XML Signature (DSig)

Einführung, Anwendungsbeispiele und Ausblick

heiko@vegan-welt.de

GPN4: 22.05.2005

Übersicht

- Wofür Signaturen?
- Wieso ein weiteres Signaturverfahren?
- Grundlagen
- Signatur-Typen
- Juristische Aspekte von Signaturen
- Einsatzgebiete
- Implementierungen
- Ausblick

Wofür Signaturen?

- **Authentizität**
  - wer hat die Daten erstellt?
- **Integrität**
  - wurden die Daten seit der Signierung verändert?
- **Non-Repudiation**
  - Nachweis, wer welche Daten (wann) erstellt hat.

Wieso ein weiteres Signaturverfahren?

- herkömmliche Verfahren können nur binäre Daten signieren
- herkömmliche Verfahren (z.B. PKCS#7) verstehen kein XML
- XML Signature kann beides
- komplette XML-Dokumente oder nur Fragmente signieren

```
<info prio="1" lang="de" xmlns:a="myns">
<a:A>Fleisch essen ist scheiße!</a:A>
</info>
```

```
<info lang="de" prio="1" xmlns:b="myns">
  <b:A>Fleisch essen ist schei&szlig;e!</b:A>
</info>
```

Grundlagen

- **W3C Recommendation „XML-Signature Syntax and Processing“**
- **Darstellung der Signatur als XML-Element**
- **basiert auf mehreren Standards**
  - XML-Algorithmen: Canonical XML, XPath, XSLT
  - Base64-Encoding
  - Hash-Algorithmus: SHA1
  - Signatur-Algorithmen: DSA, RSA-SHA1, (HMAC)
  - Zertifikate/Keys: X.509, PGP, SPKI
- **kann auf beliebigen Daten angewendet werden, inkl. XML**

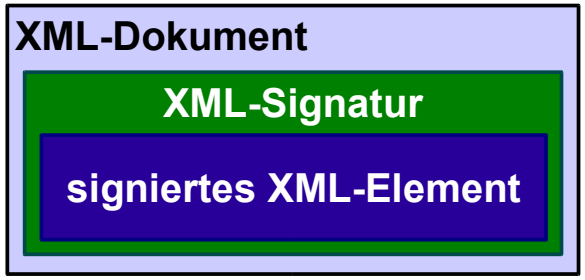
Allgemeine Syntax

```
<Signature>
    <SignedInfo>
        (CanonicalizationMethod)
        (SignatureMethod)
        (<Reference (URI=)? >
            (Transforms)?
            (DigestMethod)
            (DigestValue)
        </Reference>)+
    </SignedInfo>
    (SignatureValue)
    (KeyInfo)?
    (Object)*
</Signature>
```

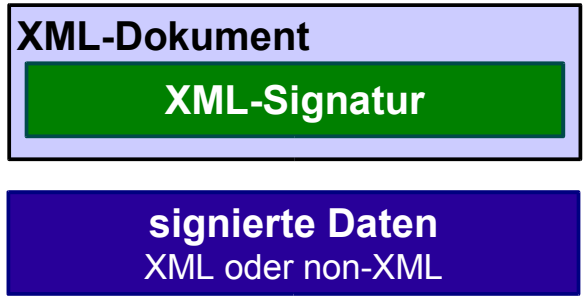
Signatur-Typen

- **Enveloped**
  - Signatur als Element im signierten Dokument enthalten

- **Enveloping**
  - Signatur bezogen auf XML innerhalb der Signatur (im Object-Element)



- **Detached**
  - Signatur auf Daten außerhalb des Signatur-Dokuments bezogen
  - Daten referenziert über URI oder Transformation
  - auch non-XML-Daten



Signatur-Beispiel: Detached

```
<Signature Id="DemoSig" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod
      Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
  <KeyInfo>
    <KeyValue>
      <DSAKeyValue>
        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
      </DSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

Juristische Aspekte von Digitalen Signaturen

- **EU Signaturrichtlinie – definiert qualifizierte Signaturen**
- **Signaturgesetz (SigG)**
  - 2001 novelliert aufgrund der EU Signaturrichtlinie
  - definiert einfache, fortgeschrittene und qualifizierte Signaturen

Einfache elektronische Signatur
- dem Dokument angefügte elektronische Daten
- dient der Authentifizierung

Fortgeschrittene elektronische Signatur
- schützt signiertes Dokument vor Veränderung
- verwendet Signaturschlüssel
- an Schlüsselinhaber gebunden

Qualifizierte elektronische Signatur
- Speicherung des privaten Schlüssels auf Chipkarte
- qualifizierte Zertifikate

Qualifizierte elektronische Signatur mit Anbieter-Akkreditierung

Aktuelle Einsatzgebiete

- **XML Web Services Security / SOAP**
  - Spezifikationen von OASIS
- **OSCI / Virtuelle Poststelle (BSI / bos)**
  - Behörden Datenaustausch-Standard
- **Langzeitarchivierung**
  - z.B. in Datenbanksystemen wie Tamino XML Server
- **SAML**
  - Security Assertion Markup Language von OASIS

Geplante Einsatzgebiete

- elektronische GesundheitsKarte, elektronisches Rezept
- ELSTER
- Bund Online 2005 - Behördenvorgänge

Elektronische GesundheitsKarte (eGK)

- **eRezept**
  - wird vom verschreibenden Arzt und empfangenden Patienten signiert
  - bei Erhalt der Medikamente dann noch von der Apotheke
- **eGesundheitsakte**
  - wird von Ärzten signiert
- **Probleme**
  - signierte XML-Dokumente sind relativ groß und SmartCards haben sehr wenig Datenspeicher
  - Validierung von Signaturen in Notfällen, wenn keine Verbindung zur CA möglich ist

Implementierungen von XML Signature

- **Apache XML Security** (Apache License 2.0)
  - http://xml.apache.org/security/
  - Java-Library
- **XML Security Library** (MIT License)
  - http://www.aleksey.com/xmlsec/
  - C-Library basierend auf der LibXML2
- **Gapxse** (LGPL)
  - http://gapxse.sourceforge.net/
  - Java-Library – no longer maintained...
- dazu kommen noch einige kommerzielle (RSA, Baltimore, Entrust, Verisign, NEC, ...)

Ausblick

- **Standards**
  - sind sinnvoll, wieso also nicht einen Standard für Signaturen benutzen der auch XML versteht?
- **Emails per XML Signature signieren**
  - mit XML Encryption verschlüsseln
  - Erweiterung für GnuPG?
- **Signierung von Office-Dokumenten**
  - OASIS OpenDocument-Format oder MS Metro oder Office XML-Format könnten Signaturen direkt beinhalten
- **PHP-Extension für XML Signature / Encryption**
  - PHP-XML basiert ja sowieso schon auf LibXML2

Weiterführende Infos zu dem Thema

- **W3C XML Signature Syntax and Processing**
  http://www.w3.org/TR/xmldsig-core/
- **W3C Canonical XML Version 1.0**
  http://www.w3.org/TR/2001/REC-xml-c14n-20010315
- **JSR 105: XML Digital Signature APIs**
  http://www.jcp.org/en/jsr/detail?id=105
- **OASIS Web Services Security (WSS)**
  http://www.oasis-open.org/committees/wss

Fragen ?

heiko@vegan-welt.de