

Eclipse XML-Security Plug-In

Signieren, Verifizieren, Ver-
und Entschlüsseln mit Eclipse

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

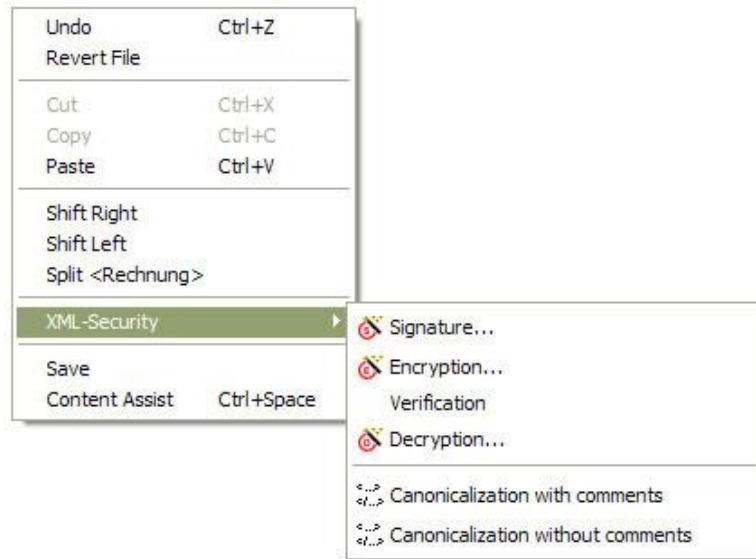


- Entwicklungsumgebung und Rich Client Plattform
- Open Source

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

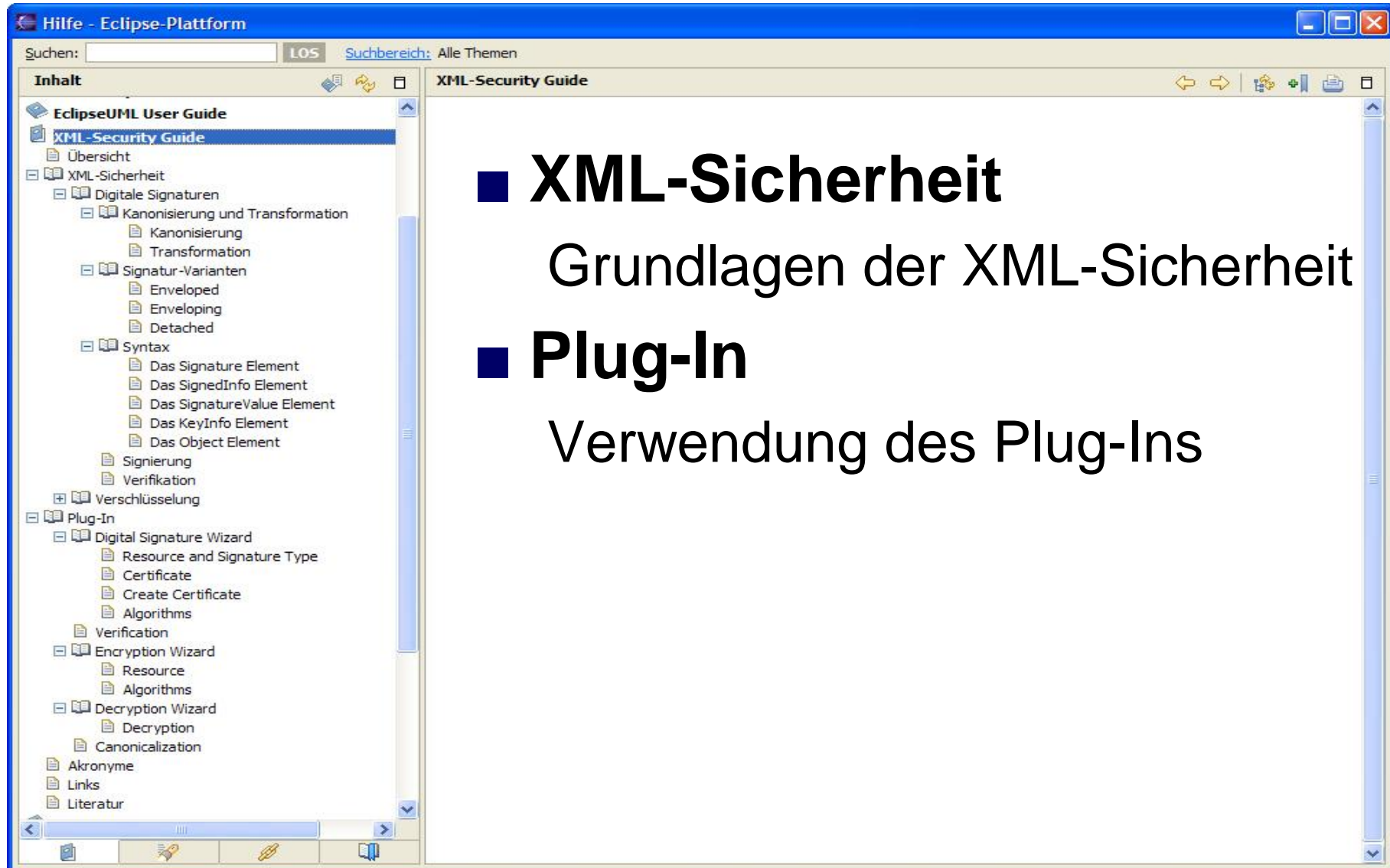
Apache XML-Security API

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

Alternativen

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

Plug-In: Online-Hilfe



The screenshot shows the Eclipse help system window titled "Hilfe - Eclipse-Plattform". The search bar contains "LOS" and "Suchbereich: Alle Themen". The left pane, titled "Inhalt", shows a tree view of the "XML-Security Guide" content. The right pane, titled "XML-Security Guide", displays the following text:

- **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

 Canonicalization with comments

 Canonicalization without comments

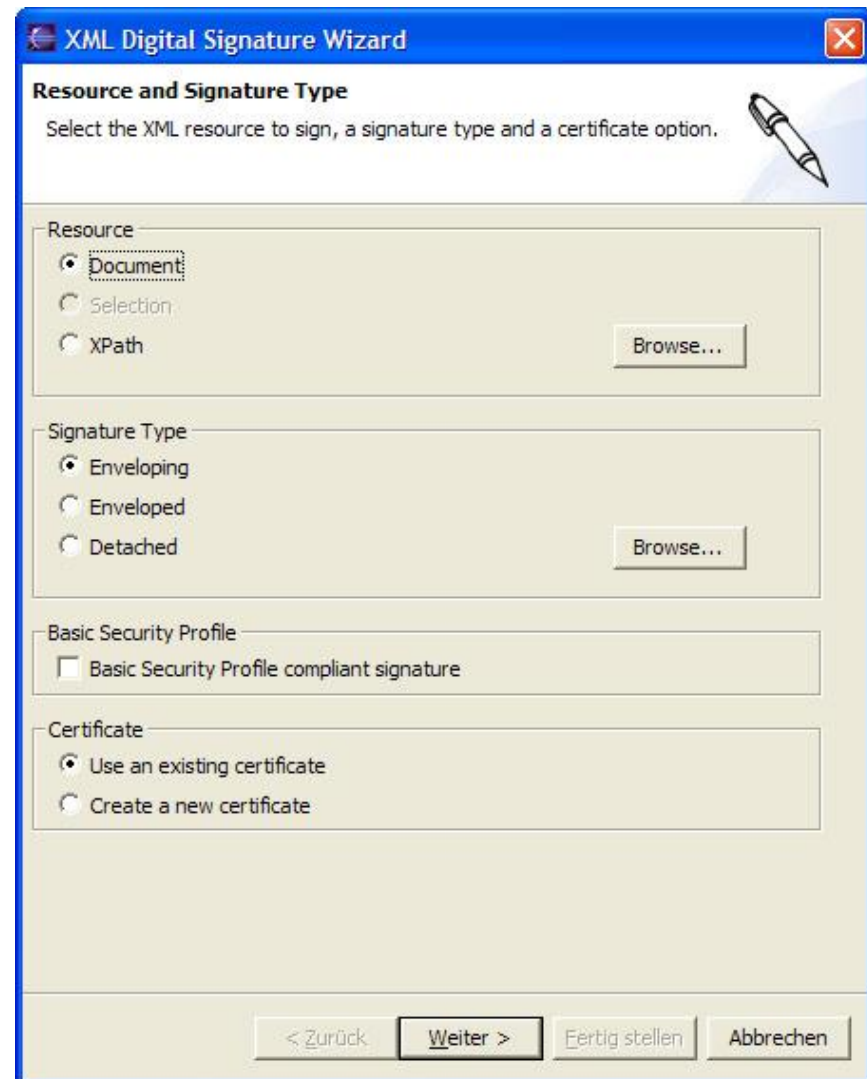
Plug-In: Signieren

Assistent

- Ressource
- Signatortyp
- Java KeyStore
- Algorithmen

Optional

Basic Security Profile



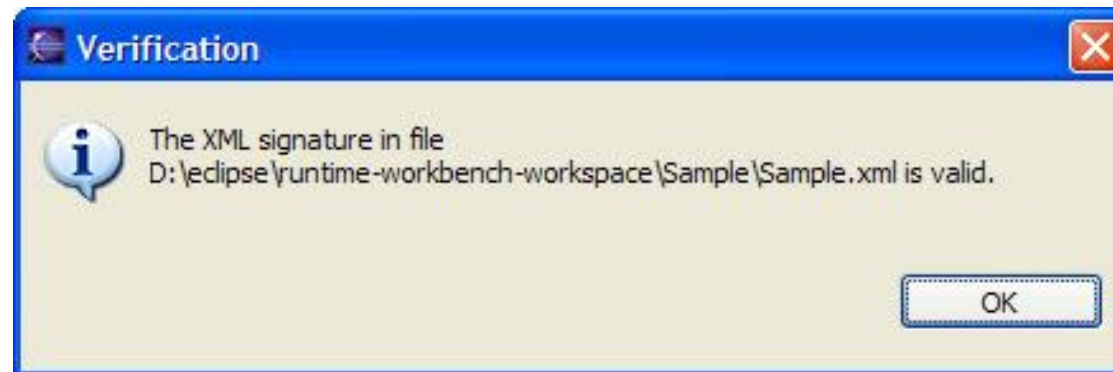
The screenshot shows the 'XML Digital Signature Wizard' dialog box. The title bar reads 'XML Digital Signature Wizard'. The main heading is 'Resource and Signature Type' with a sub-instruction: 'Select the XML resource to sign, a signature type and a certificate option.' There is a pen icon in the top right corner. The dialog is divided into several sections:

- Resource:** Contains three radio buttons: 'Document' (selected), 'Selection', and 'XPath'. A 'Browse...' button is located to the right.
- Signature Type:** Contains three radio buttons: 'Enveloping' (selected), 'Enveloped', and 'Detached'. A 'Browse...' button is located to the right.
- Basic Security Profile:** Contains a checkbox labeled 'Basic Security Profile compliant signature', which is currently unchecked.
- Certificate:** Contains two radio buttons: 'Use an existing certificate' (selected) and 'Create a new certificate'.

At the bottom of the dialog, there are four buttons: '< Zurück', 'Weiter >', 'Fertig stellen', and 'Abbrechen'.

Plug-In: Verifizieren

- Schnelle Rückmeldung
 - ✗ Gültig
 - ✗ Ungültig
- Benötigt *KeyInfo* Element



Plug-In: Verschlüsseln



The screenshot shows the 'XML Encryption Wizard' dialog box. The title bar reads 'XML Encryption Wizard'. The main area is titled 'Algorithms' and contains the instruction 'Please select an encryption algorithm.' with a padlock icon. The dialog is divided into three sections: 'Encryption and Cipher Algorithms' with 'Encryption Algorithm' and 'Key Cipher Algorithm' dropdowns; 'Data Encryption and Key Transport' with 'Data Encryption Key', 'Data Encryption Key Size', 'Key Transport Algorithm', and 'Key Transport Algorithm Size' dropdowns; and 'Key file' with a text input field and a 'Browse...' button. At the bottom, there are four buttons: '< Zurück', 'Weiter >', 'Fertig stellen', and 'Abbrechen'.

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