# Authorised Translations of Electronic Documents

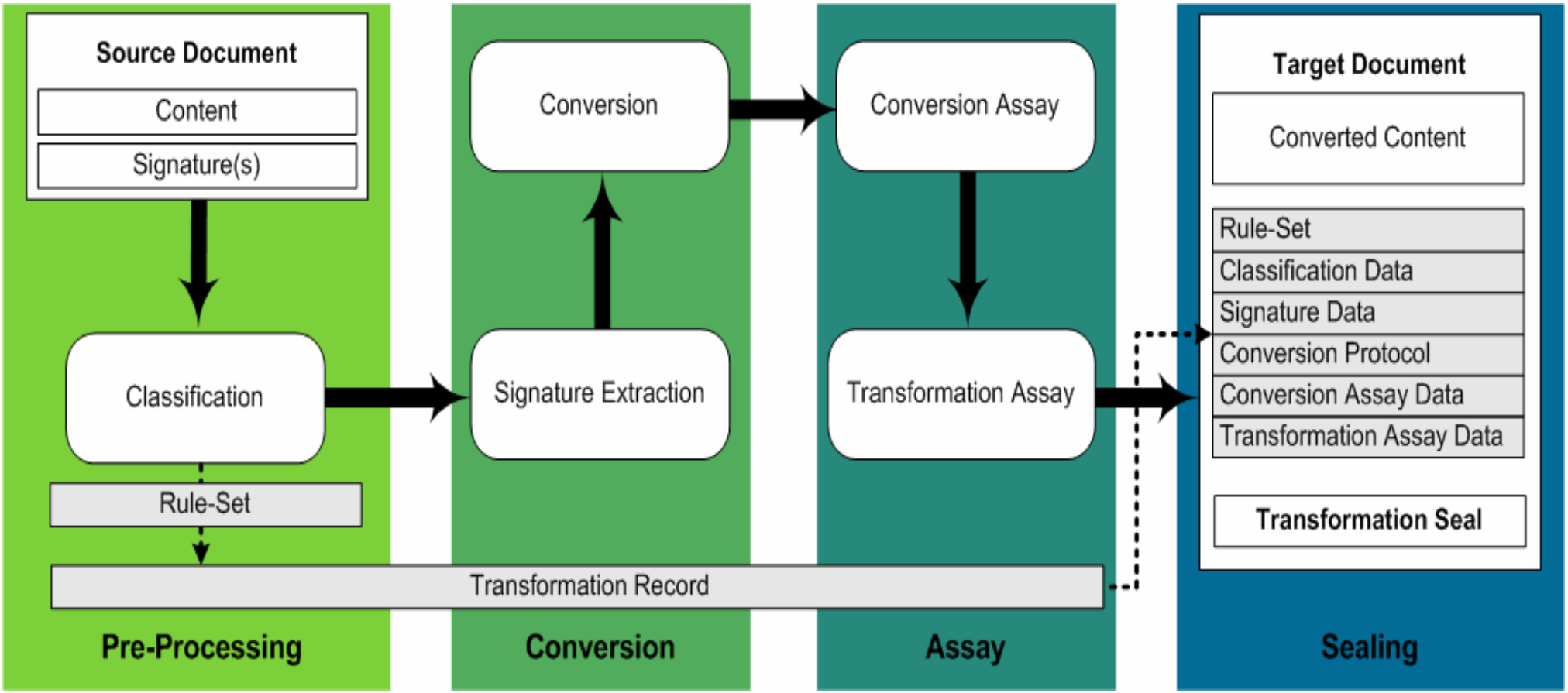
**Jan Piechalski**

**28 July, 2006**

Fraunhofer SIT Institut Sichere Informations-Technologie

TransiDoc

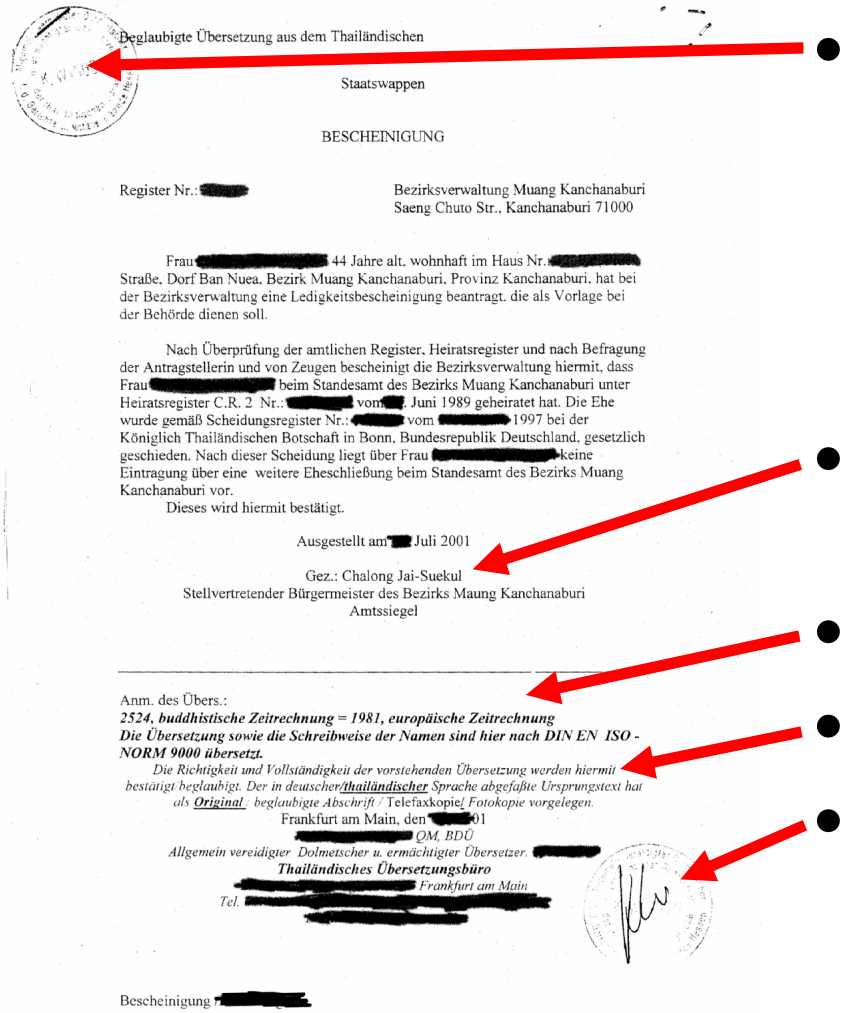
# Process Analysis of Secure Transformations



# 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

# 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.*

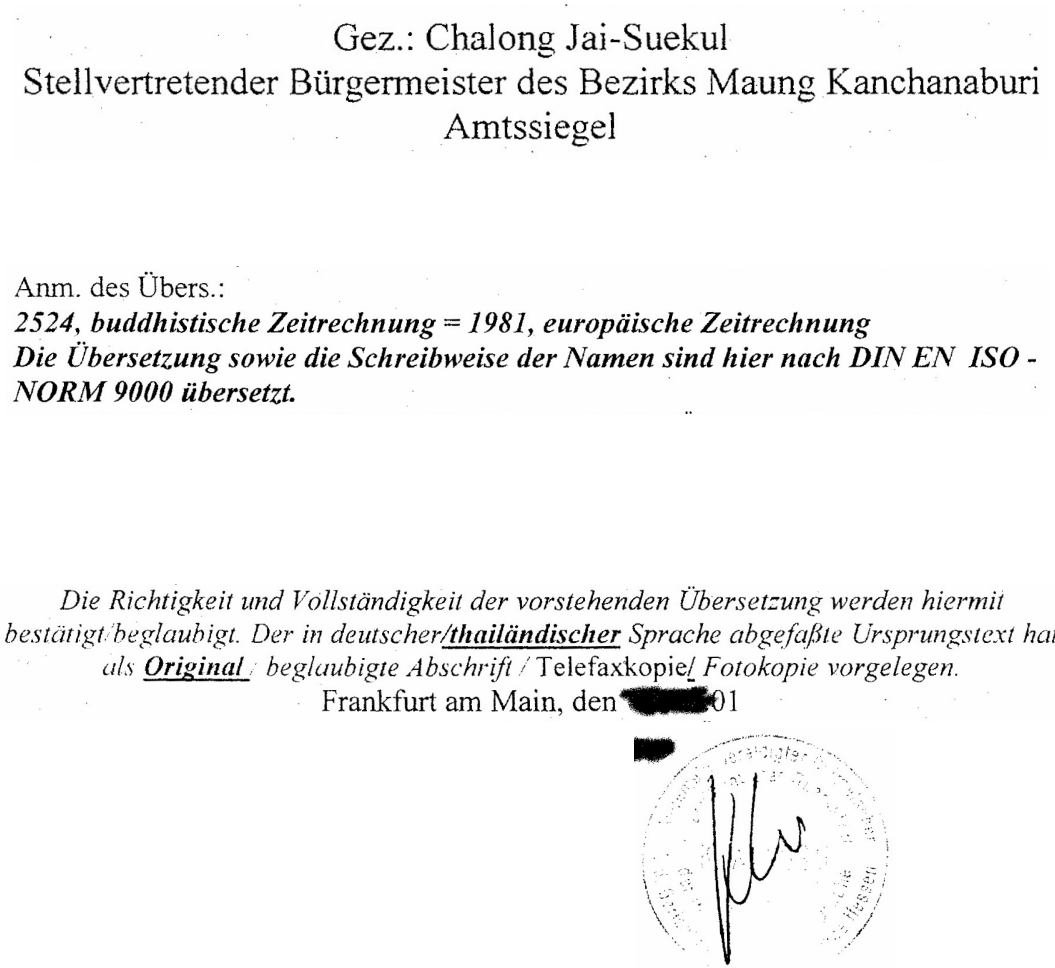
Frankfurt am Main, den [redacted]01

[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

# 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)

# Certifications under German Law

- Detailed legal regulations concerning the performing of certifications, both for paper and electronic documents, exist
- A certification's annotation according to § 33 *Verwaltungsverfahrensgesetz* has to contain following elements:
  1. Name of the source document
  2. An optional indication that the usage of the certified target document is restricted to a certain authority
  3. An optional description of defects found in the original document
  4. Information about original signatures, including validation results
  5. Attestation that the content of the source and the target are identical
  6. Creation time of the certification
  7. Creation place of the certification
  8. A qualified signature of a person authorised to perform the certification
- A translation's annotation is similar
- Elements 1 and 2 are not required for translations

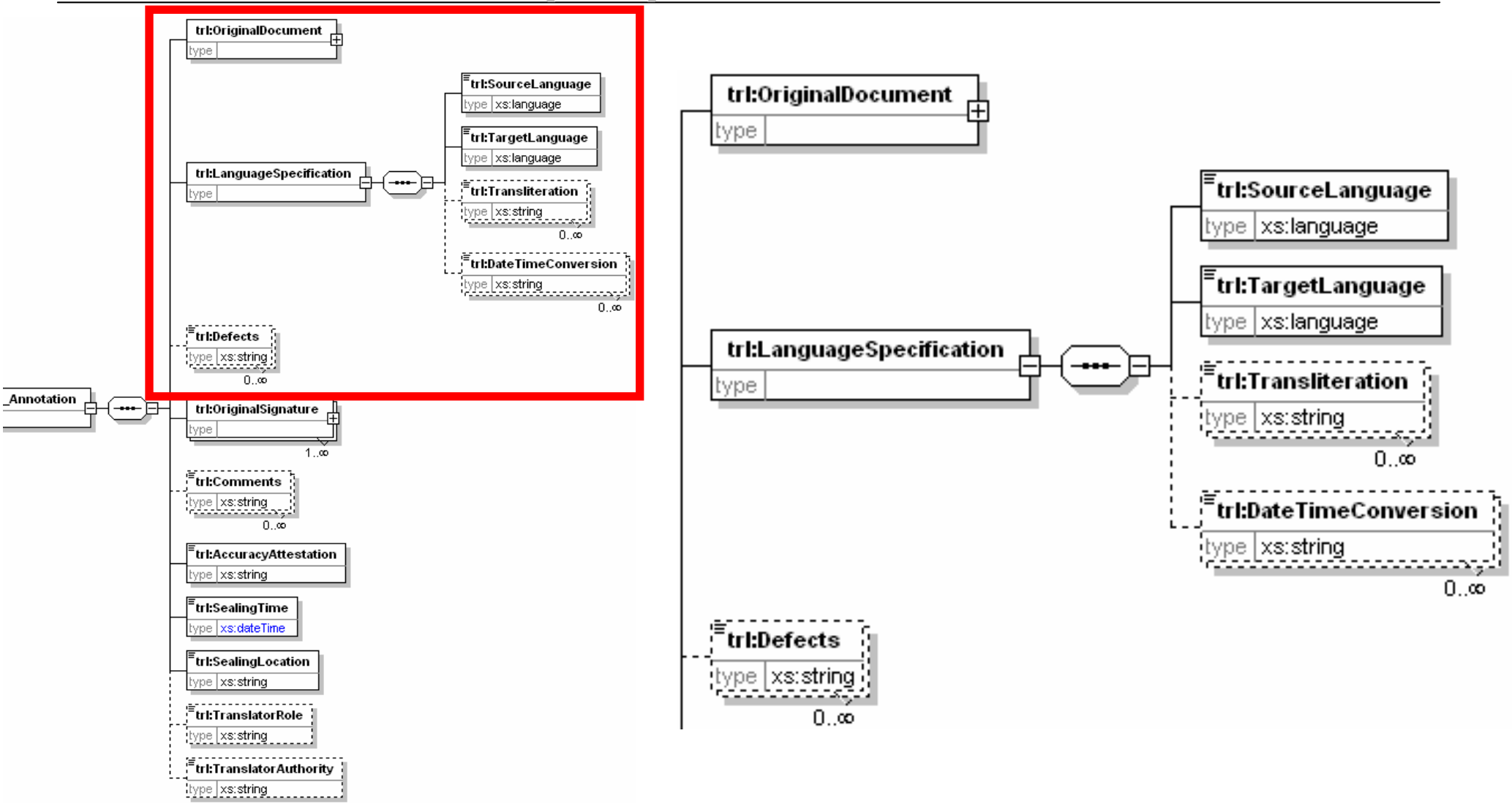
# Requirements for Electronic Translations

- 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

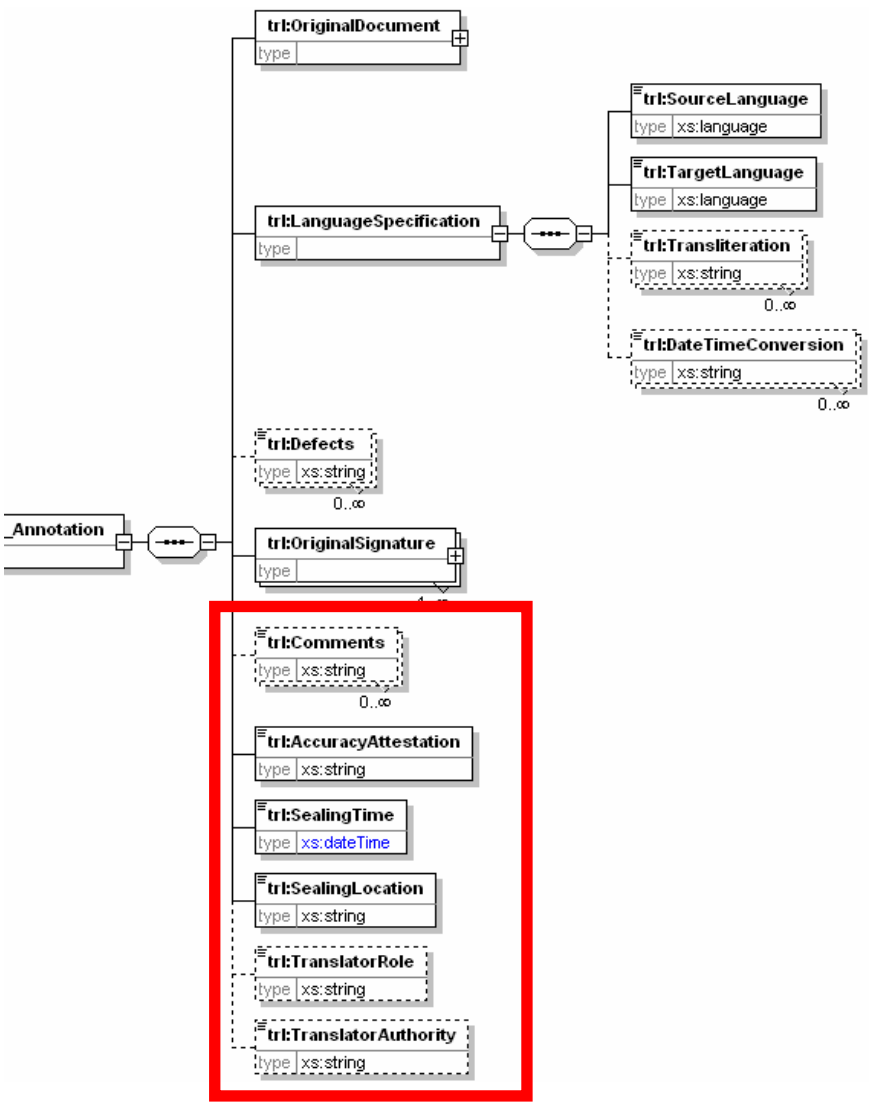
# Applicable Internationalisation Standards

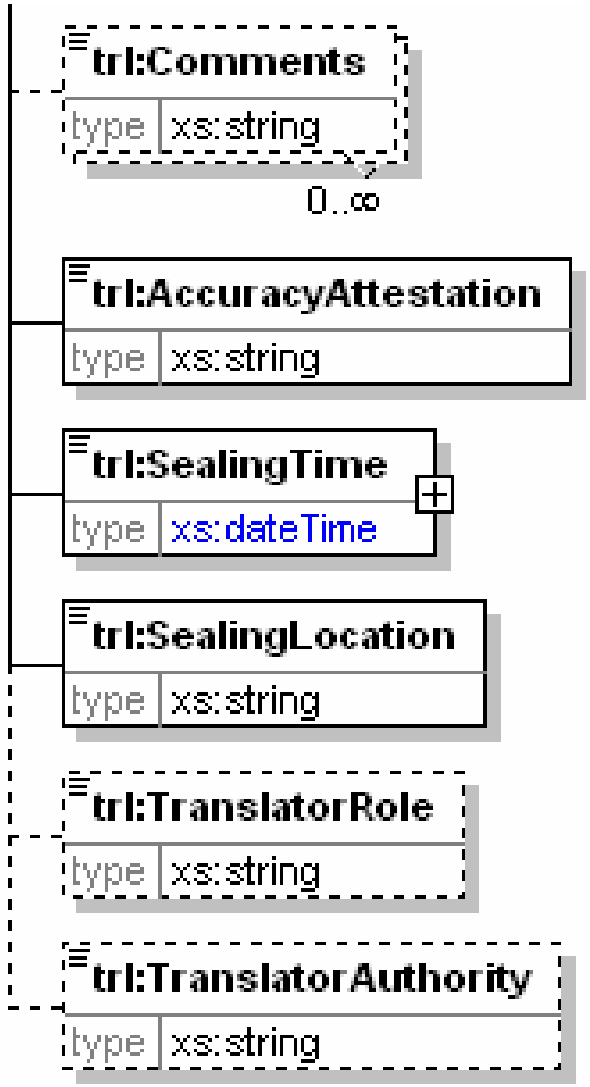
- Specification of source and target language with ISO 639-2 codes (e. g. “eng” for English)
  - The XML schema type ‘xs:language’ applies ISO 639-2
- Standards for transliteration of names (e. g. ISO 9 for Cyrillic → Latin)
- Date and time conversion during translation
  - ISO 8601 and ISO 2015 – Standards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

# Translation Seal (1/8)

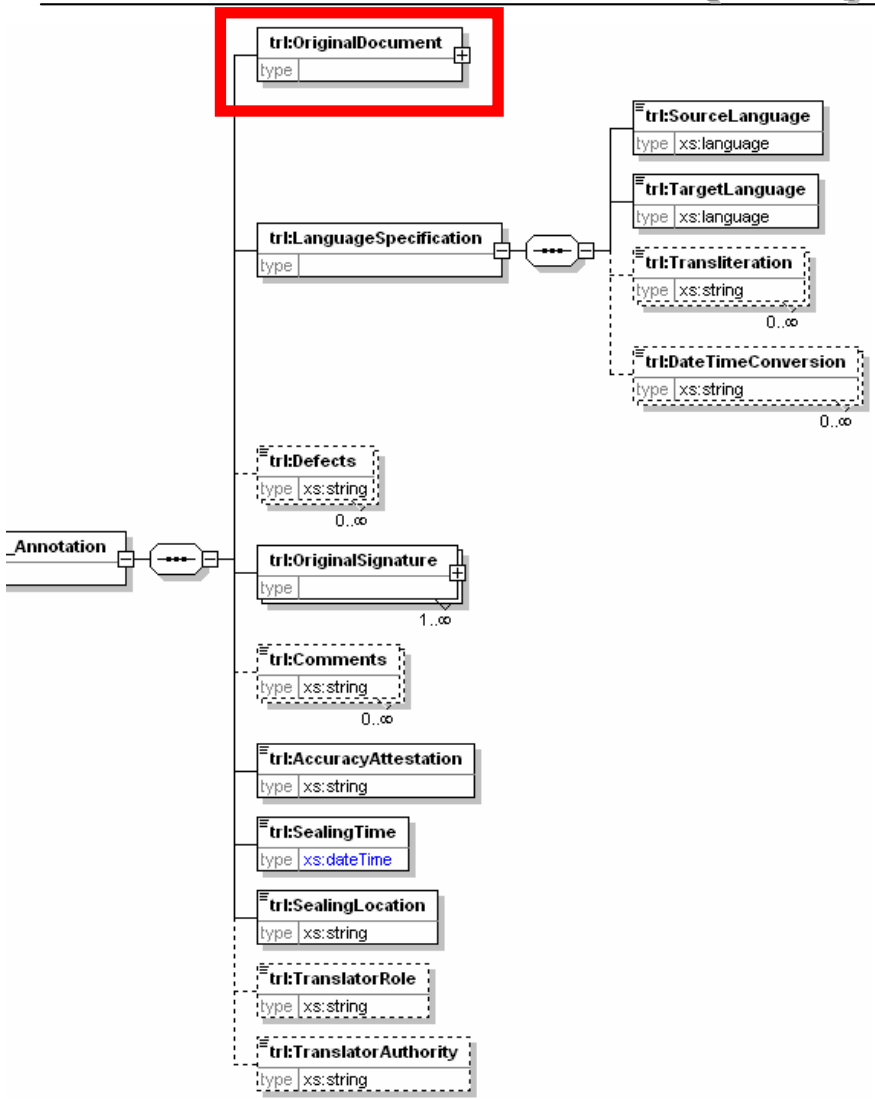


# Translation Seal (2/8)

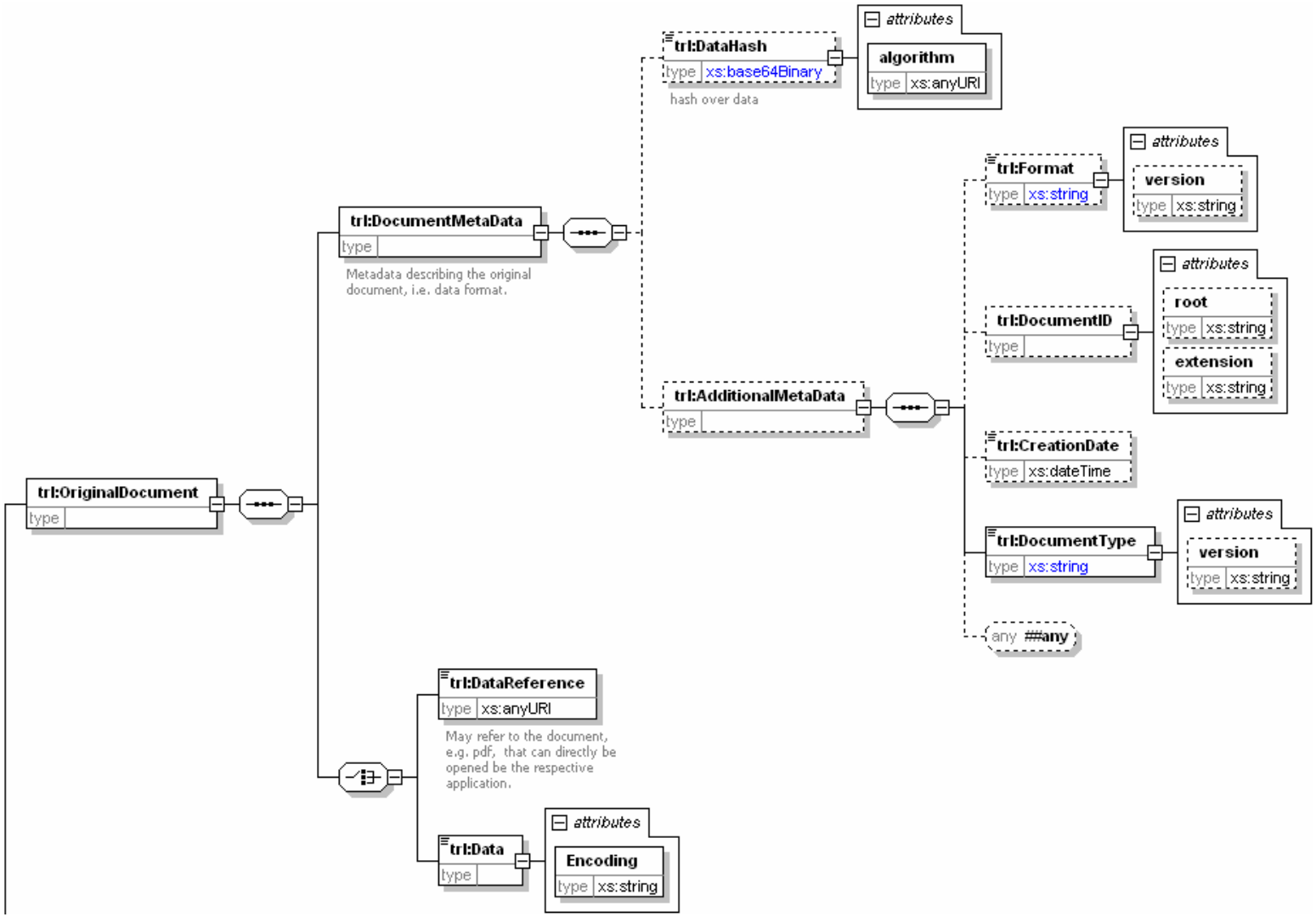


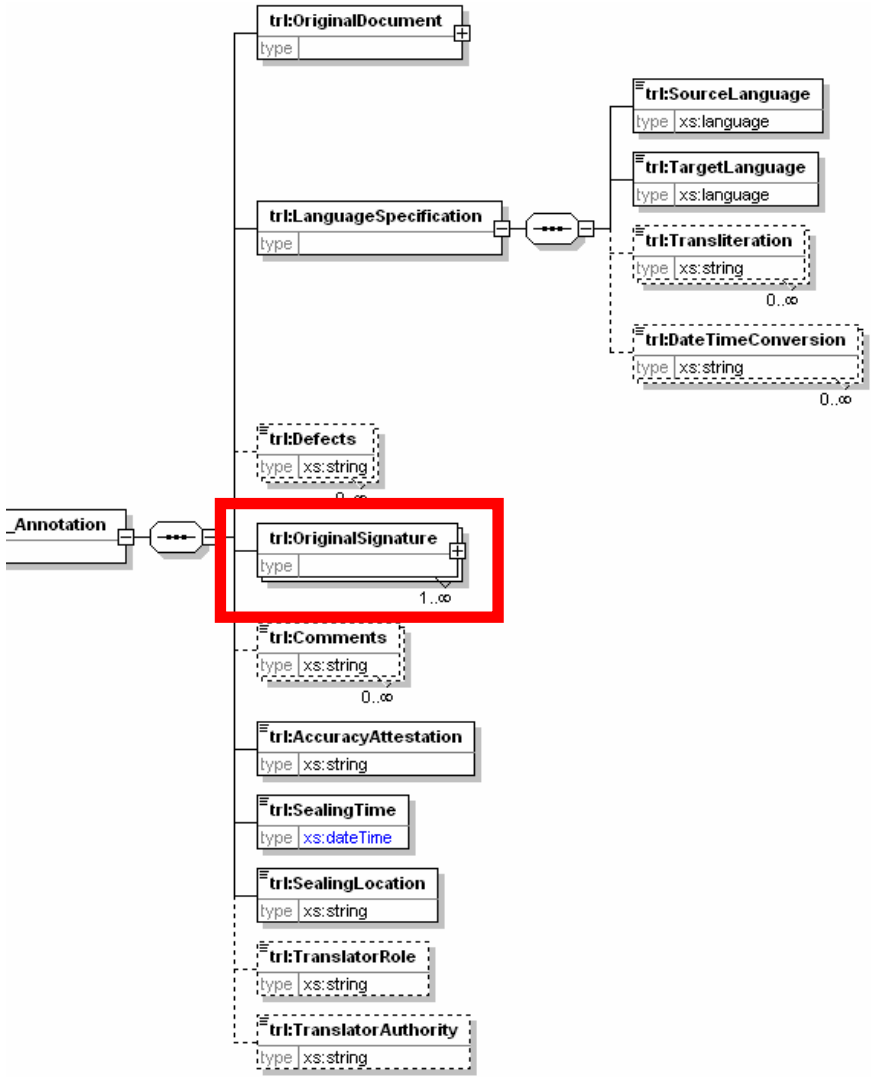
# Translation Seal (3/8)



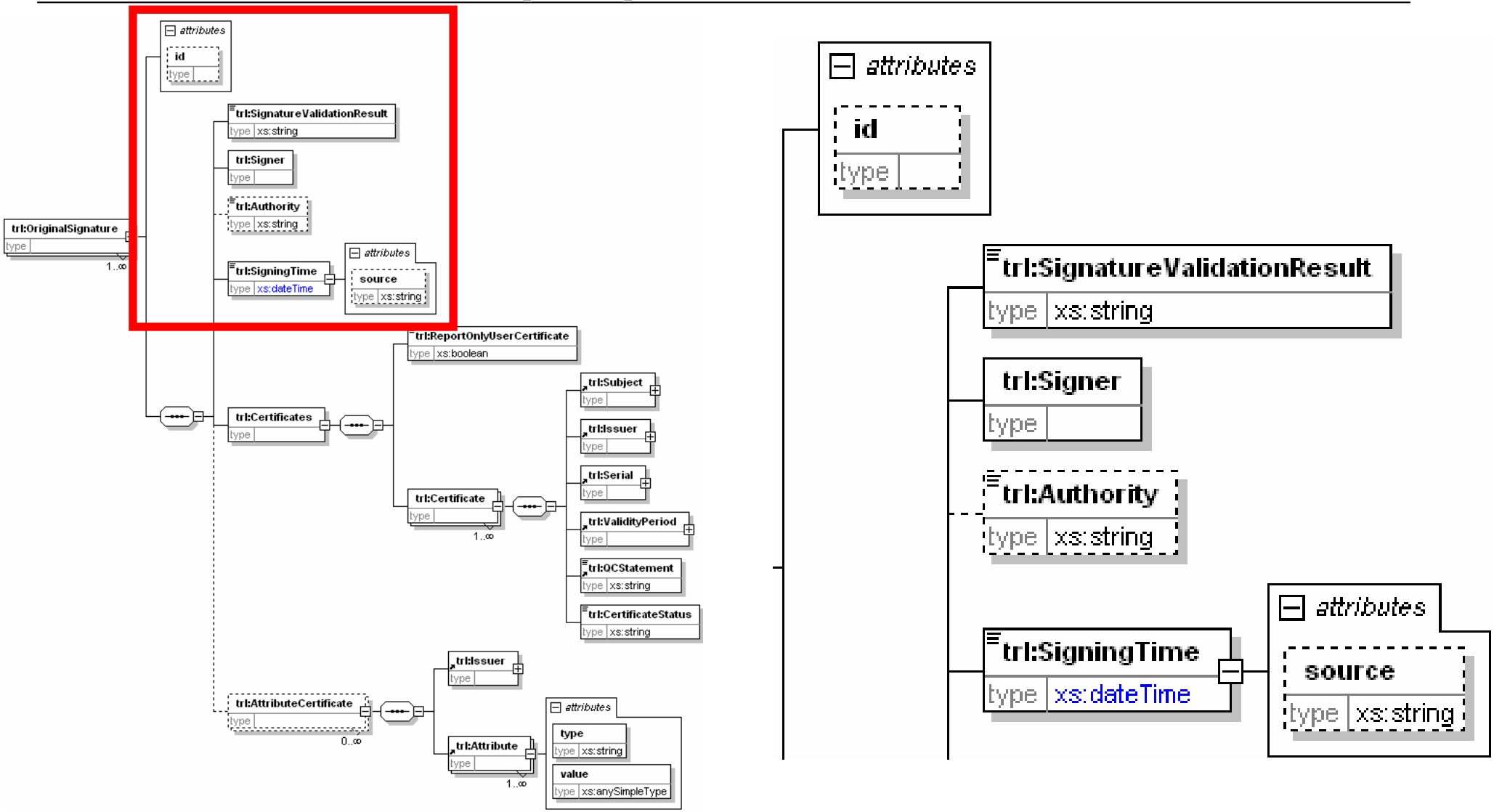
# Translation Seal (4/8)



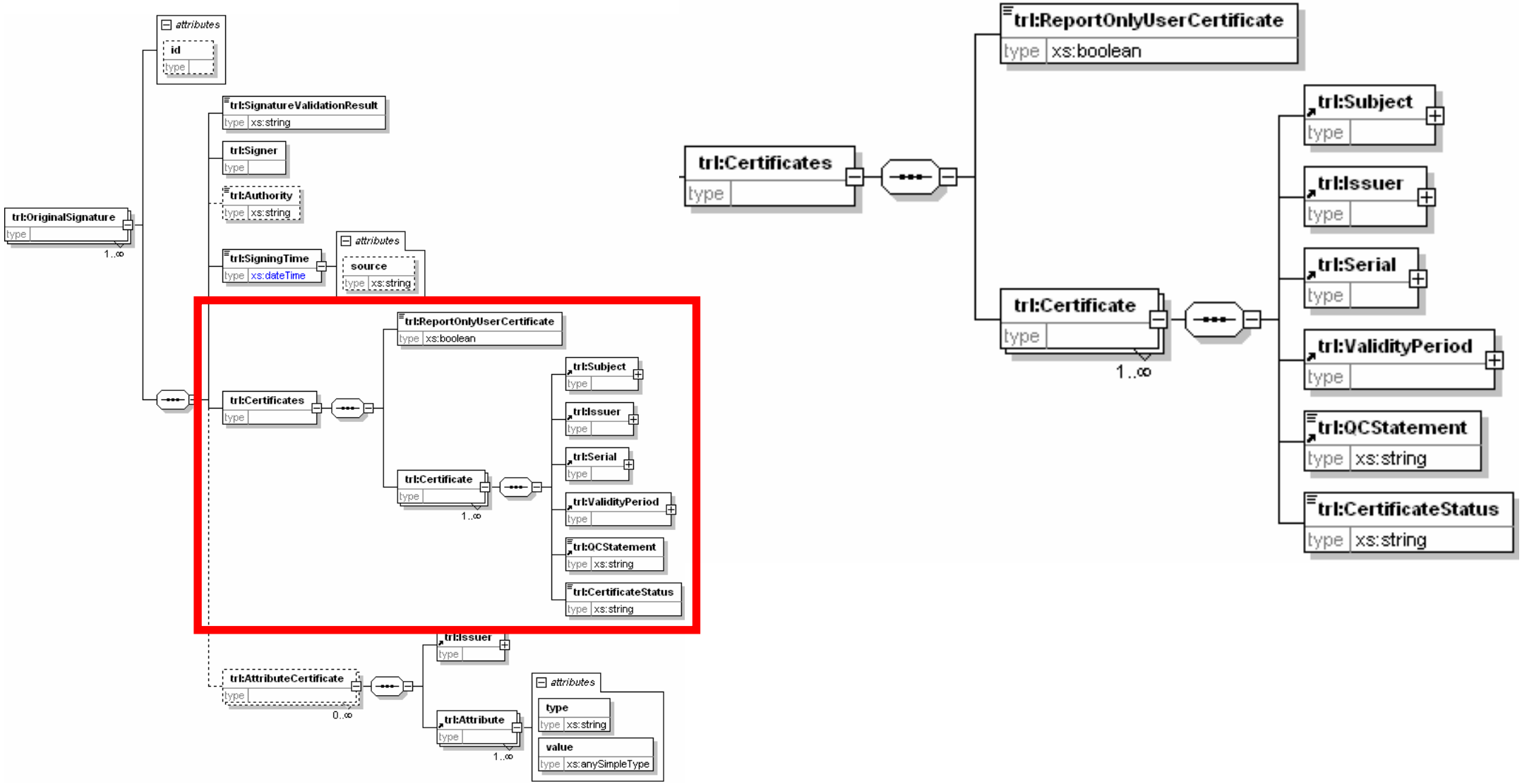
# Translation Seal (5/8)



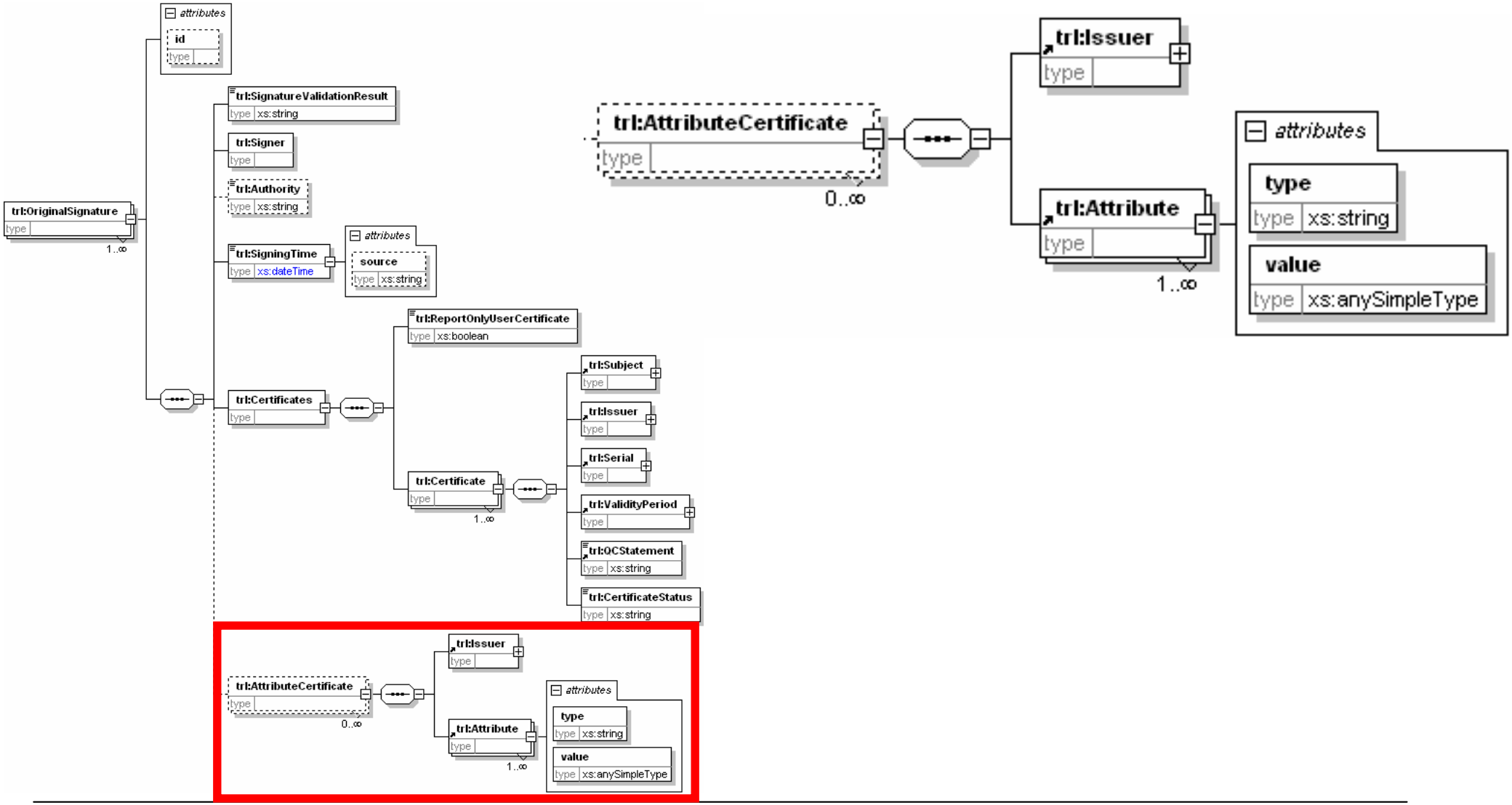
# Translation Seal (6/8)



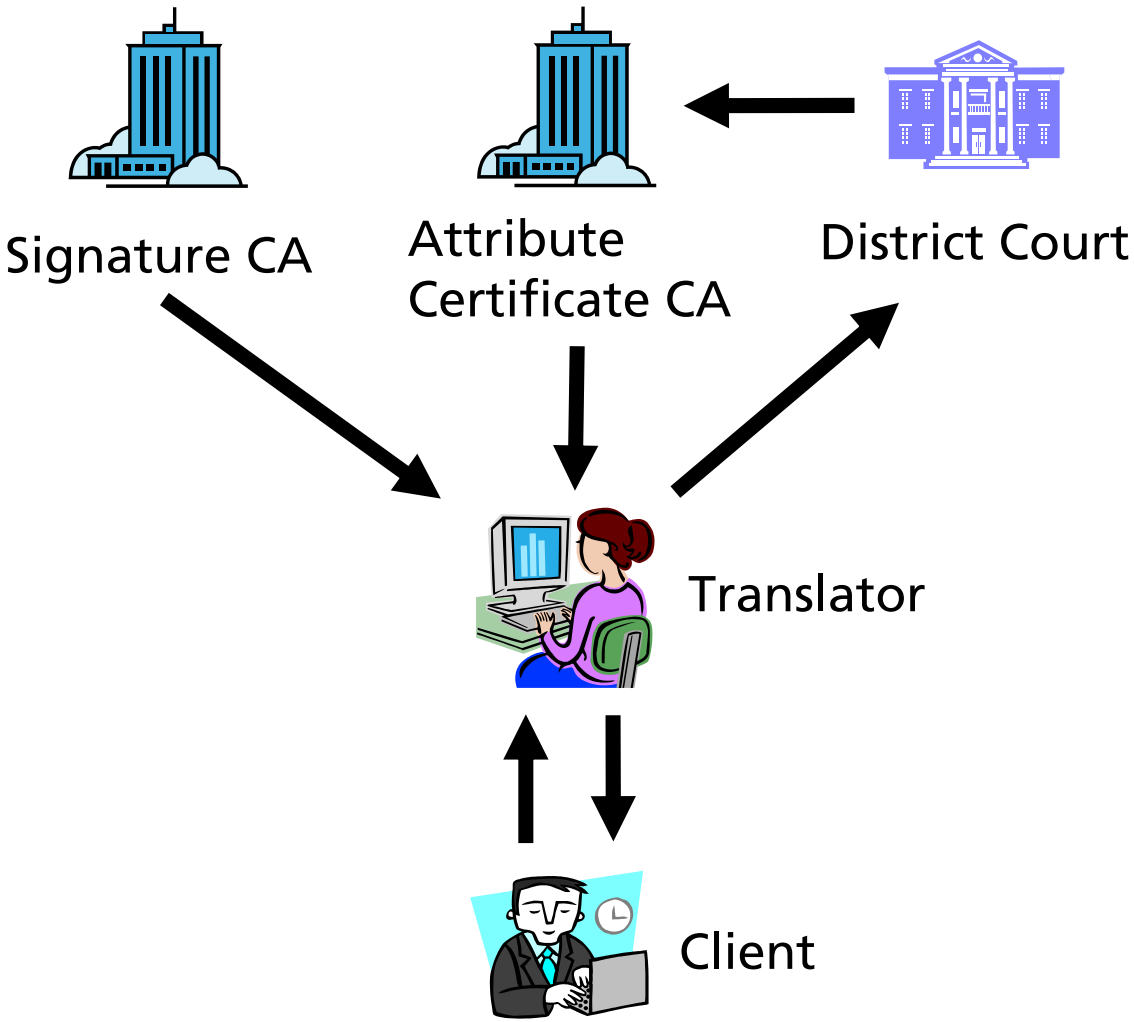
# Translation Seal (7/8)



# Translation Seal (8/8)

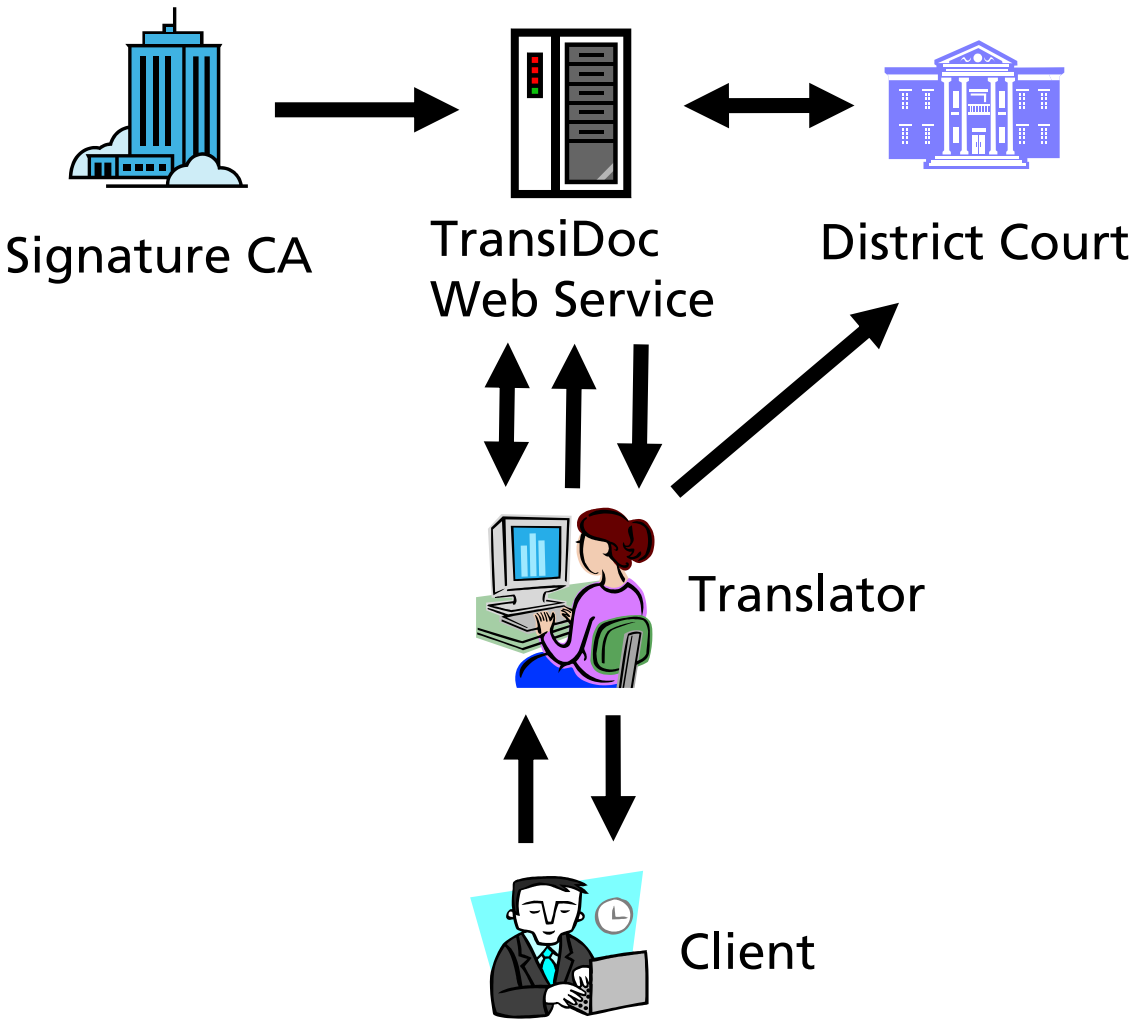


# PKI-based Solution



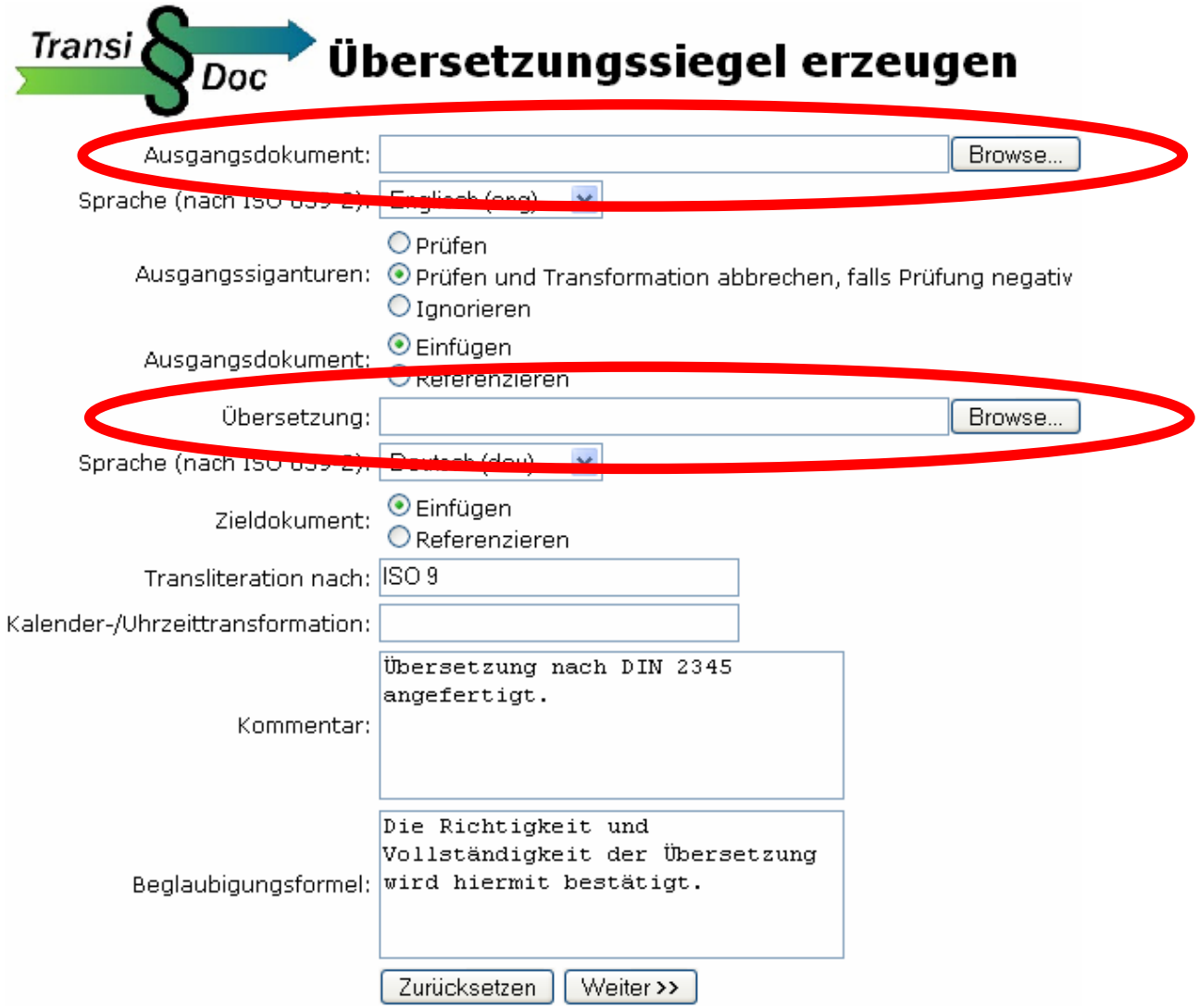

1. The translator receives a public key, a private key and an “ordinary” certificate from the signature CA
2. The translator applies for authorisation at the district court
3. The district court initiates the issue of an attribute certificate by the attribute certificate CA
4. The translator receives 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

# Stand-alone Web Service Solution



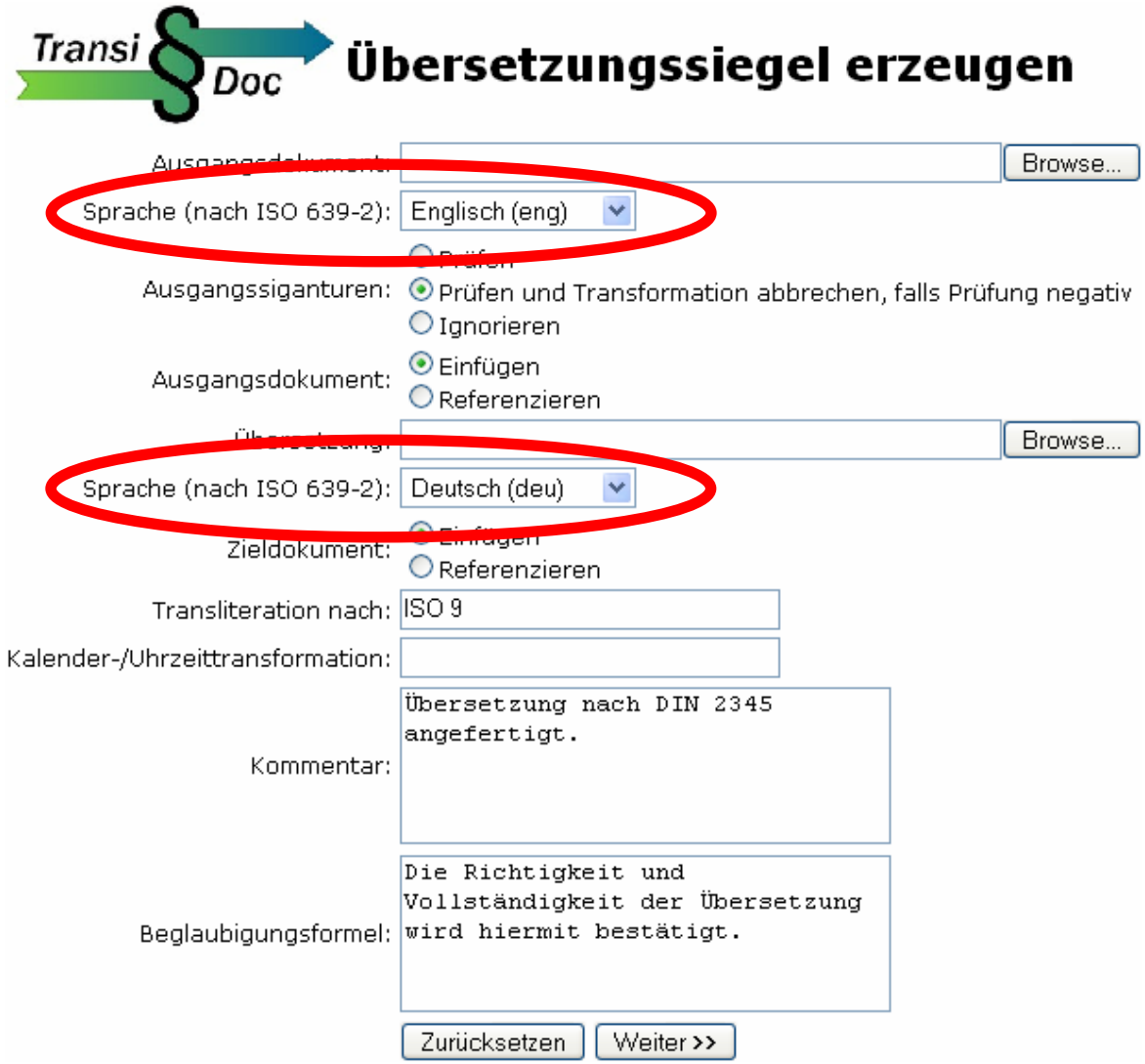

1. The web service receives a public key, a private key and an “ordinary” certificate from the CA
2. The translator applies for authorisation at the district court
3. The translator registers with the web service
4. The web service checks the translator’s authorisation at the district court and adds 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

# Web Service – Classification (1/6)



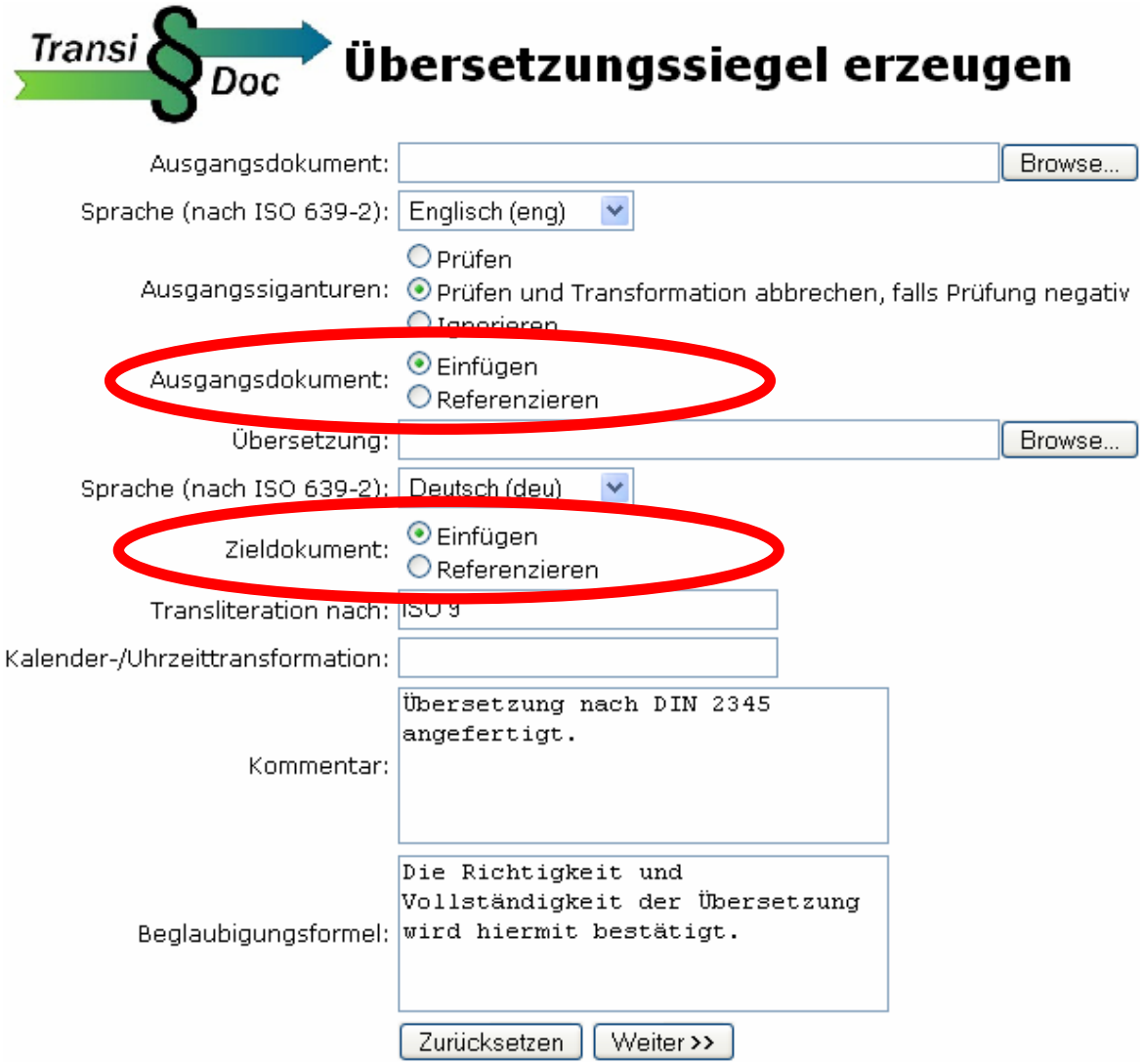

- File upload of original document and translation

# Web Service – Classification (2/6)



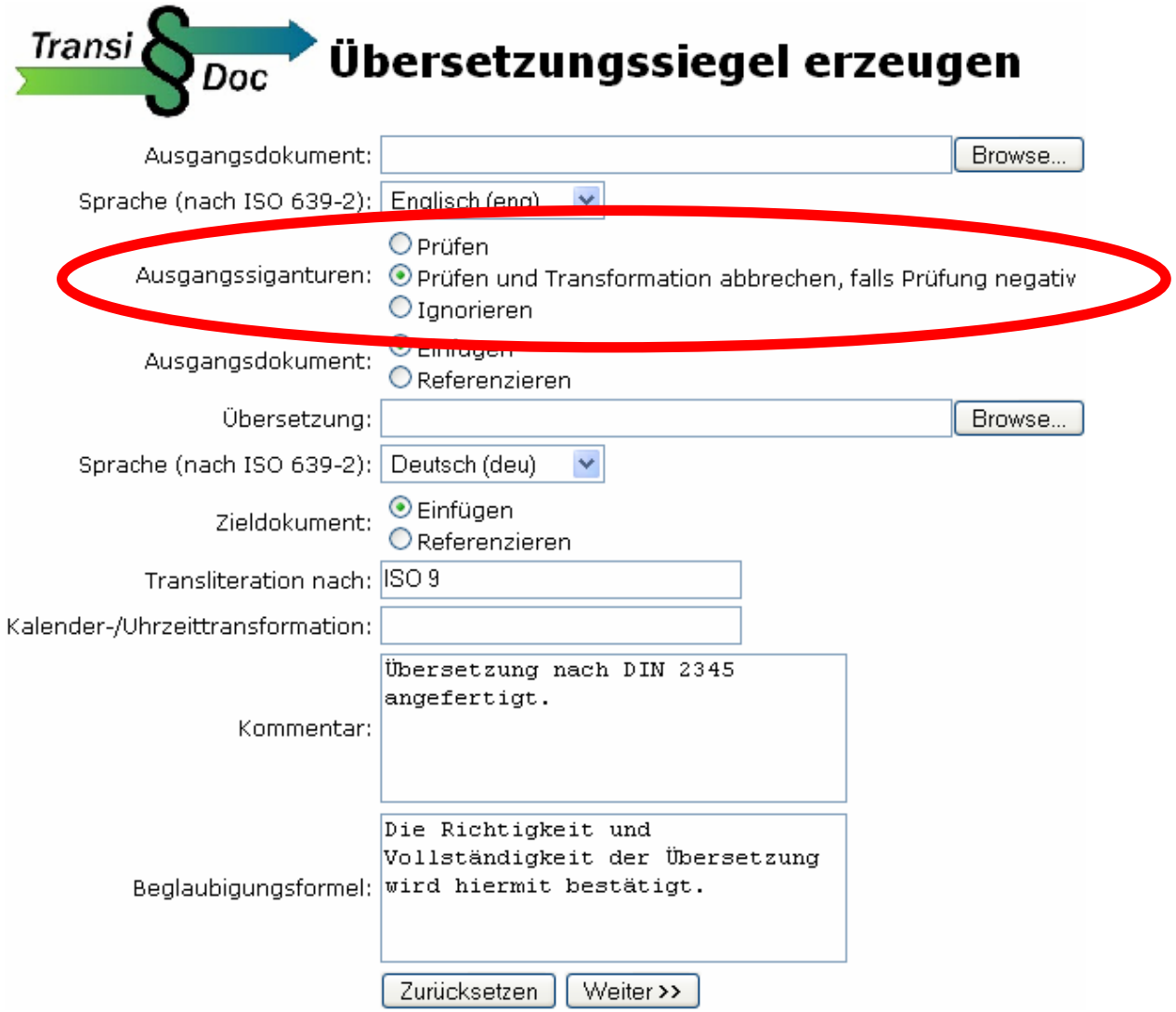

- Source and target language specification according to ISO 639-2

# Web Service – Classification (3/6)



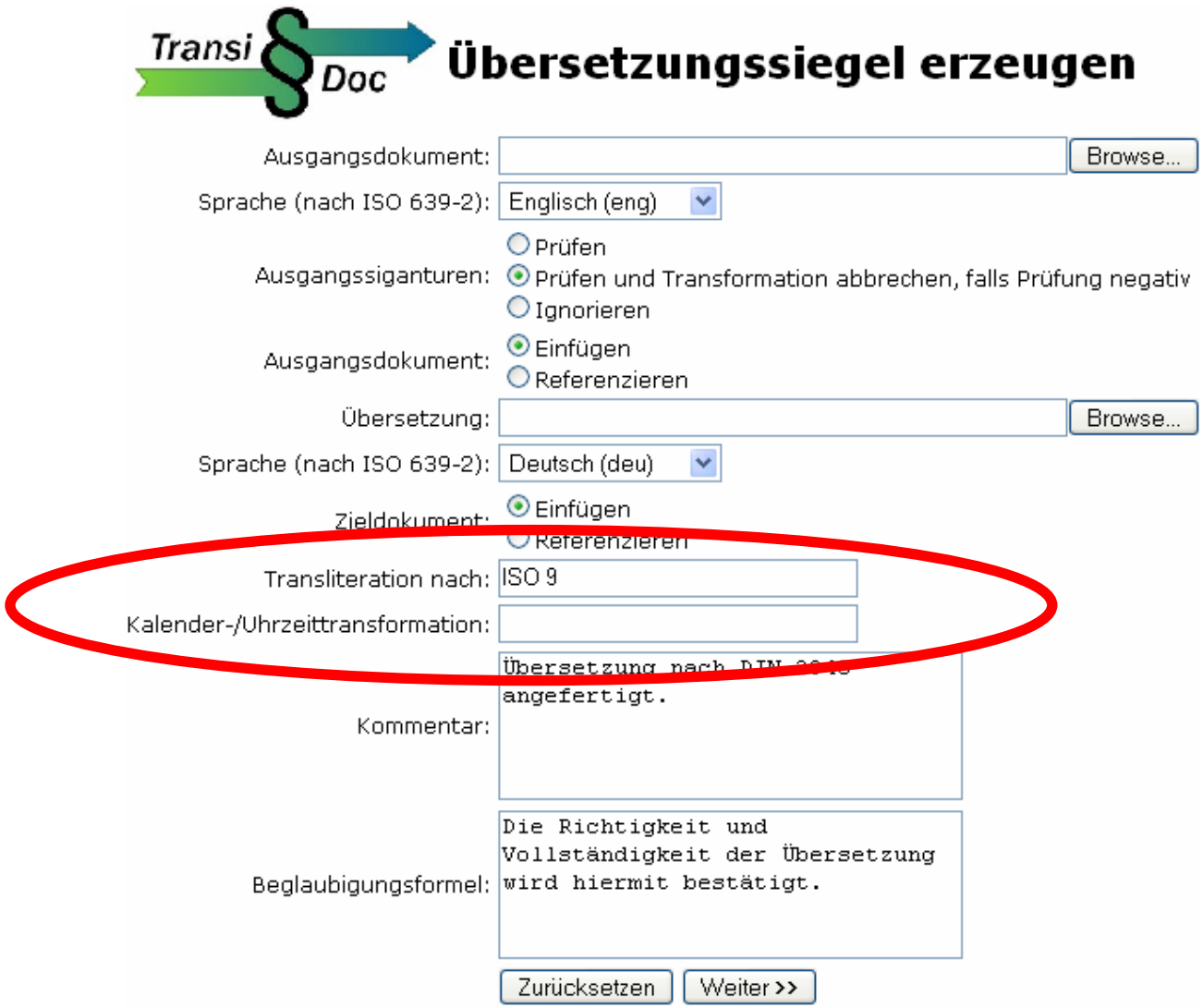

- Insert or reference source and target document

# Web Service – Classification (4/6)



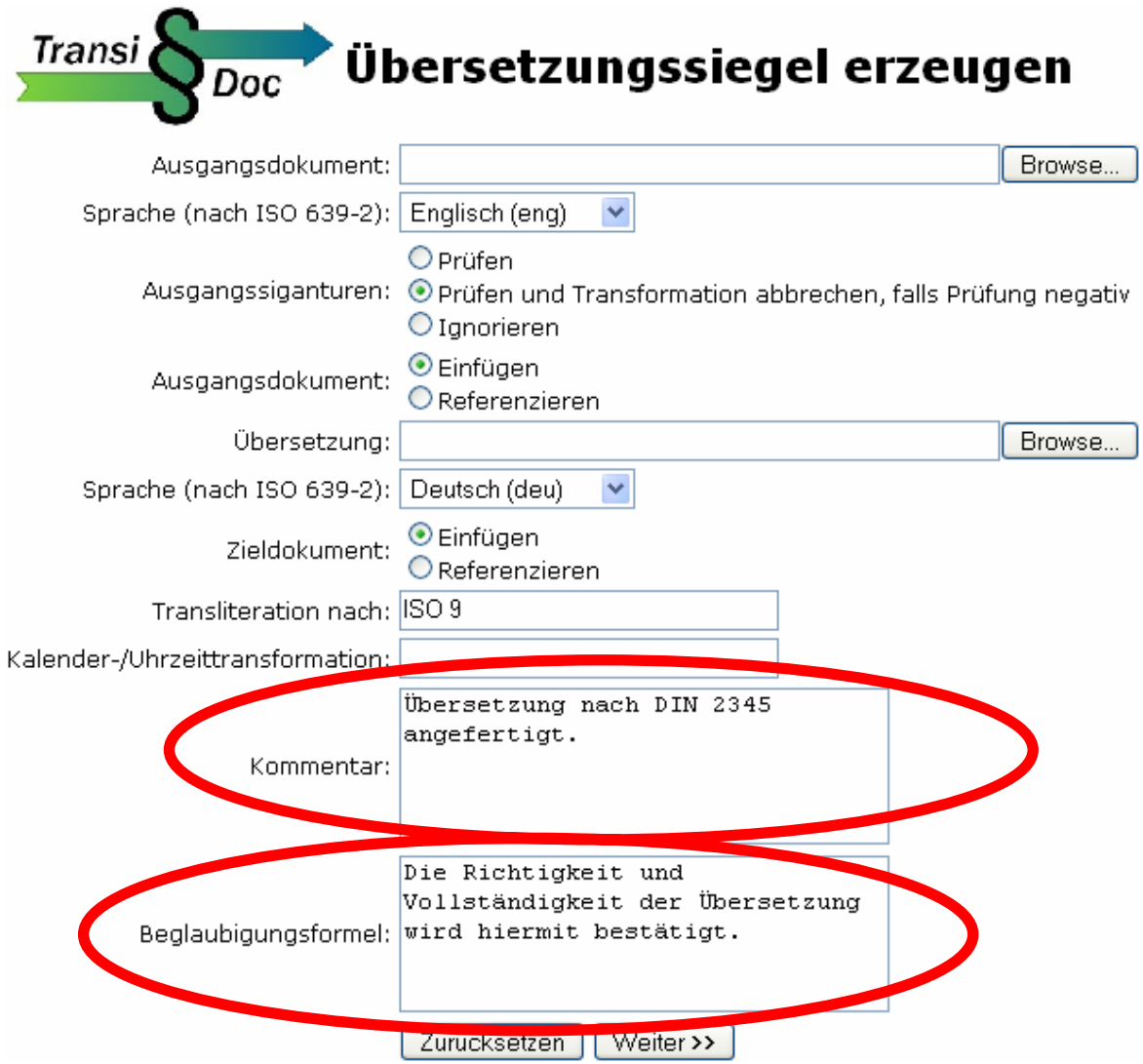

- Original signatures policy
  - Validate signatures and continue transformation in any case
  - Validate signatures and abort transformation, if validation result negative
  - Ignore original signatures

# Web Service – Classification (5/6)




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

# Web Service – Classification (6/6)




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

# 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

# Web Service – Show Translated Document

TransiDoc **Transformationsergebnis**

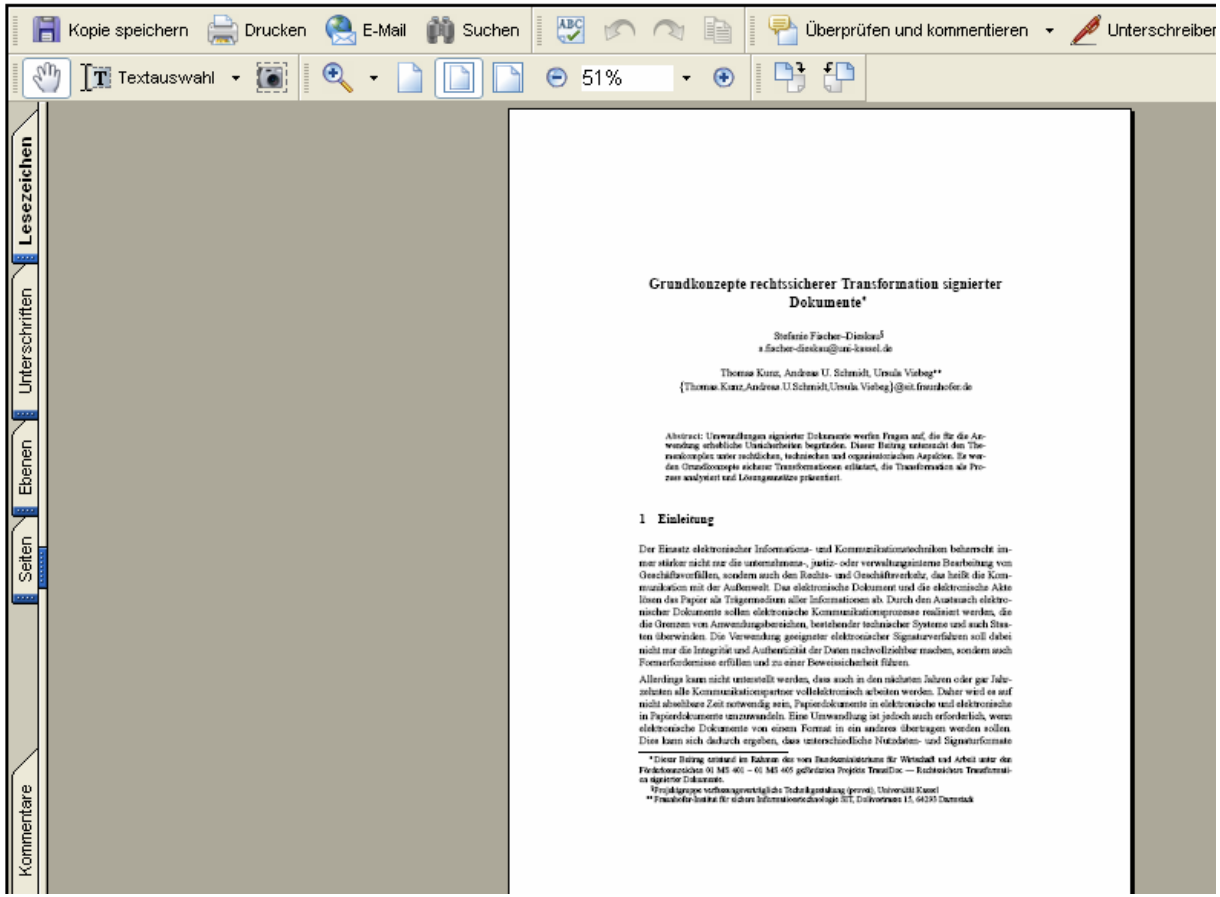
Konvertierter Inhalt

Metadaten zum konvertierten Inhalt

Workflow-Bericht

Vermerk

Signatur



# Web Service – Show Workflow Report

## 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" | |

# Web Service – Show Annotation

## 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 |

Thank you!