Legal Security for Transformations of Signed Documents Fundamental Concepts

Zbynek Loebl
CEAG, Prague

Andreas U. Schmidt
Fraunhofer-SIT, Darmstadt

Second European PKI Workshop
The University of Kent, England
30 June - 1 July 2005

Fraunhofer Institut
Sichere Informations-
Technologie

Transformations of Signed Doc's – Application cases

- Healthcare: (E→E)
  - *Anonymisation* of patient records for use in clinical studies.
  - *Migration* between common data formats, e.g. in disease management programmes (like specified by the HL7 group)
  - ***Retain authenticity and attributatbility expressed by physicians signature!***
- E-Government: (P→E, E→E)
  - *Conversion* of paper and electronic plans of a **building application** into suitable data formats for office use
  - ***Retain non-repudiation expressed by applicant's/plaintiff's signature!***
  - ***Respect metric and colour gauging!***

Transformations of Signed Doc's – Application cases

- **Notaries:** (P→P, future: P→E E→E)
  - *Attestation* of the identity of contents for two documents after conversion between data formats and/or media types
  - *Retain authenticity and attributatbility expressed by original signature(s)!*
  - *Raise the 'level of trustworthiness' through attestation by an authorised person or institution.*
- **Long-term archiving** (E→E)
  - *Convert* to long-term secure data formats
  - *Re-sign documents with a scalable method*

Principal Legal Issues

- Development of adequate legal assumptions that a certain transformation will be considered secure unless contrary is proven;
- Legal assumptions must relate to the whole transformation process, not just one of its stages- an electronic document;
- Currently, we can see preparation of new legislation (e.g. e-invoicing) but lack of business applications;
- Widespread business application will need development of secure e-transformation and e-archiving certification service provider

Problem Statement

Application scenarios are diversified - security requirements vary

- Common problems:
  - Original signatures break
  - Originals are no longer available or readable
  - Legal regulations come into play and
  - entail special requirements on transformations

- Common goal:
  Ensure that documents can be used in their **application contexts** in the desired way, i.e., have the necessary level of **trustworthiness.**

- First step: A basic set of concepts and notions
  - to characterise **secure transformations** in a context- and technology-neutral way
  - Clearly separate **application context** from **transformation system**

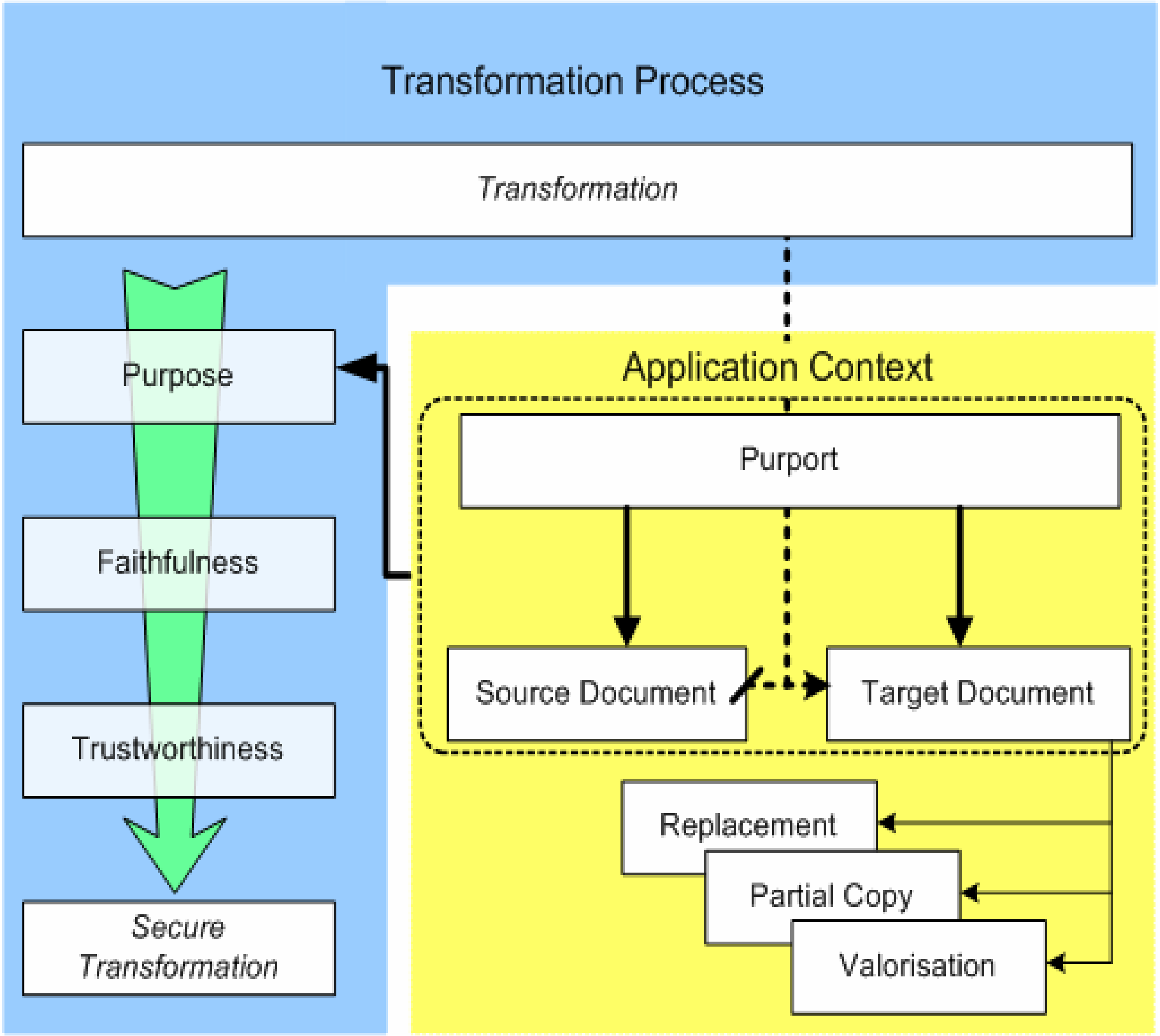
Basic Notions and Concepts

What characterises secure Document transformations?

Mnemonic:

A secure transformation is ensured through the trustworthiness of faithfulness for a given purpose.

In turn, the purpose is the conversion between source and Target with their respective purports.

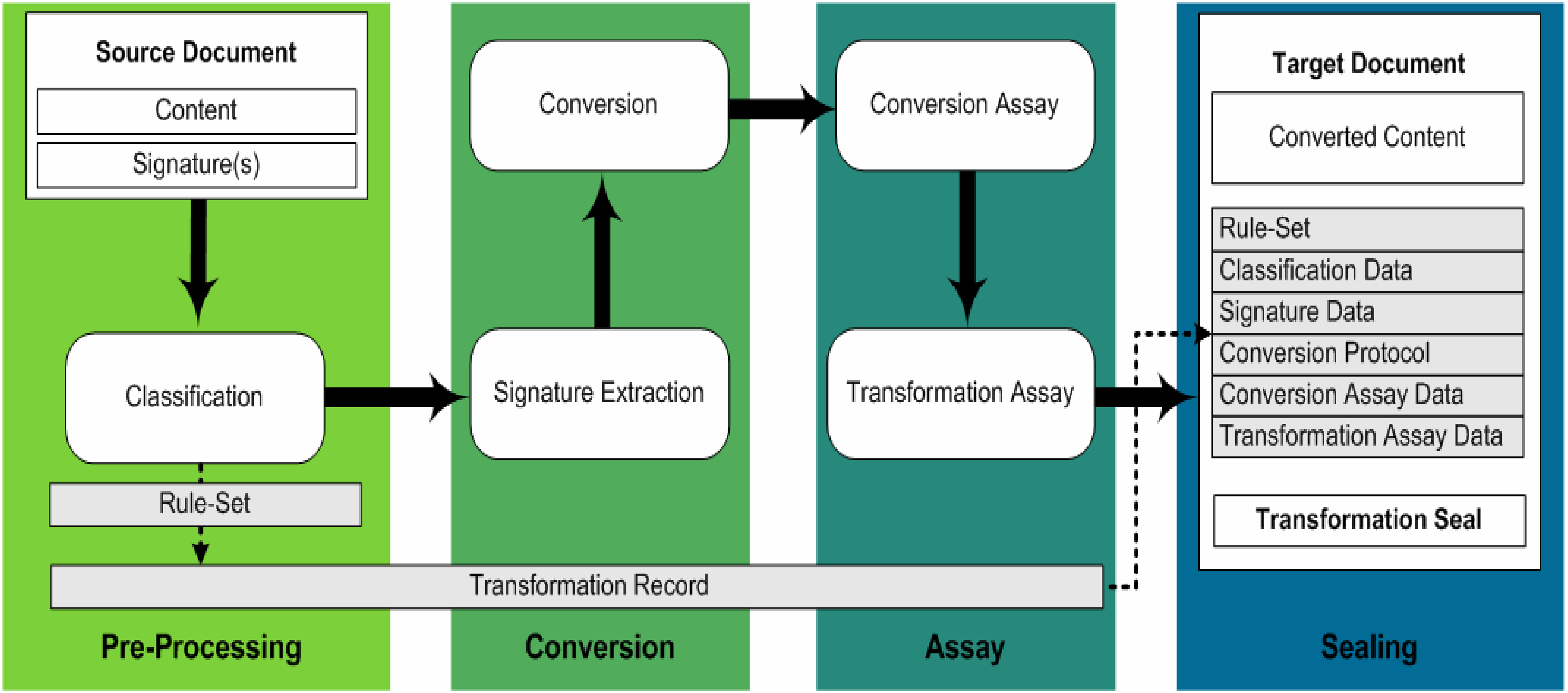


Common Requirements for Secure Transformations

- Reach the required faithfulness
  - ⇨ Determine the purpose of the transformation
  - ⇨ Apply a faithful conversion method to the content
- Trustworthiness
  - ⇨ Record precisely who did what in an *ex post* provable way, i.e., keep a transformation protocol with the target
  - ⇨ Check the results (target contents and protocols)
  - ⇨ Make the results attributable to a responsible party by (electronic) signatures

⇨ Transformation is a step-wise process leading from source to target document

Processual Analysis of Secure Transformations



Correct Classification is Central!

- Depending on app. context and transformation's purpose
- Source doc is classified at assessed properties like
  - (contextual) Document type (patient record, building plan)
  - Document format (Word, PDF, TIFF, XML, …)
- Classification result and purpose determine
  - *Which properties* are relevant for *faithfulness*
  - *How* faithfulness is to be *reached and audited*
  - *How* and *by whom* the results are to be *attested* to ensure *trustworthiness*

➔ A unique **rule-set** that governs all subsequent steps

➔ A **transformation record** that carries all relevant information (rule-set, doc at intermediate stages, protocols, etc.)

Rule-Sets

- Rule-Sets are a flexible *generic* concept comprising
  - *Technical rules*, e.g., conversion components, algorithms and parameters
  - *Security rules* for the *transformation system*, its *operation* and *process organisation*
  - *Format rules* for source and target, e.g.,
    - reject Word docs with comments or review marks
    - Target must validate against specified (XML) schema
  - *Contextual rules*
    - Require the names of two signatories in the target (a contract), agreeing with the signer names in the original's signatures
  - *Policies* for signature *verification*, *extraction*, and *creation* (advanced or qualified sigs, OCSP requests, …)
  - *Limits for automation*, e.g., necessity for human inspection with a trusted display component at a certain stage

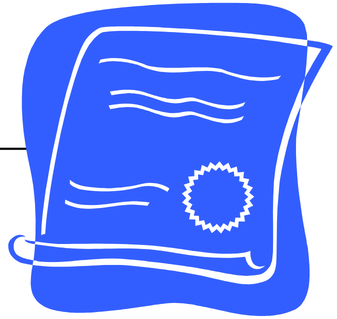
Rule-Set Instantiation and Profiling

- Rule-Sets are as such too generic to be very useful
  Current work aims at
  - A *generic data structure* for rule-sets, structured along the transformation phases, and
  - Interface points which separate *automatable* rules from those which are only *human-understandable*
  - Means to *refer* to resources (standards, parameters), e.g., by OIDs
  - Common hooks to link *profiles* which are *application specific* and respect the *legal domain* (national rules, official vs. private use, etc.)
  - Make examples:
    - *Automated* conversion of XML patient records
    - *Attestation and legalisation* (by notaries or public officials) *according to German law*
    - *Authorised translations*

Transformation Seal

- **The Transformation Seal is the central concept for the creation of the target document**
  - Carries all data (from the trf. record) necessary for a forensic auditing of the transformation and its results and thus enables ***probative force***
  - Carries an electronic signature over said data and target contents, to
  - Secure the ***integrity*** of the target document
  - ***Attest*** the correctness of transformation process and result
  - ***Attribute*** this attestation to a ***responsible, authorised*** party
- **Profiling and Instantiation follows the same paths as for Rule-Sets**

Legalisation/Official Certification



- Scenario based on German law (§ 33 VwVfG)
  - An authority issues a doc to a citizen using an E→E trf.
    (e.g. excerpts from public record; purport ‘for presentation at authority XY’)
  - Source carries qualified signature and is ***classified*** by type
  - ***Signature extraction*** validates signature, records sig time, cert holder and cert data, failure is ***stop criterion***
  - ***Seal*** must carry an official’s ***qualified signature*** and additionally
    - ***Denotation*** of ***source*** doc (e.g.’family register’)
    - ***Signature data*** (not further specified by law)
    - ***Time*** and ***location*** of certification
    - ***Name*** of the attesting public servant
    - ***Denotation*** of the issuing authority
    - An ***express statement of agreement*** of source and target contents
  - ***Signing*** can be partially automated by multi-sig creation

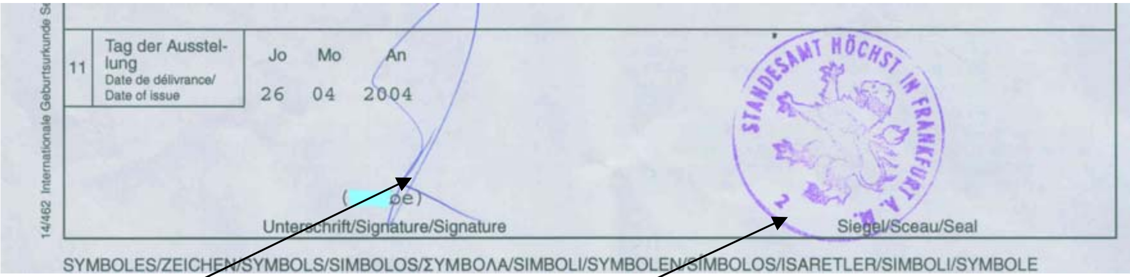
Attestor Authorisation - Problem

An attestation/legalisation/official certification of paper docs carries *two* authentication chararcteristics

- A signature authenticates the *attestor as a person*
- A seal authenticates *his/her role* as one *authorised* to carry out the attestation

A *single* (qualified) signature is insufficient to convey *both* assurances. A *second*, cryptographically secured item will generally be necessary.

(Remarkably, German legislation currently ignores the issue)



14/462 Internationale Geburtsurkunde S

11	Tag der Ausstellung Date de délivrance/ Date of issue	Jo	Mo	An
		26	04	2004

([redacted] oe)

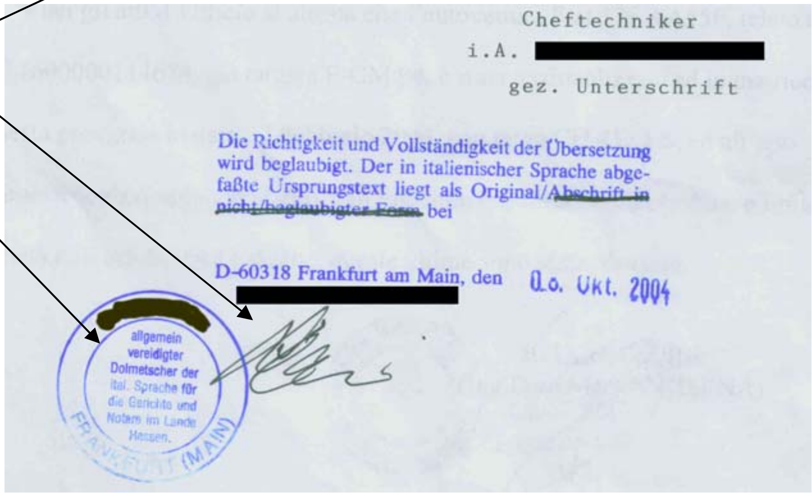
Unterschrift/Signature/Signature

STANDESAMT HÖCHST IN FRANKFURT A. M. 2

Siegel/Sceau/Seal

SYMBOLES/ZEICHEN/SYMBOLS/SIMBOLOS/ΣΥΜΒΟΛΑ/SIMBOLI/SYMBOLEN/SIMBOLOS/ISARETLER/SIMBOLI/SYMBOLE

Excerpt from family register



Cheftechniker

i.A. [redacted]

gez. Unterschrift

Die Richtigkeit und Vollständigkeit der Übersetzung wird beglaubigt. Der in italienischer Sprache abgefaßte Ursprungstext liegt als Original/~~Abschrift in nicht/beglaubigter Form~~ bei

D-60318 Frankfurt am Main, den 0.o. Okt. 2004

[redacted]

[redacted] allgemein vereidigter Dolmetscher der ital. Sprache für die Gerichte und Notare im Lande Hessen. FRANKFURT (MAIN)

Authorised translation

Attestor Authorisation by Attribute Certificates

- **ACs are the self-evident solution approach but bear problems and bring up new tasks**
  - Define of a common set of attestor roles
  - Build a registry for the authorities for the corresponding roles, i.e., the entities which exert authority over issuance and revocation of the ACs
  - Build a (central?, de-centralised?) cert. Infrastructure
  - This infrastructure might have to bear special longevity requirements for certificate data
    - ➢ An additional cost-factor for E-Gov and E-notaries

Thank You for Your attention !