

XML-Security Plug-In

eLearning mit der
Eclipse Plattform

Dominik Schadow
JUGS – SIG Eclipse 01.12.2005

Das Plug-In in Kürze

IT-Sicherheitsbewusstsein

- Lernsoftware für XML-Sicherheit
 - signieren, verifizieren, verschlüsseln, entschlüsseln
- div. Erweiterungen (Views/ Editoren)
- Cheat Sheets
- Online-Hilfe
- Freeware für Eclipse 3.0/3.1
- Weiterverwendung gesichertes XML



- **XML-Sicherheit**
 - Features
 - Digitale Signaturen
 - Verschlüsselung
- **XML-Security Plug-In**
 - Features
 - Demo
 - eLearning mit Eclipse

XML-Sicherheit – Übersicht

- **XML Signature**

W3C Empfehlung vom 12. Februar 2002

- **XML Encryption**

W3C Empfehlung vom 10. Dezember 2002



Geringe Bekanntheit

Geringes Interesse

Geringe Verwendung

XML-Sicherheit – Eigenschaften



- XML-Dokument enthält
 - Schlüsselinformationen
 - Algorithmen
- Sichern von
 - beliebigen Daten (Dateien)
Base-64 Kodierung
 - XML-Dokumenten (Fragmenten)
Zugriffsrechte

XML-Sicherheit – Eigenschaften

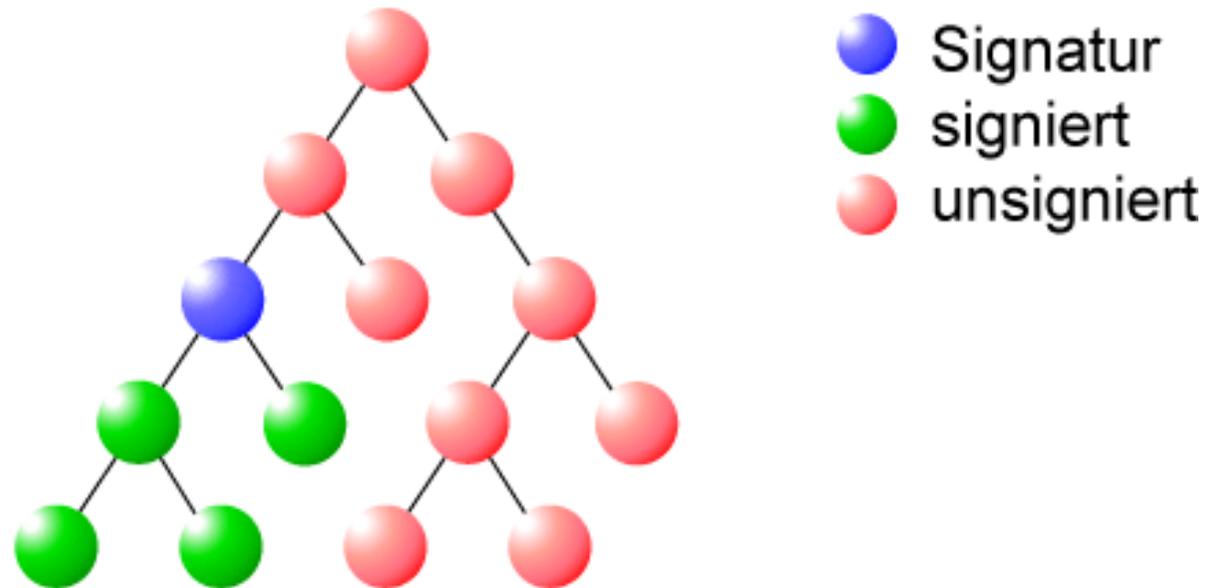
- **Informationsbasierte Sicherheit**
 - Ende-zu-Ende
 - Verarbeitung während Transport
 - Teilbereiche (Fragmente)

- **Dienstbasierte Sicherheit**
 - Punkt-zu-Punkt
 - Verarbeitung am Ende
 - Ganz oder gar nicht

XML-Sicherheit – Digitale Signaturen

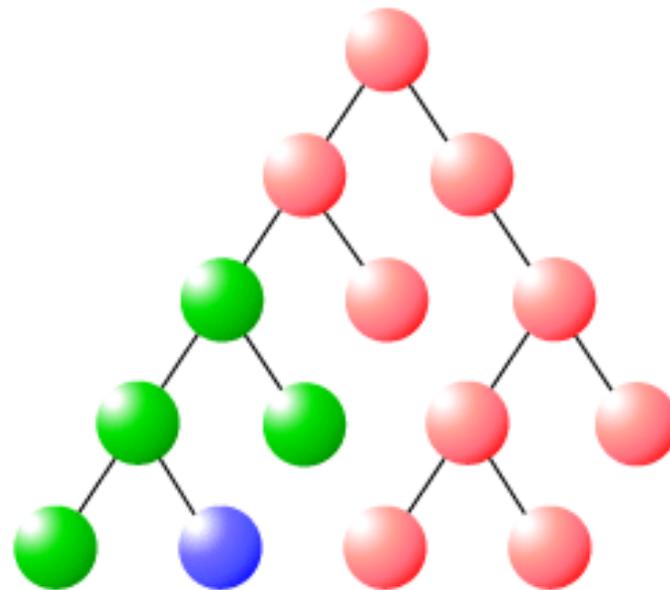
- Integrität, Authentizität, Verbindlichkeit
- Kanonisierung
 - UTF-8
 - Attributwerte normalisieren
 - Zeilenumbrüche
- Präsentationsproblem
 - *What You See Is What You Sign (WYSIWYS)*
 - aber: XSLT

Signaturen – enveloping



```
<Signature>  
  <DocumentData>...</DocumentData>  
</Signature>
```

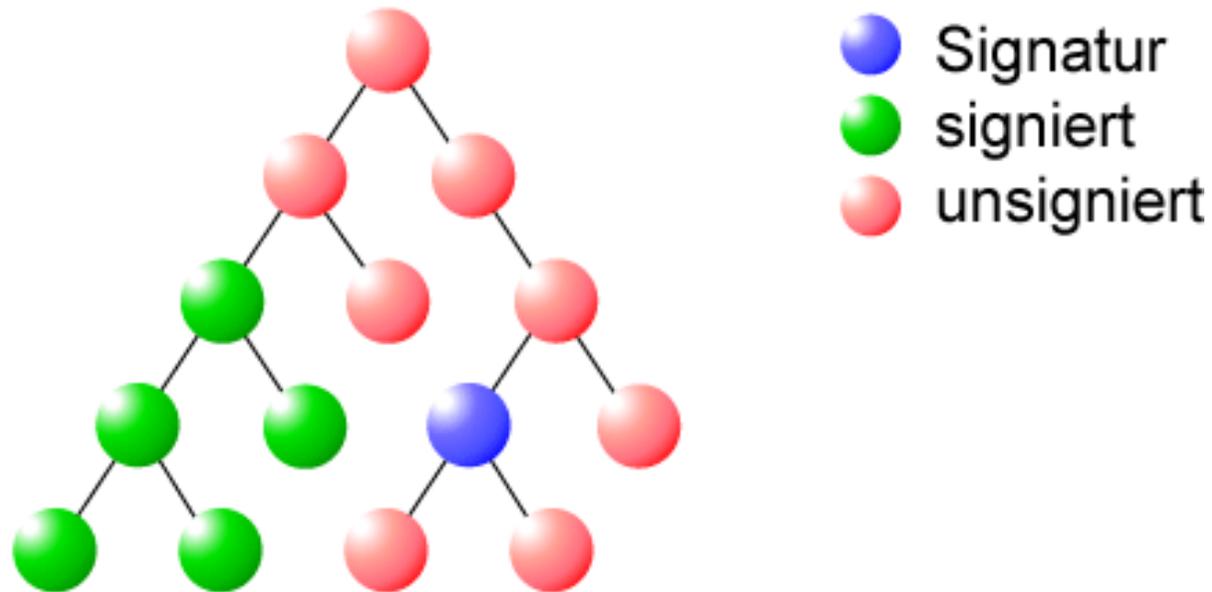
Signaturen – enveloped



- Signatur
- signiert
- unsigned

```
<DocumentData>  
  <Signature>...</Signature>  
</DocumentData>
```

Signaturen – detached



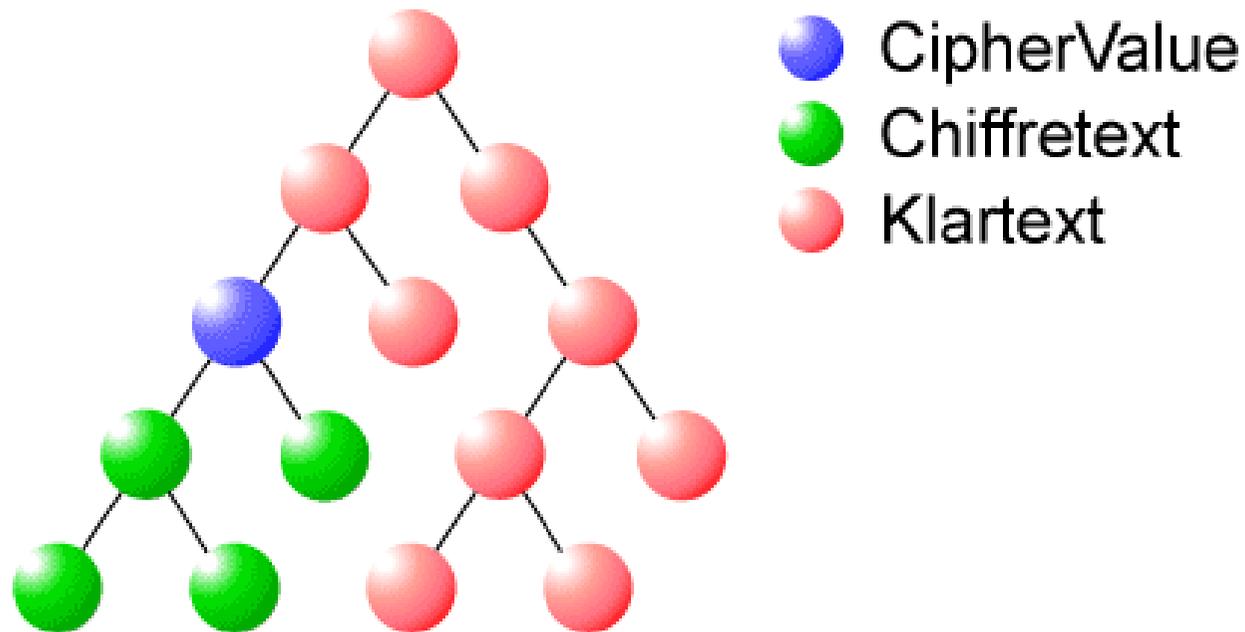
<Signature>...</Signature>

<DocumentData>...</DocumentData>

XML-Sicherheit – Verschlüsselung

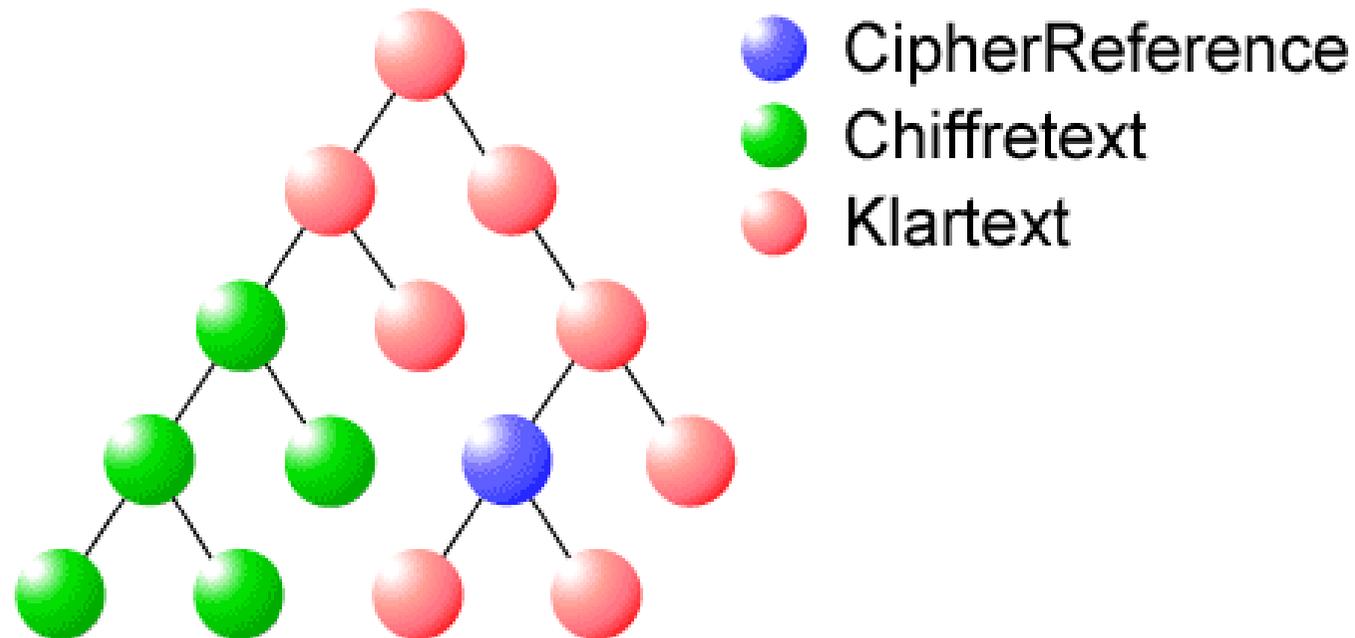
- Vertraulichkeit
- symmetrische & asymmetrische Algorithmen
- Super-Encryption
 - *Mehrfachverschlüsselung*
 - *fein abgestufte Zugriffsrechte*

Verschlüsselung – enveloping



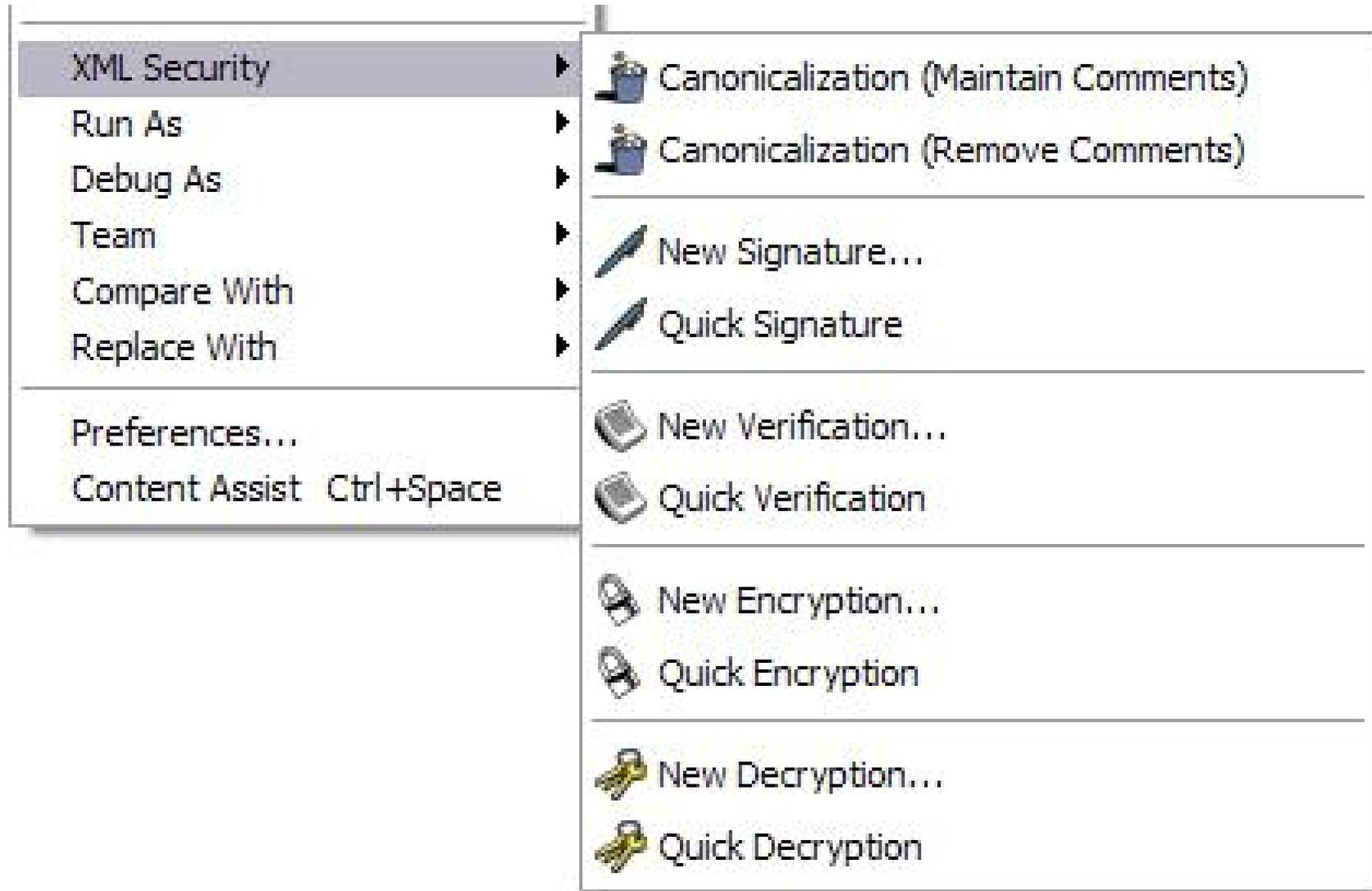
Verschlüsselter Inhalt im *Base-64 encoding*
im Kindelement *CipherValue*

Verschlüsselung – detached



CipherReference verweist mit *URI* Attribut auf die verschlüsselten Daten

XML-Security Plug-In



XML-Security Plug-In

Live-Demo

eLearning mit Eclipse

- ✗ Hohe Verbreitung
- ✗ Flexibel erweiterbar
- ✗ Zahlreiche Plug-Ins (XML)
- ✗ Einfache Installation



- ✗ Komplexität
- ✗ Downloadgröße

JCryptTool

- Eclipse RCP
- Kryptografie-Lernsoftware
 - CryptTool Nachfolger
(Support von Deutscher Bank)
 - Standard-Kryptografie
 - XML-Sicherheit
 - ...

verfügbar im Laufe von 2006

www.cryptool.de

Download & Kontakt

**Download, Tutorials, Forum,
Newsletter, Tipps & Tricks, ...**

unter

www.xml-sicherheit.de

Dominik Schadow
Pasingerstrasse 28
82152 Planegg

info@xml-sicherheit.de
www.xml-sicherheit.de