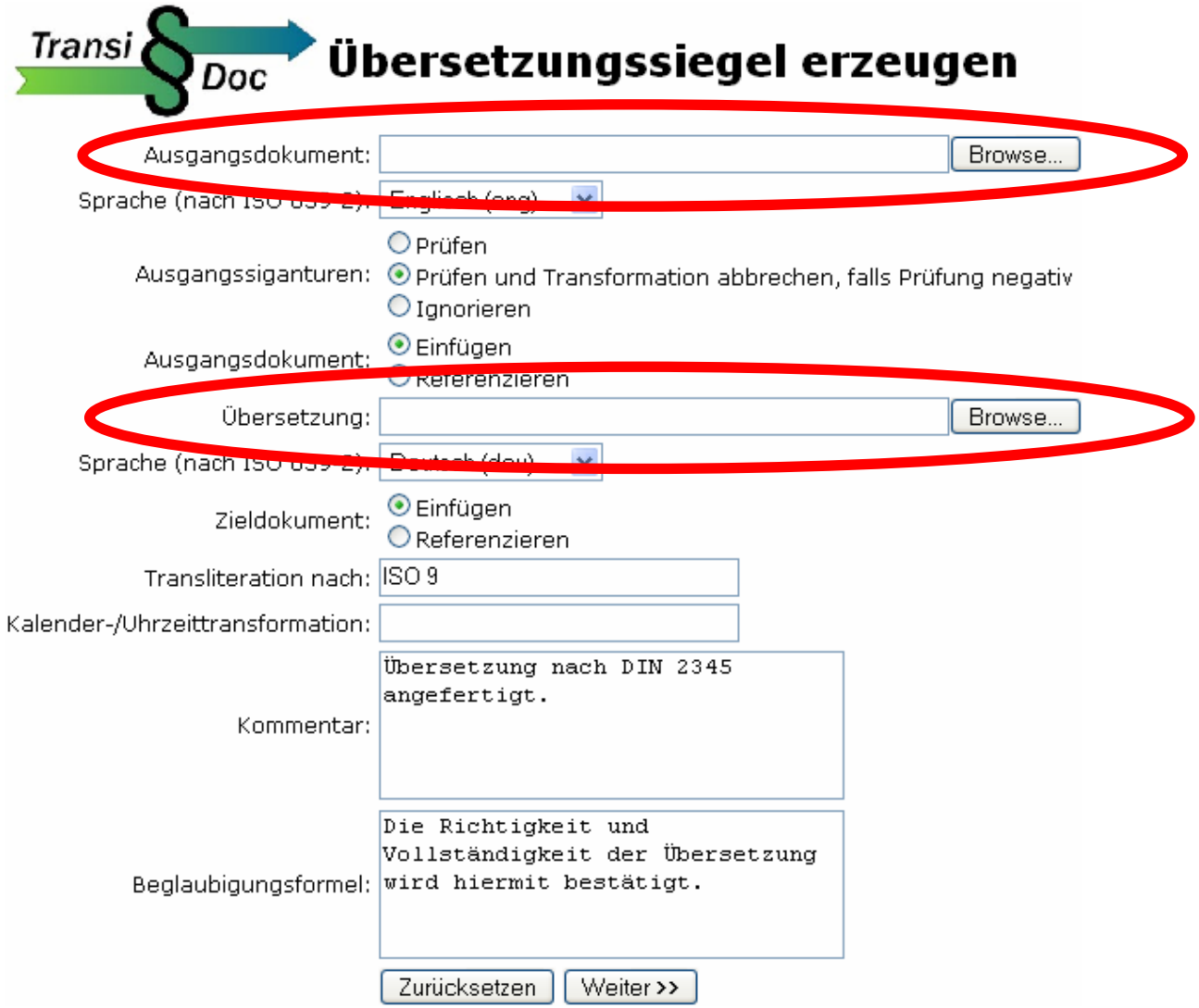
4.6 Applicable Internationalisation Standards

- Specification of source and target language with ISO 639-2 codes (e. g. “eng” for English)
  - The XML schema type ‘xs:language’ applies ISO 639-2
- Standards for transliteration of names (e. g. ISO 9 for Cyrillic → Latin)
- Date and time conversion during translation
  - ISO 8601 and ISO 2015 – Standards concerning notation of date and time

4.7 Translation Seal (from 20000 feet)

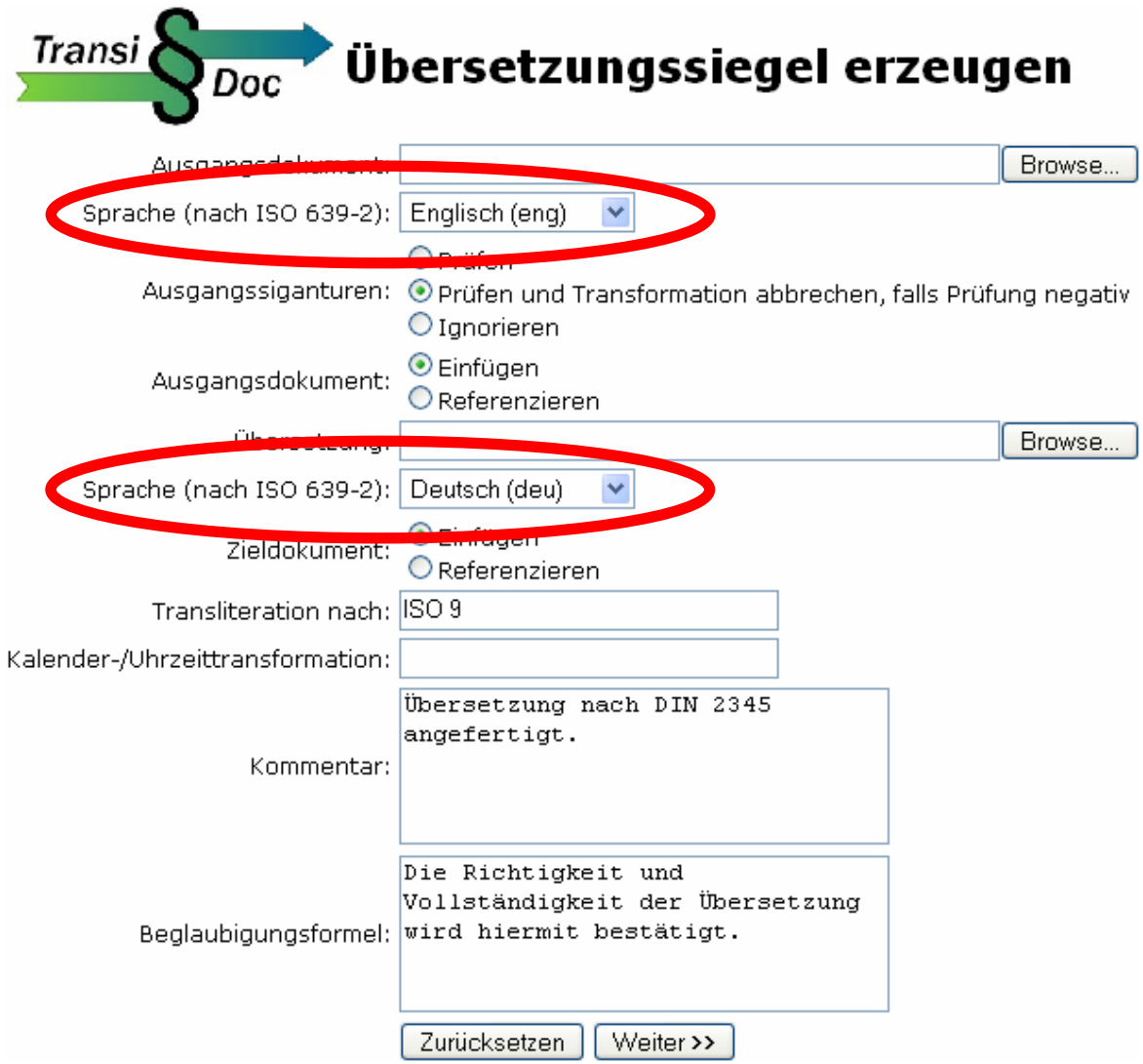


4.8 TransiDoc Web Service – Classification (1/6)



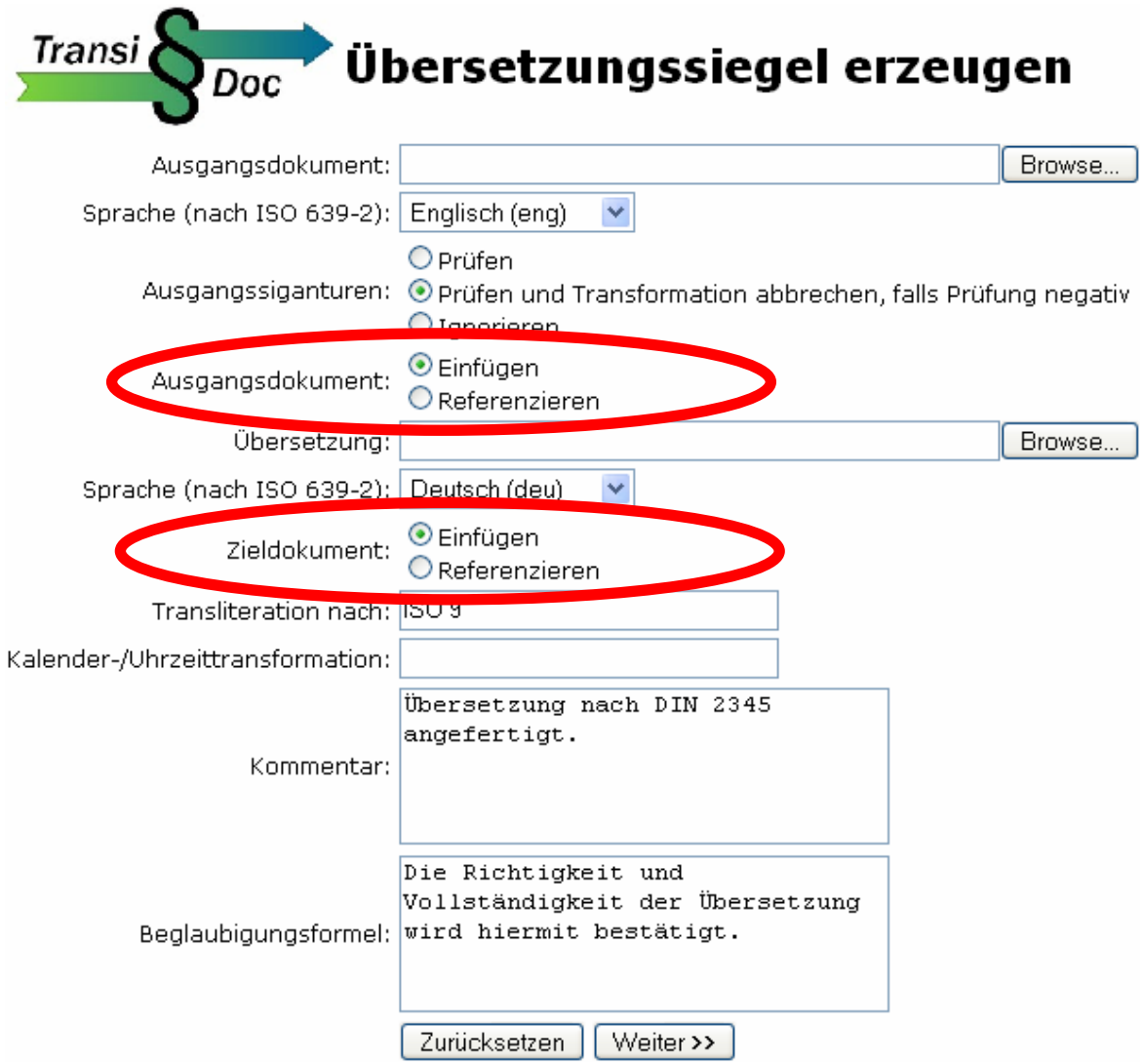
- File upload of original document and translation

4.9 Web Service – Classification (2/6)



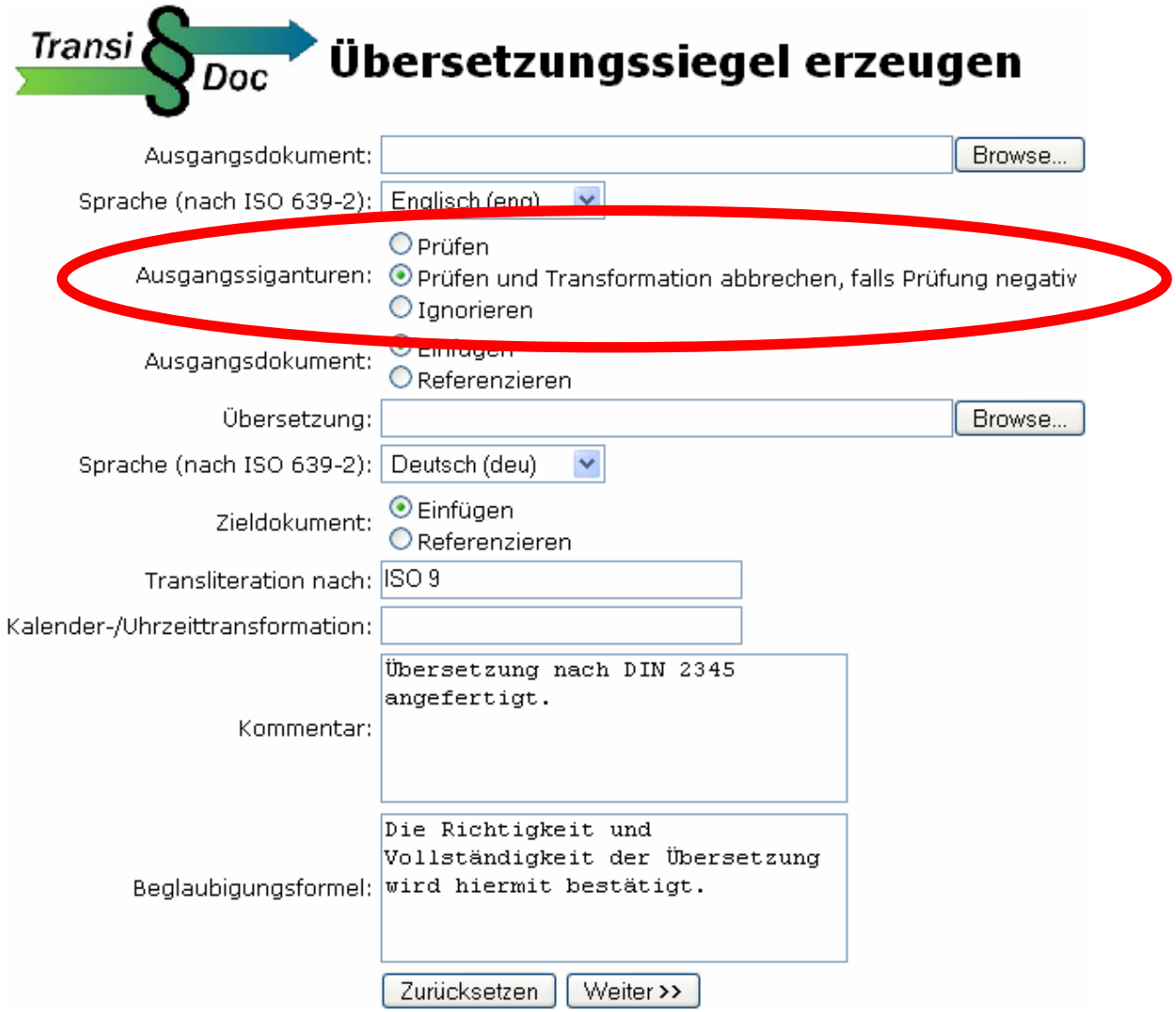
- Source and target language specification according to ISO 639-2

4.10 Web Service – Classification (3/6)



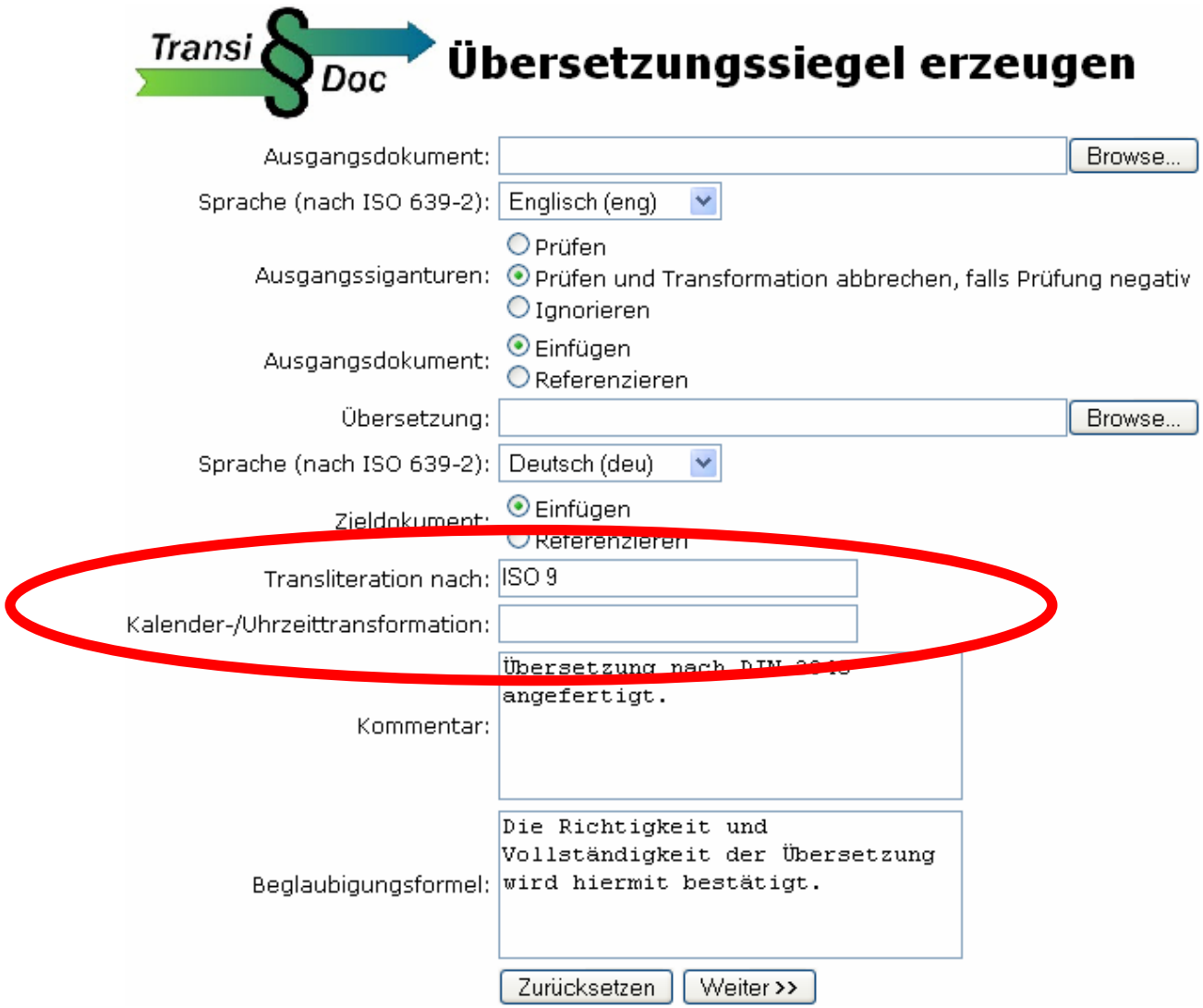
- Insert or reference source and target document

4.11 Web Service – Classification (4/6)



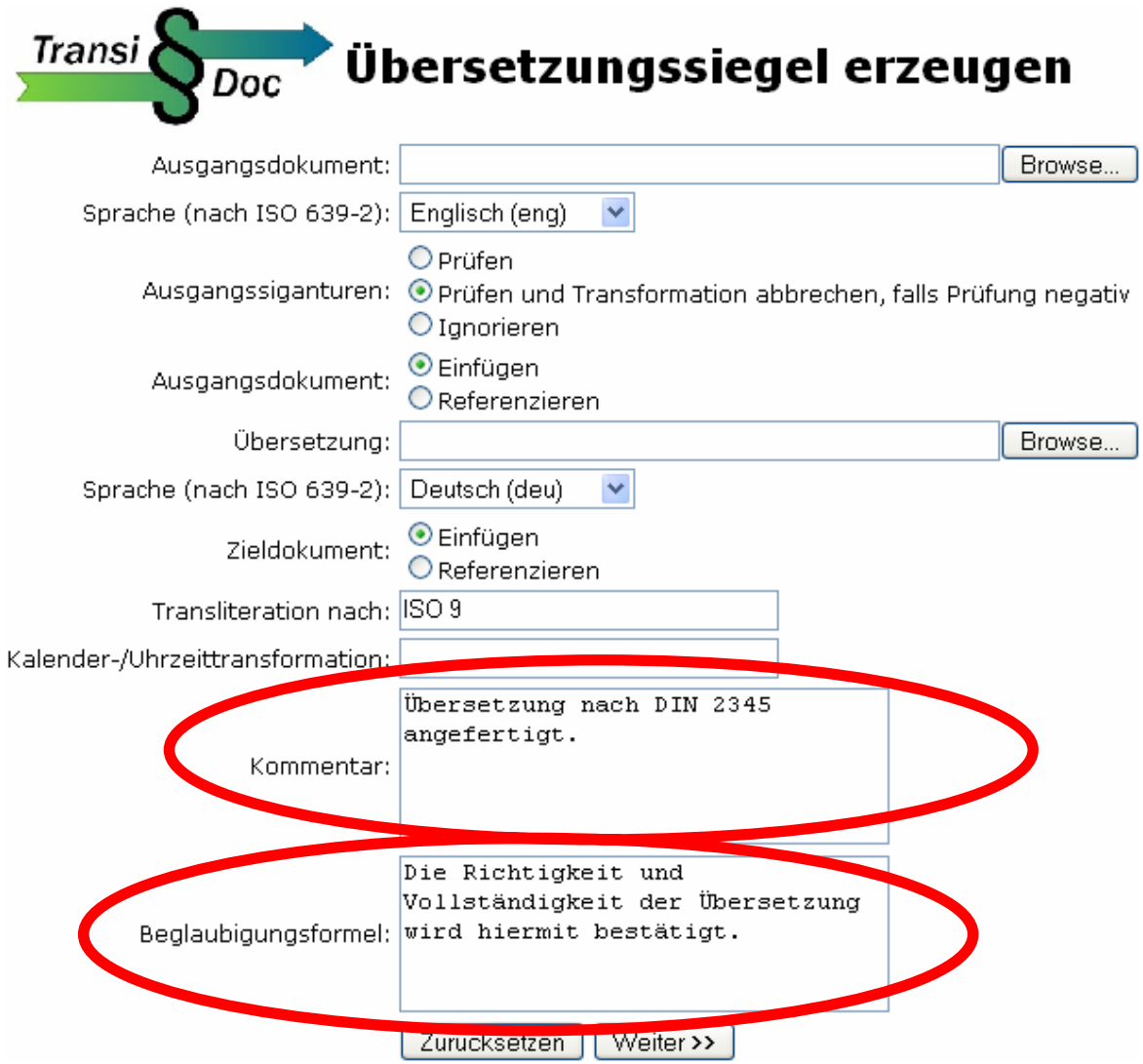
- Original signatures policy
  - Validate signatures and continue transformation in any case
  - Validate signatures and abort transformation, if validation result negative
  - Ignore original signatures

4.12 Web Service – Classification (5/6)



- Transliteration standard of names
- Conversion method of date and time

4.13 Web Service – Classification (6/6)



- Translator's comment
- Attestation of accuracy and completeness of the translation

4.14 Web Service – Signature Extraction

Algorithm: http://www.w3.org/2000/09/xmldsig#sha1

Algorithm: http://www.w3.org/2000/09/xmldsig#dsa-sha1

Result of IntegrityCheck: 0

Verification Result: true

Signer Name: CN=X/Secure 1024-bit DSA crt, OU=X/Secure, O="Baltimore Technologies, Ltd.", ST=Dublin, C=IE

Hashalgorithm: http://www.w3.org/2000/09/xmldsig#sha1

PK Algorithm: http://www.w3.org/2000/09/xmldsig#dsa-sha1

Parameter q: Value=160

Parameter p: Value=1024

Weiter

- Signature verification results
- Used algorithms

4.15 Web Service – Show Translated Document

TransiDoc **Transformationsergebnis**

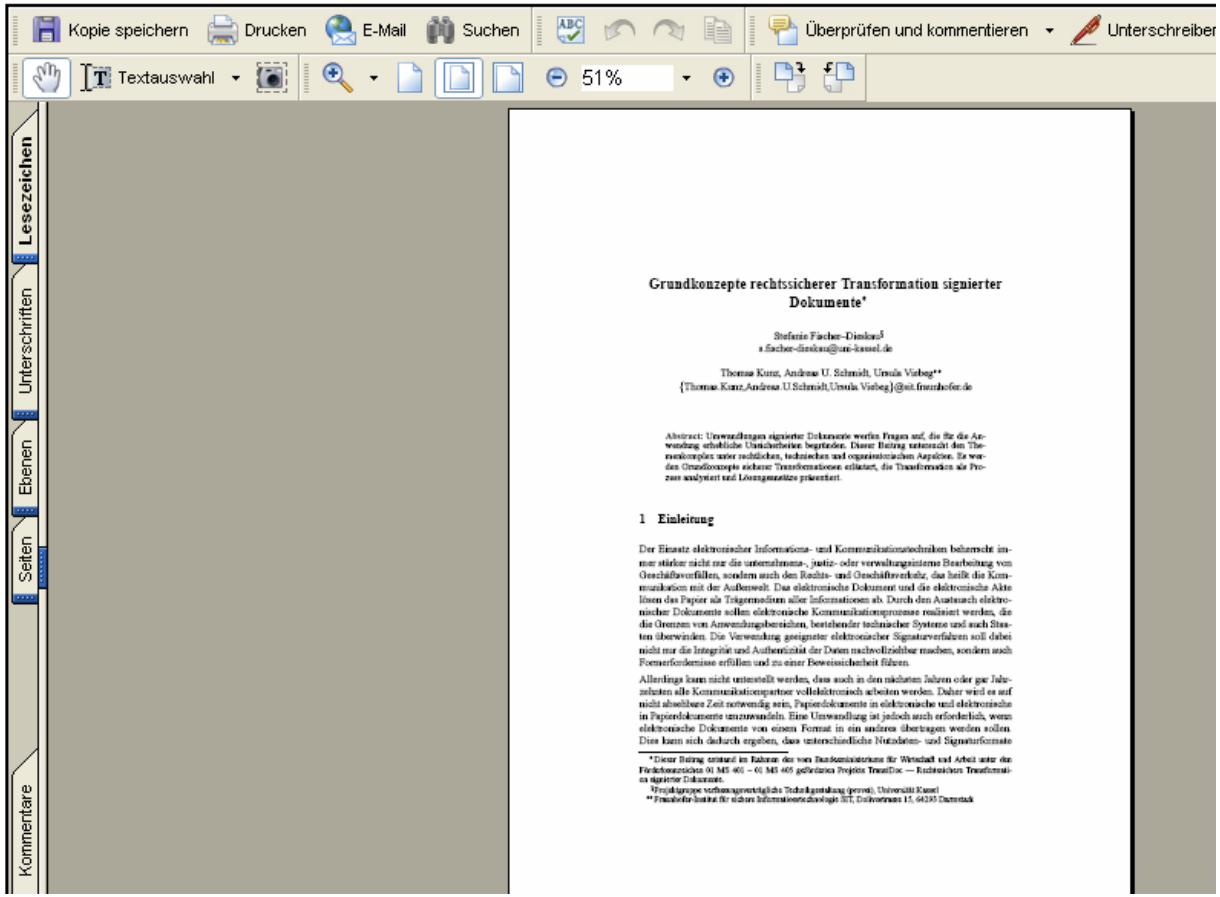
Konvertierter Inhalt

Metadaten zum konvertierten Inhalt

Workflow-Bericht

Vermerk

Signatur



4.16 Web Service – Show Workflow Report

TransiDoc Transformationsergebnis

Konvertierter Inhalt

Metadaten zum konvertierten Inhalt

Workflow-Bericht

Vermerk

Signatur

Bitte wählen Sie eine der ausgeführten Transformationsphasen:

Klassifikation | Signaturextraktion | Konvertierung | Konvertierungsprüfung | Transformationsprüfung

Ablauf und Ergebnis der Phase "Signaturextraktion"

Aufgabe: Prüfung aller Originalsignaturen und Erfassen aller Signaturdaten

Ausführungsende: 2006-03-30T09:42:47.0Z

Eingesetzte Komponenten:

"TransiDoc-Signature-Verification Component", Version 1.1

Hersteller: TransiTrust AG

Adresse: Hauptstr. 3, 64295 Darmstadt, Deutschland

"SafeGuard;SignCrypt;Software;Development;Kit", Version 2.0

Hersteller: Utimaco Safeware AG

Adresse: Dornbachstr. 30, 61440 Oberursel, Deutschland

Einzelergebnisse der Phase:

Bedeutung	Einzelergebnis		
Ergebnis der Signaturprüfung:	*Prüfungsergebnis:*	"Signatur erfolgreich geprüft"	
	Prüfkriterien:	"Konformität mit dem Signaturgesetz"	
	Gültigkeitszeitpunkt:	"entspricht Zeitpunkt der Signaturerstellung: 2006-02-10T09:41:47.0Z"	
Signaturdaten:	*Name des Signierers:*	"Dr. Gisela Musterfrau"	
	Dienststelle/Arbeitgeber:	"Hessisches Kultusministerium (HKM)"	
	Signiererzertifikat:	*Zertifikatsinhaber:*	"CN=Dr. Gisela Musterfrau, O=Hessisches Kultusministerium, C=DE"
		Zertifikatsaussteller:	"CN = CA HKM D85 1:PN, O=Hessisches Kultusministerium, C=DE"
		QC-Statement:	"id-etsi-qcs-QcCompliance: Certificate is issued as a Qualified certificate"
		Zertifikatstatus:	"good"
		Weitere Zertifikatsinformationen	
	Signaturzeitpunkt:	"2006-02-10T09:41:47.0Z Zeit ermittelt von: Systemzeit des verwendeten Rechners"	
	Signaturalgorithmus:	"sha1RSA, Parameter: Schlüssellänge: 1024"	

4.17 Web Service – Show Annotation

Transi§Doc **Transformationsergebnis**

Konvertierter Inhalt

Metadaten zum konvertierten Inhalt

Workflow-Bericht

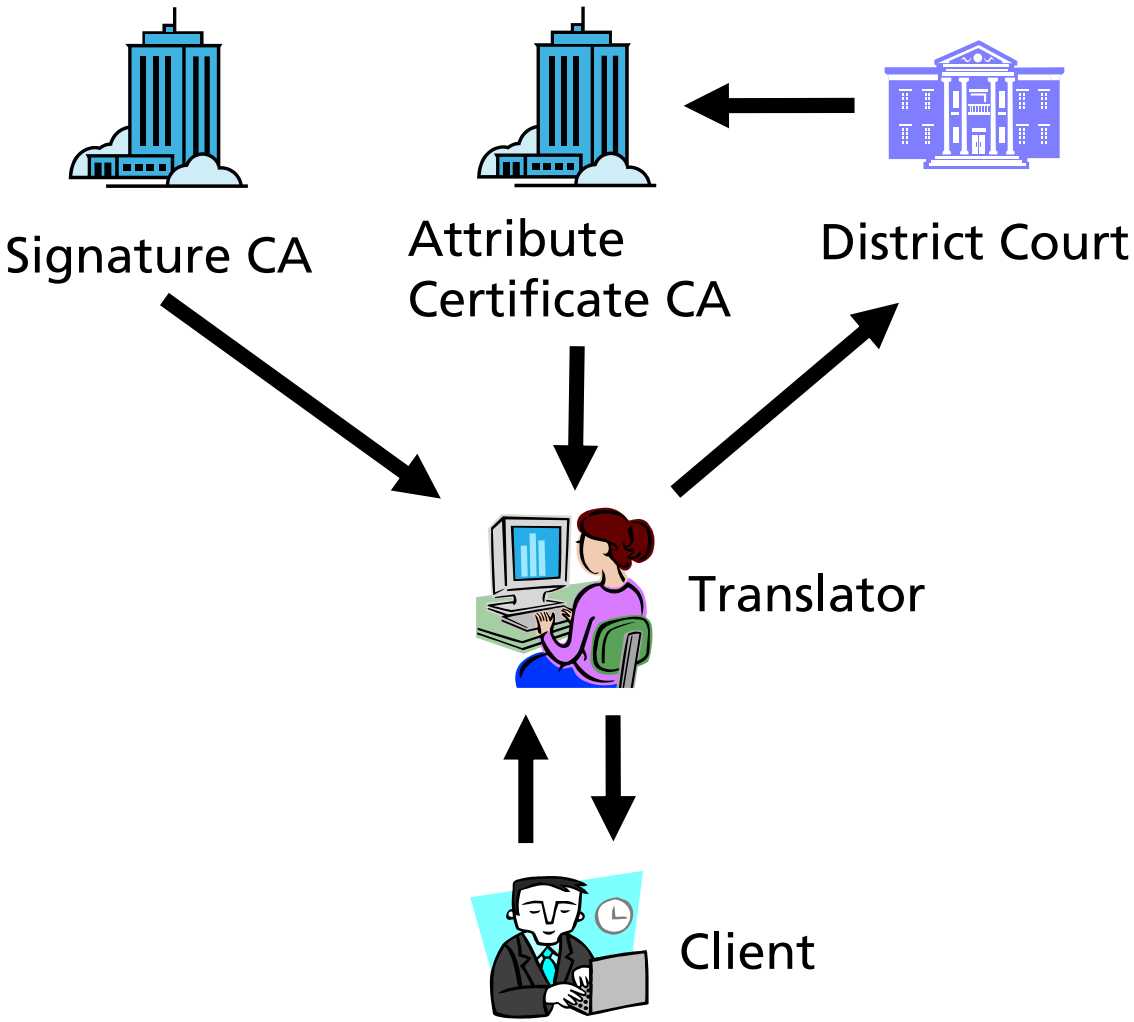
Vermerk

Signatur

Beglaubigungsvermerk

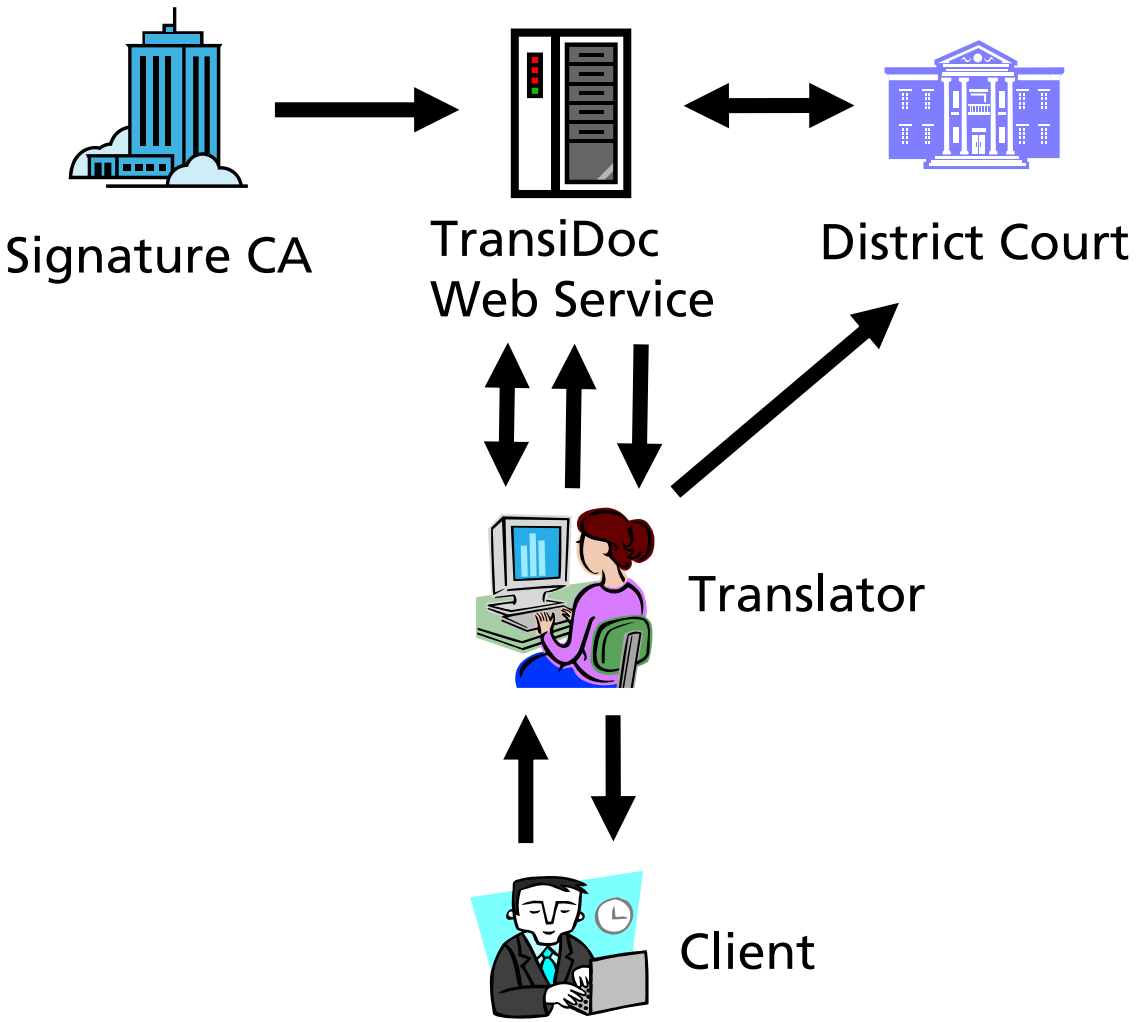
Source language	rus
Target language	deu
Transliteration	ISO 9
Conversion of date and time	Keine Konvertierung notwendig
Defects in original document	
Comments	Übersetzung nach DIN 2345 angefertigt.
Accuracy attestation	Die Richtigkeit und Vollständigkeit der Übersetzung wird hiermit bestätigt.
Sealing time	2006-03-30T09:49:47.0Z
Sealing time source	
Sealing location	Darmstadt
Translator role	
Translator authority	
Original document	
Data hash	UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi
Data hash algorithm	http://www.altova.com
Format	application/pdf
Format version	6.0
Document ID root	c:\test
Document ID extension	abcd
Creation date	2006-03-30T09:30:47.0Z
Document type	Geburtsurkunde
Document type version	
Data reference	http://www.transidoc.de/OriginalDocument.pdf
Original signature	
Original signature ID	
Signature validation result	Signatur erfolgreich geprüft
Signer	Dr. Gisela Musterfrau

4.18 PKI-based Solution



1. The translator receives a public key, a private key and an “ordinary” certificate from the signature CA
2. The translator applies for authorisation at the district court
3. The district court initiates the issue of an attribute certificate by the attribute certificate CA
4. The translator receives an attribute certificate from the attribute certificate CA
5. The client sends a source document to the translator
6. The translator performs the translation, seals the target document with a transformation seal including his attribute certificate and signs the target
7. The translator sends the target document to the client

4.19 Stand-alone Web Service Solution



1. The web service receives a public key, a private key and an “ordinary” certificate from the CA
2. The translator applies for authorisation at the district court
3. The translator registers with the web service
4. The web service checks the translator’s authorisation at the district court and adds him to his database
5. The client sends a source document to the translator
6. The translator performs the translation
7. The translator sends the source document and the translation to the web service
8. The web service seals the target document with a transformation seal including his certificate and signs the target
9. The web service sends the target document to the translator
10. The translator sends the target document to the client

Literaturauswahl

•Ulrich Pordesch, Andreas U. Schmidt: Digital? Mit Sicherheit! Ar¬chivierung signierter Dokumente. Card-Forum Dezember 2004.

•Stefanie Fischer-Dieskau, Thomas Kunz, Andreas U. Schmidt, Ur-sula Viebeg: Grundkonzepte rechtssicherer Transformation sig¬nierter Dokumente. Workshop (QSIG2005) bei der Konferenz Sicherheit 2005, In: Konferenzband der "Sicherheit 2005", GI-Edition, Lecture Notes in Informatics (LNI), Vol. P-62, S. 401-412.

•Roßnagel, A., Elektronische Signaturen mit der Bankkarte?, Das Erste Gesetz zur Änderung des Signaturgesetzes, NJW 2005, 385.

•Hollerbach A, Brandner R, Bess A, Schmücker P, Bergh B. Daten-for¬mate und Transformation elektronisch signierter Dokumente. In: Informatik, Biometrie und Epidemiologie in Medi¬zin und Bio-logie. Abstracts der 49. Jahrestagung der Deutschen Gesell-schaft für Medizinische Informatik, Biometrie und Epide¬miologie (GMDS), Innsbruck, 26.-30. September 2004, Ammenwerth E et. al. (Eds.). Niebüll: videel, 2004, S. 18-20.

•Hollerbach A, Brandner R, Bess A, Schmücker P, Bergh B. Elec-tronically signed documents in health care – analysis and as-sessment of data formats and transformation. Methods of Infor-mation in Medicine 2005; 44(4): 520-7.

•Andreas U. Schmidt, Zbynek Loebl: Legal Security for Transfor-mations of Signed Documents: Fundamental Concepts. In: Proceedings of the Second European PKI Workshop, D. Chadwick and G. Zhao (Eds.) Lecture Notes in Computer Science, vol. 3545, pp. 255-270, Springer-Verlag, 2005.

•Thomas Kunz, Andreas U. Schmidt, Ursula Viebeg: Konzepte für rechtssichere Transformationen sig¬nierter Dokumente. Daten-schutz und Datensicherheit (DuD) 29 (2005) 5, 279-285.

•H. Roßnagel, S. Fischer-Dieskau, D. Wilke: Transformation von Dokumenten – Zur Notwendigkeit einer Technik- und Rechtsgestal-tung, Computer und Recht 2005, 903-908.

•U. Viebeg: Warum elektronische Signaturen altern und brechen – und wie man ihren Beweiswert erhält, IT-Sicherheit & Datenschutz Ausgabe 03/06

•Andreas U. Schmidt, Jan Piechalski: Authorised Translations of Electronic Documents. Refereed contribution to the Conference Information Security South Africa (ISSA 2006) Sandton, South Africa, 5 -7 July 2006.

•Stefanie Fischer-Dieskau, Daniel Wilke: Electronically Signed Documents: Legal Requirements and Measures for their Long-term Conservation, Digital Evidence Journal 2006, 38-42.

•Alexander Roßnagel, Stefanie Fischer-Dieskau: Elektronische Do-kumente als Beweismittel - Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz, NJW, 2006, 806-809.

•Alexander Roßnagel, Daniel Wilke: Die rechtliche Bedeutung ges-cannter Dokumente, NJW 2006, 2145-2150.

Danke für Ihre Aufmerksamkeit !

Fraunhofer-Institut SIT

Forschungsbereich Transktions- und Dokumentensicherheit

Andreas U. Schmidt
Dr. phil. nat.

Rheinstraße 75

64295 Darmstadt
Telefon: +49-6151-869-60227
Fax: +49-6151-869-224

E-Mail: Andreas. U.Schmidt@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de

Private Homepage: http://www.math.uni-frankfurt.de/~aschmidt