XML-Signaturen und das Präsentationsproblem

Fraunhofer Institut
Sichere Telekooperation

XML-Signaturen und das Präsentationsproblem

Vortrag im Rahmen des Workshops

„XML-Signaturen“ an der TU-Ilmenau,

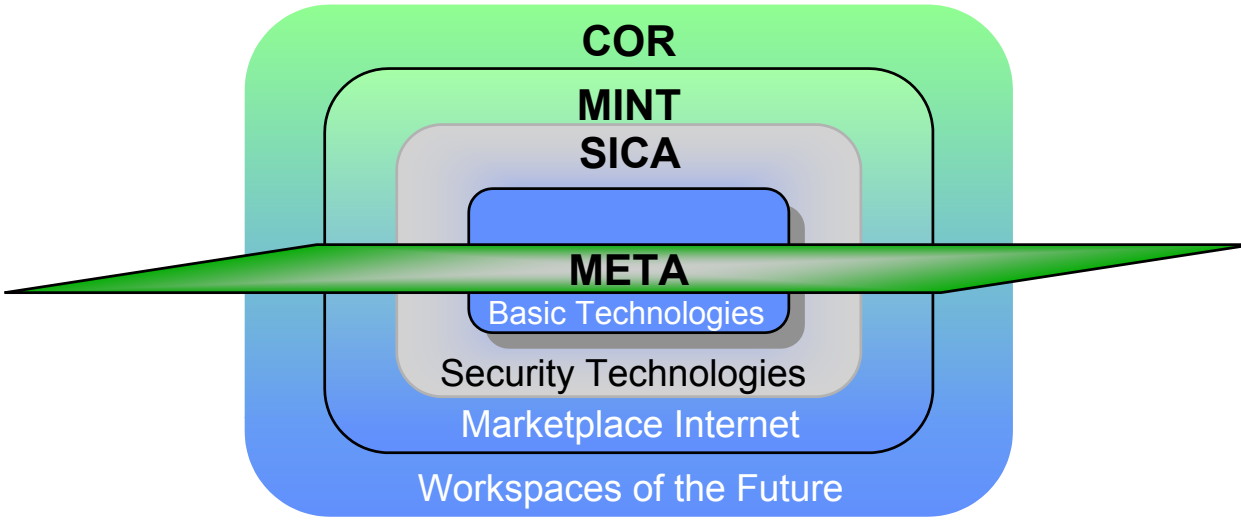
03. – 04.04.2003

Thomas Kunz, Ulrich Pordesch, Andreas Schmidt

Fraunhofer Institut
Sichere Telekooperation

Fraunhofer Institut für Sichere Telekooperation (SIT)

- Entwicklung von Sicherheitstechnologien
- Einbettung von Sicherheitstechnologien in etablierte Anwendungen
- Realisierung neuer innovativer Formen der Zusammenarbeit
- XML-Aktivitäten, z.B.
  - TMF - Telematikplattform für med. Forschungsnetze: Medizinische Daten in XML
  - Media@com: X.509 Authentifizierungsprotokoll
  - Diplomarbeiten zu XML-Encryption, Versteigerungssystem über XML



Fraunhofer Institut Sichere Telekooperation

Vortragende

Thomas Kunz
- Informatikstudium Uni Frankfurt/Main
- Seit 2001 wiss. Mitarbeiter bei SIT. MINT
- Schwerpunkte: Sicherheit in elektronischen Geschäftsprozessen, Security-Policies

Ulrich Pordesch
- Informatikstudium TU-Darmstadt
- Seit 1997 Doktorand/Mitarbeiter SIT
- Schwerpunkt: Rechtliche Anforderungsanalyse
- Dissertation (Ilmenau): Die elektronische Form und das Präsentationsproblem

Dr. Andreas U. Schmidt
- Studium der Mathematik und Physik, Uni Frankfurt/Main, 1999 Promotion in Mathematik
- 1999/2000 Wiss. Mitarbeiter am GMD Institut SIT, AG MINT. Schwerpunkt: Digitale Signaturen in XML
- 2000/01/02 Forschungsaufenthalte in Südafrika und Italien
- Seit Oktober 2002 wiss. Mitarbeiter bei SIT. MINT. Schwerpunkt: Security-Policies

Überblick

1. Herkömmliche Content- und Signaturformate
2. Präsentationsproblem
3. Vorteile vom XML als Content- und Signatur-Format
4. Verbleibende Probleme und Lösungsansätze

Herkömmliche Content-Formate

Textverarbeitung: Word

Tabellenkalkulation: Excel

E-Mail: Mime-ASCII

Internet: HTML

Datenaustausch: EDIFACT

Archivierung: PDF

Fax/Scannen: TIFF

Bilder/Grafiken: JPEG, GIF

„Sicherheitseigenschaften“

- Bislang kein Integritätsschutz
- Inhalt und Urheberschaft abstreitbar
- Kaum Beweiskraft vor Gericht

deshalb auch heute noch zumeist

- Ausdrucken
- Unterschreiben
- Wieder eingeben, als Papier ablegen …

Herkömmliche Signaturformate (I): CMS

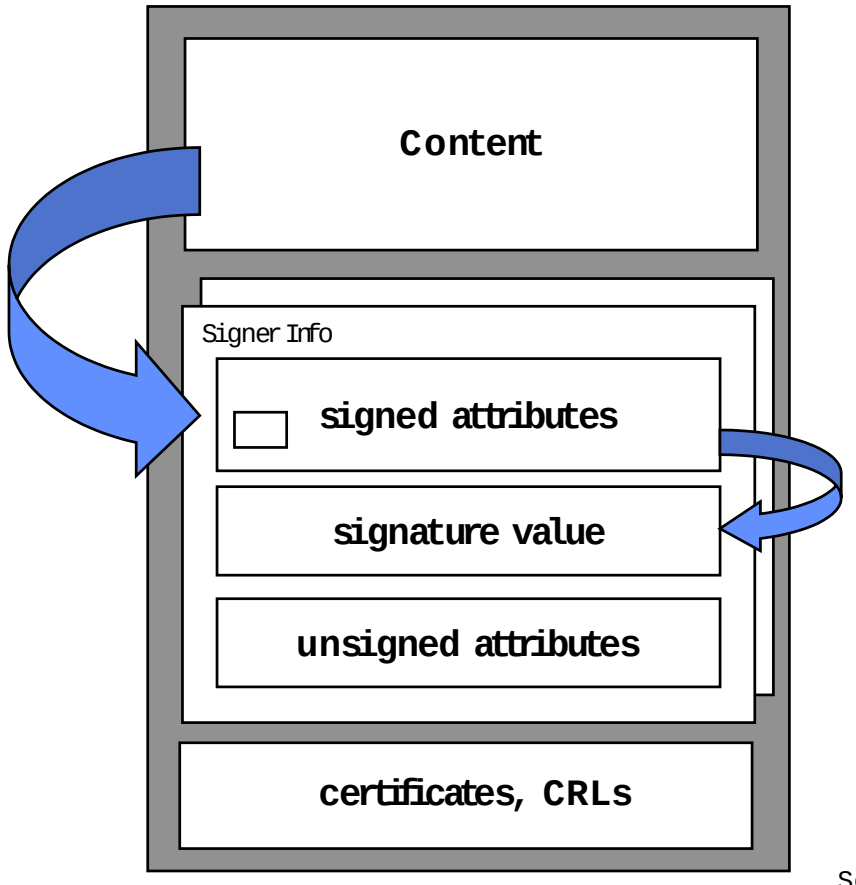
ASN.1-Syntax, Binärcodierung

Signaturerzeugung

- Content (=Nutzdaten, z.B. Datei) hashen
- Hashwert und weitere Attribute (Zeitangabe, Algorithmus, Content-Format) hashen
- Signaturwert bilden
- Zertifikate und weitere Attribute hinzufügen (Gegenzeichnungsignatur, Zeitstempel,..)....

CMS-Container bilden: Content integriert oder extern

Zahlreiche ASN.1-basierte Standards für Attribute, Zertifikate, Sperrlisten - integrierbar



Fraunhofer SIT Institut Sichere Telekooperation

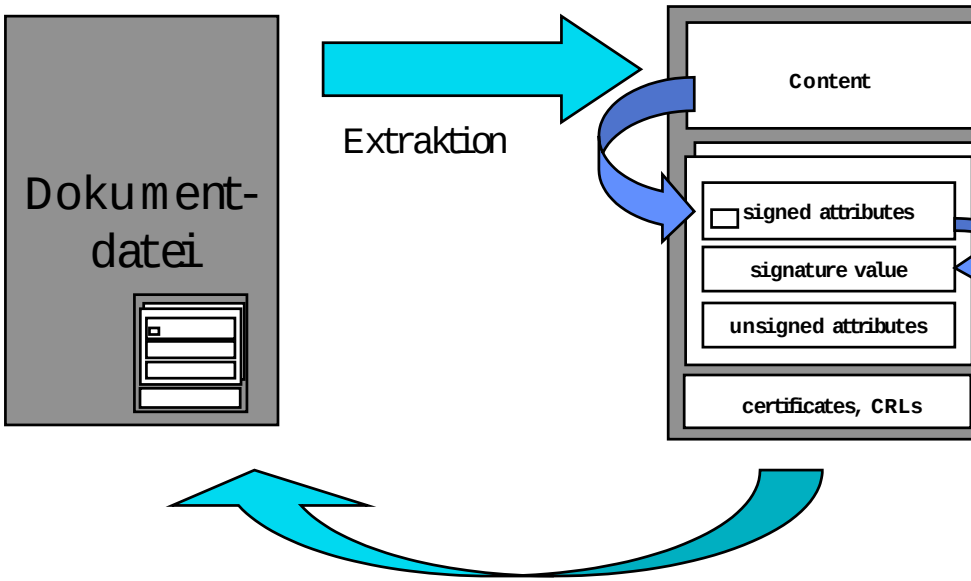
Herkömmliche Signaturformate (II): Anwendung

Signierte Nachricht in Datei mit CMS-Dateiformat

Dokumentdatei unverändert, Signatur in zusätzliche Datei mit CMS-Dateiformat

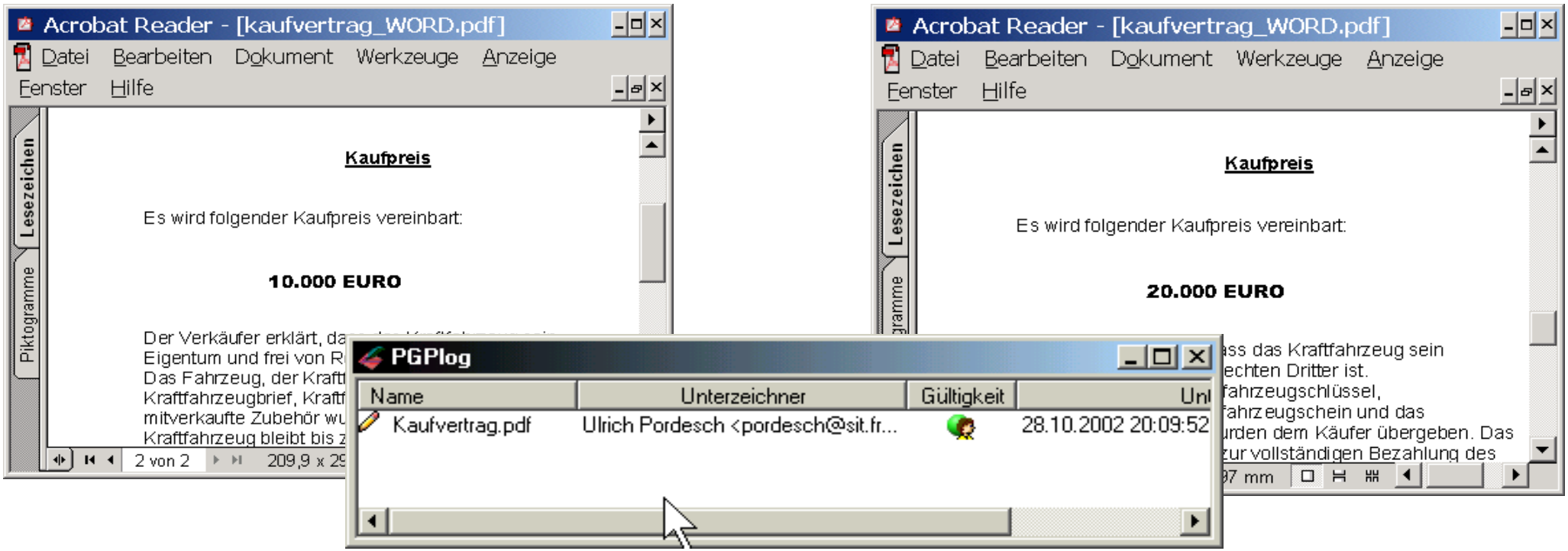
Integration in herkömmliche Dokumentformate

- Selektion, Transformation und Codierung der Dokumentdaten durch Anwendungsprogramm ergibt zu signierenden / signierten Content
- Signatur wird in Dokumentdatei gespeichert, Datenformat-Syntax dazu erweitert um CMS-Block
- Beispiel PDF



Fraunhofer SIT Institut Sichere Telekooperation

Das Präsentationsproblem (I)



Präsentationen der selben signierten bzw. zu signierenden Daten weichen so voneinander ab, dass sie unterschiedlich interpretiert werden.

SIT
Fraunhofer Institut
Sichere Telekooperation

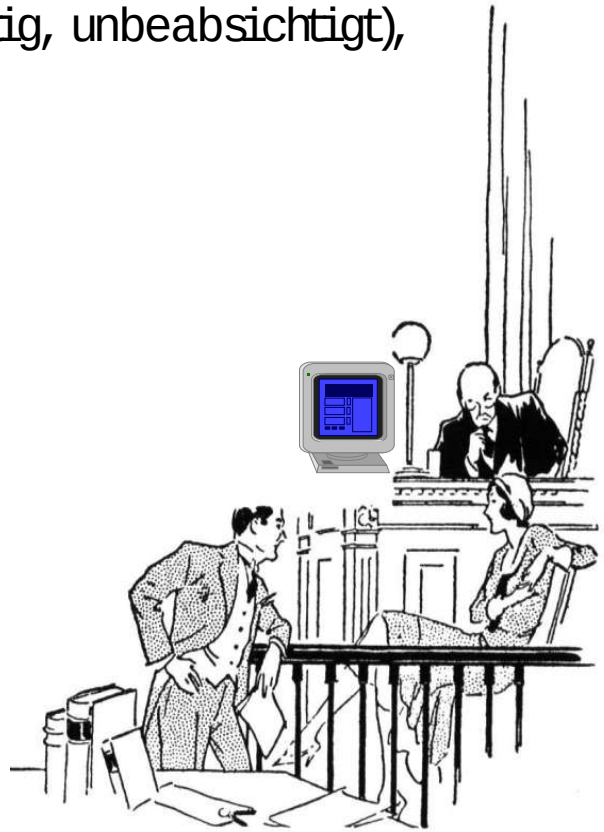
Präsentationsproblem (II)

Präsentationsvarianten in Folge von Mehrdeutigkeit (beabsichtig, unbeabsichtigt), und Falschpräsentation durch Fehler oder Missbräuche

Fehlende eindeutige Festlegungen

- Datenformat und Syntax
- Darstellung der Inhalte
- Benutzerschnittstelle
- Interaktionsregeln

Beweiswert u.U. eingeschränkt trotz Signatur



Präsentationsproblem bei herkömmlichen Datenformaten

Contentformat

- Content ist häufig hinsichtlich der Präsentation mehrdeutig
- Was signiert wird, ist nicht erkennbar:
  - Herkunft, Selektion, Transformation, Codierung nicht erkennbar
  - Content nicht menschenlesbar, Syntax und Semantik oft nicht offengelegt
- Nur eine Datei signierbar, nicht aber z.B. Layoutvorlagendatei und Textdatei

Signaturformat

- Angabe des Contentformats vorgesehen, aber meist unspezifisch belegt („data“)
- Angabe verschiedener Contentformate in parallelen Signaturen möglich
- Präsentation der Signaturdaten nicht festgelegt, sondern implementierungsabhängig

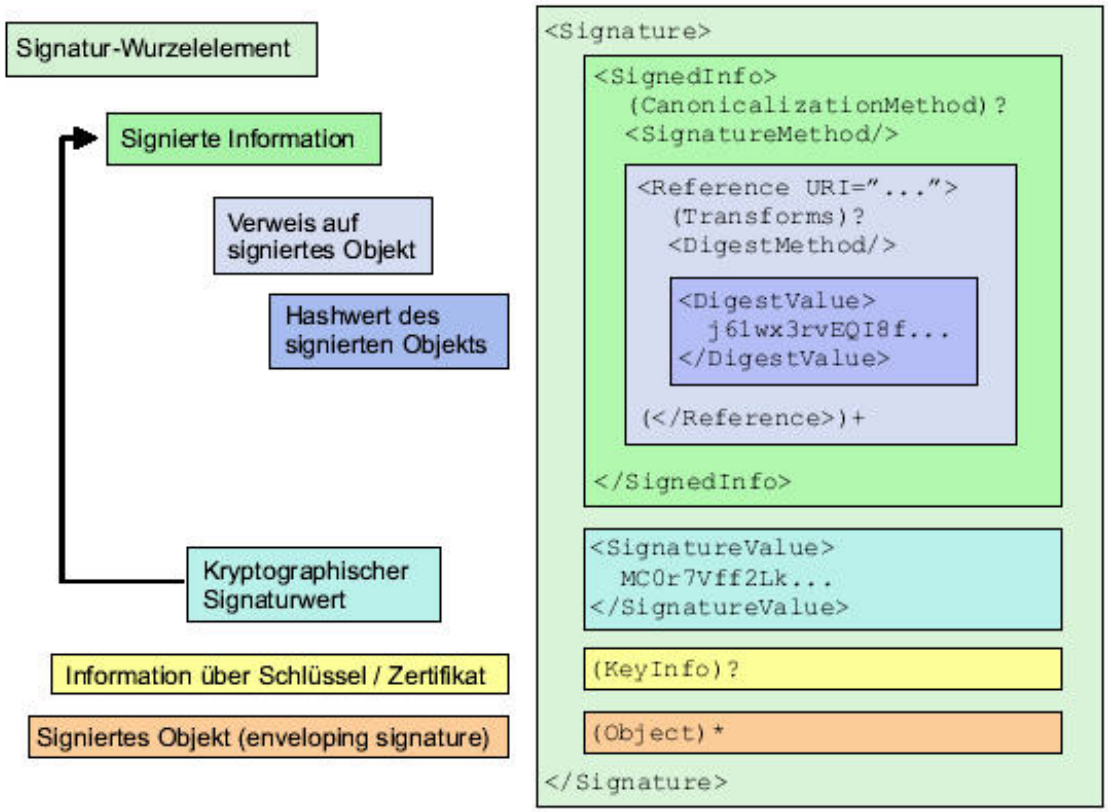
XML als Signatur- und Content-Format

Der gemeinsame IETF/W3C Standard für XML-Signaturen (XMLDsig, W3C Recommendation 12.4.2002) hat hohe Ansprüche:

Er bietet Signaturen

- strukturierter Daten
- aus verschiedenen Anwendungskontexten (Interoperabilität),
- die Web-weit verteilt oder lokal vorliegen,
- beweglich oder mit fester Lokation,
- die nur geringe Anforderungen an die Implementation stellen und
- verwendet gängige kryptographischen Standards,
- mit Open-Source Implementierungen

Grundstruktur von XML-Signaturen (XMLDSig)



Fraunhofer Institut Sichere Telekooperation

XML Komponenten

Syntax: Schemata

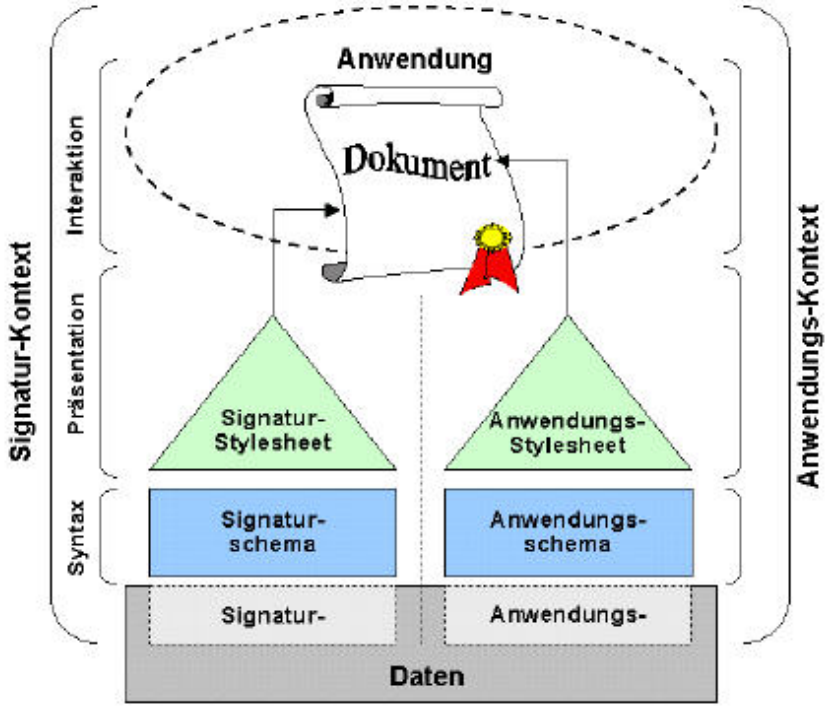
- DTD - das `Erbe´ von SGML
- XML-Schema - der Nachfolgestandard, in XML & für XML

Präsentation: Stylesheets

- CSS - das `Erbe´ von HTML
- XSL Extensible Stylesheet Language:

  XSL Transformations (XML nach XML, Text, oder HTML)

  XSL Formatting Language: Detaillierte Darstellungsvorschriften für XML-Dokumente



Fraunhofer SIT Institut Sichere Telekooperation

Vorteile von XML hinsichtlich des Präsentationsproblems (I)

- **Trennung von Anwendungs- und Signaturkontext:**

  Die Bestimmung von Syntax und Darstellung kann getrennt für Anwendung und Signatur vorgenommen werden

  Diese Komponenten können wiederum einzeln jeweils Verantwortlichen zurechenbar gemacht (XML-signiert) werden

- Transparente Kodierung (im Optimalfall menschenlesbar)
- Angepasste Ansichten durch die Zuweisung von Stylesheets möglich
- Eindeutigkeit der Syntax durch Namespaces (Bedeutungskontext der Elemente) erreichbar

Vorteile von XML hinsichtlich des Präsentationsproblems (II)

- Signieren mehrerer Datenobjekte: Mitsignieren von Stylesheets und Schemadefinition möglich
- Transformation (XSLT): Datenobjekte können vor dem Signieren verändert werden. Ungeeignete Formate vor dem Signieren konvertieren (z.B. Skriptcode eliminieren)
- Transparente überprüfbare Selektion von Teil-Content vor dem Signieren über XPath
- Transparente und überprüfbare Normalisierung

Fraunhofer SIT Institut Sichere Telekooperation

XML-Signaturen: Flexibilität/Interoperabilität *versus* Sicherheit

Flexibilität

- Explizierung von Auswahlprozessen, Umcodierungen, die externe Operationen vor dem Signieren durchführen
- Content-Selektion mit XPath: Formularanwendungen (Teile zu signieren)
- Inhalts-irrelevante Umcodierungen erhalten Signatur (Kanonisierung)

Unsicherheit

- Anwendung von Selektion, Transformation und Kanonisierung: Signiertes Dokument hat möglicherweise völlig andere Bedeutung als das Ausgangsdokument.
- Möglicherweise Probleme bei Kanonisierung, z.B. I18n, mit Zeichensätzen und Kodierung (z.Zt.: intern stets UTF-8).
- Was wird signiert? Interpretation signierter Daten? (Standard definiert keinen Content-Type)

Fraunhofer SIT Institut Sichere Telekooperation

Präsentationsprobleme bei XML

- **Nicht signierte Sylesheets**: Wird das für die Präsentation notwendige Stylesheet nicht signiert, kann die Darstellung verfälscht werden.
- **Kontextbindung**: High-level Semantik zur Bindung von Schemata und Stylesheets in Signatur- und Anwendungskontext existieren nicht in XMLDSig:
  - Integrität der Kontext-Komponenten wird problematisch (Ist das mit*signierte* Schema/Stylesheet auch das, welches zur Verarbeitung/Präsentation des Dokuments benutzt wurde?
  - Mehrdeutigkeit: Sollen alle Datenobjekte präsentiert werden und in welcher Reihenfolge? Sollen auch mitsignierte Stylesheets und Schemata angezeigt werden?
- **Darstellung der Signatur**:
  - Wie sollen Signatur, Zertifikate usw. präsentiert werden? Standard sieht nicht vor, der Signatur ein Stylesheet zuzuweisen.
- **Interaktionsebene unterspezifiziert:**
  - Bsp: XML-Formularbeschreibungssprachen bieten dies nicht

XAdES (ETSI – Spezifikation)

Erweiterung der W3C-Spezifikation (Erfolg?)
um Signaturattribute

- ASN.1-Zeitstempel, -Zertifikate, -Sperrlisten (z.B. CRLs)
- Gegenzeichnungen

Bedeutsam für Präsentationsproblem: Zuweisen und mitsignieren von Datenformaten (optional)

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

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

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


Fraunhofer Institut Sichere Telekooperation

Weitere Lösungsmöglichkeiten

Syntax und Darstellung der Datenobjekte

- Zu anwendungsspezifisch für zentrale Festlegungen -> Guidelines !?
- Evaluierung, Registrierung und Signierung evaluierter Stylesheets und Schemata durch zentrale vertrauenswürdige Stellen

Darstellung der Signatur

- Von zentraler Stelle vorgegebene, evaluierte und zertifizierte Stylesheets !?

Bindung der Kontextelemente

- Ein auf XMLDSig aufbauender Metastandard könnte die entsprechende Semantik definieren.

Ausdruckselemente für Interaktionsregeln