Signaturprofile

Notwendigkeit, Ansätze und Standards

Prof. Mario Jeckle

Fachhochschule Furtwangen
mario@jeckle.de
http://www.jeckle.de

Signatur-Workshop, Ilmenau, 2004-04-30

Was bisher geschah …

XML-Signaturworkshop, Ilmenau, 2003-04-04:

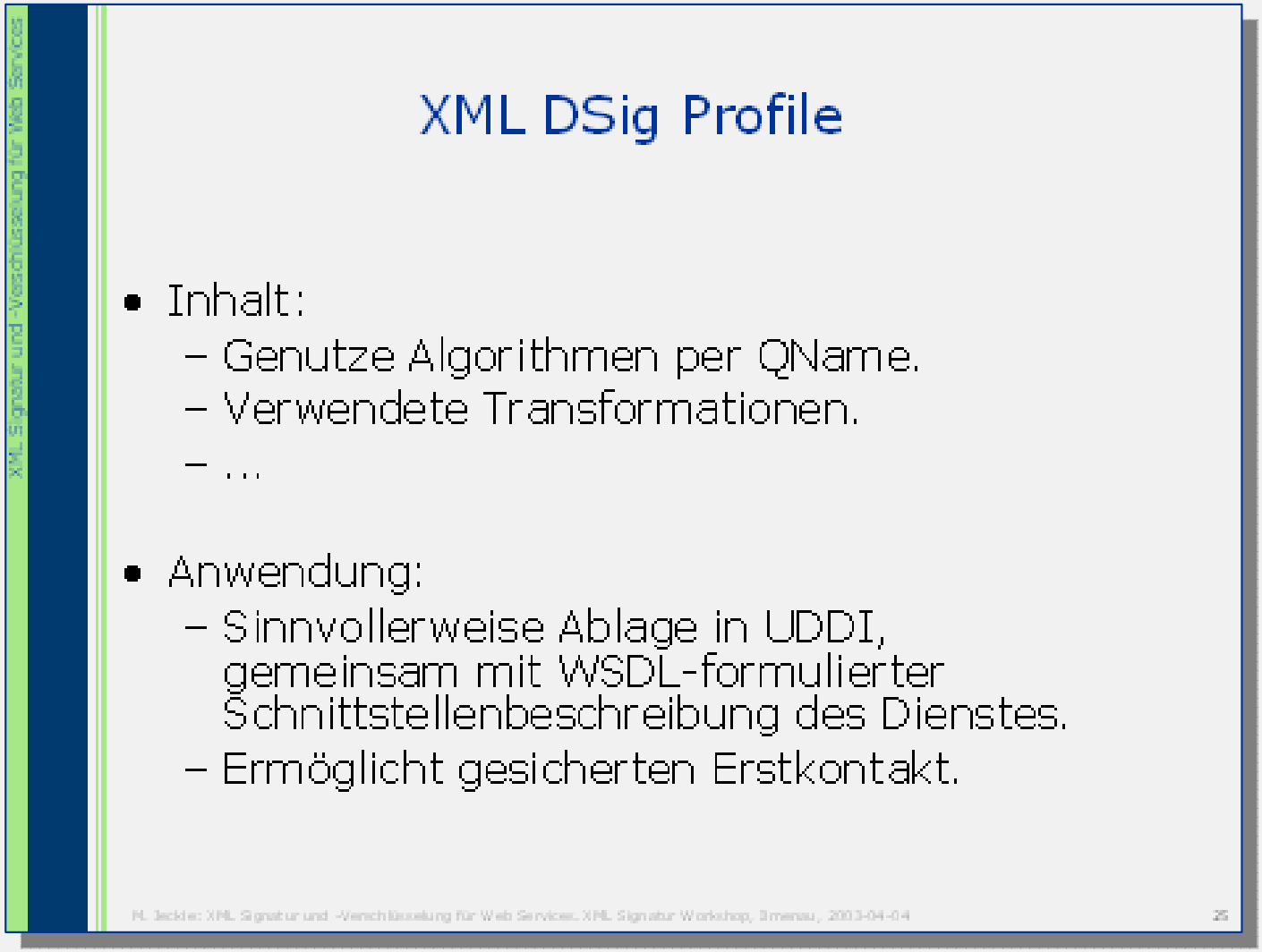
Lessons Learned

Standards nutzen – Standards setzen

- Standard-basiertheit unbedingt sinnvoll.
- Plattformübergreifende Standards ermöglichen Einsatz der Technik überhaupt erst.
- Implementierungen noch in Kinderschuhen und daher mit Kinderkrankheiten behaftet.
- Konkrete Einsatzkonfiguration des Standards nicht standardisiert ausdrückbar.
  => Erschwert Kontrahierung signifikant.
  XML DSig Profile könnte Lösung sein.

Was bisher geschah …

XML-Signaturworkshop, Ilmenau, 2003-04-04:



Hinweis

In den vorgestellten Ansätzen und Standards fällt die Benennung der darin auftretenden Konzepte mit den vorgesehenen (XML-)Syntaxelementen zusammen.

Aus diesem Grunde wurden die entsprechenden Bezeichner im folgenden nicht übersetzt.

Daher ist ein gewisser „denglischer” Einschlag, durch die Vermischung deutscher Sätze und englischsprachig bezeichneter Konzepte, unvermeidlich.

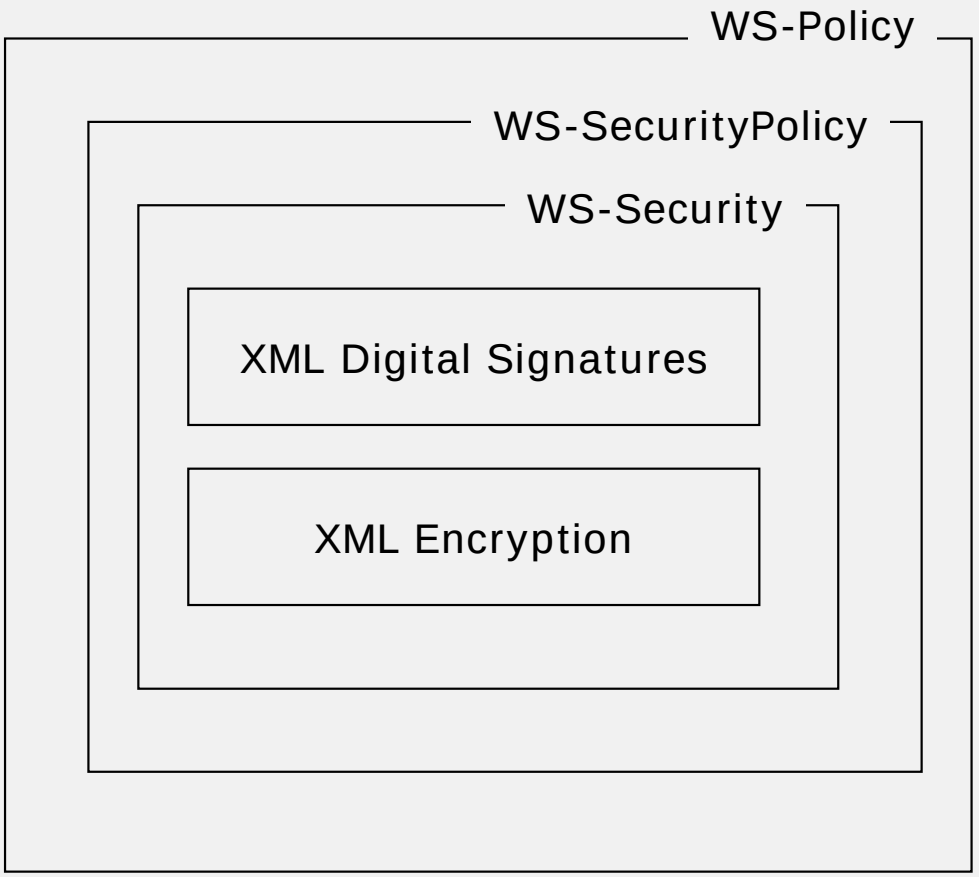
Notwendigkeit

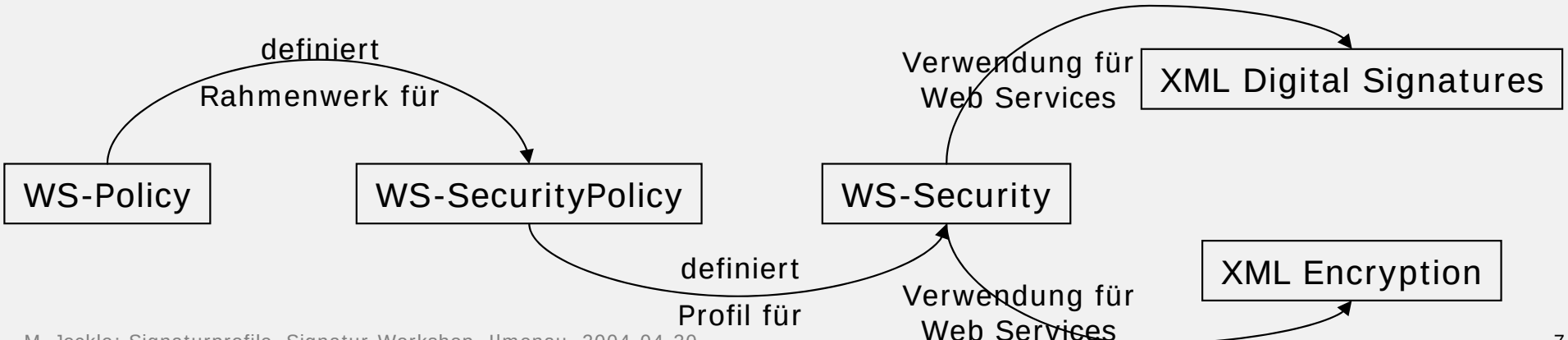
- Ausdruck von Anforderungen an Dienstnutzer *vor* Erstnutzung.
- Explizierung von Service Level Agreements.
- Erweiterung der (durch WSDL) bis dato ausschließlich syntaktisch festgelegten Web-Service-Schnittstelle.

Ansätze

- WSDL:
  - Syntaktische Schnittstellenspezifikation
  - Interaktionsmuster
- WS-Policy:
  - Rahmenwerk zur Strukturierung und Darstellung von Anforderungen
- WS-SecurityPolicy:
  - Semantik für WS-Policy-konforme Inhalte zur Darstellung von Sicherheitsanforderungen

Ansätze

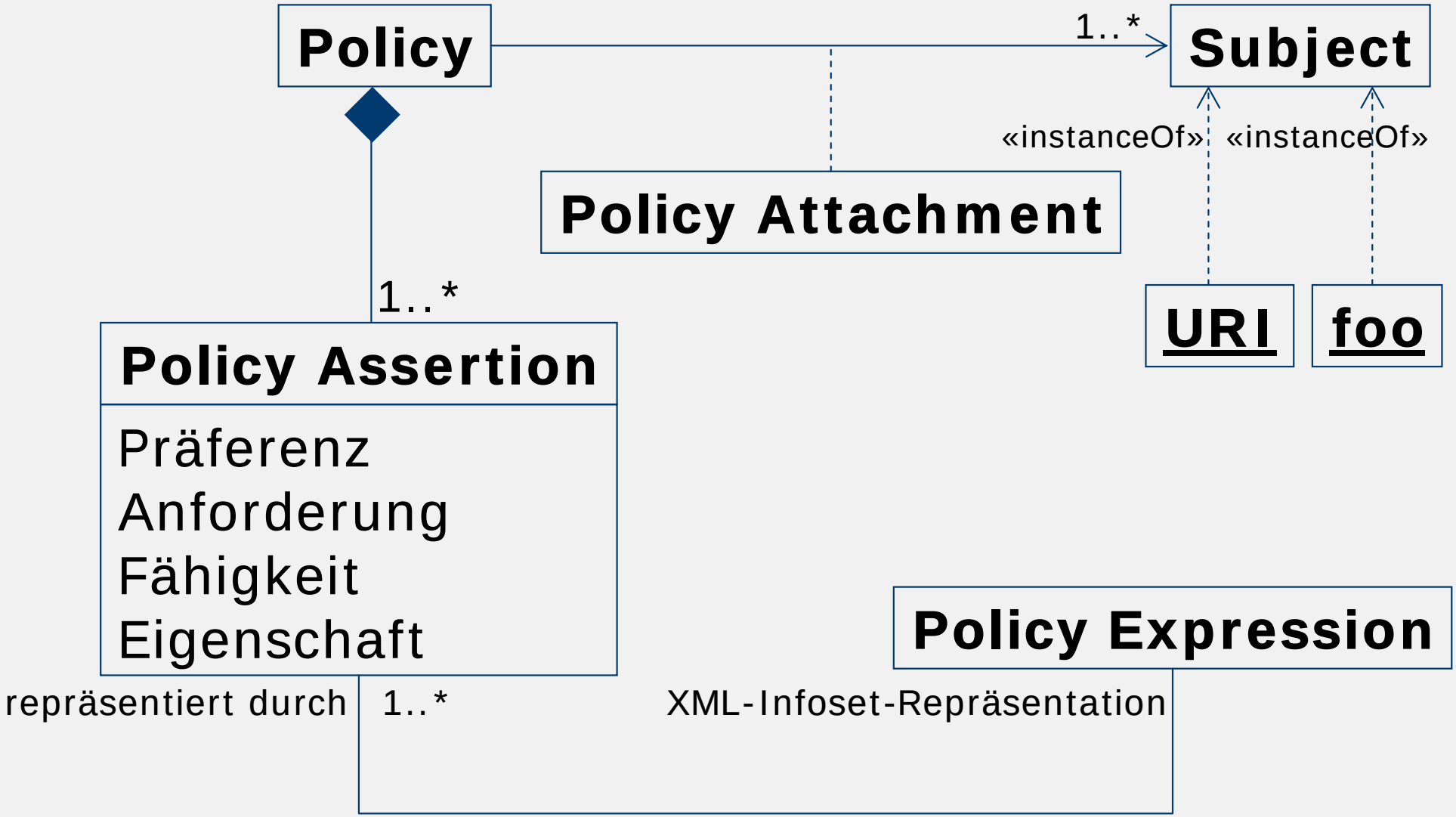

WS-Policy
WS-SecurityPolicy
WS-Security
XML Digital Signatures
XML Encryption


definiert
Rahmenwerk für
WS-Policy
WS-SecurityPolicy
WS-Security
Verwendung für
Web Services
XML Digital Signatures
definiert
Profil für
Verwendung für
Web Services
XML Encryption

Standards: WS-Policy

- Veröffentlicht: 2003
- Getragen durch: Microsoft, IBM, BEA und SAP
- Teil der WS*-Spezifikationsfamilie
- Definiert: Rahmenwerk und XML-basierte Syntax
- Anwendungsgebiet: Policies für Web Services
- Durch andere Spezifikationen erweitert
- Inhalt:
  - Anforderungen
  - Voraussetzungen
  - Fähigkeiten

Standards: WS-Policy-Artefakte



Standards: WS-Policy-Artefakte

- **Policy**: Beschreibt Charakteristika von „Entitäten eines Web Service Systems“ als Menge von *Policy Assertions.*
- **Policy Assertion**: Individuelle Präferenz, Anforderung, Fähigkeit oder Eigenschaft.
- ***Policy Expression***: XML-Infosetrepräsentation einer nichtleeren Menge von *Policy Assertions*.
- ***Policy Subject***: Entität (Web-Service-Endpunkt, Objekt oder Ressource) deren Eigenschaften durch *Policy Assertion* beschrieben wird.
- ***Policy Attachment***: Mechanismus um *Policy Expressions* mit einer nichtleeren Menge von *Policy Attachments* zu assoziieren.

Standards: WS-Policy-Formulierung

Policy Assertion: Individuelle Präferenz, Anforderung, Fähigkeit oder Eigenschaft.
Klassifizierung individueller Anforderungen:

- **Required**: Verletzung der Zusicherung führt zu Fehler.
- **Rejected**: Eigenschaft wird (ausdrücklich) nicht unterstützt und ihre Nutzung führt zu einem Fehler.
- **Optional**: Eigenschaft kann genutzt werden. Eine Verarbeitung ist jedoch nicht zugesichert.
- **Observed**: Policy wird für alle Entitäten (Subjects) angewandt und Aufrufer wird darüber informiert.
- **Ignored**: Zusicherung wird erkannt, aber ignoriert. Adressierte Entitäten und Aufrufer werden.

Standards: WS-Policy-Formulierung

- Operatoren anonymer Policy-Gruppen:
  - **`All`** (Synonym: **`Policy`**)
    Zusicherungen aller Kindelemente müssen erfüllt sein.
  - **`ExactlyOne`**
    Genau eine der durch die Kinelemente formulierten Zusicherungen muß erfüllt sein.
  - **`OneOrMore`**
    Eine oder mehrere der durch die Kindelemente formulierten Zusicherungen müssen erfüllt sein.

Standards: WS-SecurityPolicy

- Veröffentlicht: 2002(!)
- Getragen durch: Microsoft, VeriSign, IBM und RSA Security
- Erweiterung/Anwendung des WS-Security-Standards
- Teil der WS*-Spezifikationsfamilie
- Definiert: *Policy Assertions* für WS-Security
- Anwendungsgebiet: Policies zur Absicherung von Web Services
- Inhalt:
  - *Security Token*-Zusicherung
  - Integritätszusicherungen
  - Vertraulichkeitszusicherung
  - *Security Header*-Zusicherung
  - *Message Age*-Zusicherung

Zusammenspiel zwischen WS-SecurityPolicy und anderen Standards

```
<Element
      Type="..."
      URI="..."
      wsp:Preference="..."/>
```

- `Element`: WS-Security-Artefakt (z.B. Algorithm)
- `Type`: Weitere Eigenschaften des beschränkten Artefakts (Type nur für Algorithmen genutzt)
- `URI`: Verweis auf DSig-spezifizierte URI
- `Preference`: Indikator für Anbieterpräferenz für einen Algorithmus gegenüber Alternativen.

Zusammenspiel zwischen WS-SecurityPolicy und anderen Standards

Standard: WS-SecurityPolicy-Beispiel

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext"
   xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
      <wsp:SpecVersion wsp:Usage="wsp:Required"
         URI="http://schemas.xmlsoap.org/ws/2002/07/secext"/>
        <Integrity wsp:Preference="999" wsp:Usage="wsp:Required">
           <wsp:ExactlyOne>
              <Algorithm Type="wsse:AlgCanonicalization"
                 URI="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
                 wsp:Preference="10"/>
              <Algorithm Type="wsse:AlgCanonicalization"
                URI="http://www.w3.org/TR/2001/REC-xml-c14n-
                20010315#WithComments" wsp:Preference="1"/>
           </wsp:ExactlyOne>
           <wsp:ExactlyOne>
              <Algorithm Type="wsse:AlgSignature"
                URI="http://www.w3.org/2000/09/xmldsig#dsa-sha1"
                wsp:Preference="100"/>
              <Algorithm Type="wsse:AlgSignature"
                URI="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
                wsp:Preference="200"/>
           </wsp:ExactlyOne>
        ...
```

Standard: WS-SecurityPolicy-Beispiel

```
...
      <wsp:ExactlyOne>
         <Algorithm Type="wsse:AlgTransform"
            URI="http://www.w3.org/TR/1999/REC-xpath-19991116"
            wsp:Preference="1">
               <ThePath xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                  not(ancestor-or-self::dsig:Signature)</ThePath>
          </Algorithm>
      </wsp:ExactlyOne>
      <wsp:ExactlyOne>
         <Algorithm Type="wsse:AlgDigest"
            URI="http://www.w3.org/2000/09/xmldsig#sha1"
            wsp:Preference="100"/>
               <Algorithm Type="wsse:AlgDigest"
                  URI="http://www.example.com/myDigest"
                  wsp:Preference="200"/>
      </wsp:ExactlyOne>
      ...
```

Standard: WS-SecurityPolicy-Beispiel

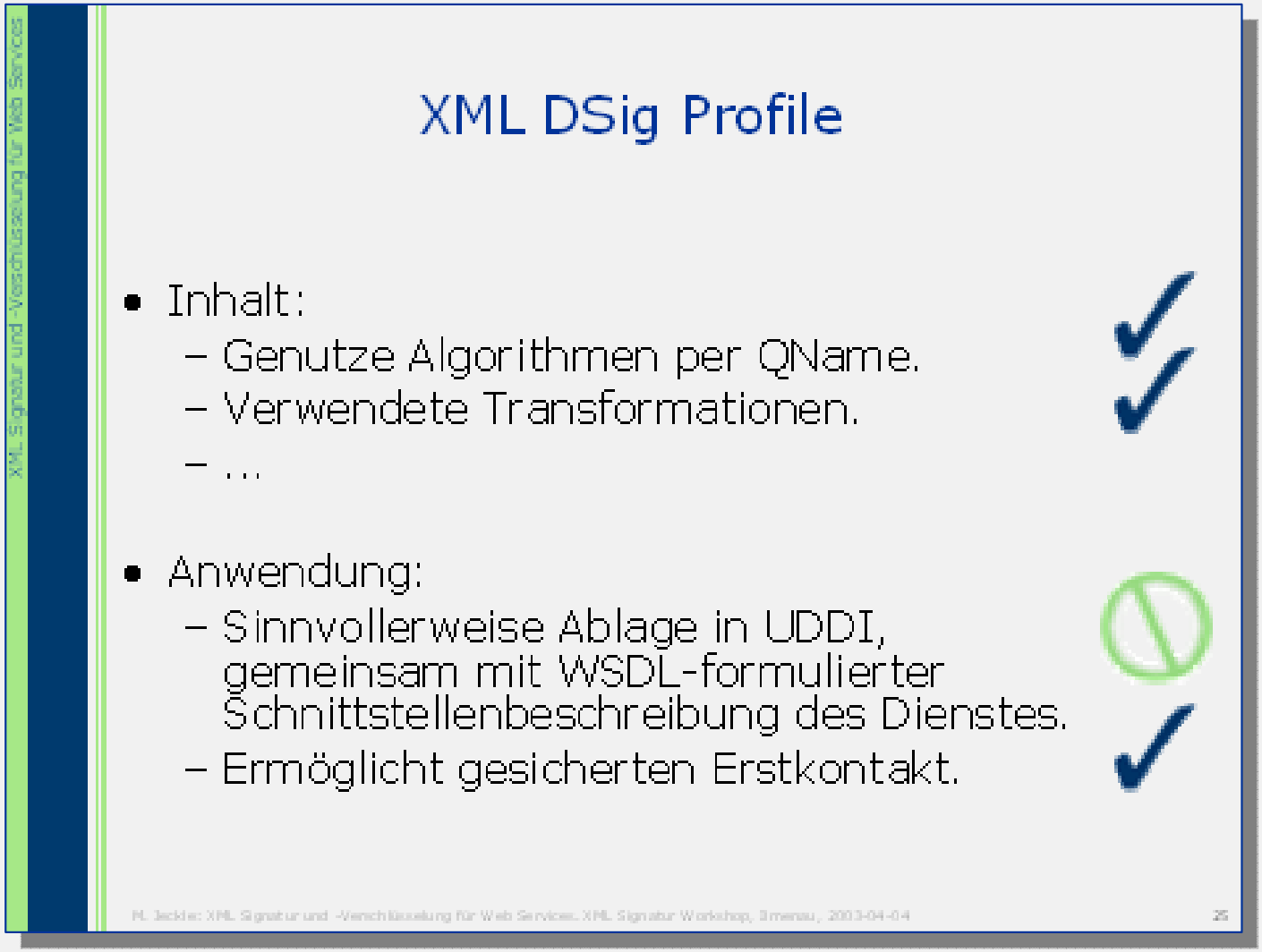
```
...
      <TokenInfo>
         <SecurityToken wsp:Usage="wsp:Required">
             <TokenType>wsse:X509v3</TokenType>
         </SecurityToken>
      </TokenInfo>
      <TokenInfo>
         <SecurityToken wsp:Usage="wsp:Rejected">

         <TokenType>wsse:Kerberosv5TGT</TokenType>
                              </SecurityToken>
      </TokenInfo>
      <MessageParts
          Dialect="http://schemas.xmlsoap.org/2002/12/wsse#soap"
          xmlns:exns="http://www.example.com">
          S:Body exns:Order
      </MessageParts>
   </Integrity>
</wsp:Policy>
```

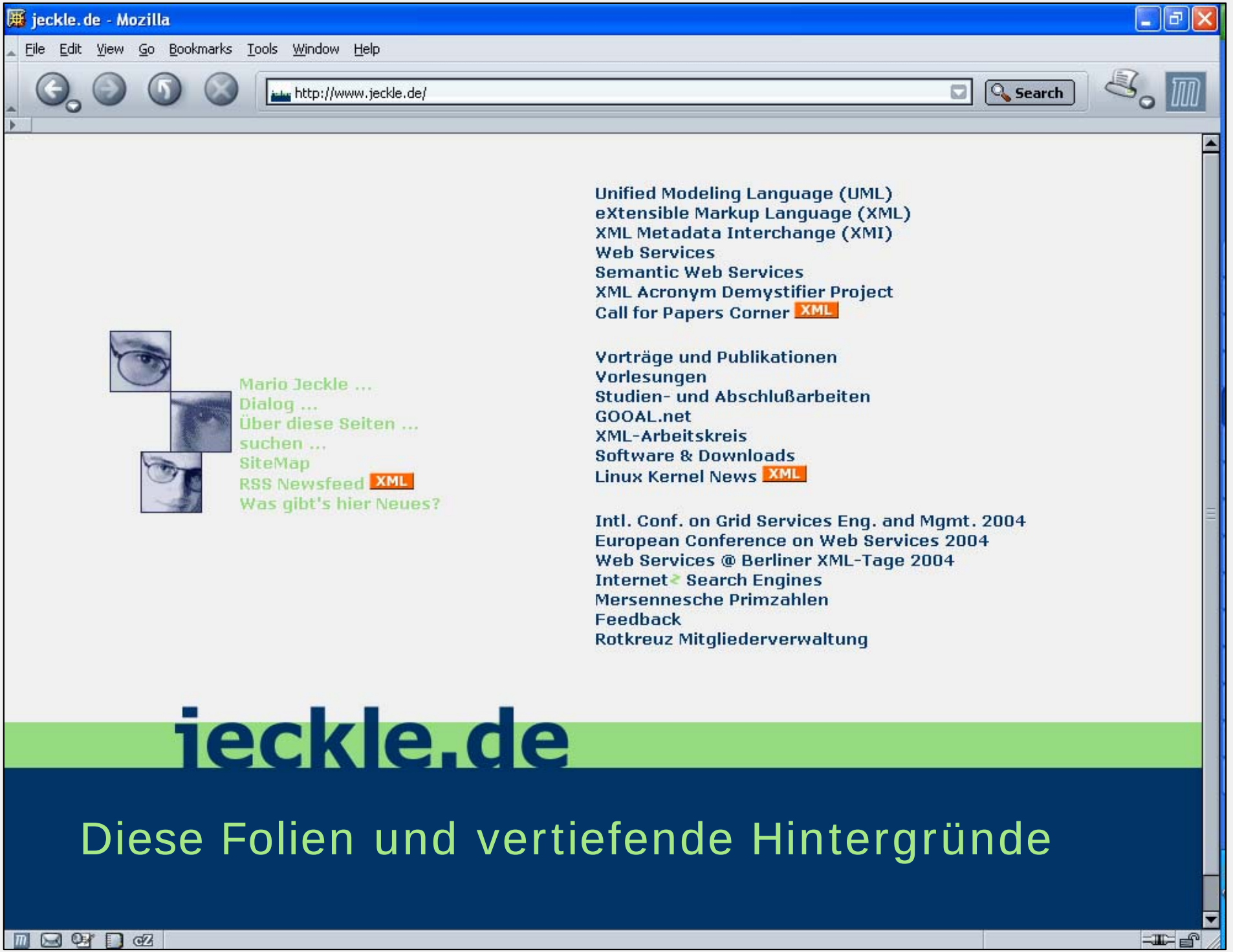
Schwächen des verfügbaren Ansatzes

- Erste Umsetzungen, jedoch keine nennswerten Praxiseinsätze.
- Nutzung des `Preference`-Element kaum interoperabel.
- Keine Korrelation von Elementen aus unterschiedlichen anonymen Policy-Gruppen.
- Inkonsistente syntaktische Darstellung (vgl. unterschiedliche Darstellung des Token-Typs und des Algorithmentyps.)
- Unklare Operationalitätsaspekte (Profil-Bereitstellung, WSDL-/UDDI-Integration)
- Trotz Infoset-Basiertheit normative XML-Syntax.
- „Propietäres“ XML-Vokabular (Alternative: RDF).

Wo stehen wir heute?

XML-Signaturworkshop, Ilmenau, 2004-04-30:




jeckle.de - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://www.jeckle.de/
Search
Unified Modeling Language (UML)
eXtensible Markup Language (XML)
XML Metadata Interchange (XMI)
Web Services
Semantic Web Services
XML Acronym Demystifier Project
Call for Papers Corner XML
Vorträge und Publikationen
Vorlesungen
Studien- und Abschlußarbeiten
GOOAL.net
XML-Arbeitskreis
Software & Downloads
Linux Kernel News XML
Intl. Conf. on Grid Services Eng. and Mgmt. 2004
European Conference on Web Services 2004
Web Services @ Berliner XML-Tage 2004
Internet Search Engines
Mersennesche Primzahlen
Feedback
Rotkreuz Mitgliederverwaltung
Mario Jeckle ...
Dialog ...
Über diese Seiten ...
suchen ...
SiteMap
RSS Newsfeed XML
Was gibt's hier Neues?
jeckle.de
Diese Folien und vertiefende Hintergründe