XML Signature Verifier

This topic explains how to configure and apply the XML Signature Verifier tool that verifies XML documents for security purposes.

Sections include:

Understanding XML Signature Verifier

The XML Signature standard recommended by the W3C defines a process that allows any data in XML documents to be digitally signed. OASIS specifies how this can be used with SOAP. With XML Signature, Web service users can verify the identity of others involved in a transaction and can be ensured that the data has not been altered since the document was signed.

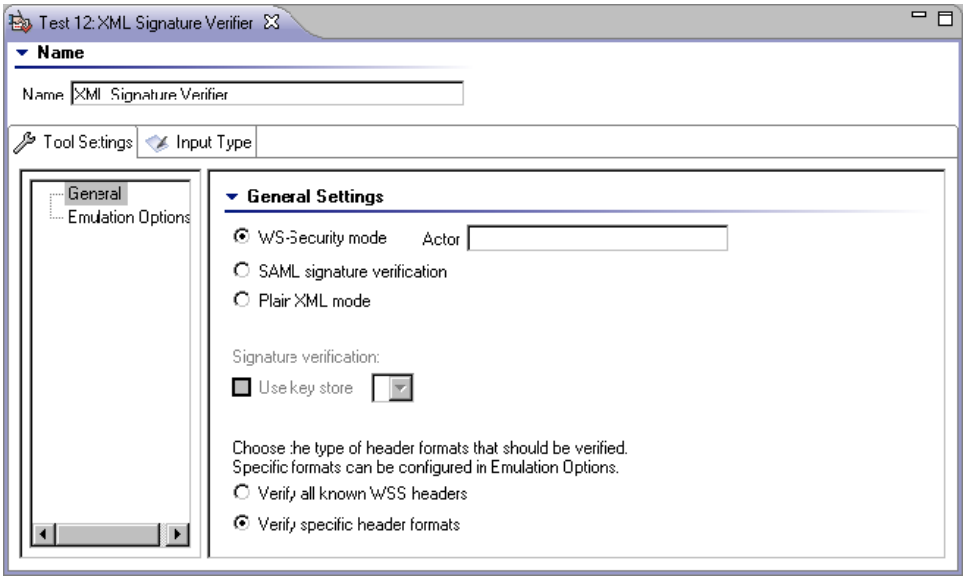
Configuring the XML Signature Verifier Tool

The XML Signature Verifier Tool allows you to verify the authenticity of digital signatures sent with Web service transactions.

Tool Settings

The following options display in the left pane of the Tool Settings tab:

- General
- Emulation Options



General

When selecting General from the left pane of the Tools Settings tab, the following options are available:

- **WS-Security Mode:** Select to use OASIS WS-Security 1.0 to verify SOAP messages.
- **Actor:** Enter a value to specify a SOAP actor.
- **SAML signature verification:** Select to use OpenSAML to perform signature verification. When WS-Security mode is selected, proper verifications will be performed by WSS4J on SAML and/or other tokens.
- **Plain XML Mode:** Select to use plain XML to perform signature verification.
- **Use Key Store:** Select the Key Store used from the **Key Store** drop-down menu. The Key Stores available in this menu are dependent on the Key Stores you added at the test suite level. Depending on whether your service includes the certificate, you may or may not need this option. For more information on adding Key Stores, see Global Key Stores.
- **Verify all known WSS headers:** Enable this option to process all known Web service security header formats.
- **Verify specific header formats:** Enable this option to process specific headers. Enabling this option enables the **Emulation Options**.

Emulation Options

When selecting **Emulation Options** from the left pane of the Tools Settings tab, the following options are available:

Note: The following options are available only if **WS-Security Mode** and **Verify specific header formats** are selected in the **General** tab.

- **Emulate:** Select the application server you are using to automatically configure the emulation options. You can also select the appropriate version number of your application server from the **Version** drop-down menu.
    - To manually configure the emulation options, select **Custom** from the **Emulate** drop-down menu. The following options will be available for you to manually configure:
        - **wsse URI:** Select the namespace URI of the WS-Security specification used.
        - **wsu URI:** Select the utility namespace URI of the WS-Security specification used.
        - **Qualify signed element ID attribute:** Select to qualify signed element ID attribute.
        - **Qualify BinarySecurity Token attributes:** Select to qualify binary security token attributes with the wsse namespace.
        - **Prefix BinarySecurity Token attribute values:** Select to prefix binary security token attributes with the wsse URI.

Input Type Tab

The **Input Type** tab is only available if the XML Signer tool is added as a stand-alone tool and not chained to another tool. The following options are available from the Input Type tab:

- **Text:** Use this option if you want to type or copy the XML document into the UI. Select the appropriate **MIME type**, enter the XML in the text field below the **Text** radio button.
- **File:** Use this option if you want to use an existing file. Click the Browse button to choose a file.
    - Check the **Persist as Relative Path** option if you want the path to this file to be saved as a path that is relative to the current configuration file. Enabling this option makes it easier to share tests across multiple machines. If this option is not enabled, the test suite will save the path to this file as an absolute path.

Usage Notes

You can use the XML Signature Verifier tool as a standalone tool at the test case level by right-clicking the main test suite node and selecting **Add New> Test** from the shortcut menu and then selecting **XML Signature Verifier** from the dialog that opens.

Important: In order to perform security tests using the XML Signature Verifier, XML Signer, or XML Encryption tools, or if using Key Stores, you will need to download and install the Unlimited Strength Java Cryptography Extension. For details, see JCE Prerequisite.

Related Tutorials

The following tutorial lesson demonstrates how to use this tool:

- WS-Security