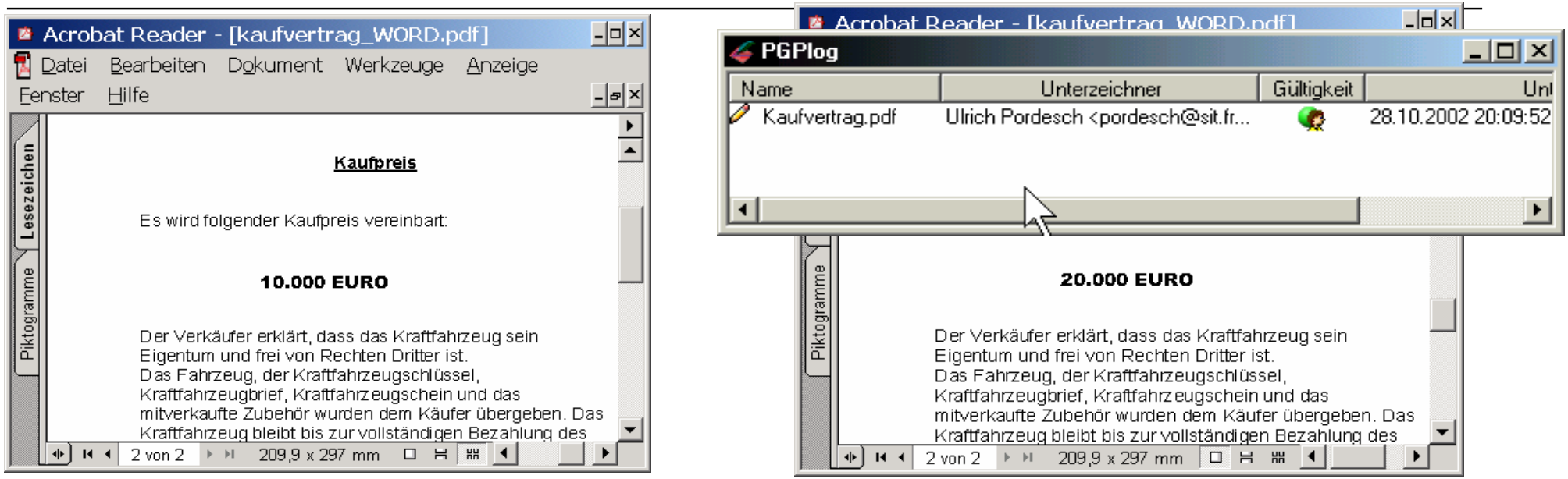
# XML-Signatur Anwendungsprofile aus Sicht der Präsentationsproblematik

Thomas Kunz / Ulrich Pordesch / Andreas U. Schmidt


Fraunhofer Institut
Sichere Telekooperation

# Präsentationsproblem




Präsentationen der selben signierten bzw. zu signierenden Daten weichen so voneinander ab, dass sie unterschiedlich interpretiert werden (Mehrdeutigkeit oder Falschpräsentation).

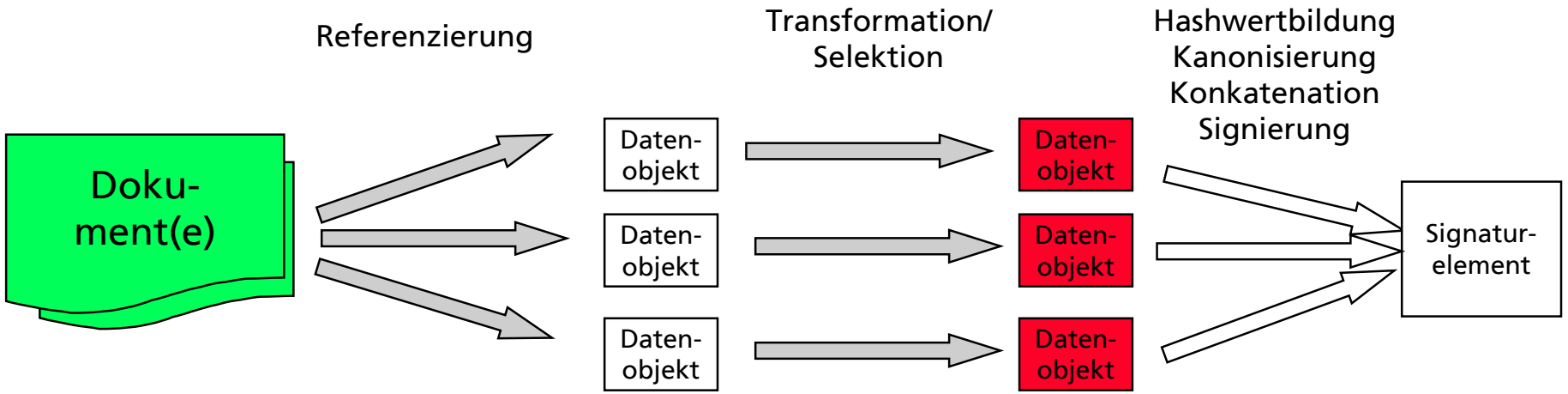
Ebenen des Mehrdeutigkeitsproblem:

- Datenformat, Darstellung, Interaktion



Fraunhofer SIT Institut Sichere Telekooperation

# XML-Signaturen




An **welcher Stelle** wird **was** präsentiert?



Fraunhofer Institut
Sichere Telekooperation

# Präsentationsprobleme bei XMLDSig

- **Bezug:** Inhaltlicher Zusammenhang von Ausgangsdokumente und signierten Datenobjekten ist durch Transformation/Selektion möglicherweise zerstört
- **Kontextbindung**: Bindung von Schemata und Stylesheets nicht gegeben in XMLDSig:
  - Nicht signierte Stylesheets: Wird das für die Präsentation notwendige Stylesheet nicht signiert, kann die Darstellung verfälscht werden.
  - Integrität der Kontext-Komponenten wird problematisch, z.B. Ist das mit*signierte* Schema/Stylesheet auch das, welches zur Verarbeitung/Präsentation des Dokuments benutzt wurde?
  - Nicht signierte Schemata, können Ungültigkeit des Dokuments oder veränderte Interpretation zur Folge haben
- **Mehrdeutigkeit**:
  - Was bedeutet es, mehrere Datenobjekte zu signieren? Sollen alle Datenobjekte (auch mitsignierte Stylesheets und Schemata) präsentiert werden und in welcher Reihenfolge?
- **Darstellung der Signatur**:
  - Standard sieht nicht vor, der Signatur ein Stylesheet zuzuweisen. Die Signatur gehört aber zum Kontext des Dokuments

# Anforderungen

**Ziele im Zusammenhang mit elektronischen Willenserklärungen**

- Rechtliche Zurechenbarkeit erreichen
- In der Regel nicht: Die tatsächlich vom Signierer durchgeführte Präsententation

**Anforderungen**

- **Eindeutigkeit**
  - Ob und Wie der Präsentation festlegen
- **Transparenz**
  - Erkennen können, was signiert wird bzw. wurde
- **Sicherheit**
  - Nutzerfehler vermeiden, Komplexität der Interaktion verringern
- **Beweiseignung**
  - Kontextelemente mitsignieren oder sicher hinterlegen

Betrifft signierte Datenobjekte, aber auch deren Bezug zum Ausgangsdokument:
**Kontextbindung** muss erreicht werden.



Fraunhofer SIT Institut Sichere Telekooperation

# Lösungselemente im Rahmen von XML-Standards

**XSLT** Beschreibt Transformationen im Rahmen eines offenen Standards

**XSL-FO** Als detaillierte, statische Seitenbeschreibungssprache gut geeignet zur Darstellung der endgültig zu präsentierenden Daten (Zielformat)

**Stylesheet-Assoziation** ist nicht geeignet, die nötige, enge Kontextbindung zu erreichen

**XML Schema** (und verwandte Sprachen) Einschränkung von XML-DSig, zum Beispiel von Transformationen können formuliert werden. Andererseits kann die Syntax der zu signierenden Dokumente genau festgelegt werden

**Namespaces** können Elemente verschiedener Anwendungen syntaktisch trennen und ihre Interpretation erleichtern

Alle genannten Elemente können das Präsentationsproblem *erschweren oder erleichtern* indem sie die Begutachtungsmöglichkeit und damit die Beweiseignung verändern.

# XMLDsig-Erweiterungen? - Beispiel XAdES

Erweiterung der W3C-Spezifikation (Erfolg?)
um Signaturattribute, u. a

- textuelle Beschreibung der Daten
- Formatangabe über Object Identifier (OID) oder MIME-Type mit Encoding

Dies ist unzureichend.

Denkbar wäre z.B. detaillierterer Aufbau des Signaturelements unter Einbeziehung von Stylesheets, Schemata und zu verwendender Präsentationskomponente

Gehört dies noch in einen XML-Signaturstandard??

```
<ds:Object>
    <QualfyingProperties>
      <SignedProperties>
        <SignedSignatureProperties>
          (SigningTime)
          (SigningCertificate)
          (SignaturePolicyIdentifier)
          (SignatureProductionPlace)?
          (SignerRole)?
        </SignedSignatureProperties>
        <SignedDataObjectProperties>
          (DataObjectFormat)*
          (CommitmentTypeIndication)*
          (AllDataObjectsTimeStamp)*
          (IndividualDataObjectsTimeStamp)*
        </SignedDataObjectProperties>
      </SignedProperties>

    </QualifyingProperties>
</ds:Object>
```

# Alternative: XML-Standards für signierbare Dokumente

**Generische Datenformate für signierbare Dokumente**:
Definieren fest vorzugebende Bestandteile, z.B. Stylesheets und Schemata, sowie ihre Bindung an das Dokument. Bestimmte, and die Anwendung angepasste Einschränkungen von XML-DSig werden Bestandteil eines solchen Datenformats. Sowohl ein eindeutiges Zielformat, wie auch die Verwendung weiterer Ressourcen zur Transformation, Darstellung und Interpretation sollen möglich sein.

Dazu ist sinnvoll:

**Repositories mit evaluierten Ressourcen**:
Stylesheets, Schemata und evtl. Anwendungen, die für bestimmte Anwendungskontexte evaluiert und gegebenenfalls zertifiziert wurden. Das Dokumentformat enthält Felder, die diese Ressourcen referenzieren und in eindeutiger Weise zu interpretieren sind.

**Ansätze,** aber noch unzureichend sind Initiativen wie 1dok, eDOK