

Incubating XML Security Tools

Dominik Schadow



Agenda



XML-Security Plug-In started as an e-learning tool

XML Security Tools are part of the Web Tools Platform

A lot more XML data can be secured in the future

Agenda



XML-Security Plug-In started as an e-learning tool

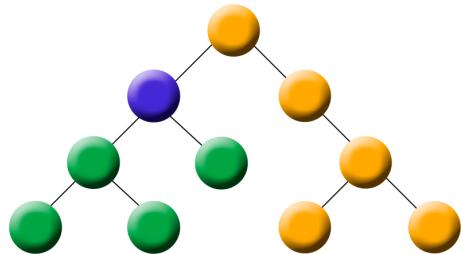
XML Security Tools are part of the Web Tools Platform

A lot more XML data can be secured in the future

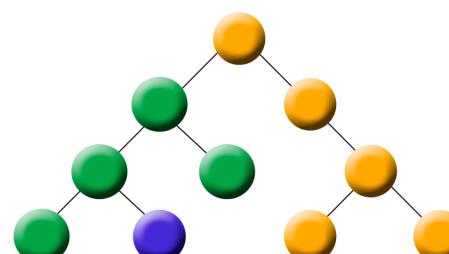
XML Signature signs arbitrary data



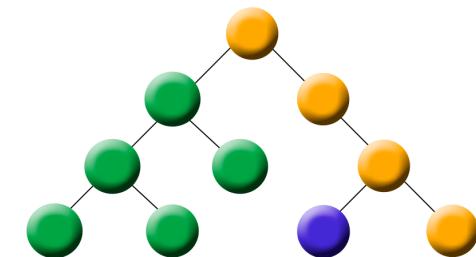
- Three signature types



enveloping



enveloped



detached

- XML structure remains intact

- Can still be parsed
 - Possible to sign only selected element(s)

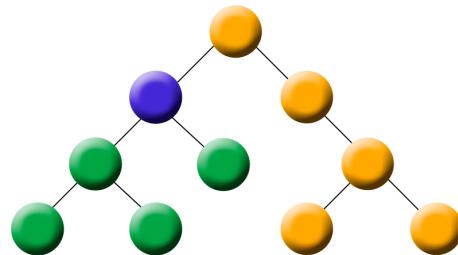
- Requires XML Canonicalization

- Normalizes the XML data

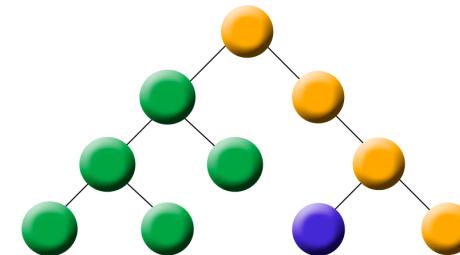
XML Encryption encrypts everything



- Two encryption types



enveloping



detached

- XML structure remains intact
 - Can still be parsed
 - Possible to encrypt only selected element(s)

e-learning plug-in for XML Security



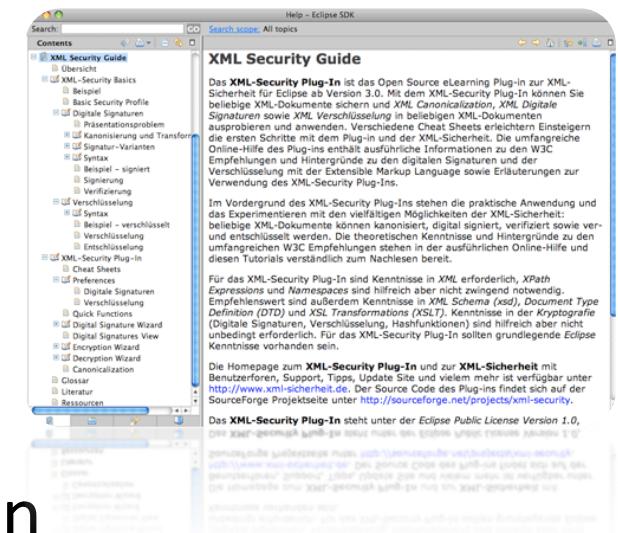
Learning...

- Familiarize users with XML Signature and Encryption
- Extensive German online help
- Cheat sheets for total beginners



...by doing

- XML Canonicalization
- XML Signatures and Verification
- XML Encryption and Decryption



Apache XML Security (Santuario)



- Provides XML Security functionality
 - Version 1.4.2
 - Most complete open source implementation of W3C recommendations
 - Mature
- Minor drawbacks
 - Requires
 - Commons Logging
 - Xalan and Xerces



<http://santuario.apache.org>

Agenda



XML-Security Plug-In started as an e-learning tool

XML Security Tools are part of the Web Tools Platform

A lot more XML data can be secured in the future

Part of the Web Tools Platform incubator

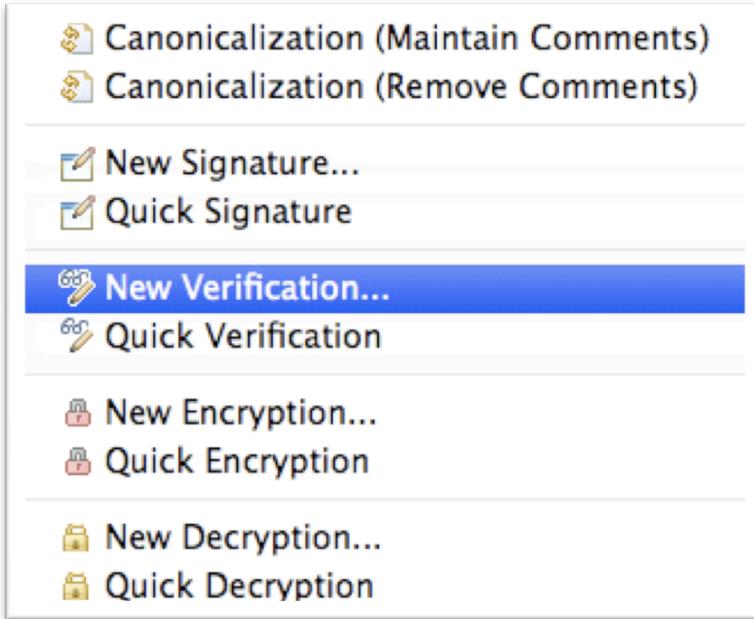


- org.eclipse.wst.xml.security
- org.eclipse.wst.xml.security.core
- org.eclipse.wst.xml.security.doc
- org.eclipse.wst.xml.security.ui



- org.apache.commons.logging (1.0.4)
- org.apache.xalan (2.7.1)
- org.apache.xerces (2.9.0)
- org.apache.xml.security (1.4.2, not yet in Orbit)

It's all about the context



Extends

- (XML) editors
- Package Explorer / Navigator
- Preferences
- Online help / cheat sheets

Provides

- Wizard based signatures, en- and decryption
- View based verification
- Preference based quick signatures, en- and decryption

Signature and Verification



The screenshot shows the Eclipse IDE interface with the XML Signature Wizard open. The wizard is titled "XML Signature" and asks to "Select the resource to sign, the signature type and a key option." The "Resource" section is set to "Document". The "Signature Type" section has "Enveloping" selected. The "Keystore and Key" section has "Use a key from an existing keystore" selected. The "Basic Security Profile" section has a checkbox for "Generate a Basic Security Profile compliant signature" which is unchecked. In the background, there is an "FirstSteps.xml" file open in the editor, showing XML code for an envelope and a certificate. Below the editor, there is a "Design" tab and an "XML Signatures" view showing one valid signature named "myDemoSignature".

Encryption and Decryption



The screenshot shows the Eclipse IDE interface with the XML Security Tools plugin. On the left, there is a code editor window titled "FirstSteps.xml" displaying XML code for encryption. The XML code includes elements like <xenc:EncryptedData>, <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"/>, and <xenc:CipherValue>z7qk613XaWjMSRYlMhK1iyavBHGJraW</xenc:CipherValue>. On the right, a "XML Decryption Wizard" dialog box is open, prompting for decryption information. It has sections for "Keystore" (Name: /Users/dos/XML-Sicherheit/Ecli, Password: *****), "Key" (Name: encrypt, Password: *****), and "Encryption ID" (myDemoEncryption). At the bottom of the dialog are "Cancel" and "Finish" buttons.

FirstSteps.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="myDemoEncryption" Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes192-cbc"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:KeyName>encrypt</ds:KeyName>
    <xenc:EncryptedKey>
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes192"/>
        <xenc:CipherData>
            <xenc:CipherValue>z7qk613XaWjMSRYlMhK1iyavBHGJraW</xenc:CipherValue>
        </xenc:CipherData>
    </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
        <xenc:CipherValue>cvqq08oFdMC6CfUiHty0YEn3m6ewNgqnp2P+CeyUJNCoVy8cS0
xSwRW2916ipI1QNUgSAqBqFzo8MAci90zUghCVH10BKNRBYwBy3PyADBzbJRP69Ww8KxQ
G8zdJFtHASTxfyR2zJMAxFt3dSLBLqS9Nj/1zLG+c+R2036uSryd4u+jHECIismbPdvCsIJ
xViNy7GMSlKh0oUz0WkuGDyIhAHIRU0SaYBF13woZjwTmjCn2dl6tYfMampsdNMK4gZnqaiQ35
FoT+equ4yCCrMhwHGzU5gCyil9FZ5UG/DPDFcxM6d4g4YrhsCeIW9E7Gohl0MswJ3acnkNA41esr
D1RGWMBjvJAkoPhHra01XTxvTWIyLqZgIc/3ZuToiVPS90f6rQtWG6uhI2LNVi1369vopc
eFE30pwIFxiSmbxTVySwobbsEyZ8czYzDqhK7sfoTFvF56oZIWT0YWEEQkoBb5EyI0YhiDFjXF
KuTI6rQTctmxKoH3Z1TPh1jsL7eXF3o6L0Rw7upTyvAwHhLwQ4Dzpwd3F0D01cquKK/0ac88FVY
ijvoouL5Lf3rod0Ur0ro3LFk1jd1Lgepld3xB7Qvq3puweo3blssLFW6TFS5veUerhY8phidpi6F
tSPAHws32+G6J/vQsmAJ0mWRhr/HEvLG8v5yg0HU1FbhN1RFzjaEHwjIIGA3LKxay0zj89xf17
LYP8NLc9CZLpHxejWQp2XEZAsm7yqB0chslxwXfa0Cwqjuzd1gkXAdCay0XODML1wKj9ULg9yf3s
mM/gFXUEGLSa4RZkr/VH152Y//TBc25pQboEJpk11CE+hbmj1xfed9a3jekMXOnYHPbei+k4ThA
N/mQD8t+VTbqJXeMj9dmrt+4sXaTQ3cpRcMCV72pNTs7KSRTAGPCMQHxWWQ0Xtm02mbgkWh4qjWW
gjk2jueJVLU9/uUsx9Ljwy0/xsuEJfH1QXF9LRV+sl+TapGgNy70VxCPltFansw9qmA16+husW
Jg7nGfM0gtAptZEqcNsHfd2Ggmnndns8F6RqbIUsos1FToP3xcX/+rFW&vC1hQrEMgIHj0tgMthC
u+rLi+CSciRvooZVRdCYk4n9Z+PAx022asJ7D7HS/lyccLe9o8vnCBWA+LXDF/Zn6KVymbBnUq6
AVF29VoTYP8zYK6z6/rxsLfh08rmy7oa9KkjPk8iAD1n0ldFARx32e8ob216k10PxbcvBK1BYdcP
wVx3Q6Ni1Q==</xenc:CipherValue>
    </xenc:CipherData>
</xenc:EncryptedData>
```

XML Decryption Wizard

XML Decryption

Provide the information to decrypt the XML data.

Keystore

Name: /Users/dos/XML-Sicherheit/Ecli Open..

Password: *****

Key

Name: encrypt Open..

Password: *****

Encryption ID

myDemoEncryption

Cancel Finish

XML Security Tools in action.

Agenda



XML-Security Plug-In started as an e-learning tool

XML Security Tools are part of the Web Tools Platform

A lot more XML data can be secured in the future

Scheduled tasks and future development



Make Apache XML Security library replaceable
Complete detached encryption functionality



Provide (English) end user help



General refactoring and clean up work

Extending the tooling



Extensions

- Better and tighter integration with other WTP plug-ins



- Web Services Tools
- XML editor
- XPath view



- Depending on community requests

- ...

Extension Points

Building a community



- No milestone release yet
 - Version 0.5 available as committer download
<http://build.eclipse.org/webtools/committers>
- Milestone plan coming soon
 - First 'official' release
 - <http://wiki.eclipse.org/WTP/XMLSecurityTools>
- Graduation

Key messages



XML Security Tools are ready to secure your XML documents.



Integration with other Eclipse (WTP) plug-ins will be extended.



A first milestone release will be available in the near future.

Thank you!

info@xml-sicherheit.de

<http://blog.xml-sicherheit.de>

www.eclipse.org/webtools/incubator

Pictures (except screenshots) from www.everystockphoto.com