

**Oracle® WebLogic Server**  
Securing WebLogic Web Services  
10g Release 3 (10.3)

July 2008

---

Oracle WebLogic Server Securing WebLogic Web Services, 10g Release 3 (10.3)

Copyright © 2007, 2008, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# Contents

## 1. Overview of Web Services Security

Overview of Web Services Security .....	1-1
What Type of Security Should You Configure? .....	1-2

## 2. Configuring Message-Level Security

Overview of Message-Level Security .....	2-2
Web Services Security Supported Standards .....	2-3
Main Use Cases of Message-Level Security .....	2-4
Using Policy Files for Message-Level Security Configuration .....	2-5
Using Policy Files With JAX-WS .....	2-5
WS-Policy Namespace .....	2-5
WS-SecurityPolicy Namespace .....	2-6
Version-Independent Policy Supported .....	2-6
Configuring Simple Message-Level Security: Main Steps .....	2-7
Ensuring That WebLogic Server Can Validate the Client's Certificate .....	2-10
Updating the JWS File with @Policy and @Policies Annotations .....	2-11
Using Key Pairs Other Than the Out-Of-The-Box SSL Pair .....	2-15
Updating a Client Application to Invoke a Message-Secured Web Service .....	2-17
Invoking a Message-Secured Web Service From a Client Running in a WebLogic Server Instance. ....	2-20
Creating and Using a Custom Policy File .....	2-21
Configuring the WS-Trust Client. ....	2-22
Supported Token Types. ....	2-23

Configuring WS-Trust Client Properties . . . . .	2-23
Configuring and Using Security Contexts and Derived Keys (WS-SecureConversation) . . . . .	2-29
Specification Backward Compatibility. . . . .	2-30
WS-SecureConversation and Clusters . . . . .	2-31
Updating a Client Application to Negotiate Security Contexts . . . . .	2-31
Associating Policy Files at Runtime Using the Administration Console . . . . .	2-33
Using Security Assertion Markup Language (SAML) Tokens For Identity . . . . .	2-34
Using SAML Tokens for Identity: Main Steps. . . . .	2-35
Specifying the SAML Confirmation Method. . . . .	2-36
Associating a Web Service with a Security Configuration Other Than the Default . . . . .	2-40
Valid Class Names and Token Types for Credential Provider . . . . .	2-41
Using System Properties to Debug Message-Level Security . . . . .	2-42
Using a Client-Side Security Policy File . . . . .	2-42
Associating a Policy File with a Client Application: Main Steps . . . . .	2-43
Updating clientgen to Generate Methods That Load Policy Files . . . . .	2-44
Updating a Client Application To Load Policy Files (JAX-RPC Only) . . . . .	2-44
Using WS-SecurityPolicy 1.2 Policy Files . . . . .	2-47
Transport Level Policies. . . . .	2-48
Protection Assertion Policies . . . . .	2-49
WS-Security 1.0 Username and X509 Token Policies. . . . .	2-50
WS-Security 1.1 Username and X509 Token Policies. . . . .	2-52
WS-SecureConversation Policies. . . . .	2-53
SAML Token Profile Policies . . . . .	2-56
Choosing a Policy . . . . .	2-57
Unsupported WS-SecurityPolicy 1.2 Assertions. . . . .	2-58
Using the Optional Policy Assertion . . . . .	2-60
Configuring Element-Level Security. . . . .	2-61

Define and Use a Custom Element-Level Policy File . . . . .	2-62
Implementation Notes . . . . .	2-65
Smart Policy Selection . . . . .	2-66
Example of Security Policy With Policy Alternatives . . . . .	2-66
Configuring Smart Policy Selection . . . . .	2-69
Multiple Transport Assertions . . . . .	2-72
Example of Adding Security to MTOM Web Service . . . . .	2-73
Files Used by This Example . . . . .	2-73
SecurityMtomService.java . . . . .	2-74
MtomClient.java . . . . .	2-78
configWss.py Script File . . . . .	2-83
Build.xml File . . . . .	2-88
Building and Running the Example . . . . .	2-94
Deployed WSDL for SecurityMtomService . . . . .	2-95
Example of Adding Security to Reliable Messaging Web Service . . . . .	2-103
Overview of Secure and Reliable SOAP Messaging . . . . .	2-103
Overview of the Example . . . . .	2-104
Files Used by This Example . . . . .	2-106
Revised ReliableEchoServiceImpl.java . . . . .	2-107
Revised configWss.py . . . . .	2-108
Revised configWss_Service.py . . . . .	2-109
Building and Running the Example . . . . .	2-111
Proprietary Web Services Security Policy Files (JAX-RPC Only) . . . . .	2-111
Abstract and Concrete Policy Files . . . . .	2-112
Auth.xml . . . . .	2-113
Sign.xml . . . . .	2-114
Encrypt.xml . . . . .	2-116
Wssc-dk.xml . . . . .	2-116

Wssc-sct.xml .....	2-119
--------------------	-------

### 3. Configuring Transport-Level Security

Configuring Transport-Level Security Through Policy .....	3-1
Configuring Transport-Level Security Through Policy: Main Steps .....	3-3
Configuring Transport-Level Security Via UserDataConstraint: Main Steps (JAX-RPC Only) .....	3-4
Configuring Two-Way SSL for a Client Application .....	3-6
Using a Custom SSL Adapter with Reliable Messaging .....	3-7

### 4. Configuring Access Control Security (JAX-RPC Only)

Configuring Access Control Security: Main Steps .....	4-1
Updating the JWS File With the Security-Related Annotations .....	4-4
Updating the JWS File With the @RunAs Annotation .....	4-6
Setting the Username and Password When Creating the Service Object .....	4-7

# Overview of Web Services Security

The following sections describe how to configure security for your Web Service:

- [“Overview of Web Services Security”](#) on page 1-1
- [“What Type of Security Should You Configure?”](#) on page 1-2

## Overview of Web Services Security

To secure your WebLogic Web Service, you configure one or more of three different types of security.

**Table 1-1 Web Services Security**

Security Type	Description
Message-level security	Data in a SOAP message is digitally signed or encrypted. May also include identity tokens for authentication. See <a href="#">Chapter 2, “Configuring Message-Level Security.”</a>
Transport-level security	SSL is used to secure the connection between a client application and the Web Service. See <a href="#">Chapter 3, “Configuring Transport-Level Security.”</a>
Access control security	Specifies which roles are allowed to access Web Services. See <a href="#">Chapter 4, “Configuring Access Control Security (JAX-RPC Only).”</a>

## What Type of Security Should You Configure?

**Message-level security** includes all the security benefits of SSL, but with additional flexibility and features. Message-level security is end-to-end, which means that a SOAP message is secure even when the transmission involves one or more intermediaries. The SOAP message itself is digitally signed and encrypted, rather than just the connection. And finally, you can specify that only individual parts or elements of the message be signed, encrypted, or required. Transport-level security, however, secures only the connection itself. This means that if there is an intermediary between the client and WebLogic Server, such as a router or message queue, the intermediary gets the SOAP message in plain text. When the intermediary sends the message to a second receiver, the second receiver does not know who the original sender was. Additionally, the encryption used by SSL is “all or nothing”: either the entire SOAP message is encrypted or it is not encrypted at all. There is no way to specify that only selected parts of the SOAP message be encrypted. Message-level security can also include identity tokens for authentication.

**Transport-level security** secures the connection between the client application and WebLogic Server with Secure Sockets Layer (SSL). SSL provides secure connections by allowing two applications connecting over a network to authenticate the other's identity and by encrypting the data exchanged between the applications. Authentication allows a server, and optionally a client, to verify the identity of the application on the other end of a network connection. A client certificate (two-way SSL) can be used to authenticate the user.

Encryption makes data transmitted over the network intelligible only to the intended recipient.

Transport-level security includes HTTP BASIC authentication as well as SSL.

**Access control security** answers the question “who can do what?” First you specify the security roles that are allowed to access a Web Service; a *security role* is a privilege granted to users or groups based on specific conditions. Then, when a client application attempts to invoke a Web Service operation, the client authenticates itself to WebLogic Server, and if the client has the authorization, it is allowed to continue with the invocation. Access control security secures only WebLogic Server resources. That is, if you configure *only* access control security, the connection between the client application and WebLogic Server is not secure and the SOAP message is in plain text.



# Configuring Message-Level Security

In this release of WebLogic Server, message-level security features are supported in both the JAX-RPC and JAX-WS stacks.

The following sections describe how to configure security for your Web Service:

- [“Overview of Message-Level Security” on page 2-2](#)
- [“Main Use Cases of Message-Level Security” on page 2-4](#)
- [“Using Policy Files for Message-Level Security Configuration” on page 2-5](#)
- [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#)
- [“Updating a Client Application to Invoke a Message-Secured Web Service” on page 2-17](#)
- [“Creating and Using a Custom Policy File” on page 2-21](#)
- [“Configuring the WS-Trust Client” on page 2-22](#)
- [“Configuring and Using Security Contexts and Derived Keys \(WS-SecureConversation\)” on page 2-29](#)
- [“Associating Policy Files at Runtime Using the Administration Console” on page 2-33](#)
- [“Using Security Assertion Markup Language \(SAML\) Tokens For Identity” on page 2-34](#)
- [“Associating a Web Service with a Security Configuration Other Than the Default” on page 2-40](#)
- [“Valid Class Names and Token Types for Credential Provider” on page 2-41](#)

- [“Using System Properties to Debug Message-Level Security”](#) on page 2-42
- [“Using a Client-Side Security Policy File”](#) on page 2-42
- [“Using WS-SecurityPolicy 1.2 Policy Files”](#) on page 2-47
- [“Choosing a Policy”](#) on page 2-57
- [“Unsupported WS-SecurityPolicy 1.2 Assertions”](#) on page 2-58
- [“Using the Optional Policy Assertion”](#) on page 2-60
- [“Configuring Element-Level Security”](#) on page 2-61
- [“Smart Policy Selection”](#) on page 2-66
- [“Multiple Transport Assertions”](#) on page 2-72
- [“Example of Adding Security to Reliable Messaging Web Service”](#) on page 2-103
- [“Proprietary Web Services Security Policy Files \(JAX-RPC Only\)”](#) on page 2-111

## Overview of Message-Level Security

Message-level security specifies whether the SOAP messages between a client application and the Web Service invoked by the client should be digitally signed or encrypted, or both. It also can specify a shared security context between the Web Service and client in the event that they exchange multiple SOAP messages. You can use message-level security to assure:

- Confidentiality, by encrypting message parts
- Integrity, by digital signatures
- Authentication, by requiring username, X.509, or SAML tokens

See [“Configuring Simple Message-Level Security: Main Steps”](#) on page 2-7 for the basic steps you must perform to configure simple message-level security. This section discusses configuration of the Web Services runtime environment, as well as configuration of message-level security for a particular Web Service and how to code a client application to invoke the service.

You can also configure message-level security for a Web Service at runtime, after a Web Service has been deployed. See [“Associating Policy Files at Runtime Using the Administration Console”](#) on page 2-33 for details.

**Note:** You cannot digitally sign or encrypt a SOAP attachment.

## Web Services Security Supported Standards

**Note:** [Standards Supported by WebLogic Web Services](#) is the definitive source of Web Service standards supported in this release.

WebLogic Web Services implement the following [OASIS Standard 1.1 Web Services Security \(WS-Security 1.1\)](#) specifications, dated February 1, 2006:

- WS-Security 1.0 and 1.1
- Username Token Profile 1.0 and 1.1
- X.509 Token Profile 1.0 and 1.1
- SAML Token Profile 1.0 and 1.1

These specifications provide security token propagation, message integrity, and message confidentiality. These mechanisms can be used independently (such as passing a username token for user authentication) or together (such as digitally signing and encrypting a SOAP message and specifying that a user must use X.509 certificates for authentication).

## Web Services Trust and Secure Conversation

**Note:** WS-Trust and WS-SecureConversation are supported for JAX-RPC only.

WebLogic Web Services implement the Web Services Trust (WS-Trust 1.3) and Web Services Secure Conversation (WS-SecureConversation 1.3) specifications, which together provide secure communication between Web Services and their clients (either other Web Services or standalone Java client applications).

The WS-Trust specification defines extensions that provide a framework for requesting and issuing security tokens, and to broker trust relationships.

The WS-SecureConversation specification defines mechanisms for establishing and sharing security contexts, and deriving keys from security contexts, to enable the exchange of multiple messages. Together, the security context and derived keys potentially increase the overall performance and security of the subsequent exchanges.

## Web Services SecurityPolicy 1.2

The WS-Policy specification defines a framework for allowing Web Services to express their constraints and requirements. Such constraints and requirements are expressed as policy assertions.

WS-SecurityPolicy defines a set of security policy assertions for use with the WS-Policy framework to describe how messages are to be secured in the context of WSS: SOAP Message Security, WS-Trust and WS-SecureConversation.

You configure message-level security for a Web Service by attaching one or more policy files that contain security policy statements, as specified by the WS-SecurityPolicy specification. See [“Using Policy Files for Message-Level Security Configuration” on page 2-5](#) for detailed information about how the Web Services runtime environment uses security policy files.

For information about the elements of the Web Services SecurityPolicy 1.2 that are not supported in this release of WebLogic Server, see [“Unsupported WS-SecurityPolicy 1.2 Assertions” on page 2-58](#).

## Main Use Cases of Message-Level Security

The implementation of the *Web Services Security: SOAP Message Security* specification supports the following use cases:

- Use X.509 certificates to sign and encrypt a SOAP message, starting from the client application that invokes the message-secured Web Service, to the WebLogic Server instance that is hosting the Web Service and back to the client application.
- Specify the SOAP message targets that are signed, encrypted, or required: the body, specific SOAP headers, or specific elements.
- Include a token (username, SAML, or X.509) in the SOAP message for authentication.
- Specify that a Web Service and its client (either another Web Service or a standalone application) establish and share a security context when exchanging multiple messages using WS-SecureConversation (WSSC).
- Derive keys for *each* key usage in a secure context, once the context has been established and is being shared between a Web Service and its client. This means that a particular SOAP message uses two derived keys, one for signing and another for encrypting, and each SOAP message uses a different pair of derived keys from other SOAP messages. Because each SOAP message uses its own pair of derived keys, the message exchange between the client and Web Service is extremely secure.

# Using Policy Files for Message-Level Security Configuration

You specify the details of message-level security for a WebLogic Web Service with one or more security policy files. The WS-SecurityPolicy specification provides a general purpose model and XML syntax to describe and communicate the security policies of a Web Service.

**Note:** Previous releases of WebLogic Server, released before the formulation of the WS-SecurityPolicy specification, used security policy files written under the WS-Policy specification, using a proprietary schema for security policy.

This release of WebLogic Server supports either security policy files that conform to the WS-SecurityPolicy 1.2 specification or the Web Services security policy schema first included in WebLogic Server 9, but not both in the same Web Service. The formats are mutually incompatible.

For information about the packaged WS-SecurityPolicy 1.2 security policy files, see [“Using WS-SecurityPolicy 1.2 Policy Files” on page 2-47](#).

The security policy files used for message-level security are XML files that describe whether and how the SOAP messages resulting from an invoke of an operation should be digitally signed or encrypted. They can also specify that a client application authenticate itself using a username, SAML, or X.509 token.

You use the `@Policy` and `@Policies` JWS annotations in your JWS file to associate policy files with your Web Service. You can associate any number of policy files with a Web Service, although it is up to you to ensure that the assertions do not contradict each other. You can specify a policy file at both the class- and method level of your JWS file.

## Using Policy Files With JAX-WS

For maximum portability, Oracle recommends that you use WS-Policy 1.2 and OASIS WS-SecurityPolicy 1.2 with JAX-WS.

## WS-Policy Namespace

WebLogic Server supports WS-Policy 1.2 with the following namespace:

`http://schemas.xmlsoap.org/ws/2004/09/policy`

**Note:** WebLogic Server also now supports WS-Policy 1.5 (now a W3C standard) with the following namespace:

`http://www.w3.org/ns/ws-policy`

## WS-SecurityPolicy Namespace

In this release, the following OASIS WS-SX TC Web Services SecurityPolicy namespace is now supported:

`http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702`

In addition to this new version of the namespace, WebLogic Server continues to support the following Web Services SecurityPolicy namespace:

`http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512`

In most of the cases, the policy assertions are identical for either namespaces, with the following exceptions.

- Trust10 and Trust13 assertion. Both Trust10 and Trust13 assertions are supported in this release.
- SC10SecurityContextToken and SC13SecurityContextToken, as described in [“Specification Backward Compatibility” on page 2-30](#).
- Derived Key using different WSSC versions (200502, 1.3).

## Version-Independent Policy Supported

This version of WebLogic Server supports version-independent policy. You can combine protocol-specific policies such as WS-SecurityPolicy and WS-ReliableMessaging policy that are based on different versions of the WS-Policy specification. At runtime, the merged policy file then contains two or more different namespaces.

There are three versions of WS-SecurityPolicy in this release of WebLogic Server:

- (1) WS-SecurityPolicy 1.2 OASIS standard.
- (2) WS-SecurityPolicy 1.2, as included in WebLogic Server 10.0.
- (3) Proprietary format WebLogic Server 9.x-style policies (deprecated).

You can mix and match any version of WS-Policy with (1), (2), or a combination of (1) and (2). However, you cannot mix and match (3) with (1) or (2) and with different versions of WS-Policy.

The version match possibilities are shown in [Table 2-1](#).

**Table 2-1 Version-Independent Matrix**

	WS-Policy 1.5	WS-Policy 1.2	WS-Policy 1.5 AND WS-Policy 1.2
WS-SecurityPolicy 1.2 OASIS standard	Y	Y	Y
WS-SecurityPolicy 1.2 (WebLogic Server 10.0)	Y	Y	Y
WS-SecurityPolicy 1.2 OASIS standard AND WS-SecurityPolicy 1.2 (WebLogic Server 10.0)	Y	Y	Y
WebLogic Server 9.x-style	Y	Y	N
WebLogic Server 9.x-style AND WS-SecurityPolicy 1.2 OASIS standard or WS-SecurityPolicy 1.2 (WebLogic Server 10.0)	N	N	N

If the client program wants to know what version of the policy or security policy is used, use the versioning API to return the namespace and versioning information.

## Configuring Simple Message-Level Security: Main Steps

The following procedure describes how to configure simple message-level security for the Web Services security runtime, a particular WebLogic Web Service, and a client application that invokes an operation of the Web Service. In this document, *simple message-level security* is defined as follows:

- The message-secured Web Service uses the pre-packaged WS-SecurityPolicy files to specify its security requirements, rather than a user-created WS-SecurityPolicy file. See [“Using Policy Files for Message-Level Security Configuration” on page 2-5](#) for a description of these files.

- The Web Service makes its associated security policy files publicly available by attaching them to its deployed WSDL, which is also publicly visible.
- The Web Services runtime uses the out-of-the-box private key and X.509 certificate pairs, store in the default keystores, for its encryption and digital signatures, rather than its own key pairs. These out-of-the-box pairs are also used by the core WebLogic Server security subsystem for SSL and are provided for demonstration and testing purposes. For this reason Oracle highly recommends you use your own keystore and key pair in production. To use key pairs other than out-of-the-box pairs, see [“Using Key Pairs Other Than the Out-Of-The-Box SSL Pair”](#) on page 2-15.

**WARNING:** If you plan to deploy the Web Service to a cluster in which different WebLogic Server instances are running on different computers, you *must* use a keystore and key pair other than the out-of-the-box ones, even for testing purposes. The reason is that the key pairs in the default WebLogic Server keystore, `DemoIdentity.jks`, are not guaranteed to be the same across WebLogic Servers running on different machines.

If you were to use the default keystore, the WSDL of the deployed Web Service would specify the public key from one of these keystores, but the invoke of the service might actually be handled by a server running on a different computer, and in this case the server’s private key would not match the published public key and the invoke would fail. This problem only occurs if you use the default keystore and key pairs in a cluster, and is easily resolved by using your own keystore and key pairs.

- The client invoking the Web Service uses a username token to authenticate itself, rather than an X.509 token.
- The client invoking the Web Service is a stand-alone Java application, rather than a module running in WebLogic Server.

Later sections describe some of the preceding scenarios in more detail, as well as additional Web Services security uses cases that build on the simple message-level security use case.

It is assumed in the following procedure that you have already created a JWS file that implements a WebLogic Web Service and you want to update it so that the SOAP messages are digitally signed and encrypted. It is also assumed that you use Ant build scripts to iteratively develop your Web Service and that you have a working `build.xml` file that you can update with new information. Finally, it is assumed that you have a client application that invokes the non-secured Web Service. If these assumptions are not true, see:

- [Getting Started With WebLogic Web Services Using JAX-WS](#)



- [Getting Started With WebLogic Web Services Using JAX-RPC](#)

To configure simple message-level security for a WebLogic Web Service:

1. Update your JWS file, adding WebLogic-specific `@Policy` and `@Policies` JWS annotations to specify the pre-packaged policy files that are attached to either the entire Web Service or to particular operations.

See [“Updating the JWS File with @Policy and @Policies Annotations”](#) on page 2-11, which describes how to specify *any* policy file.

2. Recompile and redeploy your Web Service as part of the normal iterative development process.

See [Developing WebLogic Web Services](#) in *Getting Started With WebLogic Web Services Using JAX-WS* and [Developing WebLogic Web Services](#) in *Getting Started With WebLogic Web Services Using JAX-RPC*.

3. Create a keystore used by the client application. Oracle recommends that you create one client keystore per application user.

You can use the Cert Gen utility or Sun Microsystem's `keytool` utility to perform this step. For development purposes, the `keytool` utility is the easiest way to get started.

See [Obtaining Private Keys, Digital Signatures, and Trusted Certificate Authorities”](#) in *Securing WebLogic Server*.

4. Create a private key and digital certificate pair, and load it into the client keystore. The same pair will be used to both digitally sign the client's SOAP request and encrypt the SOAP responses from WebLogic Server.

Make sure that the certificate's key usage allows both encryption and digital signatures.

Also see [“Ensuring That WebLogic Server Can Validate the Client's Certificate”](#) on [page 2-10](#) for information about how WebLogic Server ensures that the client's certificate is valid.

**WARNING:** Oracle requires a key length of 1024 bits or larger.

You can use Sun Microsystem's `keytool` utility to perform this step.

See [Obtaining Private Keys, Digital Signatures, and Trusted Certificate Authorities”](#) in *Securing WebLogic Server*.

5. Using the Administration Console, create users for authentication in your security realm.

See [“Users, Groups, and Security Roles”](#) in *Securing WebLogic Resources Using Roles and Policies*.

6. Update your client application by adding the Java code to invoke the message-secured Web Service.

See [“Using a Client-Side Security Policy File”](#) on page 2-42.

7. Recompile your client application.

See [“Invoking Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-WS* and [“Invoking Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC* for general information.

See the following sections for information about additional Web Service security use cases that build on the basic message-level security use case:

- [“Using Key Pairs Other Than the Out-Of-The-Box SSL Pair”](#) on page 2-15
- [“Creating and Using a Custom Policy File”](#) on page 2-21
- [“Configuring and Using Security Contexts and Derived Keys \(WS-SecureConversation\)”](#) on page 2-29
- [“Associating Policy Files at Runtime Using the Administration Console”](#) on page 2-33
- [“Using Security Assertion Markup Language \(SAML\) Tokens For Identity”](#) on page 2-34
- [“Invoking a Message-Secured Web Service From a Client Running in a WebLogic Server Instance”](#) on page 2-20
- [“Associating a Web Service with a Security Configuration Other Than the Default”](#) on page 2-40

See [“Using System Properties to Debug Message-Level Security”](#) on page 2-42 for information on debugging problems with your message-secured Web Service.

## Ensuring That WebLogic Server Can Validate the Client’s Certificate

You must ensure that WebLogic Server is able to validate the X.509 certificate that the client uses to digitally sign its SOAP request, and that WebLogic Server in turn uses to encrypt its SOAP responses to the client. Do one of the following:

- Ensure that the client application obtains a digital certificate that WebLogic Server automatically trusts, because it has been issued by a trusted certificate authority.

- Create a certificate registry which lists all the individual certificates trusted by WebLogic Server, and then ensure that the client uses one of these registered certificates.

For more information, see [“SSL Certificate Validation”](#) in *Securing WebLogic Server*.

## Updating the JWS File with @Policy and @Policies Annotations

Use the @Policy and @Policies annotations in your JWS file to specify that the Web Service has one or more policy files attached to it. You can use these annotations at either the class or method level.

See [“Loading a Policy From the CLASSPATH”](#) on page 2-15 for an additional policy option.

The @Policies annotation simply groups two or more @Policy annotations together. Use the @Policies annotation if you want to attach two or more policy files to the class or method. If you want to attach just one policy file, you can use @Policy on its own.

The @Policy annotation specifies a single policy file, where it is located, whether the policy applies to the request or response SOAP message (or both), and whether to attach the policy file to the public WSDL of the service.

**WARNING:** As is true for all JWS annotations, the @Policy annotation cannot be overridden at runtime, which means that the policy file you specify at buildtime using the annotation will always be associated with the Web Service. This means, for example, that although you can view the associated policy file at runtime using the Administration Console, you cannot delete (unassociate) it. You can, however, associate additional policy files, as described in [“Associating Policy Files at Runtime Using the Administration Console”](#) on page 2-33.

Use the uri attribute to specify the location of the policy file, as described below:

- To specify one of the pre-packaged security policy files that are installed with WebLogic Server, use the policy: prefix and the name of one of the policy files, as shown in the following example:

```
@Policy(uri="policy:Wssp1.2-2007-Https-BasicAuth.xml")
```

If you use the pre-packaged policy files, you do not have to create one yourself or package it in an accessible location. For this reason, Oracle recommends that you use the pre-packaged policy files whenever you can.

See [“Using Policy Files for Message-Level Security Configuration”](#) on page 2-5 for information on the various types of message-level security provided by the pre-packaged policy files.

- To specify a user-created policy file, specify the path (relative to the location of the JWS file) along with its name, as shown in the following example:

```
@Policy(uri=" ../policies/MyPolicy.xml" )
```

In the example, the `MyPolicy.xml` file is located in the `policies` sibling directory of the one that contains the JWS file.

- You can also specify a policy file that is located in a shared J2EE library; this method is useful if you want to share the file amongst multiple Web Services packaged in different J2EE archives.

**Note:** In this case, it is assumed that the policy file is in the `META-INF/policies` or `WEB-INF/policies` directory of the shared J2EE library. Be sure, when you package the library, that you put the policy file in this directory.

To specify a policy file in a shared J2EE library, use the `policy` prefix and then the name of the policy file, as shown in the following example:

```
@Policy(uri="policy:MySharedPolicy.xml" )
```

See [“Creating Shared J2EE Libraries and Optional Packages”](#) in *Developing Applications With WebLogic Server* for information on creating shared libraries and setting up your environment so the Web Service can find the shared policy files.

You can also set the following attributes of the `@Policy` annotation:

- `direction`—Specifies whether the policy file should be applied to the request (inbound) SOAP message, the response (outbound) SOAP message, or both. The default value if you do not specify this attribute is both. The `direction` attribute accepts the following values:
  - `Policy.Direction.both`
  - `Policy.Direction.inbound`
  - `Policy.Direction.outbound`
- `attachToWsd1`—Specifies whether the policy file should be attached to the WSDL file that describes the public contract of the Web Service. The default value of this attribute is `false`.

The following example shows how to use the `@Policy` and `@Policies` JWS annotations, with the relevant sections shown in bold:

**Listing 2-1 Using @Policy and @Policies Annotations**

---

```

package wsspl2.wss10;

import weblogic.jws.WLHttpTransport;
import weblogic.jws.Policy;
import weblogic.jws.Policies;

import javax.jws.WebService;
import javax.jws.WebMethod;
import javax.jws.Oneway;

/**
 * This Web Service demonstrates how to use WS-SecurityPolicy 1.2
 * to enable message-level security specified in WS-Security 1.0.
 *
 * The service authenticates the client with a username token.
 * Both the request and response messages are signed and encrypted with X509
 * certificates.
 */
@WebService(name="Simple", targetNamespace="http://example.org")
@WLHttpTransport(contextPath="/wsspl2/wss10",
    serviceUri="UsernameTokenPlainX509SignAndEncrypt")
@Policy(uri="policy:Wsspl.2-2007-Wss1.0-UsernameToken-Plain-X509-Basic256.
xml")
public class UsernameTokenPlainX509SignAndEncrypt {

    @WebMethod
    @Policies({
        @Policy(uri="policy:Wsspl.2-2007-SignBody.xml"),
        @Policy(uri="policy:Wsspl.2-2007-EncryptBody.xml")})
    public String echo(String s) {

        return s;
    }

    @WebMethod

```

## Configuring Message-Level Security

```
@Policies({
    @Policy(uri="policy:Wsspl.2-2007-SignBody.xml"),
    @Policy(uri="policy:Wsspl.2-2007-Sign-Wsa-Headers.xml")})
public String echoWithWsa(String s) {
    return s;
}

@WebMethod
@Policy(uri="policy:Wsspl.2-2007-SignBody.xml",
direction=Policy.Direction.inbound)
@Oneway
public void echoOneway(String s) {
    System.out.println("s = " + s);
}

@WebMethod
@Policies({
    @Policy(uri="policy:Wsspl.2-2007-Wss1.0-X509-Basic256.xml",
direction=Policy.Direction.inbound),
    @Policy(uri="policy:Wsspl.2-2007-SignBody.xml",
direction=Policy.Direction.inbound)
})
@Oneway
public void echoOnewayX509(String s) {
    System.out.println("X509SignEncrypt.echoOneway: " + s);
}
}
```

The following section of the example is the binding policy for the Web Service, specifying the policy:

```
@WebService(name="Simple", targetNamespace="http://example.org")
@WLHttpTransport(contextPath="/wsspl2/wss10",
    serviceUri="UsernameTokenPlainX509SignAndEncrypt")
@Policy(uri="policy:Wsspl.2-2007-Wss1.0-UsernameToken-Plain-X509-Basic256.xml")
```

In the example, security policy files are attached to the Web Service at the method level. The specified policy files are those pre-packaged with WebLogic Server, which means that the developers do not need to create their own files or package them in the corresponding archive.

The `Wsspl.2-2007-SignBody.xml` policy file specifies that the body and WebLogic system headers of both the request and response SOAP message be digitally signed. The `Wsspl.2-2007-EncryptBody.xml` policy file specifies that the body of both the request and response SOAP messages be encrypted.

## Loading a Policy From the CLASSPATH

This release of WebLogic Server includes a 'load policy as resource from CLASSPATH' feature. This feature allows you to copy a policy file to the root directory of your Web application and then reference it directly by its name (for example, `mypolicy.xml`) from an `@POLICY` annotation in your JWS file.

To enable this feature, start WebLogic Server with

```
-Dweblogic.wsee.policy.LoadFromClassPathEnabled=true.
```

If you enable this feature, be aware of the following caveat: If you were to then move the policy file to the `WEB-INF/policies` directory, the same `'mypolicy.xml'` reference in the `@POLICY` annotation will no longer work. You would need to add the policy prefix to the `@POLICY` annotation; for example, `'policy:mypolicy.xml'`.

## Using Key Pairs Other Than the Out-Of-The-Box SSL Pair

In the simple message-level configuration procedure, documented in [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#), it is assumed that the Web Services runtime uses the private key and X.509 certificate pair that is provided out-of-the-box with WebLogic Server; this same key pair is also used by the core security subsystem for SSL and is provided mostly for demonstration and testing purposes. In production environments, the Web Services runtime typically uses its own two private key and digital certificate pairs, one for signing and one for encrypting SOAP messages.

The following procedure describes the additional steps you must take to enable this use case.

1. Obtain two private key and digital certificate pairs to be used by the Web Services runtime. One of the pairs is used for digitally signing the SOAP message and the other for encrypting it.

Although not required, Oracle recommends that you obtain two pairs that will be used *only* by WebLogic Web Services. You must also ensure that both of the certificate's key usage matches what you are configuring them to do. For example, if you are specifying that a

certificate be used for encryption, be sure that the certificate's key usage is specified as for encryption or is undefined. Otherwise, the Web Services security runtime will reject the certificate.

**WARNING:** Oracle requires that the key length be 1024 bits or larger.

You can use the Cert Gen utility or Sun Microsystem's `keytool` utility to perform this step. For development purposes, the `keytool` utility is the easiest way to get started.

See [Obtaining Private Keys, Digital Signatures, and Trusted Certificate Authorities](#) in *Securing WebLogic Server*.

2. Create, if one does not currently exist, a custom identity keystore for WebLogic Server and load the private key and digital certificate pairs you obtained in the preceding step into the identity keystore.

If you have already configured WebLogic Server for SSL, then you have already created an identity keystore which you can also use in this step.

You can use WebLogic's `ImportPrivateKey` utility and Sun Microsystem's `keytool` utility to perform this step. For development purposes, the `keytool` utility is the easiest way to get started.

See [Creating a Keystore and Loading Private Keys and Trusted Certificate Authorities Into the Keystore](#) in *Securing WebLogic Server*.

3. Using the Administration Console, configure WebLogic Server to locate the keystore you created in the preceding step. If you are using a keystore that has already been configured for WebLogic Server, you do not need to perform this step.

See [Configuring Keystores for Production](#) in *Securing WebLogic Server*.

4. Using the Administration Console, create the default Web Service security configuration, which must be named `default_wss`. The default Web Service security configuration is used by *all* Web Services in the domain unless they have been explicitly programmed to use a different configuration.

See [Create a Web Service security configuration](#) in the Administration Console Online Help.

5. Update the default Web Services security configuration you created in the preceding step to use one of the private key and digital certificate pairs for digitally signing SOAP messages.

See [Specify the key pair used to sign SOAP messages](#) in Administration Console Online Help. In the procedure, when you create the properties used to identify the keystore and key pair, enter the exact value for the Name of each property (such as



`IntegrityKeyStore`, `IntegrityKeyStorePassword`, and so on), but enter the value that identifies your own previously-created keystore and key pair in the Value fields.

6. Similarly, update the default Web Services security configuration you created in a preceding step to use the second private key and digital certificate pair for encrypting SOAP messages.

See [“Specify the key pair used to encrypt SOAP messages”](#) in Administration Console Online Help. In the procedure, when you create the properties used to identify the keystore and key pair, enter the exact value for the Name of each property (such as `ConfidentialityKeyStore`, `ConfidentialityKeyStorePassword`, and so on), but enter the value that identifies your own previously-created keystore and key pair in the Value fields.

## Updating a Client Application to Invoke a Message-Secured Web Service

When you update your Java code to invoke a message-secured Web Service, you must load a private key and digital certificate pair from the client’s keystore and pass this information, along with a username and password for user authentication if so required by the security policy, to the secure WebLogic Web Service being invoked.

If the security policy file of the Web Service specifies that the SOAP request must be encrypted, then the Web Services client runtime automatically gets the server’s certificate from the policy file that is attached to the WSDL of the service, and uses it for the encryption. If, however, the policy file is not attached to the WSDL, or the entire WSDL itself is not available, then the client application must use a client-side copy of the policy file; for details, see [“Using a Client-Side Security Policy File”](#) on page 2-42.

[Listing 2-2](#) shows a Java client application that invokes the message-secured WebLogic Web Service described by the JWS file in [“Updating the JWS File With the Security-Related Annotations”](#) on page 4-4. The client application takes five arguments:

- Client username for client authentication
- Client password for client authentication
- Client private key file
- Client digital certificate
- WSDL of the deployed Web Service

## Configuring Message-Level Security

The security-specific code in the sample client application is shown in bold (and described after the example):

### Listing 2-2 Client Application Invoking a Message-Secured Web Service

---

```
package examples.webservices.security_jws.client;

import weblogic.security.SSL.TrustManager;

import weblogic.xml.crypto.wss.provider.CredentialProvider;
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.wsee.security.bst.ClientBSTCredentialProvider;
import weblogic.wsee.security.unt.ClientUNTCredentialProvider;

import javax.xml.rpc.Stub;
import java.util.List;
import java.util.ArrayList;

import java.security.cert.X509Certificate;

/**
 * Copyright © 1996, 2008, Oracle and/or its affiliates.
 * All rights reserved.
 */
public class SecureHelloWorldClient {
    public static void main(String[] args) throws Throwable {

        //username or password for the UsernameToken
        String username = args[0];
        String password = args[1];

        //client private key file
        String keyFile = args[2];

        //client certificate
        String clientCertFile = args[3];

        String wsdl = args[4];

        SecureHelloWorldService service = new SecureHelloWorldService_Impl(wsdl +
        "?WSDL" );

        SecureHelloWorldPortType port = service.getSecureHelloWorldServicePort();

        //create credential provider and set it to the Stub
        List credProviders = new ArrayList();

        //client side BinarySecurityToken credential provider -- x509
        CredentialProvider cp = new ClientBSTCredentialProvider(clientCertFile,
```

```

keyFile);
    credProviders.add(cp);

    //client side UsernameToken credential provider
    cp = new ClientUNTCredentialProvider(username, password);
    credProviders.add(cp);

    Stub stub = (Stub)port;
    stub._setProperty(WSSecurityContext.CREDENTIAL_PROVIDER_LIST,
credProviders);

    stub._setProperty(WSSecurityContext.TRUST_MANAGER,
        new TrustManager(){
            public boolean certificateCallback(X509Certificate[] chain, int
validateErr){
                return true;
            }
        } );

    String response = port.sayHello("World");
    System.out.println("response = " + response);
}
}

```

The main points to note about the preceding code are:

- Import the WebLogic security TrustManager API:

```
import weblogic.security.SSL.TrustManager;
```

- Import the following WebLogic Web Services security APIs to create the needed client-side credential providers, as specified by the policy files that are associated with the Web Service:

```
import weblogic.xml.crypto.wss.provider.CredentialProvider;
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.wsee.security.bst.ClientBSTCredentialProvider;
import weblogic.wsee.security.unt.ClientUNTCredentialProvider;
```

- Use the ClientBSTCredentialProvider WebLogic API to create a binary security token credential provider from the client's certificate and private key:

```
CredentialProvider cp =
    new ClientBSTCredentialProvider(clientCertFile, keyFile);
```

- Use the ClientUNTCredentialProvider WebLogic API to create a username token from the client's username and password, which are also known by WebLogic Server:

```
cp = new ClientUNTCredentialProvider(username, password);
```

- Use the `WSSecurityContext.CREDENTIAL_PROVIDER_LIST` property to pass a `List` object that contains the binary security and username tokens to the JAX-RPC Stub:

```
stub._setProperty(WSSecurityContext.CREDENTIAL_PROVIDER_LIST,
credProviders)
```

For JAX-WS, you might code this as follows:

```
import javax.xml.ws.BindingProvider;
:
Map<String, Object> rc = ((BindingProvider) port).getRequestContext();
rc.put(WSSecurityContext.CREDENTIAL_PROVIDER_LIST, credProviders);
```

- Use the `weblogic.security.SSL.TrustManager` WebLogic security API to verify that the certificate used to encrypt the SOAP request is valid. The Web Services client runtime gets this certificate from the deployed WSDL of the Web Service, which in production situations is not automatically trusted, so the client application must ensure that it is okay before it uses it to encrypt the SOAP request:

```
stub._setProperty(WSSecurityContext.TRUST_MANAGER,
    new TrustManager(){
        public boolean certificateCallback(X509Certificate[] chain, int
validateErr){
            return true;
        }
    } );
```

This example shows the `TrustManager` API on the client side. The Web Service application must implement proper verification code to ensure security.

## Invoking a Message-Secured Web Service From a Client Running in a WebLogic Server Instance

In the simple Web Services configuration procedure, described in [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#), it is assumed that a *stand-alone* client application invokes the message-secured Web Service. Sometimes, however, the client is itself running in a WebLogic Server instance, as part of an EJB, a servlet, or another Web Service. In this case, you can use the core WebLogic Server security framework to configure the credential providers and trust manager so that your EJB, servlet, or JWS code contains only the simple invoke of the secured operation and no other security-related API usage.

The following procedure describes the high level steps you must perform to make use of the core WebLogic Server security framework in this use case.

1. In your EJB, servlet, or JWS code, invoke the Web Service operation as if it were *not* configured for message-level security. Specifically, do not create a `CredentialProvider` object that contains username or X.509 tokens, and do not use the `TrustManager` core security API to validate the certificate from the WebLogic Server hosting the secure Web Service. The reason you should not use these APIs in your client code is that the Web Services runtime will perform this work for you.
2. Using the Administration Console, configure the required credential mapping providers of the core security of the WebLogic Server instance that hosts your client application. The list of required credential mapper providers depends on the policy file that is attached to the Web Service you are invoking. Typically, you must configure the credential mapper providers for both username/password and X.509 certificates. See [“Valid Class Names and Token Types for Credential Provider” on page 2-41](#) for the possible values.

**Note:** WebLogic Server includes a credential mapping provider for username/passwords and X.509. However, only username/password is configured by default.

3. Using the Administration Console, create the actual credential mappings in the credential mapping providers you configured in the preceding step. You must map the user principal, associated with the client running in the server, to the credentials that are valid for the Web Service you are invoking. See [“Configuring a WebLogic Credential Mapping Provider” in \*Securing WebLogic Server\*](#).
4. Using the Administration Console, configure the core WebLogic Server security framework to trust the X.509 certificate of the invoked Web Service. See [“Configuring the Credential Lookup and Validation Framework” in \*Securing WebLogic Server\*](#).

You are not required to configure the core WebLogic Server security framework, as described in this procedure, if your client application does not want to use the out-of-the-box credential provider and trust manager. Rather, you can override all of this configuration by using the same APIs in your EJB, servlet, and JWS code as in the stand-alone Java code described in [“Using a Client-Side Security Policy File” on page 2-42](#). However, using the core security framework standardizes the WebLogic Server configuration and simplifies the Java code of the client application that invokes the Web Service.

## Creating and Using a Custom Policy File

Although WebLogic Server includes a number of pre-packaged Web Services security policy files that typically satisfy the security needs of most programmers, you can also create and use your own `WS-SecurityPolicy` file if you need additional configuration. See [“Using Policy Files for Message-Level Security Configuration” on page 2-5](#) for general information about security policy files and how they are used for message-level security configuration.

**Note:** Use of element-level security always requires one or more custom policy files to specify the particular element path and name to be secured.

When you create a custom policy file, you can separate out the three main security categories (authentication, encryption, and signing) into three separate policy files, as do the pre-packaged files, or create a single policy file that contains all three categories. You can also create a custom policy file that changes just one category (such as authentication) and use the pre-packaged files for the other categories (`Wsspl.2-2007-SignBody.xml`, `Wsspl.2-SignBody.xml` and `Wsspl.2-2007-EncryptBody`, `Wsspl.2-EncryptBody`). In other words, you can mix and match the number and content of the policy files that you associate with a Web Service. In this case, however, you must always ensure yourself that the multiple files do not contradict each other.

Your custom policy file needs to comply with the standard format and assertions defined in WS-SecurityPolicy 1.2. Note, however, that this release of WebLogic Server does not completely implement WS-SecurityPolicy 1.2. For more information, see [“Unsupported WS-SecurityPolicy 1.2 Assertions” on page 2-58](#). The root element of your WS-SecurityPolicy file must be `<Policy>` and include the following namespace declarations:

```
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
```

or

```
http://www.w3.org/ns/ws-policy
```

```
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512"
```

or

```
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702
```

You can also use the pre-packaged WS-SecurityPolicy files as templates to create your own custom files. See [“Using WS-SecurityPolicy 1.2 Policy Files” on page 2-47](#).

## Configuring the WS-Trust Client

**Note:** In this release, WS-Trust is supported under JAX-RPC only.

WebLogic Server implements a WS-Trust client that retrieves security tokens from a Security Token Service (STS) for use in Web Services Security. This WS-Trust client is used internally by the client side WebLogic Server Web Service runtime.

You can configure the WS-Trust client as follows:

- Through properties on the Web Service client stub for a standalone Web Service client.
- Through MBean properties for a Web Service client running on the server.

In prior releases of WebLogic Server, the WS-Trust client could use only security tokens from an STS that was co-located with a Web Service and hosted by WebLogic Server. However, in this release, the STS need only be accessible to the WS-Trust client; it does not need to be co-located.

The WS-Trust client in prior releases supported only WS-SecureConversation tokens. It now also supports SAML tokens.

## Supported Token Types

Web Service Secure Conversation Language (WS-SecureConversation) and SAML tokens are supported. The tokens have the following namespace and URI:

- For WS-SecureConversation 1.3:

```
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512
```

```
http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/sct
```

- For WS-SecureConversation 1.2:

```
http://schemas.xmlsoap.org/ws/2005/02/sc
```

```
http://schemas.xmlsoap.org/ws/2005/02/sc/sct
```

- For SAML 1.1:

```
urn:oasis:names:tc:SAML:1.0:assertion
```

```
Supported confirmation method is sender-vouches.
```

- For SAML 2.0:

```
urn:oasis:names:tc:SAML:2.0:assertion
```

```
Supported confirmation methods are sender-vouches and bearer.
```

## Configuring WS-Trust Client Properties

You set some of the configuration properties specifically for the WS-Trust client; others are determined through configuration information generally present for a Web Service client. For example, the type of token retrieved is determined by the security policy of the Web Service that the Web Service client is invoking.

The properties that you can explicitly set and the token type they apply to are as follows. Subsequent sections show how to set these properties.

- STS URI (WS-SecureConversation and SAML)
- STS security policy (SAML)
- STS SOAP version (SAML)
- STS WS-Trust version (SAML)

### Obtaining the URI of the Secure Token Service

There are three sources from which the WS-Trust client can obtain the URI of the secure token service (STS). The order of precedence is as follows:

- The URI for the STS, as contained in the `sp:Issuer/wsa:Address` element of the token assertion in the Web Service's security policy.
- A configured STS URI.
- The co-located STS URI. This is the default if there is no other source (WS-SecureConversation only).

### Configuring STS URI: Standalone Client

The following code example demonstrates setting the STS URI on a client stub. The example assumes that the location of the STS URI is already known to the client.

```
String wsdl = "http://myserver/wsscsecuredservice?wsdl";
WsscSecuredService service = new WsscSecuredService_Impl(wsdl);
WsscSecured port = service.getWsscSecuredSoapPort();
Stub stub = (Stub) port;
String sts = "https://stsserver/standaloneSTS/wssc13/STS";
stub._setProperty("weblogic.wsee.wst.sts_endpoint_uri", sts);
```

### Configuring STS URI Using WLST: Client Running On Server Side

[Listing 2-3](#) demonstrates using the WebLogic Scripting Tool (WLST) to create a credential provider for the WS-Trust client and then configuring the STS URI, as indicated by bold text.

The provider class name can be one of the following:

- `weblogic.wsee.security.wssc.v200502.sct.ClientSCCredentialProvider`
- `weblogic.wsee.security.wssc.v13.sct.ClientSCCredentialProvider`
- `weblogic.wsee.security.saml.SAMLTrustCredentialProvider`



**Listing 2-3 Configuring STS URI Using WLST**

---

```

userName = sys.argv[1]
passWord = sys.argv[2]
host = sys.argv[3]+":"+sys.argv[4]
sslhost = sys.argv[3]+":"+sys.argv[5]
url="t3://" + host connect(userName, passWord, url)
edit()
startEdit()

defaultWss = cmo.lookupWebserviceSecurity('default_wss')
#Create credential provider for SCT Trust Client
wtm = defaultWss.createWebserviceCredentialProvider('trust_client_sct_cp')
wtm.setClassName('weblogic.wsee.security.wssc.v13.sct.ClientSCCredentialPr
ovider')
wtm.setTokenType('sct_trust')
cpm = wtm.createConfigurationProperty('StsUri')
cpm.setValue("https://" + sslhost + "/standaloneSTS/wssc13/STS")

save()
activate(block="true")
disconnect()
exit()

```

---

**Configuring STS URI Using Console: Client Running On Server Side**

Configuring the STS URI through the WebLogic Server Administration Console allows the decision about which URI to use to be made at runtime, and not during the Web Service development cycle.

Follow these steps to configure the STS URI through the Console:

1. [Create a Web Services security configuration](#), as described in the online help. This creates an empty configuration.
2. Edit the Web Services security configuration to [create a credential provider](#), as described in the online help:
  - On the Create Credential Provider tab, enter the following:
    - A provider name, which is your name for this MBean instance.

- The provider class name, which can be  
`weblogic.wsee.security.wssc.v200502.sct.ClientSCCredentialProvider`  
  
or  
`weblogic.wsee.security.wssc.v13.sct.ClientSCCredentialProvider`  
  
or  
`weblogic.wsee.security.saml.SAMLTrustCredentialProvider`
- The token type, which is a short name to identify the token. For example, `sct` or `saml`.

3. Select Next.
4. Enter the name/value pairs for the STS URI.
5. Select Finish.
6. On the Security Configuration General tab, set the value of the Default Credential Provider STS URI.

The Default Credential Provider STS URL is the default STS endpoint URL for all WS-Trust enabled credential providers of this Web Service security configuration.

### Configuring STS Security Policy: Standalone Client

The following code example demonstrates setting the STS security policy on a client stub, as indicated in bold.

```
String wsdl = "http://myserver/samlsecuredservice?wsdl";  
SamlSecuredService service = new SamlSecuredService_Impl(wsdl);  
SamlSecured port = service.getSamlSecuredSoapPort();  
Stub stub = (Stub) port;  
InputStream policy = loadPolicy();  
stub._setProperty("weblogic.wsee.security.wst_bootstrap_policy", policy);
```

### Configuring STS Security Policy Using WLST: Client Running On Server Side

[Listing 2-4](#) demonstrates using WLST to create a credential provider for the default Web Services security configuration, and then configuring the STS security policy, as indicated by bold text. The value for the `StsPolicy` property must be either a policy included in WebLogic Server (see

[“Using WS-SecurityPolicy 1.2 Policy Files” on page 2-47](#)) or a custom policy file in a J2EE library (see [“Creating and Using a Custom Policy File” on page 2-21](#)).

#### Listing 2-4 Configuring STS Security Policy Using WLST

---

```

userName = sys.argv[1]
passWord = sys.argv[2]
host = sys.argv[3]+":"+sys.argv[4]
sslhost = sys.argv[3]+":"+sys.argv[5]
samlstsurl = sys.argv[6]
url="t3://" + host

print "Connect to the running adminSever"
connect(userName, passWord, url)
edit()
startEdit()

defaultWss = cmo.lookupWebserviceSecurity('default_wss')

#Create credential provider for SAML Trust Client

wtm =
defaultWss.createWebserviceCredentialProvider('trust_client_saml_cp')
wtm.setClassName('weblogic.wsee.security.saml.SAMLTrustCredentialProvider'
)
wtm.setTokenType('saml_trust')
cpm = wtm.createConfigurationProperty('StsUri')
cpm.setValue(samlstsurl)

cpm = wtm.createConfigurationProperty('StsPolicy')
cpm.setValue("Wsspl.2-2007-Https-UsernameToken-Plain")

save()
activate(block="true")
disconnect()
exit()

```

---

## Configuring STS Security Policy: Using the Console

Perform the following steps to configure the STS security policy using the console:

1. [Create a Web Services security configuration](#), as described in the online help. This creates an empty configuration.
2. Edit the Web Services security configuration to [create a credential provider](#), as described in the online help:
  - On the Create Credential Provider tab, enter the following:
    - A provider name, which is your name for this MBean instance.
    - The provider class name, which can be  
`weblogic.wsee.security.wssc.v200502.sct.ClientSCCredentialProvider`  
or  
`weblogic.wsee.security.wssc.v13.sct.ClientSCCredentialProvider`  
or  
`weblogic.wsee.security.saml.SAMLTrustCredentialProvider`
    - The token type, which is a short name to identify the token. For example, `sct` or `saml`.
3. Select Next.
4. Enter the name/value pairs for the STS policy.
5. Select Finish.

## Configuring the STS SOAP Version and WS-Trust Version: Standalone Client

For a SAML STS, you need to configure the WS-Trust version only if it is not the default (WS-Trust 1.3). The supported values for `WSEEConstants.TRUST_VERSION` are as follows:

- <http://docs.oasis-open.org/ws-sx/ws-trust/200512> (WS-Trust 1.3)
- <http://schemas.xmlsoap.org/ws/2005/02/trust>

You also need to configure the SOAP version if it is different from the SOAP version of the target Web Service for which you generated the standalone client. (See [Interface SOAPConstants](#) for

the definitions of the constants.) The supported values for `WSEESecurityConstants.TRUST_SOAP_VERSION` are as follows:

- `javax.xml.soap.SOAPConstants.URI_NS_SOAP_1_1_ENVELOPE` (as per <http://schemas.xmlsoap.org/soap/envelope/>)
- `javax.xml.soap.SOAPConstants.URI_NS_SOAP_1_2_ENVELOPE` (as per <http://www.w3.org/2003/05/soap-envelope>)

[Listing 2-5](#) shows an example of setting the WS-Trust and SOAP versions.

---

#### Listing 2-5 Setting the WS-Trust and SOAP Versions

---

```
// set WS-Trust version
stub._setProperty(WSEESecurityConstants.TRUST_VERSION,
"http://docs.oasis-open.org/ws-sx/ws-trust/200512");

// set SOAP version
stub._setProperty(WSEESecurityConstants.TRUST_SOAP_VERSION,
SOAPConstants.URI_NS_SOAP_1_1_ENVELOPE);
```

---

## Configuring and Using Security Contexts and Derived Keys (WS-SecureConversation)

**Note:** In this release, SecureConversation is supported under JAX-RPC only.

Oracle provides the following pre-packaged WS-SecurityPolicy files to configure security contexts and derived keys:

- WS-SecureConversation 1.2 (2005/2) specification:
  - `Wssp1.2-Wssc200502-Bootstrap-Https.xml`
  - `Wssp1.2-Wssc200502-Bootstrap-Wss1.0.xml`
  - `Wssp1.2-Wssc200502-Bootstrap-Wss1.1.xml`
- WS-SecureConversation 1.3 versions of the WS-SecureConversation 1.2 (2005/2) policy files:

- Wssp1.2-Wssc1.3-Bootstrap-Https.xml
- Wssp1.2-Wssc1.3-Bootstrap-Wss1.0.xml
- Wssp1.2-Wssc1.3-Bootstrap-Wss1.1.xml
- Additional WS-SecureConversation 1.3 policy files:
  - Wssp1.2-Wssc1.3-Bootstrap-Https-BasicAuth.xml
  - Wssp1.2-Wssc1.3-Bootstrap-Https-ClientCertReq.xml

It is recommended that you use the pre-packaged files if you want to configure security contexts, because these security policy files provide most of the required functionality and typical default values. See [“WS-SecureConversation Policies” on page 2-53](#) for more information about these files.

**WARNING:** If you are deploying a Web Service that uses shared security contexts to a cluster, then you are required to also configure cross-cluster session state replication. For details, see [“Failover and Replication in a Cluster”](#) in *Using WebLogic Server Clusters*.

Code or configure your application to use the policy through policy annotations, policy attached to the application’s WSDL, or runtime policy configuration.

## Specification Backward Compatibility

WebLogic Web Services implement the Web Services Trust (WS-Trust 1.3) and Web Services Secure Conversation (WS-SecureConversation 1.3) specifications. Take note of the following differences from the WS-SecureConversation version of 02/2005:

- The Web Services Secure Conversation (WS-SecureConversation 1.3) specification requires a token service to return `wst:RequestSecurityToken` to the initiating party in response to a `wst:RequestSecurityToken`. One or more `wst:RequestSecurityTokenResponse` elements are contained within a single `wst:RequestSecurityTokenResponseCollection`.

This differs from the previous version of the specification, in which `wst:RequestSecurityTokenResponse` was returned by the token service.

The token service can return `wst:RequestSecurityTokenResponse` if the service policy specifies the `SC10SecurityContextToken`, as described in the next bullet item.

- The WS-SecurityPolicy 1.2 Errata document describes the following change to `SecureConversationToken` Assertion:

```
<sp:SC10SecurityContextToken />
```

changes to

```
<sp:SC13SecurityContextToken />
```

sp:SC10SecurityContextToken continues to be supported only when used with the WS-SecureConversation version of 02/2005.

## WS-SecureConversation and Clusters

WS-SecureConversation is pinned to a particular WebLogic Server instance in the cluster. If a SecureConversation request lands in the wrong server, it is automatically rerouted to the correct server. If the server instance hosting the WS-SecureConversation fails, the SecureConversation will not be available until the server instance is brought up again.

## Updating a Client Application to Negotiate Security Contexts

A client application that negotiates security contexts when invoking a Web Service is similar to a standard client application that invokes a message-secured Web Service, as described in [“Using a Client-Side Security Policy File” on page 2-42](#). The only real difference is that you can use the `weblogic.wsee.security.wssc.utils.WSSCClientUtil` API to explicitly cancel the secure context token.

**Note:** WebLogic Server provides the `WSSCClientUtil` API for your convenience only; the Web Services runtime automatically cancels the secure context token when the configured timeout is reached. Use the API only if you want to have more control over when the token is cancelled.

[Listing 2-6](#) shows a simple example of a client application invoking a Web Service that is associated with a pre-packaged security policy file that enables secure conversations; the sections in bold which are relevant to security contexts are discussed after the example:

### Listing 2-6 Client Application Using WS-SecureConversation

---

```
package examples.webservices.wssc.client;
import weblogic.security.SSL.TrustManager;
import weblogic.xml.crypto.wss.provider.CredentialProvider;
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.wsee.security.bst.ClientBSTCredentialProvider;
import weblogic.wsee.security.bst.StubPropertyBSTCredProv;
```

## Configuring Message-Level Security

```
import weblogic.wsee.security.wssc.utils.WSSCClientUtil;
import weblogic.wsee.security.util.CertUtils;

import javax.xml.rpc.Stub;
import java.util.List;
import java.util.ArrayList;
import java.security.cert.X509Certificate;

/**
 * Copyright © 1996, 2008, Oracle and/or its affiliates.
 * All rights reserved.
 */
public class WSSecureConvClient {
    public static void main(String[] args) throws Throwable {

        String clientKeyStore = args[0];
        String clientKeyStorePass = args[1];
        String clientKeyAlias = args[2];
        String clientKeyPass = args[3];
        String serverCert = args[4];
        String wsdl = args[5];

        WSSecureConvService service = new WSSecureConvService_Impl(wsdl);
        WSSecureConvPortType port = service.getWSSecureConvServicePort();

        //create credential provider and set it to the Stub
        List credProviders = new ArrayList();

        //use x509 to secure wssc handshake
        credProviders.add(new ClientBSTCredentialActionProvider(clientKeyStore,
            clientKeyStorePass, clientKeyAlias, clientKeyPass));

        Stub stub = (Stub)port;

        stub._setProperty(WSSecurityContext.CREDENTIAL_PROVIDER_LIST,
            credProviders);
        stub._setProperty(StubPropertyBSTCredProv.SERVER_ENCRYPT_CERT,
            CertUtils.getCertificate(serverCert));

        stub._setProperty(WSSecurityContext.TRUST_MANAGER,
            new TrustManager(){
                public boolean certificateCallback(X509Certificate[] chain, int
                    validateErr){
                    //need to validate if the server cert can be trusted
                    return true;
                }
            }
        );
    }
}
```



```

System.out.println (port.sayHelloWithWSSC("Hello World, once"));
System.out.println (port.sayHelloWithWSSC("Hello World, twice"));
System.out.println (port.sayHelloWithWSSC("Hello World, thrice"));

//cancel SecureContextToken after done with invocation
WSSCClientUtil.terminateWssc(stub);
System.out.println("WSSC terminated!");
}
}

```

The points to notice in the preceding example are:

- Import the WebLogic API used to explicitly terminate the secure context token:

```
import weblogic.wsee.security.wssc.utils.WSSCClientUtil;
```

- Set a property on the JAX-RPC stub which specifies that the client application must encrypt its request to WebLogic Server to cancel the secure context token with WebLogic Server's public key:

```
stub._setProperty(StubPropertyBSTCredProv.SERVER_ENCRYPT_CERT,
CertUtils.getCertificate(serverCert));
```

- Use the `terminateWssc()` method of the `WSSCClientUtil` class to terminate the secure context token:

```
WSSCClientUtil.terminateWssc(stub);
```

## Associating Policy Files at Runtime Using the Administration Console

The simple message-level configuration procedure, documented in [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#), describes how to use the `@Policy` and `@Policies` JWS annotations in the JWS file that implements your Web Service to specify one or more policy files that are associated with your service. This of course implies that you must already know, at the time you program your Web Service, which policy files you want to associate with your Web Service and its operations. This might not always be possible, which is why you can also associate policy files at *runtime*, after the Web Service has been deployed, using the Administration Console.

You can use no `@Policy` or `@Policies` JWS annotations at all in your JWS file and associate policy files only at runtime using the Administration Console, or you can specify some policy files using the annotations and then associate additional ones at runtime. However, once you

associate a policy file using the JWS annotations, you cannot change this association at runtime using the Administration Console.

At runtime, the Administration Console allows you to associate as many policy files as you want with a Web Service and its operations, even if the policy assertions in the files contradict each other or contradict the assertions in policy files associated with the JWS annotations. It is up to you to ensure that multiple associated policy files work together. If any contradictions do exist, WebLogic Server returns a runtime error when a client application invokes the Web Service operation.

To use the Console to associate one or more WS-Policy files to a Web Service, the WS-Policy XML files must be located in either the META-INF/policies or WEB-INF/policies directory of the EJB JAR file (for EJB implemented Web Services) or WAR file (for Java class implemented Web Services), respectively.

See [“Associate a WS-Policy file with a Web Service”](#) in the Administration Console Online Help for detailed instructions on using the Administration Console to associate a policy file at runtime.

## Using Security Assertion Markup Language (SAML) Tokens For Identity

The [SAML Token Profile 1.1](#) is part of the core set of WS-Security standards, and specifies how SAML assertions can be used for Web Services security. WebLogic Server 10.3 supports SAML Token Profile 1.1, including support for SAML 2.0 and SAML 1.1 assertions. SAML Token Profile 1.1 is backwards compatible with SAML Token Profile 1.0.

**Note:** SAML Token Profile 1.1 is supported only through WS-SecurityPolicy.

Previous releases of WebLogic Server, released before the formulation of the WS-SecurityPolicy specification, used security policy files written under the WS-Policy specification, using a proprietary schema for security policy. These earlier security policy files support SAML Token Profile 1.0 and SAML 1.1 only.

In the simple Web Services configuration procedure, described in [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#), it is assumed that users use username tokens to authenticate themselves. Because WebLogic Server implements the [SAML Token Profile 1.1](#) of the Web Services Security specification, users can also use SAML tokens in the SOAP messages to authenticate themselves when invoking a Web Service operation, as described in this section.

Use of SAML tokens works server-to-server. This means that the client application is running inside of a WebLogic Server instance and then invokes a Web Service running in another

WebLogic Server instance using SAML for identity. Because the client application is itself a Web Service, the Web Services security runtime takes care of all the SAML processing.

In addition to this server-to-server usage, you can also use SAML tokens from a standalone client via WS-Trust, as described in [“Configuring the WS-Trust Client” on page 2-22](#).

**Note:** It is assumed in this section that you understand the basics of SAML and how it relates to core security in WebLogic Server. For general information, see [“Security Assertion Markup Language \(SAML\)”](#) in *Understanding WebLogic Security*.

It is also assumed in the following procedure that you have followed the steps in [“Configuring Simple Message-Level Security: Main Steps” on page 2-7](#) and now want to enable the additional use case of using SAML tokens, rather than username tokens, for identity.

## Using SAML Tokens for Identity: Main Steps

1. Make sure that the SAML providers you need are configured and add the appropriate partner entries. This step configures the core WebLogic Server security subsystem. For details, see the following sections in *Securing WebLogic Server*:

- [Configuring a SAML Identity Assertion Provider](#)
- [Configuring a SAML Credential Mapping Provider](#)

**Note:** You will need to configure both SAML 1.1 and SAML 2.0 security providers if you want to enable both versions of SAML for use with the SAML Token Profile.

When configuring SAML 2.0 partner entries, you must use the endpoint URL of the target Web Service as the name of the partner for both [WSSIDPartner](#) and [WSSSPartner](#) entries. Specify the URL as HTTPS if SSL will be used.

2. If you will be using policies that involve signatures related to SAML assertions (for example, SAML Holder-of-Key policies) where a key referenced by the assertion is used to sign the message, or Sender-Vouches policies where the sender’s key is used to sign the message, you need to configure keys and certificates for signing and verification.

**Note:** These keys and certificates are **not** used to create or verify signatures on the assertions themselves. Creating and verifying signatures on assertions is done using keys and certificates configured on the SAML security providers.

If you are using SAML Bearer policies, protection is provided by SSL and the PKI Credential Mapping provider is not needed.

If you are using SAML tokens from a standalone client via WS-TRUST, the tokens are passed in via the Web Service client stub, not via the PKI Credential Mapping provider.

- a. Configure a PKI Credential Mapping provider on the sending side, and populate it with the keys and certificates to be used for signing. `setKeypairCredential` creates a keypair mapping between the `principalName`, `resourceid` and `credential action` and the keystore alias and the corresponding password.

```
pkiCM.setKeypairCredential(  
    type=<remote>, protocol=http,  
    remoteHost=hostname, remotePort=portnumber,  
    path=/ContextPath/ServicePath,  
    username, Boolean('true'), None,  
    alias, passphrase)
```

The first (String) parameter is used to construct a Resource object that represents the endpoint of the target Web Service. The `userName` parameter is the user on whose behalf the signed Web Service message will be generated. The `alias` and `passphrase` parameters are the alias and passphrase used to retrieve the key/certificate from the keystore configured for the PKI Credential Mapping provider. The actual key and certificate should be loaded into the keystore before creating the `KeypairCredential`.

- b. Add the same certificates to the Certificate Registry on the receiving side, so they can be validated by the Web Service security runtime:

```
reg.registerCertificate(certalias, certfile)
```

## Specifying the SAML Confirmation Method

The WS-SecurityPolicy implies, but does not explicitly specify, the confirmation method for SAML assertions. Consider the following general guidelines:

- If the `SamlToken` assertion is inside either `<sp:AsymerticBinding>` or `<sp:SymerticBinding>`, then the Holder of Key confirmation method is used.  
See [Table 2-8](#) for examples of policies that use Holder of Key confirmation.
- If the `SamlToken` assertion is inside `<sp:SignedSupportingTokens>` then the Sender Vouches confirmation method is used.  
See [Table 2-8](#) for examples of policies that use Sender Vouches confirmation.
- If the `SamlToken` assertion is inside `<sp:SupportingTokens>` then the Bearer confirmation method is used. Use transport-level security as described in [“Configuring Transport-Level Security” on page 3-1](#) in this case.

See [Table 2-8](#) for examples of policies that use Bearer confirmation.

## Specifying the SAML Confirmation Method (Proprietary Policy Only)

This section describes how to specify the SAML confirmation method in a policy file that uses the proprietary schema for security policy.

**Note:** SAML V1.1 and V2.0 assertions use `<saml:SubjectConfirmation>` and `<saml2:SubjectConfirmation>` elements, respectively, to specify the confirmation method; the confirmation method is not directly specified in the policy file.

When you configure a Web Service to require SAML tokens for identity, you can specify one of the following confirmation methods:

- `sender-vouches`
- `holder-of-key`

See [SAML Token Profile Support in WebLogic Web Services](#), as well as the [Web Services Security: SAML Token Profile](#) specification itself, for details about these confirmation methods.

1. Use a security policy file that specifies that SAML should be used for identity. The exact syntax depends on the type of confirmation method you want to configure (`sender-vouches`, `holder-of-key`).

### To specify the sender-vouches confirmation method:

- a. Create a `<SecurityToken>` child element of the `<Identity><SupportedTokens>` elements and set the `TokenType` attribute to a value that indicates SAML token usage.
- b. Add a `<Claims><Confirmationmethod>` child element of `<SecurityToken>` and specify `sender-vouches`.

For example:

```
<?xml version="1.0"?>
<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"

  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
  ssecurity-utility-1.0.xsd"
  xmlns:wls="http://www.bea.com/wls90/security/policy/wsee#part"
  >

  <wssp:Identity>
    <wssp:SupportedTokens>
      <wssp:SecurityToken
```

```

TokenType="http://docs.oasis-open.org/wss/2004/01/oasis-2004-01-saml
-token-profile-1.0#SAMLAssertionID">
  <wssp:Claims>

<wssp:ConfirmationMethod>sender-vouches</wssp:ConfirmationMethod>
  </wssp:Claims>
  </wssp:SecurityToken>
  </wssp:SupportedTokens>
  </wssp:Identity>

</wsp:Policy>

```

**To specify the holder-of-key confirmation method:**

- a. Create a <SecurityToken> child element of the <Integrity><SupportedTokens> elements and set the TokenType attribute to a value that indicates SAML token usage.

The reason you put the SAML token in the <Integrity> assertion for the holder-of-key confirmation method is that the Web Service runtime must prove the integrity of the message, which is not required by sender-vouches.

- b. Add a <Claims><Confirmationmethod> child element of <SecurityToken> and specify holder-of-key.

For example:

```

<?xml version="1.0"?>

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"

  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
  ssecurity-utility-1.0.xsd"
  xmlns:wls="http://www.bea.com/wls90/security/policy/wsee#part">

  <wssp:Integrity>
    <wssp:SignatureAlgorithm
      URI="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <wssp:CanonicalizationAlgorithm
      URI="http://www.w3.org/2001/10/xml-exc-c14n#"/>

    <wssp:Target>
      <wssp:DigestAlgorithm
        URI="http://www.w3.org/2000/09/xmldsig#sha1" />
      <wssp:MessageParts
        Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
        wsp:Body()
      </wssp:MessageParts>
    </wssp:Target>

```

```

<wssp:SupportedTokens>
  <wssp:SecurityToken
    IncludeInMessage="true"

TokenType="http://docs.oasis-open.org/wss/2004/01/oasis-2004-01-saml
-token-profile-1.0#SAMLAssertionID">
  <wssp:Claims>

<wssp:ConfirmationMethod>holder-of-key</wssp:ConfirmationMethod>
  </wssp:Claims>
  </wssp:SecurityToken>
</wssp:SupportedTokens>
</wssp:Integrity>

</wsp:Policy>

```

- c. By default, the WebLogic Web Services runtime always validates the X.509 certificate specified in the `<KeyInfo>` assertion of any associated WS-Policy file. To disable this validation when using SAML holder-of-key assertions, you must configure the Web Service security configuration associated with the Web service by setting a property on the SAML token handler. See [“Disable X.509 certificate validation when using SAML holder\\_of\\_key assertions”](#) in Administration Console Online Help for information on how to do this using the Administration Console.

See [“Creating and Using a Custom Policy File”](#) on page 2-21 for additional information about creating your own security policy file. See [“Web Services Security Policy Assertion Reference”](#) in *WebLogic Web Services Reference* for reference information about the assertions.
2. Update the appropriate `@Policy` annotations in the JWS file that implements the Web Service to point to the security policy file from the preceding step. For example, if you want invokes of *all* the operations of a Web Service to SAML for identity, specify the `@Policy` annotation at the class-level.

You can mix and match the policy files that you associate with a Web Service, as long as they do not contradict each other and as long as you do not combine OASIS WS-SecurityPolicy 1.2 files with security policy files written under Oracle’s security policy schema.

For example, you can create a simple `MyAuth.xml` file that contains only the `<Identity>` security assertion to specify use of SAML for identity and then associate it with the Web Service together with the pre-packaged `Wssp1.2-2007-EncryptBody.xml` and `Wssp1.2-2007-SignBody.xml` files. It is, however, up to you to ensure that multiple associated policy files do not contradict each other; if they do, you will either receive a runtime error or the Web Service might not behave as you expect.

3. Recompile and redeploy your Web Service as part of the normal iterative development process.

See “[Developing WebLogic Web Services](#)” in *Getting Started With WebLogic Web Services Using JAX-RPC*.

4. Create a client application that runs in a WebLogic Server instance to invoke the main Web Service using SAML as identity. See “[Invoking a Message-Secured Web Service From a Client Running in a WebLogic Server Instance](#)” on page 2-20 for details.

## Associating a Web Service with a Security Configuration Other Than the Default

Many use cases previously discussed require you to use the Administration Console to create the default Web Service security configuration called `default_wss`. After you create this configuration, it is applied to all Web Services that either do *not* use the `@weblogic.jws.security.WssConfiguration` JWS annotation or specify the annotation with no attribute.

There are some cases, however, in which you might want to associate a Web Service with a security configuration *other* than the default; such use cases include specifying different timestamp values for different services.

To associate a Web Service with a security configuration other than the default:

1. “[Create a Web Service security configuration](#)” in the Administration Console Online Help with a name that is *not* `default_wss`.
2. Update your JWS file, adding the `@WssConfiguration` annotation to specify the name of this security configuration. See “[weblogic.jws.security.WssConfiguration](#)” in the *WebLogic Web Services Reference* for additional information and an example.

**WARNING:** If you are going to package additional Web Services in the same Web application, and these Web Services also use the `@WssConfiguration` annotation, then you must specify the *same* security configuration for each Web Service. See “[weblogic.jws.security.WssConfiguration](#)” in the *WebLogic Web Services Reference* for more details.

3. Recompile and redeploy your Web Service as part of the normal iterative development process.



See “[Invoking Web Services](#)” in *Getting Started With WebLogic Web Services Using JAX-WS* and “[Developing WebLogic Web Services](#)” in *Getting Started With WebLogic Web Services Using JAX-RPC*.

**WARNING:** All Web Services security configurations are required to specify the *same* password digest use. Inconsistent password digest use in different Web Service security configurations will result in a runtime error.

## Valid Class Names and Token Types for Credential Provider

When you create a security configuration, you need to supply the class name of the credential provider for this configuration. The valid class names and token types you can use are as follows:

- `weblogic.wsee.security.bst.ClientBSTCredentialProvider`. The token type is `x509`.
- `weblogic.wsee.security.unt.ClientUNTCredentialProvider`. The token type is `ut`.
- `weblogic.wsee.security.wssc.v13.sct.ClientSCCredentialProvider`. The token type is `sct`.
- `weblogic.wsee.security.wssc.v200502.sct.ClientSCCredentialProvider`. The token type is `sct`.
- `weblogic.wsee.security.saml.SAMLTrustCredentialProvider`. The token type is `saml`.

## Using System Properties to Debug Message-Level Security

The following table lists the system properties you can set to debug problems with your message-secured Web Service.

**Table 2-2 System Properties for Debugging Message-Level Security**

System Property	Data Type	Description
weblogic.xml.crypto.dsig.verbose	Boolean	Prints information about digital signature processing.
weblogic.xml.crypto.encrypt.verbose	Boolean	Prints information about encryption processing.
weblogic.xml.crypto.keyinfo.verbose	Boolean	Prints information about key resolution processing.
weblogic.xml.crypto.wss.verbose	Boolean	Prints information about Web Service security token and token reference processing.

## Using a Client-Side Security Policy File

The section [“Using Policy Files for Message-Level Security Configuration”](#) on page 2-5 describes how a WebLogic Web Service can be associated with one or more security policy files that describe the message-level security of the Web Service. These policy files are XML files that describe how a SOAP message should be digitally signed or encrypted and what sort of user authentication is required from a client that invokes the Web Service. Typically, the policy file associated with a Web Service is attached to its WSDL, which the Web Services client runtime reads to determine whether and how to digitally sign and encrypt the SOAP message request from an operation invoke from the client application.

Sometimes, however, a Web Service might not attach the policy file to its deployed WSDL or the Web Service might be configured to not expose its WSDL at all. In these cases, the Web Services client runtime cannot determine from the service itself the security that must be enabled for the SOAP message request. Rather, it must load a client-side copy of the policy file. This section describes how to update a client application to load a local copy of a policy file.

The client-side policy file is typically exactly the same as the one associated with a deployed Web Service. If the two files are different, and there is a conflict in the security assertions contained in the files, then the invoke of the Web Service operation returns an error.

You can specify that the client-side policy file be associated with the SOAP message request, response, or both. Additionally, you can specify that the policy file be associated with the entire Web Service, or just one of its operations.

## Associating a Policy File with a Client Application: Main Steps

The following procedure describes the high-level steps to associate a security policy file with the client application that invokes a Web Service operation.

It is assumed that you have created the client application that invokes a deployed Web Service, and that you want to update it by associating a client-side policy file. It is also assumed that you have set up an Ant-based development environment and that you have a working `build.xml` file that includes a target for running the `clientgen` Ant task.

See [“Invoking Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-WS* and [“Invoking a Web Service from a Stand-alone Client: Main Steps”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC*.

1. Create the client-side security policy files and save them in a location accessible by the client application. Typically, the security policy files are the same as those configured for the Web Service you are invoking, but because the server-side files are not exposed to the client runtime, the client application must load its own local copies.

See [“Creating and Using a Custom Policy File”](#) on page 2-21 for information about creating security policy files.

2. Update the `build.xml` file that builds your client application by specifying to the `clientgen` Ant task that it should generate additional `getXXXPort()` methods in the JAX-RPC stub, where `XXX` refers to the name of the Web Service. These methods are later used by the client application to load the client-side policy files.

See [“Updating clientgen to Generate Methods That Load Policy Files”](#) on page 2-44.

3. Update your Java client application to load the client-side policy files using the additional `getXXXPort()` methods that the `clientgen` Ant task generates.

See [“Updating a Client Application To Load Policy Files \(JAX-RPC Only\)”](#) on page 2-44.

4. Rebuild your client application by running the relevant task. For example:

```
prompt> ant build-client
```

When you next run the client application, it will load local copies of the policy files that the Web Service client runtime uses to enable security for the SOAP request message.

**Note:** If you have a Web Services operation that already have a security policy (for example, one that was set in the WSDL file that was stored when generating the client from the server policy), then when you use this procedure to programmatically set the client-side security policy, all previously-existing policies will be removed.

## Updating clientgen to Generate Methods That Load Policy Files

For JAX-RPC, set the `generatePolicyMethods` attribute of the `clientgen` Ant task to `true` to specify that the Ant task should generate additional `getXXX()` methods in the implementation of the JAX-RPC `Service` interface for loading client-side copies of policy files when you get a port, as shown in the following example:

```
<clientgen
  wsdl="http://ariel:7001/policy/ClientPolicyService?WSDL"
  destDir="${clientclass-dir}"
  generatePolicyMethods="true"
  packageName="examples.webservices.client_policy.client"/>
```

See [“Updating a Client Application To Load Policy Files \(JAX-RPC Only\)”](#) on page 2-44 for a description of the additional methods that are generated and how to use them in a client application.

For JAX-WS, you use the `weblogic.jws.jaxws.ClientPolicyFeature` class to override the effective policy defined for a service. `weblogic.jws.jaxws.ClientPolicyFeature` extends `javax.xml.ws.WebServiceFeature`.

## Updating a Client Application To Load Policy Files (JAX-RPC Only)

When you set `generatePolicyMethods="true"` for `clientgen`, the Ant task generates additional methods in the implementation of the JAX-RPC `Service` interface that you can use to load policy files, where `xxx` refers to the name of the Web Service.

You can use either an Array or Set of policy files to associate multiple files to a Web Service. If you want to associate just a single policy file, create a single-member Array or Set.

- `getXXXPort(String operationName, java.util.Set<java.io.InputStream> inbound, java.util.Set<java.io.InputStream> outbound)`

Loads two different sets of client-side policy files from `InputStreams` and associates the first set to the SOAP request and the second set to the SOAP response. Applies to a specific operation, as specified by the first parameter.

- `getXXXPort(String operationName, java.io.InputStream[] inbound, java.io.InputStream[] outbound)`

Loads two different arrays of client-side policy files from `InputStreams` and associates the first array to the SOAP request and the second array to the SOAP response. Applies to a specific operation, as specified by the first parameter.

- `getXXXPort(java.util.Set<java.io.InputStream> inbound, java.util.Set<java.io.InputStream> outbound)`

Loads two different sets of client-side policy files from `InputStreams` and associates the first set to the SOAP request and the second set to the SOAP response. Applies to all operations of the Web Service.

- `getXXXPort(java.io.InputStream[] inbound, java.io.InputStream[] outbound)`

Loads two different arrays of client-side policy files from `InputStreams` and associates the first array to the SOAP request and the second array to the SOAP response. Applies to all operations of the Web Service.

Use these methods, rather than the normal `getXXXPort()` method with no parameters, for getting a Web Service port and specifying at the same time that invokes of all, or the specified, operation using that port have an associated policy file or files.

**Note:** The following methods from a previous release of WebLogic Server have been deprecated; if you want to associate a single client-side policy file, specify a single-member Array or Set and use the corresponding method described above.

- `getXXXPort(java.io.InputStream policyInputStream);`

Loads a single client-side policy file from an `InputStream` and applies it to both the SOAP request (inbound) and response (outbound) messages.

- `getXXXPort(java.io.InputStream policyInputStream, boolean inbound, boolean outbound);`

Loads a single client-side policy file from an `InputStream` and applies it to either the SOAP request or response messages, depending on the Boolean value of the second and third parameters.

[Listing 2-7](#) shows an example of using these policy methods in a simple client application; the code in bold is described after the example.

## Listing 2-7 Loading Policies in a Client Application

---

```
package examples.webservices.client_policy.client;

import java.rmi.RemoteException;

import javax.xml.rpc.ServiceException;
import javax.xml.rpc.Stub;

import java.io.FileInputStream;
import java.io.IOException;

/**
 * This is a simple standalone client application that invokes the
 * the <code>sayHello</code> operation of the ClientPolicyService Web service.
 *
 * @author Copyright © 1996, 2008, Oracle and/or its affiliates.
 * All rights reserved.
 */

public class Main {

    public static void main(String[] args)
        throws ServiceException, RemoteException, IOException {

        FileInputStream [] inbound_policy_array = new FileInputStream[2];
        inbound_policy_array[0] = new FileInputStream(args[1]);
        inbound_policy_array[1] = new FileInputStream(args[2]);

        FileInputStream [] outbound_policy_array = new FileInputStream[2];
        outbound_policy_array[0] = new FileInputStream(args[1]);
        outbound_policy_array[1] = new FileInputStream(args[2]);

        ClientPolicyService service = new ClientPolicyService_Impl(args[0] +
"?WSDL");

        // standard way to get the Web Service port
        ClientPolicyPortType normal_port = service.getClientPolicyPort();

        // specify an array of policy files for the request and response
        // of a particular operation
        ClientPolicyPortType array_of_policy_port =
service.getClientPolicyPort("sayHello", inbound_policy_array,
outbound_policy_array);

        try {
            String result = null;
            result = normal_port.sayHello("Hi there!");
            result = array_of_policy_port.sayHello("Hi there!");
            System.out.println( "Got result: " + result );
        }
    }
}
```

```

    } catch (RemoteException e) {
        throw e;
    }
}
}

```

The second and third argument to the client application are the two policy files from which the application makes an array of `FileInputStreams` (`inbound_policy_array` and `outbound_policy_array`). The `normal_port` uses the standard parameterless method for getting a port; the `array_of_policy_port`, however, uses one of the policy methods to specify that an invoke of the `sayHello` operation using the port has multiple policy files (specified with an Array of `FileInputStream`) associated with both the inbound and outbound SOAP request and response:

```

ClientPolicyPortType array_of_policy_port =
service.getClientPolicyPort("sayHello", inbound_policy_array,
outbound_policy_array);

```

## Using WS-SecurityPolicy 1.2 Policy Files

WebLogic Server includes a number of WS-SecurityPolicy files you can use in most Web Services applications. The policy files are located in `BEA_HOME/WL_HOME/server/lib/weblogic.jar`. Within `weblogic.jar`, the policy files are located in `/weblogic/wsee/policy/runtime`.

There are two sets of these policies. In most of the cases, they perform identical functions, but the policy uses different namespace.

The first set is new in this release and has a prefix of “Wssp1.2-2007-”. These security policy files conform to the OASIS WS-SecurityPolicy 1.2 specification and have the following namespace:

```

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
>

```

The second set carries over from WebLogic Server version 10.0 and has the prefix “Wssp1.2-”:

```

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512"
>

```

Oracle recommends that you use the new policy namespace, as those are official namespaces from OASIS standards and they will perform better when interoperating with other vendors. The old policies having the prefix of “Wssp1.2-” are mainly for users who want to interoperate with existing applications that already use this version of the policies.

The following sections describe the available WS-SecurityPolicy 1.2 policy files:

- [“Transport Level Policies” on page 2-48](#)
- [“Protection Assertion Policies” on page 2-49](#)
- [“WS-Security 1.0 Username and X509 Token Policies” on page 2-50](#)
- [“WS-Security 1.1 Username and X509 Token Policies” on page 2-52](#)
- [“WS-SecureConversation Policies” on page 2-53](#)
- [“SAML Token Profile Policies” on page 2-56](#)

In addition, see [“Choosing a Policy” on page 2-57](#) and [“Configuring Smart Policy Selection” on page 2-69](#) for information about how to choose the best security policy approach for your Web Services implementation and for information about WS-SecurityPolicy 1.2 elements that are not supported in this release of WebLogic Server.

## Transport Level Policies

These policies require use of the `https` protocol to access WSDL and invoke Web Services operations:

**Table 2-3 Transport Level Policies**

Policy File	Description
Wssp1.2-2007-Https.xml	One way SSL.
Wssp1.2-2007-Https-BasicAuth.xml	One way SSL with Basic Authentication. A 401 challenge occurs if the Authorization header is not present in the request.
Wssp1.2-2007-Https-ClientCertReq.xml	Two way SSL. The recipient checks for the initiator’s public certificate. Note that the client certificate can be used for authentication.
Wssp1.2-2007-Https-UsernameToken-Digest.xml	One way SSL with digest Username Token.



**Table 2-3 Transport Level Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-2007-Https-UsernameToken-Plain.xml	One way SSL with plain text Username Token.
Wssp1.2-Https.xml	One way SSL.
Wssp1.2-Https-BasicAuth.xml	One way SSL with Basic Authentication. A 401 challenge occurs if the Authorization header is not present in the request.
Wssp1.2-Https-UsernameToken-Digest.xml	One way SSL with digest Username Token.
Wssp1.2-Https-UsernameToken-Plain.xml	One way SSL with plain text Username Token.
Wssp1.2-Https-ClientCertReq.xml	Two way SSL. The recipient checks for the initiator's public certificate. Note that the client certificate can be used for authentication.

## Protection Assertion Policies

Protection assertions are used to identify what is being protected and the level of protection provided. Protection assertion policies cannot be used alone; they should be used only in combination with X.509 Token Policies. For example, you might use `Wssp1.2-2007-Wss1.1-X509-Basic256.xml` together with `Wssp1.2-2007-SignBody.xml`. The following policy files provide for the protection of message parts by signing or encryption:

**Table 2-4 Protection Assertion Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-2007-SignBody.xml	All message body parts are signed.
Wssp1.2-2007-EncryptBody.xml	All message body parts are encrypted.

**Table 2-4 Protection Assertion Policies**

Policy File	Description
Wssp1.2-2007-Sign-Wsa-Headers.xml	WS-Addressing headers are signed.
Wssp1.2-SignBody.xml	All message body parts are signed.
Wssp1.2-EncryptBody.xml	All message body parts are encrypted.
Wssp1.2-Sign-Wsa-Headers.xml	WS-Addressing headers are signed.

## WS-Security 1.0 Username and X509 Token Policies

The following policies support the Username Token or X.509 Token specifications of WS-Security 1.0:

**Table 2-5 WS-Security 1.0 Policies**

Policy File	Description
Wssp1.2-2007-Wss1.0-X509-Basic256.xml	Mutual Authentication with X.509 Certificates. The message is signed and encrypted on both request and response. The algorithm of Basic256 should be used for both sides.
Wssp1.2-2007-Wss1.0-UsernameToken-Digest-X509-Basic256.xml	Username token with digested password is sent in the request for authentication. The encryption method is Basic256.
Wssp1.2-2007-Wss1.0-UsernameToken-Plain-X509-Basic256.xml	Username token with plain text password is sent in the request for authentication, signed with the client's private key and encrypted with server's public key. The client also signs the request body and includes its public certificate, protected by the signature in the message. The server signs the response body with its private key and sends its public certificate in the message. Both request and response messages include signed time stamps. The encryption method is Basic256.

**Table 2-5 WS-Security 1.0 Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-Wss1.0-UsernameToken-Plain-X509-Basic256.xml	Username token with plain text password is sent in the request for authentication, signed with the client's private key and encrypted with server's public key. The client also signs the request body and includes its public certificate, protected by the signature in the message. The server signs the response body with its private key and sends its public certificate in the message. Both request and response messages include signed time stamps. The encryption method is Basic256.
Wssp1.2-Wss1.0-UsernameToken-Plain-X509-TripleDesRsa15.xml	Username token with plain text password is sent in the request for authentication, signed with the client's private key and encrypted with server's public key. The client also signs the request body and includes its public certificate, protected by the signature in the message. The server signs the response body with its private key and sends its public certificate in the message. Both request and response messages include signed time stamps. The encryption method is TripleDes.
Wssp1.2-Wss1.0-UsernameToken-Digest-X509-Basic256.xml	Username token with digested password is sent in the request for authentication. The encryption method is Basic256.
Wssp1.2-Wss1.0-UsernameToken-Digest-X509-TripleDesRsa15.xml	Username token with digested password is sent in the request for authentication. The encryption method is TripleDes.
Wssp1.2-Wss1.0-X509-Basic256.xml	Mutual Authentication with X.509 Certificates. The message is signed and encrypted on both request and response. The algorithm of Basic256 should be used for both sides.
Wssp1.2-Wss1.0-X509-TripleDesRsa15.xml	Mutual Authentication with X.509 Certificates and message is signed and encrypted on both request and response. The algorithm of TripleDes should be used for both sides.
Wssp1.2-Wss1.0-X509-EncryptRequest-SignResponse.xml	This policy is used where only the server has X.509v3 certificates (and public-private key pairs). The request is encrypted and the response is signed.

## WS-Security 1.1 Username and X509 Token Policies

The following policies support the Username Token or X.509 Token specifications of WS-Security 1.1:

**Table 2-6 WS-Security 1.1 Username and X509 Token Policies**

Policy File	Description
Wssp1.2-2007-Wss1.1-X509-Basic256.xml	WSS 1.1 X509 with asymmetric binding.
Wssp1.2-2007-Wss1.1-UsernameToken-Digest-X509-Basic256.xml	WSS 1.1 X509 with asymmetric binding and authentication with digested Username Token.
Wssp1.2-2007-Wss1.1-UsernameToken-Plain-X509-Basic256.xml	WSS 1.1 X509 with asymmetric binding and authentication with plain-text Username Token.
Wssp1.2-2007-Wss1.1-EncryptedKey-X509-SignedEndorsing.xml	WSS 1.1 X509 with symmetric binding and protected by signed endorsing supporting token.
Wssp1.2-2007-Wss1.1-UsernameToken-Digest-EncryptedKey.xml	WSS 1.1 X509 with symmetric binding and authentication with digested Username Token.
Wssp1.2-2007-Wss1.1-UsernameToken-Plain-EncryptedKey.xml	WSS 1.1 X509 with symmetric binding and authentication with plain-text Username Token.
Wssp1.2-2007-Wss1.1-DK-X509-SignedEndorsing.xml	WSS 1.1 X509 with derived key symmetric binding and protected by signed endorsing supporting token.
Wssp1.2-2007-Wss1.1-UsernameToken-Digest-DK.xml	WSS 1.1 X509 with derived key symmetric binding and authentication with digested Username Token.
Wssp1.2-2007-Wss1.1-UsernameToken-Plain-DK.xml	WSS 1.1 X509 with derived key symmetric binding and authentication with plain-text Username Token.

**Table 2-6 WS-Security 1.1 Username and X509 Token Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-Wss1.1-X509-Basic256.xml	This policy is similar to policy Wssp1.2-Wss1.0-X509-Basic256.xml except it uses additional WS-Security 1.1 features, including Signature Confirmation and Thumbprint key reference.
Wssp1.2-Wss1.1-EncryptedKey.xml	This is a symmetric binding policy that uses the WS-Security 1.1 Encrypted Key feature for both signature and encryption. It also uses WS-Security 1.1 features, including Signature Confirmation and Thumbprint key reference.
Wssp1.2-Wss1.1-UsernameToken-DK.xml	WSS 1.1 X509 with derived key symmetric binding and authentication with plain-text Username Token.
Wssp1.2-Wss1.1-EncryptedKey-X509-SignedEndorsing.xml	This policy has all of the features defined in policy Wssp1.2-Wss1.1-EncryptedKey.xml, and in addition it uses sender's key to endorse the message signature. The endorsing key is also signed with the message signature.
Wssp1.2-Wss1.1-DK.xml	This policy has all of features defined in policy Wssp1.2-Wss1.1-EncryptedKey.xml, except that instead of using an encrypted key, the request is signed using DerivedKeyToken1, then encrypted using a DerivedKeyToken2. Response is signed using DerivedKeyToken3, and encrypted using DerivedKeyToken4.
Wssp1.2-Wss1.1-DK-X509-Endorsing.xml	This policy has all features defined in policy Wssp1.2-Wss1.1-DK.xml, and in addition it uses the sender's key to endorse the message signature.
Wssp1.2-Wss1.1-X509-EncryptRequest-SignResponse.xml	This policy is similar to policy Wssp1.2-Wss1.0-X509-EncryptRequest-SignResponse.xml, except that it uses additional WSS 1.1 features, including Signature Confirmation and Thumbprint key reference.
Wssp1.2-Wss1.1-X509-SignRequest-EncryptResponse.xml	This policy is the reverse of policy Wssp1.2-Wss1.1-X509-EncryptRequest-SignResponse.xml: the request is signed and the response is encrypted.

## WS-SecureConversation Policies

The following policies implement WS-SecureConversation 1.3 and WS-SecureConversation 2005/2:

**Table 2-7 WS-SecureConversation Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-2007-Wssc1.3-Bootstrap-Https-BasicAuth.xml	One way SSL with Basic Authentication. Timestamp is included. The algorithm suite is Basic256. The signature is encrypted.
Wssp1.2-2007-Wssc1.3-Bootstrap-Https-ClientCertReq.xml	Two way SSL. The recipient checks for the initiator's public certificate. Note that the client certificate can be used for authentication.
Wssp1.2-2007-Wssc1.3-Bootstrap-Https-UNT.xml	SSL Username token authentication.
Wssp1.2-2007-Wssc1.3-Bootstrap-Https.xml	WS-SecureConversation handshake (RequestSecurityToken and RequestSecurityTokenResponseCollection messages) occurs in https transport. The application messages are signed and encrypted with DerivedKeys. The signature is also encrypted.
Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.0.xml	WS-SecureConversation handshake is protected by WS-Security 1.0. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponseCollection messages are both signed and encrypted. The WS-Addressing headers are signed. Timestamp is included and signed. The signature is encrypted. The algorithm suite is Basic256.
Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.1.xml	WS-SecureConversation handshake is protected by WS-Security 1.1. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponseCollection messages are both signed and encrypted. The WS-Addressing headers are signed. Signature and encryption use derived keys from an encrypted key.
Wssp1.2-Wssc1.3-Bootstrap-Https-BasicAuth.xml	One way SSL with Basic Authentication. Timestamp is included. The algorithm suite is Basic256. The signature is encrypted.
Wssp1.2-Wssc1.3-Bootstrap-Https-ClientCertReq.xml	Two way SSL. The recipient checks for the initiator's public certificate. Note that the client certificate can be used for authentication.

**Table 2-7 WS-SecureConversation Policies**

<b>Policy File</b>	<b>Description</b>
Wssp1.2-Wssc1.3-Bootstrap-Https.xml	WS-SecureConversation handshake (RequestSecurityToken and RequestSecurityTokenResponseCollection messages) occurs in https transport. The application messages are signed and encrypted with DerivedKeys. The signature is also encrypted.
Wssp1.2-Wssc1.3-Bootstrap-Wss1.0.xml	WS-SecureConversation handshake is protected by WS-Security 1.0. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponseCollection messages are both signed and encrypted. The WS-Addressing headers are signed. Timestamp is included and signed. The signature is encrypted. The algorithm suite is Basic256.
Wssp1.2-Wssc1.3-Bootstrap-Wss1.1.xml	WS-SecureConversation handshake is protected by WS-Security 1.1. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponseCollection messages are both signed and encrypted. The WS-Addressing headers are signed. Signature and encryption use derived keys from an encrypted key.
Wssp1.2-Wssc200502-Bootstrap-Https.xml	WS-SecureConversation handshake (RequestSecurityToken and RequestSecurityTokenResponse messages) occurs in https transport. The application messages are signed and encrypted with DerivedKeys.
Wssp1.2-Wssc200502-Bootstrap-Wss1.0.xml	WS-SecureConversation handshake is protected by WS-Security 1.0. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponse messages are both signed and encrypted. The WS-Addressing headers are signed. Timestamp is included and signed. The algorithm suite is Basic128.
Wssp1.2-Wssc200502-Bootstrap-Wss1.1.xml	WS-SecureConversation handshake is protected by WS-Security 1.1. The application messages are signed and encrypted with DerivedKeys. The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponse messages are both signed and encrypted. The WS-Addressing headers are signed. Signature and encryption use derived keys from an encrypted key.

## SAML Token Profile Policies

The policies shown in [Table 2-8](#) implement WS-Security SAML Token Profile 1.0 and 1.1.

**Table 2-8 WS-Security SAML Token Profile Policies**

Policy File	Description
Wssp1.2-2007-Saml1.1-SenderVouches-Wss1.0.xml	The message is signed and encrypted on both request and response with WSS1.0 asymmetric binding. SAML 1.1 token is sent in the request for authentication with Sender Vouches confirmation method, signed by the X509 token.
Wssp1.2-2007-Saml1.1-SenderVouches-Wss1.1.xml	The message is signed and encrypted on both request and response with WSS1.1 X509 symmetric binding. SAML 1.1 token is sent in the request for authentication with Sender Vouches confirmation method, signed by the X509 token.
Wssp1.2-2007-Saml2.0-SenderVouches-Wss1.1.xml	The message is signed and encrypted on both request and response with WSS1.1 X509 symmetric binding. SAML 2.0 token is sent in the request for authentication with Sender Vouches confirmation method, signed by the X509 token.
Wssp1.2-2007-Saml2.0-SenderVouches-Wss1.1-Asymmetric.xml	The message is signed and encrypted on both request and response with WSS1.1 asymmetric binding. It uses additional WS-Security 1.1 features, including Signature Confirmation and Thumbprint key reference. SAML 2.0 token is sent in the request for authentication with Sender Vouches confirmation method, signed by the X509 token.
Wssp1.2-2007-Saml1.1-HolderOfKey-Wss1.0.xml	The message is signed and encrypted on both request and response with WSS1.0 asymmetric binding. SAML 1.1 token is sent in the request for authentication with Holder of Key confirmation method, in which the key inside the SAML Token is used for the signature.
Wssp1.2-2007-Saml1.1-HolderOfKey-Wss1.1-Asymmetric.xml	The message is signed and encrypted on both request and response with WSS1.1 asymmetric binding. It uses additional WS-Security 1.1 features, including Signature Confirmation and Thumbprint key reference. SAML 1.1 token is sent in the request for authentication with Holder of Key confirmation method, in which the key inside the SAML Token is used for the signature.



**Table 2-8 WS-Security SAML Token Profile Policies**

Policy File	Description
Wssp1.2-2007-Saml2.0-HolderOfKey-Wss1.1-Asymmetric.xml	The message is signed and encrypted on both request and response with WSS1.1 asymmetric binding. It uses additional WS-Security 1.1 features, including Signature Confirmation and Thumbprint key reference. SAML 2.0 token is sent in the request for authentication with Holder of Key confirmation method, in which the key inside the SAML Token is used for the signature.
Wssp1.2-2007-Saml2.0-Bearer-Https.xml	One way SSL uses SAML 2.0 token with Bearer confirmation method for Authentication.

## Choosing a Policy

WebLogic Server's implementation of WS-SecurityPolicy 1.2 makes a wide variety of security policy alternatives available to you. When choosing a security policy for your Web Service, you should consider your requirements in these areas:

- Performance
- Security
- Interoperability
- Credential availability (X.509 certificate, username token, clear or digest password)

Whenever possible, Oracle recommends that you:

- Use a policy packaged in WebLogic Server rather than creating a custom policy.
- Use a WS-SecurityPolicy 1.2 policy rather than a WebLogic Server 9.x style policy, unless you require features that are not yet supported by WS-SecurityPolicy 1.2 policies.
- Use transport-level policies (`wssp1.2-2007-https-*.xml`) only where message-level security is not required.
- Use WS-Security 1.0 policies if you require interoperability with that specification. Use one of the following, depending on your authentication requirements and credential availability:
  - `wssp1.2-2007-Wss1.0-UsernameToken-Plain-X509-Basic256.xml`
  - `wssp1.2-2007-Wss1.0-UsernameToken-Digest-X509-Basic256.xml`

- Wssp1.2-2007-Wss1.0-X509-Basic256.xml
- Use WS-Security 1.1 policies if you have strong security requirements. Use one of the following:
  - Wssp1.2-2007-Wss1.1-EncryptedKey-X509-SignedEndorsing.xml
  - Wssp1.2-2007-Wss1.1-DK-X509-SignedEndorsing.xml
  - Wssp1.2-Wss1.1-EncryptedKey-X509-SignedEndorsing.xml
  - Wssp1.2-Wss1.1-DK-X509-Endorsing.xml
- Use a WS-SecureConversation policy where WS-ReliableMessaging plus security are required:
  - Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.0.xml
  - Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.1.xml
  - Wssp1.2-Wssc1.3-Bootstrap-Wss1.0.xml
  - Wssp1.2-Wssc1.3-Bootstrap-Wss1.1.xml
  - Wssp1.2-Wssc200502-Bootstrap-Wss1.0.xml
  - Wssp1.2-Wssc200502-Bootstrap-Wss1.1.xml

## Unsupported WS-SecurityPolicy 1.2 Assertions

The WS-SecurityPolicy 1.2 assertions in [Table 2-9](#) are not supported in this release of WebLogic Server.

**Table 2-9 Web Services SecurityPolicy 1.2 Unsupported Assertions**

Specificati on	Assertion	Remarks
5.1.1	TokenInclusion	includeTokenPolicy=Once is not supported.
5.4.1	UsernameToken	Only <sp:UsernameToken11> and Password Derived Keys are not supported in this release. Other Username Tokens assertions are supported.
5.4.2	IssuedToken	WS-Trust Policy assertion is not supported in this release.

**Table 2-9 Web Services SecurityPolicy 1.2 Unsupported Assertions**

Specificati on	Assertion	Remarks
5.4.3	X509Token	Support all token types, except X509V1. <sp:WssX509V1Token10> and <sp:WssX509V1Token11> are not supported in this release.
5.4.4	KerberosToken	Not supported in this release.
5.4.5	SpnegoContextToken	Not supported in this release.
5.4.9	RelToken	Not supported in this release.
5.4.11	KeyValueToken	Not supported in this release.
6.5	Token Protection	Token Protection in cases where includeTokenPolicy="Never", or in cases where the Token is not in the Message, is not supported in this release.
7.1	AlgorithmSuite	/sp:AlgorithmSuite/wsp:Policy/sp:XPathFilter20 assertion, /sp:AlgorithmSuite/wsp:Policy/sp:XPath10 assertion and /sp:AlgorithmSuite/wsp:Policy/sp:SoapNormalization10 are not supported in this release.
8.1	SupportingTokens	Not supported in this release: ../sp:SignedParts assertion, ../sp:SignedElements assertion ../sp:EncryptedParts assertion ../sp:EncryptedElements assertion
8.2	SignedSupportingTokens	Not supported in this release:
8.3	EndorsingSupportingTokens	../sp:SignedParts assertion
8.4	SignedEndorsingSupportingTok ens	../sp:SignedElements assertion
8.5	SignedEnctrptedSupportingTok ens	../sp:EncryptedParts assertion ../sp:EncryptedElements assertion
		The runtime will not be able to endorse the supporting token in cases where the token is not in the Message (such as for includeTokenPolicy=Never/Once).

**Table 2-9 Web Services SecurityPolicy 1.2 Unsupported Assertions**

Specificati on	Assertion	Remarks
8.6	EncryptedSupportingTokens	UserName Token is the only EncryptionSupportingTokens supported in this release.  Other type of tokens are not supported.
8.7	EndorsingEncryptedSupportingTokens	Not supported in this release.
8.8	SignedEndorsingEncryptedSupportingTokens	Not supported in this release.
9.1	WSS10 Assertion	<sp:MustSupportRefExternalURI> and <sp:MustSupportRefEmbeddedToken> are not supported in this release.
9.2	WSS11 Assertion	<sp:MustSupportRefExternalURI> and <sp:MustSupportRefEmbeddedToken> are not supported in this release.
10.1	Trust13 Assertion	MustSupportClientChallenge, MustSupportServerChallenge are not supported in this release. This assertion is supported only in WS-SecureConversation policy.

## Using the Optional Policy Assertion

WebLogic Server 10.3 supports the `Optional` WS-Policy assertion. Consider the use of `Optional` in the following example:

```
<sp:SignedEncryptedSupportingTokens>
  <wsp:Policy>
    <sp:UsernameToken
      sp:IncludeToken=".../IncludeToken/AlwaysToRecipient"
      wsp:Optional="true" >
      <wsp:Policy>
        <sp:WssUsernameToken10/>
      </wsp:Policy>
```

```

    </sp:UsernameToken>
  </wsp:Policy>
</sp:SignedEncryptedSupportingTokens>

```

In the example, specifying the Username Token for authorization is optional. The client can continue if it cannot generate the Username Token because the user is anonymous or when there is no security context.

During the Security Policy enforcement process, the message is not rejected if the missing element has the Policy assertion with the attribute of `wsp:Optional="true"`.

The following security policy assertions are now supported by the `Optional` policy assertion:

- Username Token
- SAML Token
- Signature parts or signature elements
- Encryption parts or encryption elements
- Derive Key Token

## Configuring Element-Level Security

WebLogic Server supports the element-level assertions defined in WS-SecurityPolicy 1.2. These assertions allow you to apply a signature or encryption to selected elements within the SOAP request or response message, enabling you to target only the specific data in the message that requires security and thereby reduce the computational requirements.

In addition, the assertion `RequiredElements` allows you to ensure that the message contains a specific header element.

The following element-level assertions are available:

- [EncryptedElements](#)
- [ContentEncryptedElements](#)
- [SignedElements](#)
- [RequiredElements](#)

In order to specify an element-level assertion, you must identify the particular request element or response element to which it applies.

You use XPath expressions in policy files to identify these elements, via either XPath Version 1.0 (<http://www.w3.org/TR/xpath>) or XPath Filter Version 2.0 (<http://www.w3.org/TR/xmlsig-filter2/>) syntax. The examples in this section use the default syntax, XPath Version 1.0.

Because each of these assertions identifies one or more particular elements in Web Service message, you must use custom security policy files for all element-level security assertions. These custom policy files are typically combined with pre-packaged security policy files, with the pre-packaged files defining the way that signing or encryption is performed, and the custom policy files identifying the particular elements that are to be signed or encrypted.

## Define and Use a Custom Element-Level Policy File

The first step is to determine the XPath expression that identifies the target element. To do this, you need to understand the format of the SOAP messages used by your web service, either through direct inspection or via analysis of the service's WSDL and XML Schema.

How you determine the format of the SOAP message, and therefore the required XPath expression, is heavily dependent on the tools you have available and is outside the scope of this document. For example, you might do the following:

1. Run the Web Service without element-level security.
2. Turn on SOAP tracing.
3. Inspect the SOAP message in the logs.
4. Produce the XPath expression from the SOAP message.

Or, you might have a software tool that allows you to produce a sample SOAP request for a given WSDL, and then use it to generate the XPath expression.

Consider the example of a Web Service that has a “submitOrderRequest” operation that will receive a SOAP request of the form shown in [Listing 2-8](#).

The sections in bold will be later used to construct the custom element-level policy.

### Listing 2-8 submitOrderRequest SOAP Request

---

```
<env:Envelope
```

```
    xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
```

```
<env:Header/>
```

```

<env:Body>
  <ns1:submitOrderRequest
    xmlns:ns1="http://www.bea.com/OrderService">
    <ns1:OrderRequest>
      <ns1:orderNumber>4815162342</ns1:orderNumber>
      <ns1:creditCard>
        <ns1:cctype>MasterCard</ns1:cctype>
        <ns1:expires>12-01-2020</ns1:expires>
        <ns1:ccn>1234-567890-4444</ns1:ccn>
      </ns1:creditCard>
    </ns1:OrderRequest>
  </ns1:submitOrderRequest>
</env:Body>
</env:Envelope>

```

---

Assume that you require that the `<ns1:creditCard>` element and its child elements be encrypted. To do this, you use the information obtained from the bold sections of [Listing 2-8](#) to create a custom security policy file, perhaps called `EncryptCreditCard.xml`.

Consider the example shown in [Listing 2-9](#).

#### Listing 2-9 EncryptCreditCard.xml Custom Policy File

---

```

<?xml version="1.0"?>
<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512">
  <sp:EncryptedElements
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

```

```
<sp:XPath xmlns:myns="http://www.bea.com/OrderService">
/soapenv:Envelope/soapenv:Body/myns:submitOrderRequest/myns:OrderRequest/m
yns:creditCard
</sp:XPath>
</sp:EncryptedElements>
</wsp:Policy>
```

---

As described in the [WS-SecurityPolicy 1.2 Specification](#), the `/sp:EncryptedElements/sp:XPath` element contains a string specifying an XPath expression that identifies the nodes to be confidentiality protected. The XPath expression is evaluated against the `S:Envelope` element node of the message. Multiple instances of this element may appear within this assertion and should be treated as separate references.

Note the following:

- The root element must be `<wsp:Policy>` with the prefix (in this case `wsp`) mapping to the full WS-Policy namespace.
- The assertion (in this case `EncryptedElements`) must also be namespace-qualified with the full WS-SecurityPolicy 1.2 namespace, as indicated by the “sp” prefix.
- The `creditCard` element in the SOAP message is namespace-qualified (via the `ns1` prefix), and has parent elements: `OrderRequest`, `submitOrderRequest`, `Body`, and `Envelope`. Each of these elements is namespace-qualified.

The XPath query (beginning with `/soapenv:Envelope...`) matches the location of the `creditCard` element:

```
/soapenv:Envelope/soapenv:Body/myns:submitOrderRequest/myns:OrderRequest/myns:creditCard
```

- The namespace prefixes in the SOAP message need not match the prefixes in the custom security policy file. It is important only that the full namespaces to which the prefixes map are the same in both the message and policy assertion.
- WebLogic Server handles the mapping of SOAP 1.1 and SOAP 1.2 namespaces, and WS-Addressing 2004/08 and WS-Addressing 1.0 namespaces.



## Adding the Policy Annotation to JWS File

After you have created your custom policy, add a Policy annotation to your JWS file so that the `ElementEncryption` policy is used for `submitOrder` web service requests, as shown in [Listing 2-10](#).

---

### Listing 2-10 Adding Policy Annotation for Custom Policy File

---

```
@WebMethod
@Policies({
    @Policy(uri="policy:Wsspl.2-2007-Wss1.1-UsernameToken-Plan-X509-Basic256.xml"),
    @Policy(uri="../policies/EncryptCreditCard.xml",
            direction=Policy.Direction.inbound)})

public String submitOrderRequest (OrderRequest orderRequest) {
    return orderService.processOrder(orderRequest);
}
```

---

Because the `creditCard` element is present in the SOAP request, but not the response, the code fragment configures the `EncryptedElements` custom policy only in the “inbound” direction.

## Implementation Notes

Keep the following considerations in mind when implementing element-level security:

- You can include multiple element-level assertions in a policy; all are executed.
- You can include multiple `<sp:XPath>` expressions in a single assertions; all are executed.
- The `EncryptedElements` assertion causes the identified element and all of its children to be encrypted.
- The `ContentEncryptedElements` assertion does not encrypt the identified element, but does encrypt all of its children.

- The `RequiredElements` assertion may be used to test for the presence of a top-level element in the SOAP header. If the element is not found, a SOAP Fault will be raised.  
`RequiredElements` assertions cannot be used to test for elements in the SOAP Body.

## Smart Policy Selection

Multiple policy alternatives for any given Web Service are supported, which provides the service with significant flexibility.

Consider that a Web Service might support any of the following:

- Different versions of the standard. For example, the Web Service might allow WSRM 1.0 and WSRM 1.1, WSS1.0 and WSS 1.1, WSSC 1.1 and WWSSC 1.2, SAML 1.1 or SAML 2.0.
- Different credentials for authentication. For example, the Web Service might allow either username token, X509, or SAML token for authentication.
- Different security requirements for internal and external clients. For example, external authentication might require a SAML token, while internal employee authentication requires only a username token for authentication.

The Web Services client can also handle multiple policy alternatives. The same client can interoperate with different services that have different policy or policy alternatives.

For example, the same client can talk to one service that requires SAML 1.1 Token Profile 1.0 for authentication, while another service requires SAML 2.0 Token Profile 1.1 for authentication.

## Example of Security Policy With Policy Alternatives

[Listing 2-11](#) shows an example of a security policy that supports both WS-Security 1.0 and WS-Security 1.1.

**Note:** Within the `<wsp:ExactlyOne>` element, each policy alternative is encapsulated within a `<wsp:All>` element.

### Listing 2-11 Policy Defining Multiple Alternatives

---

```
<?xml version="1.0"?>
<wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512">
<wsp:ExactlyOne>
```

```

<wsp:All>
  <sp:AsymmetricBinding>
    <wsp:Policy>
      <sp:InitiatorToken>
        <wsp:Policy>
          <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/Inc
ludeToken/AlwaysToRecipient">
            <wsp:Policy>
              <sp:WssX509V3Token10/>
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:InitiatorToken>
      <sp:RecipientToken>
        <wsp:Policy>
          <sp:X509Token

sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/Inc
ludeToken/Never">
            <wsp:Policy>
              <sp:WssX509V3Token10/>
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:RecipientToken>
      <sp:AlgorithmSuite>
        <wsp:Policy>
          <sp:Basic256/>
        </wsp:Policy>
      </sp:AlgorithmSuite>
      <sp:Layout>
        <wsp:Policy>
          <sp:Lax/>
        </wsp:Policy>
      </sp:Layout>
      <sp:IncludeTimestamp/>
      <sp:ProtectTokens/>
      <sp:OnlySignEntireHeadersAndBody/>
    </wsp:Policy>
  </sp:AsymmetricBinding>
  <sp:SignedParts>
    <sp:Body/>
  </sp:SignedParts>
  <sp:Wss10>
    <wsp:Policy>
      <sp:MustSupportRefKeyIdentifier/>
      <sp:MustSupportRefIssuerSerial/>
    </wsp:Policy>

```

## Configuring Message-Level Security

```
</sp:Wss10>
</wsp:All>
<wsp:All>
  <sp:AsymmetricBinding>
    <wsp:Policy>
      <sp:InitiatorToken>
        <wsp:Policy>
          <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/Inc
ludeToken/AlwaysToRecipient">
            <wsp:Policy>
              <sp:RequireThumbprintReference/>
              <sp:WssX509V3Token11/>
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:InitiatorToken>
      <sp:RecipientToken>
        <wsp:Policy>
          <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/Inc
ludeToken/Never">
            <wsp:Policy>
              <sp:RequireThumbprintReference/>
              <sp:WssX509V3Token11/>
            </wsp:Policy>
          </sp:X509Token>
        </wsp:Policy>
      </sp:RecipientToken>
      <sp:AlgorithmSuite>
        <wsp:Policy>
          <sp:Basic256/>
        </wsp:Policy>
      </sp:AlgorithmSuite>
      <sp:Layout>
        <wsp:Policy>
          <sp:Lax/>
        </wsp:Policy>
      </sp:Layout>
      <sp:IncludeTimestamp/>
      <sp:ProtectTokens/>
        <sp:OnlySignEntireHeadersAndBody/>
      </wsp:Policy>
    </sp:AsymmetricBinding>
    <sp:SignedParts>
      <sp:Body/>
    </sp:SignedParts>
  </wsp:All>
</sp:Wss11>
```

```

    <wsp:Policy>
      <sp:MustSupportRefKeyIdentifier/>
      <sp:MustSupportRefIssuerSerial/>
      <sp:MustSupportRefThumbprint/>
      <sp:MustSupportRefEncryptedKey/>
      <sp:RequireSignatureConfirmation/>
    </wsp:Policy>
  </sp:Wss11>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

```

---

## Configuring Smart Policy Selection

You can configure multiple policy alternatives for a single Web Service by creating a custom policy, as shown in [Listing 2-11](#). You then configure the Web Service client to make a policy selection preference.

In this release of WebLogic Server, you can configure the policy selection preferences for the Web Service client by using the WebLogic Server Administration Console, and via stub properties.

The following preferences are supported:

- Security
- Performance
- Compatibility

### How the Policy Preference is Determined

The Web Services runtime uses your policy selection preference to examine the policy alternatives and select the best choice.

If there are multiple policy choices, the system uses the configured preference list, the availability of the credential, and setting of the optional function to determine the best selection policy.

If multiple policy alternatives exist for a client, the following selection rules are used:

- If the preference is not set, the first policy alternative will be picked, except if the policy alternative is defined as `wsp:optional=true`.

- If the preference is set to security first, then the policy that has the most security features is selected.
- If the preference is set to compatibility/interop first, then the policy that has the lowest version is selected.
- If the preference is set to performance first, then the policy with the fewest security features is selected.

For the optional policy assertions, the following selection rules are used:

- If the default policy selection preference is set, then the optional attribute on any assertion is ignored.
- If the Compatibility or Performance preference is set, then any assertion with an optional attribute is ignored; therefore the assertion is ignored.
- If the security policy selection preference is set, optional assertions are included and alternative assertions are never generated.

## Configuring Smart Policy Selection in the Console

Perform the following steps to configure smart policy selection in the Console:

1. If you do not already have a functional Web Services security configuration, [create a Web Services security configuration](#) as described in the online help.
2. Edit the Web Services security configuration. On the General tab, set the Policy Selection Preference. The following values are supported:
  - None (default)
  - Security then Compatibility then Performance (SCP)
  - Security then Performance then Compatibility (SPC)
  - Compatibility then Security then Performance (CSP)
  - Compatibility then Performance then Security (CPS)
  - Performance then Compatibility then Security (PCS)
  - Performance then Security then Compatibility (PSC)
3. Save and activate your changes.

## Understanding Body Encryption in Smart Policy

In smart policy selection scenarios, whether or not the Body will be encrypted (for example, `<sp:EncryptedParts> <sp:Body /></sp:EncryptedParts>`) depends on the following policy selection preference rules:

- Default -- The first policy alternative will be used for the determination. If the encrypted body assertion is in the first policy alternative, the body is encrypted. If the encrypted body assertion is not in the first policy alternative, the body is not encrypted.
- SCP, SPC -- encrypted
- PCS, PSC -- not encrypted
- CPS -- not encrypted
- CSP -- encrypted

Consider the following two examples. In [Listing 2-12](#), the encrypted body assertion is in the first policy alternative. Therefore, in the default preference case the body is encrypted. For policy selection preferences other than the default, the other preference rules apply.

---

### Listing 2-12 Body Assertion in First Policy Alternative

---

```
<?xml version="1.0"?>
<wsp:Policy
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
>
  <wsp:ExactlyOne>
    <sp:EncryptedParts>
      <sp:Body/>
    </sp:EncryptedParts>
  </wsp:ExactlyOne>
</wsp:Policy>
```

---

By contrast, in [Listing 2-13](#), the encrypted body assertion is not in the first policy alternative. Therefore, in the default preference case the body is not encrypted. For policy selection preferences other than the default, the other preference rules apply.

### Listing 2-13 Body Assertion Not in First Policy Alternative

---

```
<?xml version="1.0"?>
<wsp:Policy
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
>
<wsp:ExactlyOne>
<sp:EncryptedParts/>
<sp:EncryptedParts>
<sp:Body/>
</sp:EncryptedParts>
</wsp:ExactlyOne>
</wsp:Policy>
```

---

## Smart Policy Selection for a Standalone Client

You can set the policy selection preference via the stub property.

The following example sets the stub property for security, compatibility, and performance preferences:

```
stub._setProperty(WLStub.POLICY_SELECTION_PREFERENCE,
WLStub.PREFERENCE_SECURITY_COMPATIBILITY_PERFORMANCE);
```

If the policy selection preference is not set, then the default preference (None) is used.

## Multiple Transport Assertions

If there are multiple available transport-level assertions in your security policies, WebLogic Server uses the policy that requires https. If more than one policy alternative requires https, WebLogic Server randomly picks one of them. You should therefore avoid using multiple policy alternatives that contain mixed transport-level policy assertions.



## Example of Adding Security to MTOM Web Service

As described in [Optimizing Binary Data Transmission Using MTOM/XOP](#), SOAP Message Transmission Optimization Mechanism/XML-binary Optimized Packaging (MTOM/XOP) defines a method for optimizing the transmission of XML data of type `xs:base64Binary` or `xs:hexBinary` in SOAP messages.

This section describes a combination of two examples that are already included with WebLogic Server :

- `WL_HOME\samples\server\examples\src\examples\webservices\wss1.1`
- `WL_HOME\samples\server\examples\src\examples\webservices\mtom`.

These existing examples include functional code and extensive `instructions.html` files that describes their use and function, how to build them, and so forth This section does not repeat that information, but instead concentrates on the changes made to these examples, and the reasons for the changes.

## Files Used by This Example

The example uses the files shown in [Table 2-10](#). The contents of the source files are shown in subsequent sections.:

**Table 2-10 Files Used in MTOM/Security Example**

File	Description
<code>build.xml</code>	Ant build file that contains targets for building and running the example.
<code>configWss.py</code>	WLST script that configures a Web Service security configuration. This file is copied without change from <code>WL_HOME\samples\server\examples\src\examples\webservices\wss1.1</code>
<code>MtomClient.java</code>	Standalone client application that invokes the MTOM Web Service. This file uses the JAX-RPC Stubs generated by clientgen, based on the WSDL of the Web Service.
<code>SecurityMtomService.java</code>	JWS file that implements the MTOM Web Service. The JWS file uses the <code>@Policy</code> annotation to specify the WS-Policy files that are associated with the Web Service.

**Table 2-10 Files Used in MTOM/Security Example**

<b>File</b>	<b>Description</b>
clientkeyStore.jks	Client-side key store, used to create a client-side BinarySecurityToken credential provider.  This file is copied without change from <i>WL_HOME</i> \samples\server\examples\src\examples\web services\wss1.1\certs
serverkeyStore.jks	Server-side key store, used to create a Server-side BinarySecurityToken credential provider.  This file is copied without change from <i>WL_HOME</i> \samples\server\examples\src\examples\web services\wss1.1\certs
testServerCertTempCert.der	Server-side certificate, used to create a client-side BinarySecurityToken credential provider.  This file is copied without change from <i>WL_HOME</i> \samples\server\examples\src\examples\web services\wss1.1\certs

## SecurityMtomService.java

The `SecurityMtomService.java` JWS file is the same as that in `WL_HOME\samples\server\examples\src\examples\webservices\mtom\MtomService.java`, with the additional Policy annotations shown in bold.

### Listing 2-14 SecurityMtomService.java

```
package examples.webservices.security_mtom;

import weblogic.jws.Binding;
import weblogic.jws.Policy;
import weblogic.jws.Policies;
import weblogic.jws.Context;
import weblogic.jws.WLDeployment;
import weblogic.wsee.jws.JwsContext;
```

```

import weblogic.wsee.mtom.api.MtomPolicyInfo;
import weblogic.wsee.mtom.api.MtomPolicyInfoFactory;
import weblogic.wsee.policy.framework.PolicyException;

import javax.jws.WebService;
import javax.jws.WebMethod;
import java.rmi.RemoteException;

/**
 * Sample to MTOM with JAX-RPC
 *
 * @author Copyright © 1996, 2008, Oracle and/or its affiliates.
 * All rights reserved.
 */
@WebService
@Binding(Binding.Type.SOAP12)
//enable WSS + MTOM for this web service by adding the following canned
policy files
@Policies({
    @Policy(uri = "policy:Mtom.xml"),
    @Policy(uri = "policy:Wssp1.2-2007-SignBody.xml"),
    @Policy(uri = "policy:Wssp1.2-2007-EncryptBody.xml"),
    @Policy(uri = "policy:Wssp1.2-Wss1.1-EncryptedKey.xml")
})
public class SecurityMtomService {

    public SecurityMtomService() {

```

## Configuring Message-Level Security

```
}

/**
 * Input is sent as XOP'ed binary octet stream
 *
 * @param bytes input bytes
 * @return A simple String
 */
@WebMethod
public String echoBinaryAsString(byte[] bytes) {
    return new String(bytes);
}

/**
 * Output is sent as as XOP'ed binary octet stream
 *
 * @param s a simple String
 * @return byte[]
 */
@WebMethod
public byte[] echoStringAsBinary(String s) {
    return s.getBytes();
}

/**
 * input byte[] is sent as as XOP'ed binary octet stream
 *
```

```

* @param array input byte[] array
* @return String[]
*/
@WebMethod
public String[] echoBinaryArrayAsStringArray(byte[] array) {
    String[] strings = new String[1];
    strings[0] = new String(array);
    return strings;
}
}

```

---

You can specify the `@Policy` annotation at both the class- and method- level. In this example, the annotation is used at the class-level to specify the pre-packaged WS-Policy files, which means all public operations of the Web Service are associated with the specified WS-Policy files.

You use the `@Policies` annotation to group together multiple `@Policy` annotations. You can specify this annotation at both the class- and method-level. In this example, the annotation is used at the class-level to group the four `@Policy` annotations that specify the pre-packaged WS-Policy files:

- The pre-packaged WS-Policy file `Mtom.xml` enables MTOM encoding.
- As described in [“Protection Assertion Policies” on page 2-49](#), the `Wssp1.2-2007-SignBody.xml` policy file specifies that the body and WebLogic system headers of both the request and response SOAP message be digitally signed.
- The `Wssp1.2-2007-EncryptBody.xml` policy file specifies that the body of both the request and response SOAP messages be encrypted.
- The `Wssp1.2-Wss1.1-EncryptedKey.xml` symmetric binding policy uses the WS-Security 1.1 Encrypted Key feature. The client application invoking the Web Service must use the encrypted key to encrypt and sign, and the server must send Signature Confirmation.

## MtomClient.java

MtomClient.java is a standalone client application that invokes the SecurityMtomService Web Service. It uses the JAX-RPC stubs generated by clientgen, based on the WSDL of the Web Service. The MtomClient code is shown in [Listing 2-15](#).

### Listing 2-15 MtomClient.java

---

```
package examples.webservices.security_mtom.client;

import java.rmi.RemoteException;

import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.List;
import javax.xml.rpc.Stub;

import weblogic.security.SSL.TrustManager;

// Import classes to create the Binary and Username tokens
import weblogic.wsee.security.bst.ClientBSTCredentialProvider;
import weblogic.wsee.security.unt.ClientUNTCredentialProvider;

// Import classes for creating the client-side credential provider
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.xml.crypto.wss.provider.CredentialProvider;
import weblogic.wsee.security.util.CertUtils;

/**
```

```

* @author Copyright © 1996, 2008, Oracle and/or its affiliates.
* All rights reserved.
*/
public class MtomClient {
    private static final String FOO = "FOO";
    private static SecurityMtomService port;

    public MtomClient(String args[]) throws Exception {
        //client keystore file
        String clientKeyStore = args[0];
        String clientKeyStorePass = args[1];
        String clientKeyAlias = args[2];
        String clientKeyPass = args[3];

        //server certificate
        String serverCertFile = args[4];
        String wsdl = args[5];

        SecurityMtomServiceService service = new
SecurityMtomServiceService_Impl(wsdl);

        port = service.getSecurityMtomServiceSoapPort();

        X509Certificate serverCert = (X509Certificate)
CertUtils.getCertificate(serverCertFile);

        //create empty list of credential providers
        List credProviders = new ArrayList();

```

## Configuring Message-Level Security

```
//Create client-side BinarySecurityToken credential provider that uses
// X.509 for identity, based on certificate and keys parameters
CredentialProvider cp = new ClientBSTCredentialProvider(clientKeyStore,
clientKeyStorePass, clientKeyAlias, clientKeyPass, "JKS", serverCert);
credProviders.add(cp);

Stub stub = (Stub) port;

// Set stub property to point to list of credential providers
stub._setProperty(WSSecurityContext.CREDENTIAL_PROVIDER_LIST,
credProviders);

// setup the TrustManager.
stub._setProperty(WSSecurityContext.TRUST_MANAGER,
    new TrustManager() {
        public boolean certificateCallback(X509Certificate[] chain, int
validateErr) {
            //Typically in a real-life application, Java code that actually
            //verifies the certificate goes here; for sake of simplicity, this
            //example assumes the certificate is valid and simply returns true.

            return true;
        }
    });
}

public static void main(String[] args) throws Exception {
    MtomClient client = new MtomClient(args);
```



```

    client.invokeEchoBinaryAsString();
    client.invokeEchoStringAsBinary();
    client.invokeEchoBinaryArrayAsStringArray();
}

public void invokeEchoBinaryArrayAsStringArray() throws RemoteException {
    System.out.println("sending a String '" + FOO + "' as a byte array.");
    String result =
port.echoBinaryArrayAsStringArray(FOO.getBytes()).getJavaLangstring()[0];
    System.out.println("echoing '" + result + "' as a String array.");
}

public void invokeEchoStringAsBinary() throws RemoteException {
    System.out.println("sending a String '" + FOO + "'");
    String result = new String(port.echoStringAsBinary(FOO));
    System.out.println("echoing '" + result + "' as a byte array.");
}

public void invokeEchoBinaryAsString() throws RemoteException {
    System.out.println("sending a String '" + FOO + "' as a byte array.");
    String result = port.echoBinaryAsString(FOO.getBytes());
    System.out.println("echoing '" + result + "' as a String.");
}
}

```

---

The client application takes six arguments:

- Client keystore

- Client keystore password
- Client key alias
- Client key password
- The server certificate file
- WSDL of the deployed Web Service

The client application uses the following WebLogic Web Services security APIs to create the needed client-side credential providers, as specified by the WS-Policy files that are associated with the Web Service:

- `weblogic.wsee.security.bst.ClientBSTCredentialProvider` to create a binary security token credential provider, using the certificate and private key.
- `weblogic.xml.crypto.wss.WSSecurityContext` to specify the list of credential providers to the JAX-RPC stub.
- `weblogic.xml.crypto.wss.provider.CredentialProvider`, which is the main credential provider class.

When you write this client application, you need to consult the WS-Policy files associated with a Web Service to determine the types and number of credential providers that must be set in the JAX-RPC stub. Typically, if the WS-Policy file specifies that SOAP messages must be signed or encrypted, using X.509 for identity, then you must create a `ClientBSTCredentialProvider`. (If it specifies that the user provides a username token for identity, then the application must create a `ClientUNTCredentialProvider`.)

The example creates a [client BST credential provider](#) for the indicated keystore, certificate alias, and server certificate. The certificate passed for the parameter `serverCert` is used to encrypt the message body contents and to verify the received signature. Any `KeyInfo` received as part of the in-bound signature (for example, certificate thumbprint) must correctly identify the same server certificate.

The Web Services client runtime also consults this WSDL so it can correctly create the security headers in the SOAP request when an operation is invoked.

Finally, the client application must use the `weblogic.security.SSL.TrustManager` WebLogic security API to verify that the certificate used to encrypt the SOAP request is valid. The client runtime gets this certificate (`serverCert` in the example) from the deployed WSDL of the Web Service, which in real-life situations is not automatically trusted, so the client application must ensure that it is okay before it uses it to encrypt the SOAP request.

**Note:** The client-side certificate and private key used in this example have been created for simple testing purposes, and therefore are always trusted by WebLogic Server. For this reason, there is no additional server-side security configuration needed to run this example. In real life, however, the client application would use a certificate from a real certificate authority, such as Verisign. In this case, administrators would need to use the WebLogic Administration Console to add this certificate to the list that is trusted by WebLogic Server.

## configWss.py Script File

The SecurityMtomService Web Service does not explicitly invoke any WebLogic Server API to handle the requirements imposed by any associated policy files, nor does this Web Service have to understand which, if any, security providers, tokens, or other such mechanisms are involved.

The script file `configWss.py` uses WLST to create and configure the default Web Service security configuration, `default_wss`, for the active security realm. (The default Web Service security configuration is used by *all* Web Services in the domain unless they have been explicitly programmed to use a different configuration.) Further, this script makes sure that x509 tokens are supported, creates the needed security providers, and so forth.

[Listing 2-16](#) shows the `configWss.py` file. The `build.xml` file provides the command input. Sections of particular interest are shown in bold.

### Listing 2-16 configWss.py

---

```

userName = sys.argv[1]
password = sys.argv[2]
url="t3://" + sys.argv[3] + ":" + sys.argv[4]

print "Connect to the running adminServer"

connect(userName, password, url)

edit()
startEdit()
```

## Configuring Message-Level Security

```
#Enable assert x509 in SecurityConfiguration
rlm = cmo.getSecurityConfiguration().getDefaultRealm()
ia = rlm.lookupAuthenticationProvider("DefaultIdentityAsserter")
activeTypesValue = list(ia.getActiveTypes())
existed = "X.509" in activeTypesValue
if existed == 1:
    print 'assert x509 is already enabled'
else:
    activeTypesValue.append("X.509")
ia.setActiveTypes(array(activeTypesValue, java.lang.String))
ia.setDefaultUserNameMapperAttributeType('CN');
ia.setUseDefaultUserNameMapper(Boolean('true'));

#Create default WebServiceSecurity
securityName='default_wss'
defaultWss=cmo.lookupWebServiceSecurity(securityName)
if defaultWss == None:
    print 'creating new webservice security bean for: ' + securityName
    defaultWss = cmo.createWebServiceSecurity(securityName)
else:
    print 'found existing bean for: ' + securityName

#Create credential provider for DK
cpName='default_dk_cp'
wtm=defaultWss.lookupWebServiceCredentialProvider(cpName)
```

```

if wtm == None:
    wtm = defaultWss.createWebserviceCredentialProvider(cpName)

wtm.setClassName('weblogic.wsee.security.wssc.v200502.dk.DKCredentialProvider')

    wtm.setTokenType('dk')
    cpm = wtm.createConfigurationProperty('Label')
    cpm.setValue('WS-SecureConversationWS-SecureConversation')
    cpm = wtm.createConfigurationProperty('Length')
    cpm.setValue('16')

else:
    print 'found existing bean for: DK ' + cpName

#Create credential provider for x.509
cpName='default_x509_cp'
wtm=defaultWss.lookupWebserviceCredentialProvider(cpName)
if wtm == None:
    wtm = defaultWss.createWebserviceCredentialProvider(cpName)

wtm.setClassName('weblogic.wsee.security.bst.ServerBSTCredentialProvider')
    wtm.setTokenType('x509')

else:
    print 'found existing bean for: x.509 ' + cpName

#Custom keystore for xml encryption
cpName='ConfidentialityKeyStore'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:

```

## Configuring Message-Level Security

```
        cpm = wtm.createConfigurationProperty(cpName)
keyStoreName=sys.argv[5]
cpm.setValue(keyStoreName)

cpName='ConfidentialityKeyStorePassword'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
cpm.setEncryptValueRequired(Boolean('true'))
KeyStorePasswd=sys.argv[6]
cpm.setEncryptedValue(KeyStorePasswd)

cpName='ConfidentialityKeyAlias'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
keyAlias=sys.argv[7]
cpm.setValue(keyAlias)

cpName='ConfidentialityKeyPassword'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty('ConfidentialityKeyPassword')
cpm.setEncryptValueRequired(Boolean('true'))
keyPass=sys.argv[8]
cpm.setEncryptedValue(keyPass)
```

```
#Custom keystore for xml digital signature
cpName='IntegrityKeyStore'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
keyStoreName=sys.argv[5]
cpm.setValue(keyStoreName)

cpName='IntegrityKeyStorePassword'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
cpm.setEncryptValueRequired(Boolean('true'))
KeyStorePasswd=sys.argv[6]
cpm.setEncryptedValue(KeyStorePasswd)

cpName='IntegrityKeyAlias'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
keyAlias=sys.argv[7]
cpm.setValue(keyAlias)

cpName='IntegrityKeyPassword'
cpm=wtm.lookupConfigurationProperty(cpName)
if cpm == None:
    cpm = wtm.createConfigurationProperty(cpName)
```

## Configuring Message-Level Security

```
cpm.setEncryptValueRequired(Boolean('true'))
keyPass=sys.argv[8]
cpm.setEncryptedValue(keyPass)

#Create token handler for x509 token
#cpName='default_x509_handler'
th=defaultWss.lookupWebserviceTokenHandler(cpName)
if th == None:
    th = defaultWss.createWebserviceTokenHandler(cpName)

th.setClassName('weblogic.xml.crypto.wss.BinarySecurityTokenHandler')
th.setTokenType('x509')
cpm = th.createConfigurationProperty('UseX509ForIdentity')
cpm.setValue('true')

save()
activate(block="true")
disconnect()
exit()
```

---

## Build.xml File

The build.xml file has the targets shown in [Table 2-11](#).



**Table 2-11** build.xml targets

Target	Description
client	Target that builds the Security MTOM Web Service client.
config.server.security	Target that configures the Web Service security.
deploy	Target that deploys the Web Service.
server	Target that builds the Security MTOM Web Service.
clean	Deletes temporary directories.
build	Depends on server, client, and clean.
run	Target that runs the Security MTOM Web Service client.
all	Default target. Depends on build, deploy.

The complete `build.xml` file is shown in [Listing 2-17](#).

#### **Listing 2-17** build.xml File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<project name="webservices.security_mtom" default="all" basedir=".">

  <!-- set global properties for this build -->
  <property file="../../../../examples.properties"/>

  <property name="client.dir"
value="\${client.classes.dir}/webservicesSecurityMtom_Client" />
  <property name="package.dir" value="examples/webservices/security_mtom"/>
  <property name="package" value="examples.webservices.security_mtom"/>
  <property name="ws.file" value="SecurityMtomService" />
```

## Configuring Message-Level Security

```
<property name="ear.dir"
value="\${examples.build.dir}/webservicessecurityMtomEar" />
<property name="cert.dir" value="\${basedir}/certs" />
<property name="certs.dir" value="\${basedir}/certs" />

<!--client keystore-->
<property name="client-keystore-name" value="clientKeyStore.jks"/>
<property name="client-keystore-pass" value="keystorepw"/>
<property name="client-cert" value="ClientCert"/>
<property name="client-key" value="ClientKey"/>
<property name="client-key-pass" value="ClientKeyPass"/>
<property name="client-cert-alias" value="testClientCert"/>

<!--server keystore-->
<property name="server-keystore-name" value="serverKeyStore.jks"/>
<property name="server-keystore-pass" value="keystorepw"/>
<property name="server-cert" value="ServerCert"/>
<property name="server-key" value="ServerKey"/>
<property name="server-key-pass" value="ServerKeyPass"/>
<property name="server-cert-alias" value="testServerCert"/>

<path id="client.class.path">
  <pathelement path="\${client.dir}"/>
  <pathelement path="\${java.class.path}"/>
</path>

<!-- Web Service WLS Ant task definitions -->
<taskdef name="jwsc"
```

```

        classname="weblogic.wsee.tools.anttasks.JwscTask" />
<taskdef name="clientgen"
        classname="weblogic.wsee.tools.anttasks.ClientGenTask" />

<target name="all" depends="build, deploy"/>

<target name="build" depends="clean, server, client"/>

<target name="clean">
    <delete dir="${ear.dir}"/>
    <delete dir="${client.dir}"/>
</target>

<!-- Target that builds the MTOM Web Service -->
<target name="server" description="Target that builds the MTOM Web
Service">
    <jwsc
        srcdir="${examples.src.dir}/${package.dir}"
        sourcepath="${examples.src.dir}"
        destdir="${ear.dir}"
        classpath="${java.class.path}"
        fork="true"
        keepGenerated="true"
        deprecation="${deprecation}"
        debug="${debug}">
        <jws file="SecurityMtomService.java" explode="true"/>
    </jwsc>
</target>

```

## Configuring Message-Level Security

```
<!-- Target that builds the MTOM Web Service client -->
<target name="client" description="Target that builds the source Web
Service">
  <mkdir dir="${client.dir}/${package.dir}/client/" />
  <clientgen
    wsdl="${ear.dir}/${ws.file}/WEB-INF/${ws.file}Service.wsdl"
    destDir="${client.dir}"
    classpath="${java.class.path}"
    packageName="${package}.client" />
  <copy file="MtomClient.java"
todir="${client.dir}/${package.dir}/client/" />
  <javac
    srcdir="${client.dir}" destdir="${client.dir}"
    classpath="${java.class.path}"
    includes="${package.dir}/client/**/*.java" />
</target>

<!-- Target that deploys the MTOM Web Service -->
<target name="deploy" description="Target that deploys the reliable
destination Web Service">
  <wldeploy
    action="deploy"
    source="${ear.dir}"
    user="${wls.username}"
    password="${wls.password}"
    verbose="true"
    adminurl="t3://${wls.hostname}:${wls.port}"
```

```

    targets="${wls.server.name}"
    failonerror="${failondeploy}"/>
</target>

<!-- Target that runs the MTOM Web Service client -->
<target name="run" >
    <java fork="true"
        classname="examples.webservices.security_mtom.client.MtomClient"
        failonerror="true" >
        <jvmarg line="-Dweblogic.wsee.verbose=*" />
        <classpath refid="client.class.path"/>
        <arg line="
            ${basedir}/certs/${client-keystore-name}
            ${client-keystore-pass}
            ${client-cert-alias}
            ${client-key-pass}
            ${basedir}/certs/testServerCertTempCert.der
            http://${wls.hostname}:${wls.port}/SecurityMtomService/SecurityMtomService
            ?WSDL" />
        </java>
    </target>

    <!-- Target the configure the web service security -->
    <target name="config.server.security" description="Target the configure
the web service security">
        <copy todir="${examples.domain.dir}" overwrite="true">
            <fileset dir="${certs.dir}" includes="${server-keystore-name}"/>

```

```
</copy>

<java classname="weblogic.WLST" fork="true" failonerror="true">
  <arg line="configWss.py ${wls.username} ${wls.password}
${wls.hostname} ${wls.port}
  ${server-keystore-name} ${server-keystore-pass} ${server-cert-alias}
${server-key-pass}" />
</java>

</target>

</project>
```

---

## Building and Running the Example

Follow these steps to build and run the example:

1. Start the Examples server
2. Set up your environment, as described in the `BEA_HOME\WL_HOME\samples\server\examples\src\examples\examples.html` instructions file.  
  
`BEA_HOME\WL_HOME\samples\domains\wl_server>setExamplesEnv.cmd`
3. Change to the `BEA_HOME\WL_HOME\samples\server\examples\src\examples\webservices` directory and create a new subdirectory called `security_mtom`.
4. Cut and paste the contents of the `build.xml`, `configWss.py`, `MtomClient.java`, and `SecurityMtomService.java` sections to files with the same names in the `BEA_HOME\WL_HOME\samples\server\examples\src\examples\webservices\security_mtom` directory.
5. Copy all of the files (`clientKeyStore.jks`, `serverKeyStore.jks`, and `testServerCertTempCert.der`) from

```
BEA_HOME\WL_HOME\samples\server\examples\src\examples\webservices\wss1.1\certs
```

to a new `certs` subdirectory

```
BEA_HOME\WL_HOME\samples\server\examples\src\examples\webservices\security_mtom\certs
```

#### 6. Change to the

```
BEA_HOME\WL_HOME\samples\server\examples\src\examples\webservices\security_mtom directory.
```

#### 7. Execute the following command:

```
prompt> ant config.server.security
```

#### 8. Restart Weblogic Server.

#### 9. Build, deploy and run the example:

```
prompt> ant build deploy run
```

## Deployed WSDL for SecurityMtomService

The deployed WSDL for the SecurityMtomService Web Service is available at the following URL:

```
http://host:port/SecurityMtomService/SecurityMtomService?WSDL
```

The complete WSDL is shown in [Listing 2-18](#).

### Listing 2-18 Deployed WSDL for SecurityMtomService

---

```
<?xml version="1.0" encoding="UTF-8" ?>
- <s1:definitions name="SecurityMtomServiceServiceDefinitions"
targetNamespace="http://examples/webservices/security_mtom" xmlns=""
xmlns:s0="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:s1="http://schemas.xmlsoap.org/wsdl/"
xmlns:s2="http://examples/webservices/security_mtom"
xmlns:s3="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
```

## Configuring Message-Level Security

```
<wsp:UsingPolicy s1:Required="true" />
- <wsp:Policy s0:Id="Mtom.xml">
  <wsoma:OptimizedMimeSerialization
xmlns:wsoma="http://schemas.xmlsoap.org/ws/2004/09/policy/optimizedmimeser
ialization" />
  </wsp:Policy>
- <wsp:Policy s0:Id="Wsspl.2-Wss1.1-EncryptedKey.xml">
- <sp:SymmetricBinding
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512">
- <wsp:Policy>
- <sp:ProtectionToken>
- <wsp:Policy>
- <sp:X509Token
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512
/IncludeToken/Never">
- <wsp:Policy>
  <sp:RequireThumbprintReference />
  <sp:WssX509V3Token11 />
  </wsp:Policy>
  </sp:X509Token>
  </wsp:Policy>
  </sp:ProtectionToken>
- <sp:AlgorithmSuite>
- <wsp:Policy>
  <sp:Basic256 />
  </wsp:Policy>
  </sp:AlgorithmSuite>
- <sp:Layout>
- <wsp:Policy>
```



```

    <sp:Lax />
  </wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp />
<sp:OnlySignEntireHeadersAndBody />
</wsp:Policy>
</sp:SymmetricBinding>
- <sp:Wss11
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512">
- <wsp:Policy>
  <sp:MustSupportRefKeyIdentifier />
  <sp:MustSupportRefIssuerSerial />
  <sp:MustSupportRefThumbprint />
  <sp:MustSupportRefEncryptedKey />
  <sp:RequireSignatureConfirmation />
</wsp:Policy>
</sp:Wss11>
</wsp:Policy>
- <wsp:Policy s0:Id="Wsspl.2-2007-EncryptBody.xml">
- <sp:EncryptedParts
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <sp:Body />
</sp:EncryptedParts>
</wsp:Policy>
- <wsp:Policy s0:Id="Wsspl.2-2007-SignBody.xml">
- <sp:SignedParts
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
  <sp:Body />

```

## Configuring Message-Level Security

```
</sp:SignedParts>
</wsp:Policy>
- <s1:types>
- <xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
targetNamespace="java:examples.webservices.security_mtom"
xmlns:s0="http://schemas.xmlsoap.org/wsdl/"
xmlns:s1="http://examples/webservices/security_mtom"
xmlns:s2="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
- <xs:complexType name="ArrayOfJavaLangstring_literal">
- <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0" name="JavaLangstring"
nillable="true" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="ArrayOfJavaLangstring_literal"
type="java:ArrayOfJavaLangstring_literal"
xmlns:java="java:examples.webservices.security_mtom" />
  <xs:element name="base64Binary_literal" type="xs:base64Binary" />
</xs:schema>
- <xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
targetNamespace="http://examples/webservices/security_mtom"
xmlns:s0="http://schemas.xmlsoap.org/wsdl/"
xmlns:s1="http://examples/webservices/security_mtom"
xmlns:s2="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:import namespace="java:examples.webservices.security_mtom" />
- <xs:element name="echoBinaryAsString">
```

```

- <xs:complexType>
- <xs:sequence>
  <xs:element name="bytes" type="xs:base64Binary" />
</xs:sequence>
</xs:complexType>
</xs:element>
- <xs:element name="echoBinaryAsStringResponse">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="return" type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
- <xs:element name="echoBinaryArrayAsStringArray">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="array" type="xs:base64Binary" />
</xs:sequence>
</xs:complexType>
</xs:element>
- <xs:element name="echoBinaryArrayAsStringArrayResponse">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="return" type="java:ArrayOfJavaLangstring_literal"
xmlns:java="java:examples.webservices.security_mtom" />
</xs:sequence>
</xs:complexType>
</xs:element>

```

## Configuring Message-Level Security

```
- <xs:element name="echoStringAsBinary">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="s" type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
- <xs:element name="echoStringAsBinaryResponse">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="return" type="xs:base64Binary" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
</s1:types>
- <s1:message name="echoBinaryAsString">
  <s1:part element="s2:echoBinaryAsString" name="parameters" />
</s1:message>
- <s1:message name="echoBinaryAsStringResponse">
  <s1:part element="s2:echoBinaryAsStringResponse" name="parameters" />
</s1:message>
- <s1:message name="echoBinaryArrayAsStringArray">
  <s1:part element="s2:echoBinaryArrayAsStringArray" name="parameters" />
</s1:message>
- <s1:message name="echoBinaryArrayAsStringArrayResponse">
  <s1:part element="s2:echoBinaryArrayAsStringArrayResponse"
name="parameters" />
```

```

</s1:message>
- <s1:message name="echoStringAsBinary">
  <s1:part element="s2:echoStringAsBinary" name="parameters" />
</s1:message>
- <s1:message name="echoStringAsBinaryResponse">
  <s1:part element="s2:echoStringAsBinaryResponse" name="parameters" />
</s1:message>
- <s1:portType name="SecurityMtomService"
wsp:PolicyURIs="#Wssp1.2-2007-SignBody.xml #Wssp1.2-2007-EncryptBody.xml
#Wssp1.2-Wss1.1-EncryptedKey.xml">
- <s1:operation name="echoBinaryAsString" parameterOrder="parameters">
  <s1:input message="s2:echoBinaryAsString" />
  <s1:output message="s2:echoBinaryAsStringResponse" />
</s1:operation>
- <s1:operation name="echoBinaryArrayAsStringArray"
parameterOrder="parameters">
  <s1:input message="s2:echoBinaryArrayAsStringArray" />
  <s1:output message="s2:echoBinaryArrayAsStringArrayResponse" />
</s1:operation>
- <s1:operation name="echoStringAsBinary" parameterOrder="parameters">
  <s1:input message="s2:echoStringAsBinary" />
  <s1:output message="s2:echoStringAsBinaryResponse" />
</s1:operation>
</s1:portType>
- <s1:binding name="SecurityMtomServiceServiceSoapBinding"
type="s2:SecurityMtomService">
  <s3:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http" />
- <wsp:Policy>

```

## Configuring Message-Level Security

```
<wsp:PolicyReference URI="#Mtom.xml" />
</wsp:Policy>
- <s1:operation name="echoBinaryAsString">
  <s3:operation style="document" />
- <s1:input>
  <s3:body parts="parameters" use="literal" />
</s1:input>
- <s1:output>
  <s3:body parts="parameters" use="literal" />
</s1:output>
</s1:operation>
- <s1:operation name="echoBinaryArrayAsStringArray">
  <s3:operation style="document" />
- <s1:input>
  <s3:body parts="parameters" use="literal" />
</s1:input>
- <s1:output>
  <s3:body parts="parameters" use="literal" />
</s1:output>
</s1:operation>
- <s1:operation name="echoStringAsBinary">
  <s3:operation style="document" />
- <s1:input>
  <s3:body parts="parameters" use="literal" />
</s1:input>
- <s1:output>
  <s3:body parts="parameters" use="literal" />
```

```

</s1:output>
</s1:operation>
</s1:binding>
- <s1:service name="SecurityMtomServiceService">
- <s1:port binding="s2:SecurityMtomServiceServiceSoapBinding"
name="SecurityMtomServiceSoapPort">
    <s3:address
location="http://localhost:7001/SecurityMtomService/SecurityMtomService"
/>
</s1:port>
</s1:service>
</s1:definitions>

```

## Example of Adding Security to Reliable Messaging Web Service

This section describes an update to an example that is already included with WebLogic Server:

- `WL_HOME\samples\server\examples\src\examples\webservices\wsrm_security`

This section shows how to update the example to use the most recent version of the policy file. Oracle recommends that you use the new policy namespace, as shown in the revised example, as those are official namespaces from OASIS standards and they will perform better when interoperating with other vendors.

## Overview of Secure and Reliable SOAP Messaging

Reliable SOAP messaging is a framework whereby an application running in one WebLogic Server instance can reliably invoke a Web Service running on another WebLogic Server instance. Reliable is defined as the ability to guarantee message delivery between the two Web Services.

WebLogic Web Services conform to the [WS-ReliableMessaging 1.1](#) specification, which describes how two Web Services running on different WebLogic Server application servers can communicate reliably in the presence of failures in software components, systems, or networks. In particular, the specification describes an interoperable protocol in which a message sent from a source endpoint (client Web Service) to a destination endpoint (Web Service whose operations

can be invoked reliably) is guaranteed either to be delivered, according to one or more delivery assurances, or to raise an error. The WS-ReliableMessaging specification defines an interoperable way to provide security by composing WS-ReliableMessaging with WS-SecureConversation and associating a reliable sequence with a secure session. At sequence creation time, the sending side needs to present a Security Token Reference to point to a Security Context Token that will be used to identify the owner of the sequence. All subsequent sequence messages and protocol messages in both directions will need to demonstrate proof-of-possession of the referenced key.

WebLogic reliable SOAP messaging works only between two Web Services. This means that you can invoke a WebLogic Web Service reliably only from another Web Service, and not from a standalone client application. This example shows how to create both types of Web Services (source and destination). The `WsrmsSecurityClient.java` class is a standalone Java application that then invokes the source Web Service.

## Overview of the Example

The existing example shows how to provide security functionality on top of reliability for Web Services messaging by creating two WebLogic Web Services:

- Web Service whose operations can be invoked using reliable and secure SOAP messaging (destination endpoint). The destination `ReliableEchoService` Web Service has two operations that can be invoked reliably and in a secure way: `echo` and `echoOneway`.
- Client Web Service that invokes an operation of the first Web Service in a reliable and secure way (source endpoint). The source `ReliableEchoClientService` Web Service has one operation for invoking the `echo` and `echoOneway` operations of the `ReliableEchoService` Web Service reliably and in a secure way within one conversation: `echo`.

The existing example includes functional code and an extensive `instructions.html` file that describes its use and function, how to build it, and so forth. This section does not repeat that information, but instead concentrates on the changes made to the example, and the reasons for the changes.

## How the Example Sets Up WebLogic Security

The `configWSS.py` WLST script sets up security for the WebLogic Server instance that hosts the source and destination Web Service. The security requirements are dictated by the WS-SecurityPolicy files associated with the destination Web Service.



The `Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.0.xml` policy imposes the following requirements:

- WS-SecureConversation handshake is protected by WS-Security 1.0.
- The application messages are signed and encrypted with DerivedKeys.
- The soap:Body of the RequestSecurityToken and RequestSecurityTokenResponseCollection messages (part of the WS-SecureConversation handshake) are both signed and encrypted.
- The WS-Addressing headers are signed.
- Timestamp is included and signed.
- The signature is encrypted.
- The algorithm suite is Basic256.

In response, the `configWSS.py` WLST script performs the following functions:

- Enables X.509 tokens for the default IdentityAsserter in the default security realm.
- Creates the default Web Service security configuration.
- Configures a credential provider for the Security Context Token.
- Configures a credential provider for Derived Key.
- Configures a BinarySecurityTokenHandler token handler for X.509 tokens.
- Configures a ServerBSTCredentialProvider credential provider for X.509 tokens.
- Configures keystores for confidentiality and integrity.
- Configures the PKI credential mapper. This maps the initiator and target resource to a key pair or public certificate

In addition, the `configWSSRuntime.py` WLST script also performs the following functions:

- Sets up the PKI credential mapper (configured by `configWSS.py`) to invoke the destination Web Service.

## Files Used by This Example

The example uses the files shown in [Table 2-12](#). The contents of revised source files are shown in subsequent sections.:

**Table 2-12 Files Used in WSRM/Security Example**

File	Description
build.xml	Ant build file that contains targets for building and running the example.
ReliableEchoClientServiceImpl.java	JWS file that implements the source Web Service that reliably invokes the echoOneWay and echo operation of the ReliableEchoService Web Service in a secure way. This JWS file uses the @ServiceClient annotation to specify the Web Service it invokes reliably.
ReliableEchoServiceImpl.java	JWS file that implements the reliable destination Web Service. This JWS file uses the @Policy annotation to specify a WS-Policy file that contains reliable SOAP messaging assertions.
ws_rm_configuration.py	WLST script that configures a SAF Agent, FileStore, JMS Server, and JMS queue, which are required for reliable SOAP messaging. Execute this script for the WebLogic Server instance that hosts the reliable destination Web Service. The out-of-the-box Examples server has already been configured for the source Web Service that invokes an operation reliably.
configWss.py	WLST script that configures a credential provider for Security Context Token, a credential provider for Derived Key, a credential provider for x.509, KeyStores for Confidentiality and Integrity, and PKI Cred Mapper which are required for secure SOAP messaging. Execute this script for the WebLogic Server instance that hosts the source and destination Web Service. Remember to restart the Weblogic server after executing this script
configWss_Service.py	WLST script that configures a credential provider for Security Context Token, a credential provider for Derived Key, a credential provider for x.509, KeyStores for Confidentiality and Integrity which are required by the server host the destination Web Service for secure SOAP messaging. Execute this script for the WebLogic Server instance that hosts the destination Web Service when the source and destination Web Service are hosted in two servers. Remember to restart the Weblogic server after executing this script.

**Table 2-12 Files Used in WSRM/Security Example**

<b>File</b>	<b>Description</b>
configWssRuntime.py	WLST script that configures a KeyPair Credential for invoking the destination Web Service.
certs/testServerCertTempCert.der	Server-side certificate, used create client-side BinarySecurityToken credential provider.
certs/clientKeyStore.jks	Client-side key store, used to create client-side BinarySecurityToken credential provider.
certs/serverKeyStore.jks	Server-side key store, used to create Server-side BinarySecurityToken credential provider.
WsrSecurityClient.java	Standalone Java client application that invokes the source WebLogic Web Service, that in turn invokes an operation of the ReliableEchoService Web Service in a reliable and secure way.

## Revised ReliableEchoServiceImpl.java

The `ReliableEchoServiceImpl.java` JWS file is the same as that in `WL_HOME\samples\server\examples\src\examples\webservices\wsrm_security\ReliableEchoServiceImpl.java`, with the revised Policy annotation shown in bold.

**Listing 2-19 ReliableEchoServiceImpl.java**

```

@WebService(name = "ReliableEchoPort",
            serviceName = "ReliableEchoService")
@WLHttpTransport(contextPath = "WsrSecurity", serviceUri =
"ReliableEchoService")
@Policies({
    @Policy(uri="policy:Wssp1.2-2007-Wssc1.3-Bootstrap-Wss1.0.xml"),
    @Policy(uri="policy:Reliability1.1_SequenceSTR")}
)

```

You can specify the `@Policy` annotation at both the class- and method- level. In this example, the annotation is used at the class-level to specify the pre-packaged WS-Policy files, which means all public operations of the Web Service are associated with the specified WS-Policy files.

## Revised `configWss.py`

The `ReliableEchoServiceImpl` Web Service does not explicitly invoke any WebLogic Server API to handle the requirements imposed by any associated policy files, nor does this Web Service have to understand which, if any, security providers, tokens, or other such mechanisms are involved.

The script file `configWss.py` uses WLST to create and configure the default Web Service security configuration, `default_wss`, for the active security realm. (The default Web Service security configuration is used by *all* Web Services in the domain unless they have been explicitly programmed to use a different configuration.) Further, this script makes sure that x509 tokens are supported, creates the needed security providers, and so forth.

The `configWss.py` file is the same as that in `WL_HOME\samples\server\examples\src\examples\webservices\wsrm_security\configWss.py`, with the changes shown in bold. The `build.xml` file provides the command input.

### Listing 2-20 `configWss.py`

---

```
:
#Create credential provider for SCT
cpName='default_sct_cp'
wtm=defaultWss.lookupWebserviceCredentialProvider(cpName)
if wtm == None:
    print 'creating new webservice credential provider : ' + cpName
    wtm = defaultWss.createWebserviceCredentialProvider(cpName)
wtm.setClassName('weblogic.wsee.security.wssc.v13.sct.ServerSCCredentialPr
ovider')
    wtm.setTokenType('sct')
    cpm = wtm.createConfigurationProperty('TokenLifeTime')
```

```

    cpm.setValue('43200000')
else:
    print 'found existing bean for: ' + cpName

#Create credential provider for DK
cpName='default_dk_cp'
wtm=defaultWss.lookupWebServiceCredentialProvider(cpName)
if wtm == None:
    wtm = defaultWss.createWebServiceCredentialProvider(cpName)

wtm.setClassName('weblogic.wsee.security.wssc.v13.dk.DKCredentialProvider'
)

    wtm.setTokenType('dk')
    cpm = wtm.createConfigurationProperty('Label')
    cpm.setValue('WS-SecureConversationWS-SecureConversation')
    cpm = wtm.createConfigurationProperty('Length')
    cpm.setValue('16')
else:
    print 'found existing bean for: DK ' + cpName
:

```

---

## Revised configWss\_Service.py

The configWss\_Service.py script is similar to configWss.py, but it is used only when the source and destination Web Service are hosted in two servers.

The configWss\_Service.py file is the same as that in WL\_HOME\samples\server\examples\src\examples\webservices\wrm\_security\configWss\_Service.py, with the changes shown in bold. The build.xml file provides the command input.

### Listing 2-21 configWss\_Service.py

---

```
:
#Create credential provider for SCT
cpName='default_sct_cp'
wtm=defaultWss.lookupWebserviceCredentialProvider(cpName)
if wtm == None:
    print 'creating new webservice credential provider : ' + cpName
    wtm = defaultWss.createWebserviceCredentialProvider(cpName)

wtm.setClassName('weblogic.wsee.security.wssc.v13.sct.ServerSCCredentialPr
ovider')

    wtm.setTokenType('sct')
    cpm = wtm.createConfigurationProperty('TokenLifeTime')
    cpm.setValue('43200000')
else:
    print 'found existing bean for: ' + cpName

#Create credential provider for DK
cpName='default_dk_cp'
wtm=defaultWss.lookupWebserviceCredentialProvider(cpName)
if wtm == None:
    wtm = defaultWss.createWebserviceCredentialProvider(cpName)

wtm.setClassName('weblogic.wsee.security.wssc.v13.dk.DKCredentialProvider'
)

    wtm.setTokenType('dk')
    cpm = wtm.createConfigurationProperty('Label')
    cpm.setValue('WS-SecureConversationWS-SecureConversation')
```

```

        cpm = wtm.createConfigurationProperty('Length')
        cpm.setValue('16')
    else:
        print 'found existing bean for: DK ' + cpName
    :

```

---

## Building and Running the Example

After you have changed the example to use the new policy namespace, follow the steps in the `WL_HOME\samples\server\examples\src\examples\webservices\wsrm_security\instructions.html` file to build and run the example.

There are no changes needed to these steps.

# Proprietary Web Services Security Policy Files (JAX-RPC Only)

Previous releases of WebLogic Server, released before the formulation of the WS-SecurityPolicy specification, used security policy files written under the WS-Policy specification, using a proprietary schema for security policy.

**Notes:** The security policy files written under the Web Services security policy schema are deprecated in this release.

WS-SecurityPolicy 1.2 policy files and proprietary Web Services security policy schema files are not mutually compatible; you cannot define both types of policy file in the same Web Service. If you want to use WS-Security 1.1 features, you must use the WS-SecurityPolicy 1.2 policy file format.

This section describes the set of pre-packaged Web Services security policy schema files included in WebLogic Server. These policy files are all abstract; see [“Abstract and Concrete Policy Files”](#) on page 2-112 for details.

The policy assertions used in these security policy files to configure message-level security for a WebLogic Web Service are based on the assertions described in the December 18, 2002 version of the *Web Services Security Policy Language* (WS-SecurityPolicy) specification. This means that although the exact syntax and usage of the assertions in WebLogic Server are different, they

are similar in meaning to those described in the specification. The assertions are *not* based on later updates of the specification.

The pre-packaged Web Services security policy files are:

- [Auth.xml](#)—Specifies that the client must authenticate itself. Can be used on its own, or together with `Sign.xml` and `Encrypt.xml`.
- [Sign.xml](#)—Specifies that the SOAP messages are digitally signed. Can be used on its own, or together with `Auth.xml` and `Encrypt.xml`.
- [Encrypt.xml](#)—Specifies that the SOAP messages are encrypted. Can be used on its own, or together with `Auth.xml` and `Sign.xml`.
- [Wssc-dk.xml](#)—Specifies that the client and service share a security context when multiple messages are exchanged and that derived keys are used for encryption and digital signatures, as described by the WS-SecureConversation specification.

**Note:** This pre-packaged policy file is meant to be used on its own and *not* together with `Auth.xml`, `Sign.xml`, `Encrypt.xml`, or `Wssc-sct.xml`. Also, Oracle recommends that you use this policy file, rather than [Wssc-sct.xml](#), if you want the client and service to share a security context, due to its higher level of security.

- [Wssc-sct.xml](#)—Specifies that the client and service share a security context when multiple messages are exchanged, as described by the WS-SecureConversation specification.

**Note:** This pre-packaged policy file is meant to be used on its own and *not* together with `Auth.xml`, `Sign.xml`, `Encrypt.xml`, or `Wssc-dk.xml`. Also, Oracle provides this policy file to support the various use cases of the WS-SecureConversation specification; however, Oracle recommends that you use the [Wssc-dk.xml](#) policy file, rather than [Wssc-sct.xml](#), if you want the client and service to share a security context, due to its higher level of security.

## Abstract and Concrete Policy Files

The WebLogic Web Services runtime environment recognizes two slightly different types of security policy files: *abstract* and *concrete*.

**Abstract policy files** do not explicitly specify the security tokens that are used for authentication, encryption, and digital signatures, but rather, the Web Services runtime environment determines the security tokens when the Web Service is deployed. Specifically, this means the `<Identity>` and `<Integrity>` elements (or assertions) of the policy files do not contain a `<SupportedTokens><SecurityToken>` child element, and the `<Confidentiality>` element of the policy file does not contain a `<KeyInfo><SecurityToken>` child element.



If your Web Service is associated with only the pre-packaged policy files, then client authentication requires username tokens. Web Services support only one type of token for encryption and digital signatures (X.509), which means that in the case of the `<Integrity>` and `<Confidentiality>` elements, concrete and abstract policy files end up being essentially the same.

If your Web Service is associated with an abstract policy file and it is published as an attachment to the WSDL (which is the default behavior), the static WSDL file packaged in the Web Service archive file (JAR or WAR) will be slightly different than the dynamic WSDL of the deployed Web Service. This is because the static WSDL, being abstract, does not include specific `<SecurityToken>` elements, but the dynamic WSDL *does* include these elements because the Web Services runtime has automatically filled them in when it deployed the service. For this reason, in the code that creates the JAX-RPC stub in your client application, ensure that you specify the dynamic WSDL or you will get a runtime error when you try to invoke an operation:

```
HelloService service = new HelloService(Dynamic_WSDL);
```

You can specify either the static or dynamic WSDL to the `clientgen` Ant task in this case. See [“Browsing to the WSDL of the Web Service”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC* for information on viewing the dynamic WSDL of a deployed Web Service.

**Concrete policy files** explicitly specify the details of the security tokens at the time the Web Service is programmed. Programmers create concrete security policy files when they know, at the time they are programming the service, the details of the type of authentication (such as using X.509 or SAML tokens); whether multiple private key and certificate pairs from the keystore are going to be used for encryption and digital signatures; and so on.

## Auth.xml

The WebLogic Server `Auth.xml` file, shown below, specifies that the client application invoking the Web Service must authenticate itself with one of the tokens (username or X.509) that support authentication.

Because the pre-packaged Web Services security policy schema files are abstract, there is no specific username or X.509 token assertions in the `Auth.xml` file at development-time. Depending on how you have configured security for WebLogic Server, either a username token, an X.509 token, or both will appear in the actual runtime-version of the `Auth.xml` policy file associated with your Web Service. Additionally, if the runtime-version of the policy file includes an X.509 token and it is applied to a client invoke, then the entire body of the SOAP message is signed.

If you want to specify that *only* X.509, and never username tokens, be used for identity, or want to specify that, when using X.509 for identity, only certain parts of the SOAP message be signed, then you must create a custom security policy file.

### Listing 2-22 Auth.xml

---

```
<?xml version="1.0"?>

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"
  >

  <wssp:Identity/>
</wsp:Policy>
```

## Sign.xml

The WebLogic Server `Sign.xml` file specifies that the body and WebLogic-specific system headers of the SOAP message be digitally signed. It also specifies that the SOAP message include a Timestamp, which is digitally signed, and that the token used for signing is also digitally signed. The token used for signing is included in the SOAP message.

The following headers are signed when using the `Sign.xml` security policy file:

- SequenceAcknowledgement
- AckRequested
- Sequence
- Action
- FaultTo
- From
- MessageID
- RelatesTo
- ReplyTo
- To
- SetCookie

- Timestamp

The WebLogic Server `Sign.xml` file is shown below:

### Listing 2-23 Sign.xml

---

```
<?xml version="1.0"?>

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"

xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
  xmlns:wls="http://www.bea.com/wls90/security/policy/wsee#part"
  >

  <wssp:Integrity>

    <wssp:SignatureAlgorithm URI="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

    <wssp:CanonicalizationAlgorithm
      URI="http://www.w3.org/2001/10/xml-exc-c14n#" />

    <wssp:Target>
      <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1" />
      <wssp:MessageParts
        Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
        wls:SystemHeaders()
      </wssp:MessageParts>
    </wssp:Target>

    <wssp:Target>
      <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1" />
      <wssp:MessageParts
        Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
        wls:SecurityHeader(wsu:Timestamp)
      </wssp:MessageParts>
    </wssp:Target>

    <wssp:Target>
      <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1" />
      <wssp:MessageParts
        Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
        wsp:Body()
      </wssp:MessageParts>
    </wssp:Target>

  </wssp:Integrity>
```

```
<wssp:MessageAge/>
</wsp:Policy>
```

## Encrypt.xml

The WebLogic Server `Encrypt.xml` file specifies that the entire body of the SOAP message be encrypted. By default, the encryption token is *not* included in the SOAP message.

### Listing 2-24 Encrypt.xml

---

```
<?xml version="1.0"?>
<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"
  >
  <wssp:Confidentiality>
    <wssp:KeyWrappingAlgorithm URI="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
    <wssp:Target>
      <wssp:EncryptionAlgorithm
        URI="http://www.w3.org/2001/04/xmlenc#tripleDES-cbc"/>
      <wssp:MessageParts
        Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part"
        wsp:Body()
      </wssp:MessageParts>
    </wssp:Target>
    <wssp:KeyInfo/>
  </wssp:Confidentiality>
</wsp:Policy>
```

## Wssc-dk.xml

Specifies that the client and Web Service share a security context, as described by the WS-SecureConversation specification, and that a derived key token is used. This ensures the highest form of security.

This policy file provides the following configuration:

- A derived key token is used to sign all system SOAP headers, the timestamp security SOAP header, and the SOAP body.

- A derived key token is used to encrypt the body of the SOAP message. This token is different from the one used for signing.
- Each SOAP message uses its own pair of derived keys.
- For both digital signatures and encryption, the key length is 16 (as opposed to the default 32)
- The lifetime of the security context is 12 hours.

If you need to change the default security context and derived key behavior, you will have to create a custom security policy file, described in later sections.

**WARNING:** If you specify this pre-packaged security policy file, you should not also specify any other pre-packaged security policy file.

#### Listing 2-25 Wssc-dk.xml

---

```
<?xml version="1.0"?>

<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"

  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
  utility-1.0.xsd"
  xmlns:wls="http://www.bea.com/wls90/security/policy/wsee#part"
  >

  <wssp:Integrity SupportTrust10="true">
    <wssp:SignatureAlgorithm
  URI="http://www.w3.org/2000/09/xmldsig#hmac-shal"/>
    <wssp:CanonicalizationAlgorithm
  URI="http://www.w3.org/2001/10/xml-exc-c14n#"/>

    <wssp:Target>
      <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <wssp:MessageParts
  Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
        wls:SystemHeaders()
      </wssp:MessageParts>
    </wssp:Target>

    <wssp:Target>
      <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <wssp:MessageParts
  Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
```

## Configuring Message-Level Security

```
        wls:SecurityHeader(wsu:Timestamp)
    </wssp:MessageParts>
</wssp:Target>

<wssp:Target>
    <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmlsig#sha1" />
    <wssp:MessageParts Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
        wsp:Body()
    </wssp:MessageParts>
</wssp:Target>

<wssp:SupportedTokens>
    <wssp:SecurityToken IncludeInMessage="true"
        TokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/dk"
        DerivedFromTokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct">
        <wssp:Claims>
            <wssp:Label>WS-SecureConversationWS-SecureConversation</wssp:Label>
            <wssp:Length>16</wssp:Length>
        </wssp:Claims>
    </wssp:SecurityToken>
</wssp:SupportedTokens>

</wssp:Integrity>

<wssp:Confidentiality SupportTrust10="true">

    <wssp:Target>
        <wssp:EncryptionAlgorithm
URI="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
        <wssp:MessageParts Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
wsp:Body()</wssp:MessageParts>
    </wssp:Target>

    <wssp:KeyInfo>
        <wssp:SecurityToken IncludeInMessage="true"
            TokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/dk"
            DerivedFromTokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct">
            <wssp:Claims>
                <wssp:Label>WS-SecureConversationWS-SecureConversation</wssp:Label>
                <wssp:Length>16</wssp:Length>
            </wssp:Claims>
        </wssp:SecurityToken>
    </wssp:KeyInfo>

</wssp:Confidentiality>

<wssp:MessageAge/>

</wssp:Policy>
```

## Wssc-sct.xml

Specifies that the client and Web Service share a security context, as described by the WS-SecureConversation specification. In this case, security context tokens are used to encrypt and sign the SOAP messages, which differs from [Wssc-dk.xml](#) in which derived key tokens are used. The `wssc-sct.xml` policy file is provided to support all the use cases of the specification; for utmost security, however, Oracle recommends you always use [Wssc-dk.xml](#) when specifying shared security contexts due to its higher level of security.

This security policy file provides the following configuration:

- A security context token is used to sign all system SOAP headers, the timestamp security SOAP header, and the SOAP body.
- A security context token is used to encrypt the body of the SOAP message.
- The lifetime of the security context is 12 hours.

If you need to change the default security context and derived key behavior, you will have to create a custom security policy file, described in later sections.

**WARNING:** If you specify this pre-packaged security policy file, you should not also specify any other pre-packaged security policy file.

### Listing 2-26 Wssc-sct.xml

---

```
<?xml version="1.0"?>
<wsp:Policy
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssp="http://www.bea.com/wls90/security/policy"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
  xmlns:wls="http://www.bea.com/wls90/security/policy/wsee#part"
  >
  <wssp:Integrity SupportTrust10="true">
    <wssp:SignatureAlgorithm
  URI="http://www.w3.org/2000/09/xmldsig#hmac-shal"/>
    <wssp:CanonicalizationAlgorithm
  URI="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  <wssp:Target>
    <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#shal"/>
```

## Configuring Message-Level Security

```
<wssp:MessageParts
Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
  wls:SystemHeaders()
</wssp:MessageParts>
</wssp:Target>

<wssp:Target>
  <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <wssp:MessageParts
Dialect="http://www.bea.com/wls90/security/policy/wsee#part">
  wls:SecurityHeader(wsu:Timestamp)
  </wssp:MessageParts>
</wssp:Target>

<wssp:Target>
  <wssp:DigestAlgorithm URI="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <wssp:MessageParts Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
  wsp:Body()
  </wssp:MessageParts>
</wssp:Target>

<wssp:SupportedTokens>
  <wssp:SecurityToken IncludeInMessage="true"
  TokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct">
  </wssp:SecurityToken>
</wssp:SupportedTokens>

</wssp:Integrity>

<wssp:Confidentiality SupportTrust10="true">

  <wssp:Target>
  <wssp:EncryptionAlgorithm
URI="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
  <wssp:MessageParts Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
wsp:Body() </wssp:MessageParts>
  </wssp:Target>

  <wssp:KeyInfo>
  <wssp:SecurityToken IncludeInMessage="true"
  TokenType="http://schemas.xmlsoap.org/ws/2005/02/sc/sct">
  </wssp:SecurityToken>
  </wssp:KeyInfo>
</wssp:Confidentiality>

  <wssp:MessageAge />

</wssp:Policy>
```



# Configuring Transport-Level Security

Transport-level security refers to securing the connection between a client application and a Web Service with Secure Sockets Layer (SSL) or HTTP Basic authentication, either alone or in combination.

SSL provides secure connections by allowing two applications connecting over a network to authenticate the other's identity and by encrypting the data exchanged between the applications. Authentication allows a server, and optionally a client, to verify the identity of the application on the other end of a network connection. A client certificate (two-way SSL) can be used to authenticate the user.

See [“Secure Sockets Layer \(SSL\)”](#) in *Understanding WebLogic Security* for general information about SSL and the implementations included in WebLogic Server.

The following sections describe how to configure transport-level security for your Web Service:

- [“Configuring Transport-Level Security Through Policy”](#) on page 3-1
- [“Configuring Transport-Level Security Via UserDataConstraint: Main Steps \(JAX-RPC Only\)”](#) on page 3-4
- [“Configuring Two-Way SSL for a Client Application”](#) on page 3-6
- [“Using a Custom SSL Adapter with Reliable Messaging”](#) on page 3-7

## Configuring Transport-Level Security Through Policy

You can specify a policy that requires SSL, HTTP BASIC authentication, or both.

If the policy requires SSL, make sure you configure SSL for the core WebLogic Server security subsystem. You can configure one-way SSL where WebLogic Server is required to present a certificate to the client application, or two-way SSL where both the client applications and WebLogic server present certificates to each other.

To configure two-way or one-way SSL for the core WebLogic Server security subsystem, see [“Configuring SSL”](#) in *Securing WebLogic Server*.

For example, the Oracle-supplied `wssp1.2-2007-Saml2.0-Bearer-Https.xml` policy file includes the following assertion indicating that the policy is expecting a client certificate via SSL, as shown in [Listing 3-1](#).

### Listing 3-1 Specifying SSL in a Policy

---

```
<sp:TransportToken>
<wsp:Policy>
<sp:HttpsToken/>
</wsp:Policy>
</sp:TransportToken>
```

---

If two-way SSL is required, also use the `RequireClientCertificate` assertion, as shown in [Listing 3-2](#).

### Listing 3-2 Two-Way SSL in a Policy

---

```
<sp:TransportToken>
<wsp:Policy>
<sp:HttpsToken >
<wsp:Policy>
<sp:RequireClientCertificate/>
</wsp:Policy>
</sp:HttpsToken>
</wsp:Policy>
</sp:TransportToken>
```

---

The `wsspl.2-2007-Https-BasicAuth.xml` policy file requires both a client certificate via SSL and HTTP BASIC Authentication, as shown in [Listing 3-3](#).

---

### Listing 3-3 SSL and HTTP Basic Authentication in a Policy

---

```
<sp:TransportToken>
<wsp:Policy>
<sp:HttpsToken>
<wsp:Policy>
<sp:HttpBasicAuthentication/>
</wsp:Policy>
</sp:HttpsToken>
</wsp:Policy>
</sp:TransportToken>
```

---

## Configuring Transport-Level Security Through Policy: Main Steps

To configure transport-level Web Services security via one or more policy files:

1. Configure SSL for the core WebLogic Server security subsystem.

You can configure one-way SSL where WebLogic Server is required to present a certificate to the client application, or two-way SSL where both the client applications and WebLogic server present certificates to each other.

To configure two-way or one-way SSL for the core WebLogic Server security subsystem, see [“Configuring SSL”](#) in *Securing WebLogic Server*.

2. Use `@Policy` or `@Policies` JWS annotations in your JWS file, or associate policy files only at runtime using the Administration Console, or specify some policy files using the annotations and then associate additional ones at runtime.
3. If you added `@Policy` or `@Policies` JWS annotations in your JWS file, compile and redeploy your Web Service as part of the normal iterative development process.

See [“Developing WebLogic Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC*

4. When you run the client application that invokes the Web Service, specify certain properties to indicate the SSL implementation that your application should use. In particular:

- To specify the Certicom SSL implementation, use the following properties

```
-Djava.protocol.handler.pkgs=weblogic.net  
-Dweblogic.security.SSL.trustedCAKeyStore=trustStore
```

where *trustStore* specifies the name of the client-side truststore that contains the list of trusted certificates (one of which should be the server's certificate). To disable host name verification, also specify the following property:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

- To specify Sun's SSL implementation, use the following properties:

```
-Djavax.net.ssl.trustStore=trustStore
```

where *trustStore* specifies the name of the client-side truststore that contains the list of trusted certificates (one of which should be the server's certificate). To disable host name verification, also specify the following property:

```
-Dweblogic.wsee.client.ssl.strictHostChecking=false
```

See [“Configuring Two-Way SSL for a Client Application”](#) on page 3-6 for details about two-way SSL.

## Configuring Transport-Level Security Via UserDataConstraint: Main Steps (JAX-RPC Only)

The `UserDataConstraint` annotation requires that the Web Service be invoked using the HTTPS transport.

To configure transport-level Web Services security via the `UserDataConstraint` annotation in your JWS file:

1. Configure SSL for the core WebLogic Server security subsystem.

You can configure one-way SSL where WebLogic Server is required to present a certificate to the client application, or two-way SSL where both the client applications and WebLogic server present certificates to each other.

To configure two-way or one-way SSL for the core WebLogic Server security subsystem, see [“Configuring SSL”](#) in *Securing WebLogic Server*.

2. In the JWS file that implements your Web Service, add the `@weblogic.jws.security.UserDataConstraint` annotation to require that the Web Service be invoked using the HTTPS transport.  
  
For details, see “[weblogic.jws.security.UserDataConstraint](#)” in the *WebLogic Web Services Reference*.
3. Recompile and redeploy your Web Service as part of the normal iterative development process.  
  
See “[Developing WebLogic Web Services](#)” in *Getting Started With WebLogic Web Services Using JAX-RPC*
4. Update the `build.xml` file that invokes the `clientgen` Ant task to use a static WSDL to generate the JAX-RPC stubs of the Web Service, rather than the dynamic deployed WSDL of the service.

The reason `clientgen` cannot generate the stubs from the dynamic WSDL in this case is that when you specify the `@UserDataConstraint` annotation, all client applications are required to specify a truststore, including `clientgen`. However, there is currently no way for `clientgen` to specify a truststore, thus the Ant task must generate its client components from a static WSDL that describes the Web Service in the same way as the dynamic WSDL.

5. When you run the client application that invokes the Web Service, specify certain properties to indicate the SSL implementation that your application should use. In particular:
  - To specify the Certicom SSL implementation, use the following properties

```
-Djava.protocol.handler.pkgs=weblogic.net
-Dweblogic.security.SSL.trustedCAKeyStore=trustStore
```

where `trustStore` specifies the name of the client-side truststore that contains the list of trusted certificates (one of which should be the server’s certificate). To disable host name verification, also specify the following property:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```
  - To specify Sun’s SSL implementation, use the following properties:

```
-Djavax.net.ssl.trustStore=trustStore
```

where `trustStore` specifies the name of the client-side truststore that contains the list of trusted certificates (one of which should be the server’s certificate). To disable host name verification, also specify the following property:

```
-Dweblogic.wsee.client.ssl.strictHostChecking=false
```

See [“Configuring Two-Way SSL for a Client Application”](#) on page 3-6 for details about two-way SSL.

## Configuring Two-Way SSL for a Client Application

If you configured two-way SSL for WebLogic Server, the client application must present a certificate to WebLogic Server, in addition to WebLogic Server presenting a certificate to the client application as required by one-way SSL. You must also follow these requirements:

- Create a client-side keystore that contains the client’s private key and X.509 certificate pair.

The SSL package of J2SE requires that the password of the client’s private key must be the same as the password of the client’s keystore. For this reason, the client keystore can include only *one* private key and X.509 certificate pair.

- Configure the core WebLogic Server’s security subsystem, mapping the client’s X.509 certificate in the client keystore to a user. See [“Configuring a User Name Mapper”](#) in *Securing WebLogic Server*.
- Create a *truststore* which contains the certificates that the client trusts; the client application uses this truststore to validate the certificate it receives from WebLogic Server. Because of the J2SE password requirement described in the preceding bullet item, this truststore must be different from the keystore that contains the key pair that the client presents to the server.

You can use the Cert Gen utility or Sun Microsystem's `keytool` utility to perform this step. For development purposes, the `keytool` utility is the easiest way to get started.

See [“Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities”](#) in *Securing WebLogic Server*.

- When you run the client application that invokes the Web Service, specify the following properties:

```
-Djavax.net.ssl.trustStore=trustStore
-Djavax.net.ssl.trustStorePassword=trustStorePassword
```

where *trustStore* specifies the name of the client-side truststore that contains the list of trusted certificates (one of which should be the server’s certificate) and *trustStorePassword* specifies the truststore’s password.

The preceding properties are in addition to the standard properties you must set to specify the client-side keystore:

- `-Djavax.net.ssl.keyStore=keyStore`
- `-Djavax.net.ssl.keyStorePassword=keyStorePassword`

## Using a Custom SSL Adapter with Reliable Messaging

**Note:** All objects placed into Stub and MessageContext properties must be serializable and externalizable, and must have their implementations available on the server system CLASSPATH. This section describes the specific case of a custom SSLAdapter implementation.

You can use a custom [SSLAdapter](#) implementation to provide client certificates and other services needed to establish SSL connections between client and server when using reliable messaging or buffering. The reliable messaging and buffering subsystems persist the state of a request over an SSL connection. In doing so, they persist the instance of the custom SSLAdapter used to establish the connection.

When the request is restored from persistence, the persistence facility must have access to the custom SSLAdapter class in order to properly restore the custom SSLAdapter object saved with the request. To allow for this, you must provide your custom SSLAdapter class via the server's system CLASSPATH (and not within an application deployed to the server).

The custom SSLAdapter must extend [SSLAdapter](#), and is installed and enabled via the following procedure:

1. Create an instance of
 

```
weblogic.wsee.connection.transport.https.HttpsTransportInfo.
```
2. Set the custom SSL adapter on that transport info by calling
 

```
HttpsTransportInfo.setSSLAdapter(SSLAdapter adapter).
```
3. Set the transport info on the web services stub instance (stub of type
 

```
javax.xml.rpc.Stub
```

) by calling
 

```
stub._setProperty(weblogic.wsee.connection.soap.SoapClientConnection.TRANSPORT_INFO_PROPERTY, ti);
```

Where `stub` is the Web Services stub, and `ti` is the `HttpsTransportInfo` you configured.

If you do not follow this procedure and provide the custom SSLAdapter class on the system CLASSPATH, a `ClassNotFoundException` exception is generated:

```
java.io.IOException: java.lang.ClassNotFoundException:
examples.webservices.client.ServiceBase$TestSSLAdapter
```

## Configuring Transport-Level Security



# Configuring Access Control Security (JAX-RPC Only)

The following sections describe how to configure security for your Web Service:

- [“Configuring Access Control Security: Main Steps”](#) on page 4-1
- [“Updating the JWS File With the Security-Related Annotations”](#) on page 4-4
- [“Updating the JWS File With the @RunAs Annotation”](#) on page 4-6
- [“Setting the Username and Password When Creating the Service Object”](#) on page 4-7

## Configuring Access Control Security: Main Steps

Access control security refers to configuring the Web Service to control the users who are allowed to access it, and then coding your client application to authenticate itself, using HTTP/S or username tokens, to the Web Service when the client invokes one of its operations.

You specify access control security for your Web Service by using one or more of the following annotations in your JWS file:

- `weblogic.jws.security.RolesAllowed`
- `weblogic.jws.security.SecurityRole`
- `weblogic.jws.security.RolesReferenced`
- `weblogic.jws.security.SecurityRoleRef`
- `weblogic.jws.security.RunAs`

**Note:** The `@weblogic.security.jws.SecurityRoles` and `@weblogic.security.jws.SecurityIdentity` JWS annotations were deprecated as of WebLogic Server 9.1.

The following procedure describes the high-level steps to use these annotations to enable access control security; later sections in the chapter describe the steps in more detail.

**Note:** It is assumed in the following procedure that you have already created a JWS file that implements a WebLogic Web Service and you want to update it with access control security. It is also assumed that you use Ant build scripts to iteratively develop your Web Service and that you have a working `build.xml` file that you can update with new information. Finally, it is assumed that you have a client application that invokes the non-secured Web Service. If these assumptions are not true, see:

- [Getting Started With WebLogic Services Using JAX-RPC](#)

1. Update your JWS file, adding the `@weblogic.jws.security.RolesAllowed`, `@weblogic.jws.security.SecurityRole`, `@weblogic.jws.security.RolesReferenced`, or `@weblogic.jws.security.SecurityRoleRef` annotations as needed at the appropriate level (class or operation).

See [“Updating the JWS File With the Security-Related Annotations”](#) on page 4-4.

2. Optionally specify that WebLogic Server internally run the Web Service using a specific role, rather than the role assigned to the user who actually invokes the Web Service, by adding the `@weblogic.jws.security.RunAs` JWS annotation.

See [“Updating the JWS File With the @RunAs Annotation”](#) on page 4-6.

3. Optionally specify that your Web Service can be, or is required to be, invoked using HTTPS by adding the `@weblogic.jws.security.UserDataConstraint` JWS annotation.

See [“Configuring Transport-Level Security Via UserDataConstraint: Main Steps \(JAX-RPC Only\)”](#) on page 3-4 for details. This section also discusses how to update your client application to use SSL.

4. Recompile and redeploy your Web Service as part of the normal iterative development process.

See [“Developing WebLogic Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC*.

5. Using the Administration Console, create valid WebLogic Server users, if they do not already exist. If the mapping of users to roles is external, also use the Administration Console to create the roles specified by the `@SecurityRole` annotation and map the users to the roles.

**Note:** The mapping of users to roles is defined externally if you do *not* specify the `mapToPrincipals` attribute of the `@SecurityRole` annotation in your JWS file to list all users who can invoke the Web Service.

See “[Users, Groups, and Security Roles](#)” in *Securing WebLogic Resources Using Roles and Policies*.

6. Update your client application to use the `HttpTransportInfo` WebLogic API to specify the appropriate user and password when creating the `Service` object.

See “[Setting the Username and Password When Creating the Service Object](#)” on page 4-7.

7. Update the `clientgen` Ant task in your `build.xml` file to specify the username and password of a valid WebLogic user (in the case where your Web Service uses the `@RolesAllowed` annotation) and the trust store that contains the list of trusted certificates, including WebLogic Server’s (in the case you specify `@UserDataConstraint`).

You do this by adding the standard Ant `<sysproperty>` nested element to the `clientgen` Ant task, and set the `key` attribute to the required Java property, as shown in the following example.

**Note:** The example hard-codes the username and password; prompting for both provides more security. You need the username and password for `@RolesAllowed`, and `trustStore` if SSL must be used.

```
<clientgen
  wsdl="http://example.com/myapp/myservice.wsdl"
  destDir="/output/clientclasses"
  packageName="myapp.myservice.client"
  serviceName="StockQuoteService" >
  <sysproperty key="javax.net.ssl.trustStore"
    value="/keystores/DemoTrust.jks"/>
  <sysproperty key="weblogic.wsee.client.ssl.stricthostchecking"
    value="false"/>
  <sysproperty key="javax.xml.rpc.security.auth.username"
    value="juliet"/>
  <sysproperty key="javax.xml.rpc.security.auth.password"
    value="secret"/>
</clientgen>
```

8. Regenerate client-side components and recompile client Java code as usual.

## Updating the JWS File With the Security-Related Annotations

Use the WebLogic-specific `@weblogic.jws.security.RolesAllowed` annotation in your JWS file to specify an array of `@weblogic.jws.security.SecurityRoles` annotations that list the roles that are allowed to invoke the Web Service. You can specify these two annotations at either the class- or method-level. When set at the class-level, the roles apply to all public operations. You can add additional roles to a particular operation by specifying the annotation at the method level.

The `@SecurityRole` annotation has the following two attributes:

- `role`—Name of the role that is allowed to invoke the Web Service.
- `mapToPrincipals`—List of users that map to the role. If you specify one or more users with this attribute, you do not have to externally create the mapping between users and roles, typically using the Administration Console. However, the mapping specified with this attribute applies only within the context of the Web Service.

The `@RolesAllowed` annotation does not have any attributes.

You can also use the `@weblogic.jws.security.RolesReferenced` annotation to specify an array of `@weblogic.jws.security.SecurityRoleRef` annotations that list references to existing roles. For example, if the role `manager` is already allowed to invoke the Web Service, you can specify that the `mgr` role be linked to the `manager` role and any user mapped to `mgr` is also able to invoke the Web Service. You can specify these two annotations only at the class-level.

The `@SecurityRoleRef` annotation has the following two attributes:

- `role`—Name of the role reference.
- `link`—Name of the already-specified role that is allowed to invoke the Web Service. The value of this attribute corresponds to the value of the `role` attribute of a `@SecurityRole` annotation specified in the same JWS file.

The `@RolesReferenced` annotation does not have any attributes.

The following example shows how to use the annotations described in this section in a JWS file, with the relevant sections shown in bold:

```
package examples.webservices.security_roles;
```

```

import javax.jws.WebMethod;
import javax.jws.WebService;

// WebLogic JWS annotations
import weblogic.jws.WLHttpTransport;

import weblogic.jws.security.RolesAllowed;
import weblogic.jws.security.RolesReferenced;
import weblogic.jws.security.SecurityRole;
import weblogic.jws.security.SecurityRoleRef;

@WebService(name="SecurityRolesPortType",
            serviceName="SecurityRolesService",
            targetNamespace="http://example.org")

@WLHttpTransport(contextPath="security",
                 serviceUri="SecurityRolesService",
                 portName="SecurityRolesPort")

@RolesAllowed ( {
    @SecurityRole (role="manager",
                  mapToPrincipals={ "juliet","amanda" }),
    @SecurityRole (role="vp")
} )

@RolesReferenced (
    @SecurityRoleRef (role="mgr", link="manager")
)

/**
 * This JWS file forms the basis of simple Java-class implemented WebLogic
 * Web Service with a single operation: sayHello
 *
 */

public class SecurityRolesImpl {

    @WebMethod()
    public String sayHello(String message) {
        System.out.println("sayHello:" + message);
        return "Here is the message: '" + message + "'";
    }
}

```

```
}
```

The example shows how to specify that only the `manager`, `vp`, and `mgr` roles are allowed to invoke the Web Service. The `mgr` role is actually a reference to the `manager` role. The users `juliet` and `amanda` are mapped to the `manager` role within the context of the Web Service. Because no users are mapped to the `vp` role, it is assumed that the mapping occurs externally, typically using the Administration Console to update the WebLogic Server security realm.

See “[JWS Annotation Reference](#)” in *WebLogic Web Services Reference* for reference information on these annotations.

## Updating the JWS File With the @RunAs Annotation

Use the WebLogic-specific `@weblogic.jws.security.RunAs` annotation in your JWS file to specify that the Web Service is always run as a particular role. This means that regardless of the user who initially invokes the Web Service (and the role to which the user is mapped), the service is internally executed as the specified role.

You can set the `@RunAs` annotation only at the class-level. The annotation has the following attributes:

- `role`—Role which the Web Service should run as.
- `mapToPrincipal`—Principal user that maps to the role.

The following example shows how to use the `@RunAs` annotation in a JWS file, with the relevant sections shown in bold:

```
package examples.webservices.security_roles;

import javax.jws.WebMethod;
import javax.jws.WebService;

// WebLogic JWS annotations
import weblogic.jws.WLHttpTransport;

import weblogic.jws.security.RunAs;

@WebService(name="SecurityRunAsPortType",
            serviceName="SecurityRunAsService",
            targetNamespace="http://example.org")
```

```

@WLHttpTransport(contextPath="security_runas",
                 serviceUri="SecurityRunAsService",
                 portName="SecurityRunAsPort")

@RunAs (role="manager", mapToPrincipal="juliet")

/**
 * This JWS file forms the basis of simple WebLogic
 * Web Service with a single operation: sayHello
 *
 */

public class SecurityRunAsImpl {

    @WebMethod()
    public String sayHello(String message) {
        System.out.println("sayHello:" + message);
        return "Here is the message: '" + message + "'";
    }
}

```

## Setting the Username and Password When Creating the Service Object

When you use the `@RolesAllowed` JWS annotation to secure a Web Service, only the specified roles are allowed to invoke the Web Service operations. This means that you must specify the username and password of a user that maps to the role when creating the `Service` object in your client application that invokes the protected Web Service.

WebLogic Server provides the `HttpTransportInfo` class for setting the username and password and passing it to the `Service` constructor. The following example is based on the standard way to invoke a Web Service from a standalone Java client (as described in [“Invoking Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC*) but also shows how to use the `HttpTransportInfo` class to set the username and password. The sections in bold are discussed after the example.

```

package examples.webservices.sec_wsdl.client;

import weblogic.wsee.connection.transport.http.HttpTransportInfo;

import java.rmi.RemoteException;

```

## Configuring Access Control Security (JAX-RPC Only)

```
import javax.xml.rpc.ServiceException;
import javax.xml.rpc.Stub;

/**
 * This is a simple standalone client application that invokes the
 * the <code>sayHello</code> operation of the SecWsdService Web service.
 *
 * @author Copyright © 1996, 2008, Oracle and/or its affiliates.
 * All rights reserved.
 */

public class Main {

    public static void main(String[] args)
        throws ServiceException, RemoteException{

        HttpTransportInfo info = new HttpTransportInfo();
        info.setUsername("juliet".getBytes());
        info.setPassword("secret".getBytes());

        SecWsdService service = new SecWsdService_Impl(args[0] + "?WSDL",
info);
        SecWsdPortType port = service.getSecWsdPort();

        try {
            String result = null;
            result = port.sayHello("Hi there!");
            System.out.println( "Got result: " + result );
        } catch (RemoteException e) {
            throw e;
        }
    }
}
```

The main points to note in the preceding example are as follows:

- Import the `HttpTransportInfo` class into your client application:

```
import weblogic.wsee.connection.transport.http.HttpTransportInfo;
```

- Use the `setXXX()` methods of the `HttpTransportInfo` class to set the username and password:



```
HttpTransportInfo info = new HttpTransportInfo();
info.setUsername("juliet".getBytes());
info.setPassword("secret".getBytes());
```

In the example, it is assumed that the user `juliet` with password `secret` is a valid WebLogic Server user and has been mapped to the role specified in the `@RolesAllowed` JWS annotation of the Web Service.

If you are accessing a Web Service using a proxy, the Java code would be similar to:

```
HttpTransportInfo info = new HttpTransportInfo();
Proxy p = new Proxy(Proxy.Type.HTTP, new InetSocketAddress(proxyHost,
Integer.parseInt(proxyPort)));
info.setProxy(p);
info.setProxyUsername(user.getBytes());
info.setProxyPassword(pass.getBytes());
```

- Pass the `info` object that contains the username and password to the `Service` constructor as the second argument, in addition to the standard WSDL first argument:

```
SecWsdService service = new SecWsdService_Impl(args[0] + "?WSDL",
info);
```

See [“Invoking Web Services”](#) in *Getting Started With WebLogic Web Services Using JAX-RPC* for general information about invoking a non-secured Web Service.

## Configuring Access Control Security (JAX-RPC Only)