Eclipse XML-Security Plug-In

Signieren, Verifizieren, Ver- und Entschlüsseln mit Eclipse

XML-Signaturworkshop 2005 Dominik Schadow

Agenda

- Anforderungen und Ziele
- Eclipse Plattform
- Plug-In
  - Überblick
  - Komponenten
- Ausblick
- Fazit

Anforderungen und Ziele

Anwender mit XML-Kenntnissen beherrschen und verstehen nach der Beschäftigung mit dem Plug-In die Grundprinzipien der XML-Sicherheit.

Anforderungen und Ziele

- Lern- und Testsoftware
  - Vorbild CrypTool
  - Erste Schritte
  - Praktische Heranführung
  - Theorie bei Interesse
- Weiterverwendung des gesicherten XML-Dokuments
- Freeware

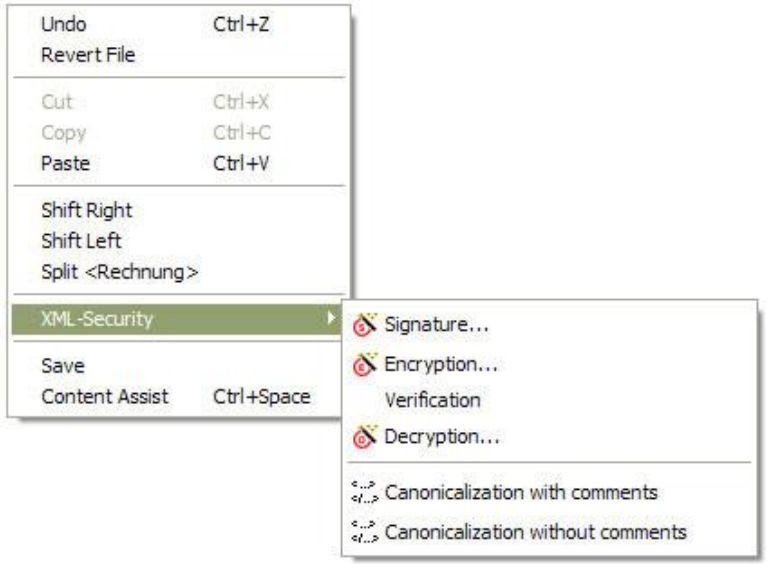
Eclipse Plattform

- Entwicklungsumgebung **und** Rich Client Platform
- Open Source

Vorteile

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

Plug-In: Überblick



Erweiterung von

- Texteditoren
- Package Explorer
- Online-Hilfe

Komponenten

- Kanonisierung
- Signierung/ Verifizierung
- Ver-/ Entschlüsselung

Plug-In: Überblick

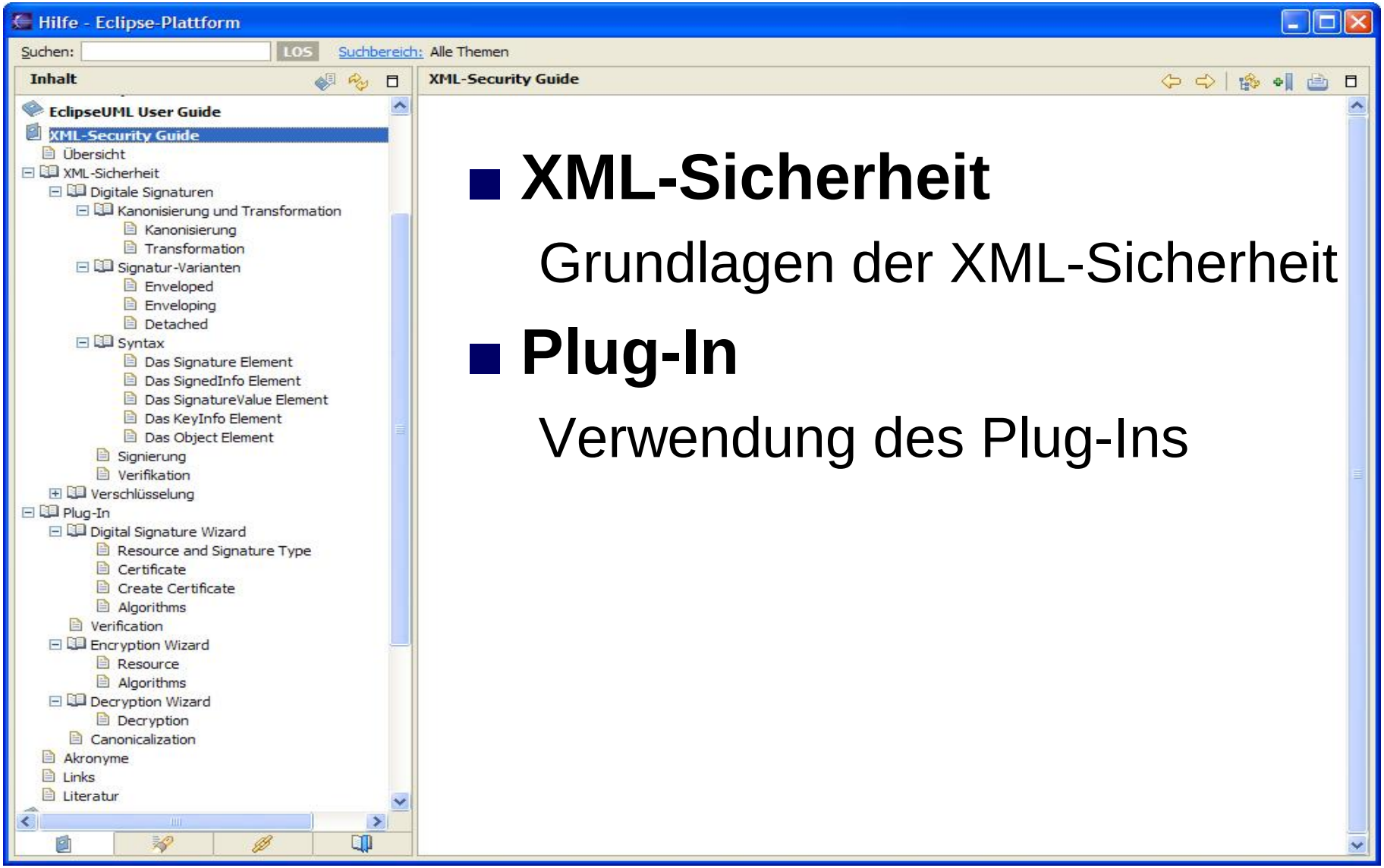
Apache XML-Security API

- ✓ Open Source (Apache Lizenz)
- ✓ Umfangreiche Implementierung
- ✗ Wenig Dokumentation

Alternativen

- ✗ Kommerziell
- ✗ Kein Sourcecode
- ✗ Nicht für Java

Plug-In: Online-Hilfe



- **XML-Sicherheit**

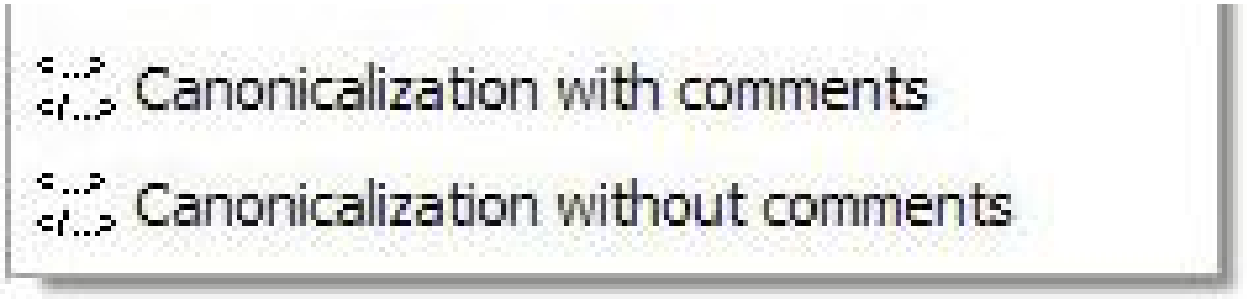
  Grundlagen der XML-Sicherheit

- **Plug-In**

  Verwendung des Plug-Ins

Plug-In: Kanonisieren

- Einfacher Einstieg
- Bedeutung des Begriffs
- Vorgang bei der digitalen Signatur
- Exclusive XML Canonicalization



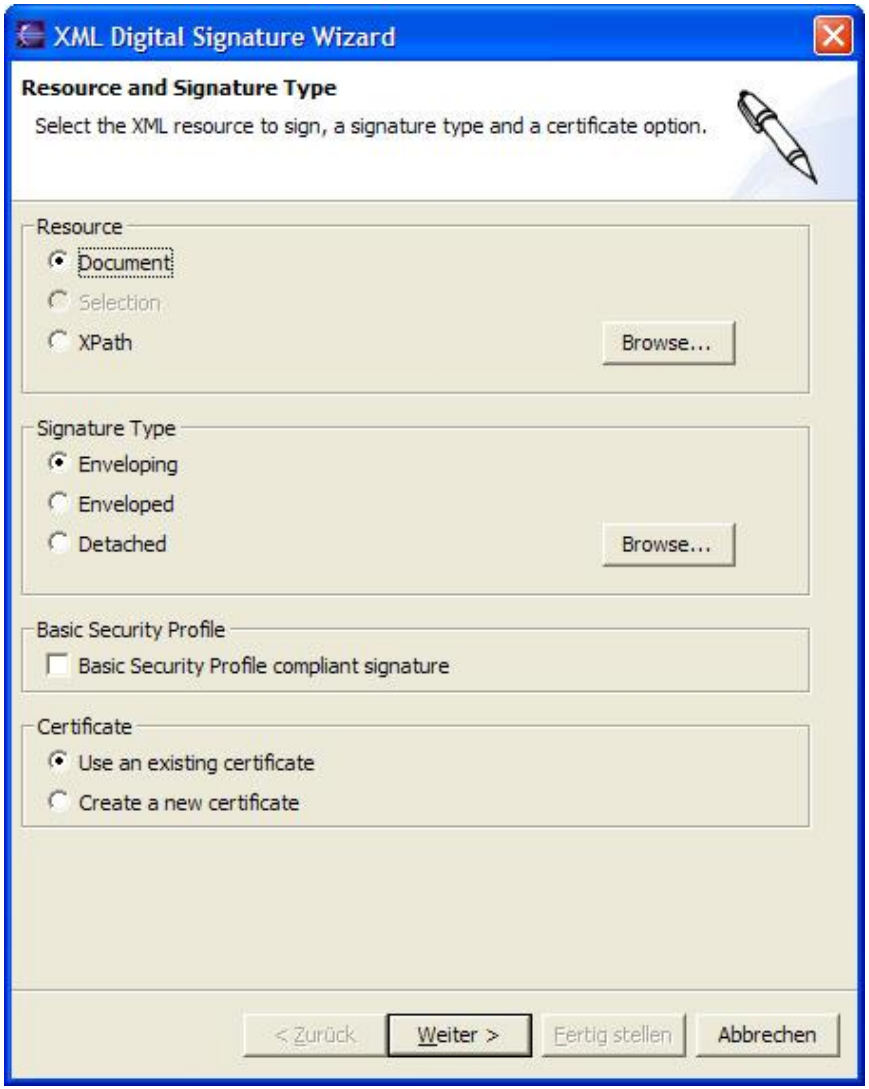
Plug-In: Signieren

Assistent

- Ressource
- Signaturtyp
- Java KeyStore
- Algorithmen

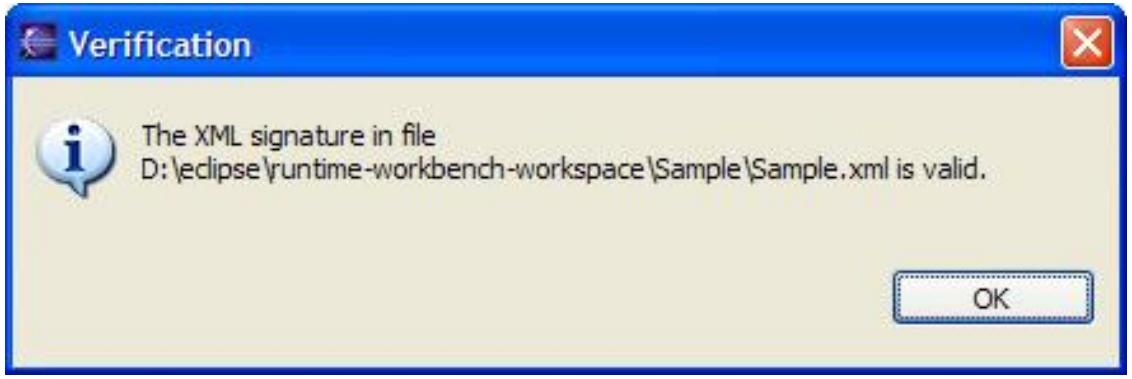
Optional

Basic Security Profile



Plug-In: Verifizieren

- Schnelle Rückmeldung
  - ✔ Gültig
  - ✘ Ungültig
- Benötigt *KeyInfo* Element



Plug-In: Verschlüsseln

Assistent

- Ressource
- Algorithmen
- Schlüsseldatei

Optional

Basic Security Profile

Plug-In: Entschlüsseln

Assistent

- Schlüsseldatei
- Transportalgorithmus

Ausblick

Geplante Weiterentwicklung

- Farbige Anzeige signierter Fragmente
- Umfangreichere Verifizierungsmöglichkeiten
- Kontexthilfe
- Ausbau der Tutorials
- *Anwenderwünsche*

Fazit

- Einstieg in die XML-Sicherheit
- Praktische Anwendung im Vordergrund
- Theorie über Online-Hilfe
- Kontinuierliche Weiterentwicklung

Website

Plug-In, Hilfe, Tutorials, ...
unter
www.xml-sicherheit.de

Dominik Schadow
Pasinger Straße 28
82152 Planegg

info@xml-sicherheit.de