Digitale Signaturen mit XML

Sicherheit *versus* Interoperabilität ?

Status des Standards XML-DSig

- Gemeinsamer Standard von IETF und W3C
- Arbeitsgruppe seit Anfang 1999 aktiv
- Aktueller Entwurf: 1. Juni 2000
- Im formalen Verabschiedungsprozeß der IESG
- Gültiger Standard bis August 2000
- Erste Open-Source Implementierungen existieren

Der Anspruch von XML-DSig

- 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
  - `Abwärtskompatibel´ zu gängigen Signatur- und Kryptographischen Standards.

XML-Dsig Grundstruktur

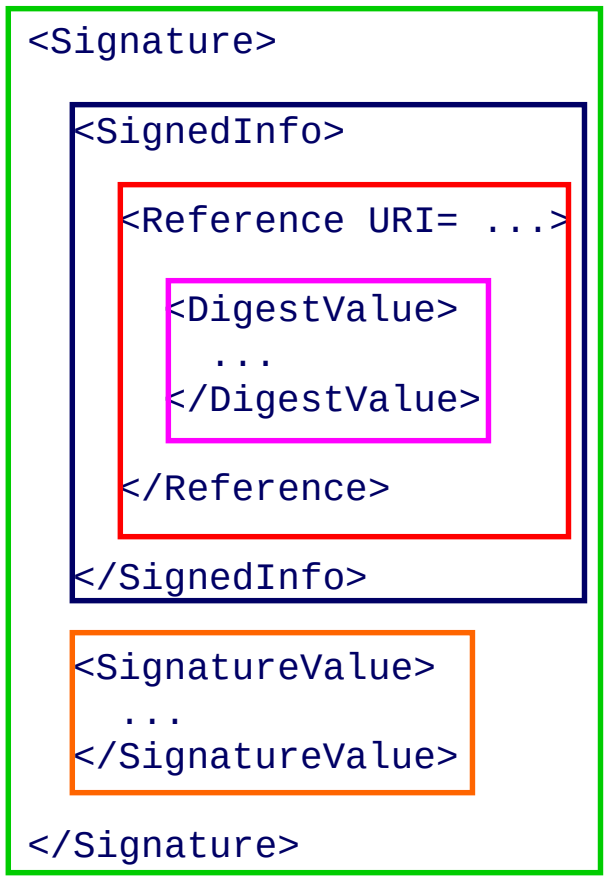
Signatur - Hüllelement

Signierte Information

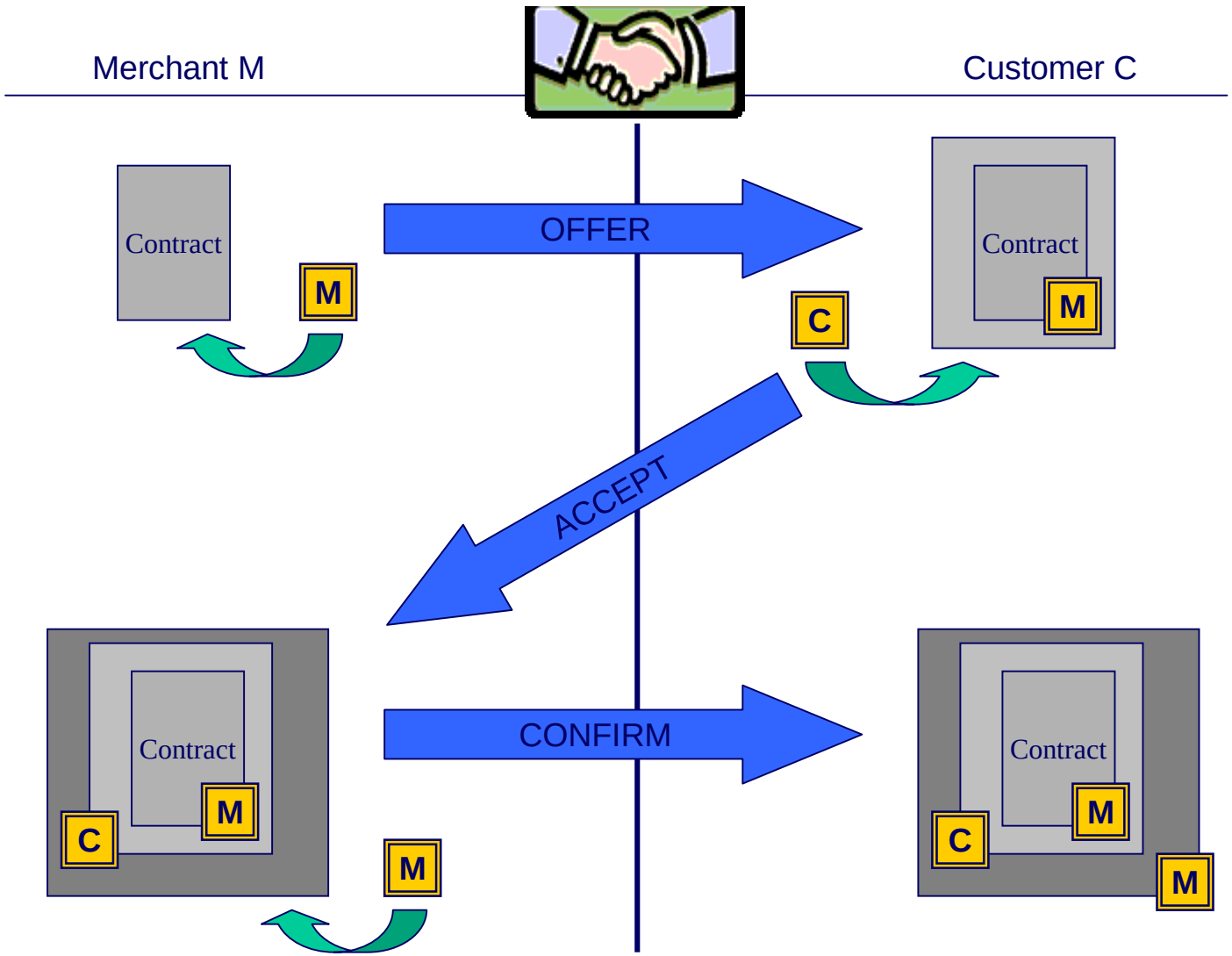
Verweis auf signiertes Objekt

Hashwert des signierten Objekts

Kryptographischer Signaturwert



BAKO - zweiseitige Verbindlichkeit



BAKO-OFFER

Signatur eines Teils des gleichen Dokuments, referenziert durch ID-Attribut Number="77393529247521"

BAKO und Dsig - Elemente werden durch Namensraum-Präfixe BAKO und dsig unterschieden.

```
<BAKO:Offer>
<BAKO:OfferLocator
URI="www.merchant.com/Offers/77393529247521"/>

<BAKO:Contract Number="77393529247521">
  Inhalt des Vertrags
</BAKO:Contract>

<dsig:Signature>

<dsig:SignedInfot>

  <dsig:SignatureMethod Algorithm= "..." />

  <dsig:Reference URI="#77393529247521"/>

     <dsig:DigestMethod Algorithm= "..." >
     <dsig:DigestValue>6...btFS74f=</dsig:DigestValue>

   </dsig:Reference>

</dsig:SignedInfot>

<dsig:SignatureValue>fgh2hDsm=</dsig:SignatureValue>

</dsig:Signature>

</BAKO:Offer>
```

BAKO-ACCEPT

Signatur eines entfernten Dokuments, referenziert durch die URI

www.merchant.com/Offers/77393529247521

`detached Signature´

Vertragsinhalt (umfangreich) wird abgehängt.

```
<BAKO:Accept>

<dsig:Signature>

<dsig:SignedInfot>

  <dsig:SignatureMethod Algorithm= "..." />

  <dsig:Reference
    URI="www.merchant.com/Offers/77393529247521"/>

      <dsig:DigestMethod Algorithm= "..." >
      <dsig:DigestValue>drtes...2s7=</dsig:DigestValue>


   </dsig:Reference>

</dsig:SignedInfot>

<dsig:SignatureValue>td43w...6=</dsig:SignatureValue>

</dsig:Signature>

</BAKO:Accept>
```

BAKO-ACCEPT

Signatur des gesamten Dokuments, das die Signatur enthält, referenziert durch die leere URI

URI=""

`enveloped Signature´

Vorkehrung zur Vermeidung von Selbsreferentialität nötig (nicht dargestellt)!

```
<BAKO:Confirm>
  <BAKO:Accept>
   ...
  </BAKO:Accept>
<dsig:Signature>
<dsig:SignedInfo>
  <dsig:SignatureMethod Algorithm= "..." />
  <dsig:Reference URI=""/>
   ...
  </dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue> ...<dsig:SignatureValue>
</dsig:Signature>
</BAKO:Confirm>
```

Zitat von BAKO-ACCEPT

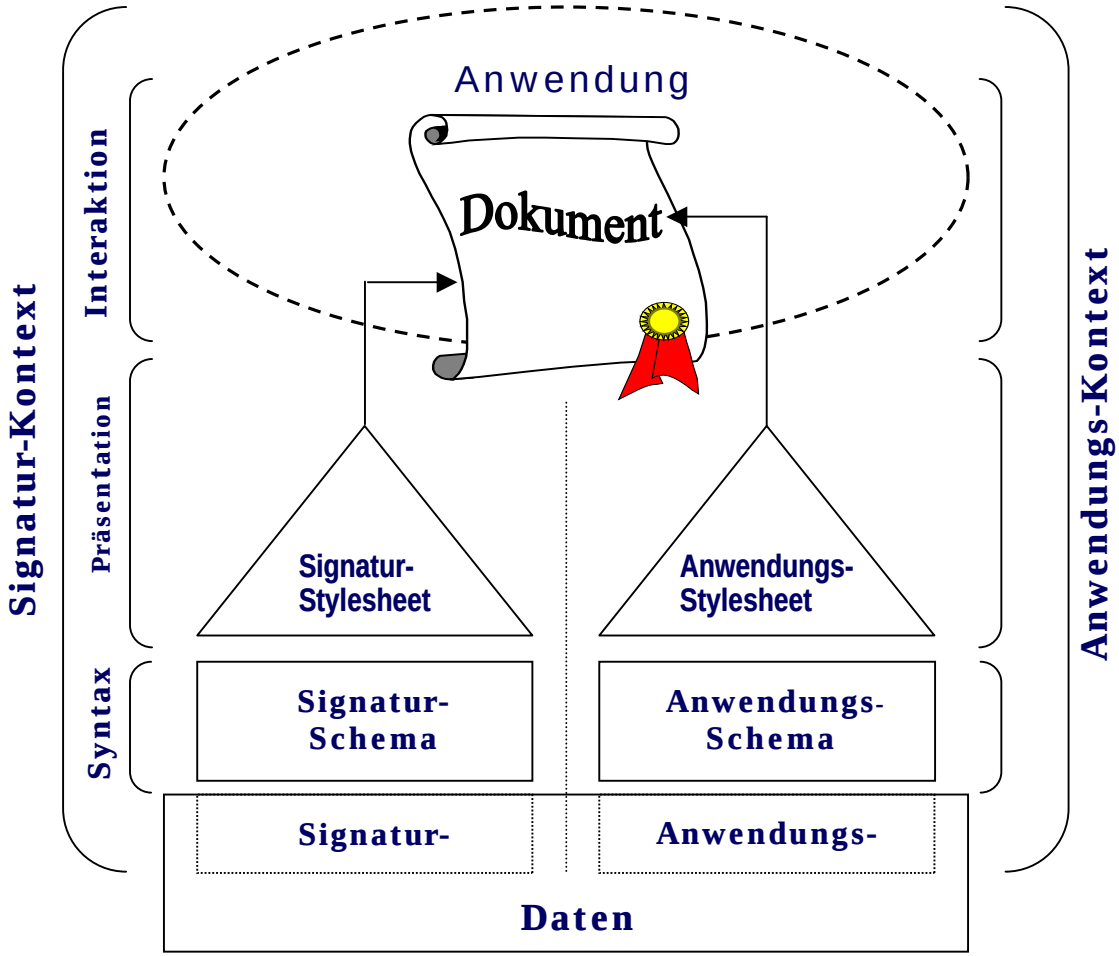
Das Kontext- und Präsentationsproblem digital signierter Dokumente

- Was muß signiert werden?
  - Alle zur Anwendung gehörigen Daten!
  - Nur die für die Anwendung nötigen Daten!
- Was muß dargestellt werden?
  - Alle signierten Daten! (Vollständige Darstellung)
  - Nur die signierten Daten! (Treue Darstellung)
- Problem:
  - Variabilität digitaler Daten
  - Gegensatz zu Automatisierung/Interoperabilität

XML-Komponenten

- Schemata
  - DTD - das `Erbe´ von SGML
  - XML-Schema - der Nachfolgestandard, in XML & für XML
- Stylesheets
  - CSS - das `Erbe´ von HTML
  - XSL Extensible Stylesheet Language:
    - XSL Transformations (XML nach XML oder HTML)
    - XSL Formatting Language: Darstellungsvorschriften für XML-Dokumente

Der Kontext eines signierten XML-Dokuments



Probleme bei der Bindung der Kontext-Komponenten an das signierte Dokument

- DTDs erlauben nur schwache Typisierung,
- sind orthogonal zu Namespaces:
  - Keine transparente Zuordnung von Namespaces zu Kontexten
  - Dokumente mit mehreren Namespaces sind im Allgemeinen nicht mehr automatisch validierbar
- XML-Schema wird diese Probleme lösen!
- XML-DSig enthält keine High-Level Instrumente zur Kontext-Bindung
- Aber: XSLT-<Transforms>: Transformation vor Signaturerzeugung

Probleme der Interoperabilität

- High-Level Auszeichnungssprache vs. Kryptographie auf Bitlevel:
  - Kanonisierung erforderlich.
  - W3C XML-Kanon. ist für diesen Zweck unterspezifiziert (Bsp. Attributordnung, c14n nur für komplette Dokumente keine Fragmente).
  - andere Methoden (infoset, DOM/SAX) liefern keine Strings, sondern interne Repräsentationen.
  - Möglicherweise Probleme bei I18n, mit Zeichensätzen und Kodierung (z.Zt.: intern stets UTF-8).

Probleme bei der Selektion von Teildokumenten

- XPath:
  - Mächtig aber kryptisch.
  - Führt selbst für einfache Anwendungsfälle zu aufwendigen Konstruktionen
  - liefert als Ausgabe Knotenmengen.

XML-DSig ist ein Low-Level-Standard mit Schwergewicht auf einfacher Implementierung, nicht einfacher Anwendung.