12

Service Bus Security

Objectives

After completing this lesson, you should be able to:

- Describe security concepts
- Compare transport-level and message-level security standards
- Describe Oracle Service Bus security features
- Use Service Bus and OWSM to secure web services
- Describe and assign access control policies to services

Agenda

- Security concepts
  - Transport-level versus message-level security
  - WS-Policy and WS-Security
  - SAML security token
- Oracle WSM security
  - Oracle WSM concepts
  - Securing services with OWSM policies
- Access control policies

Web Services Security: Overview

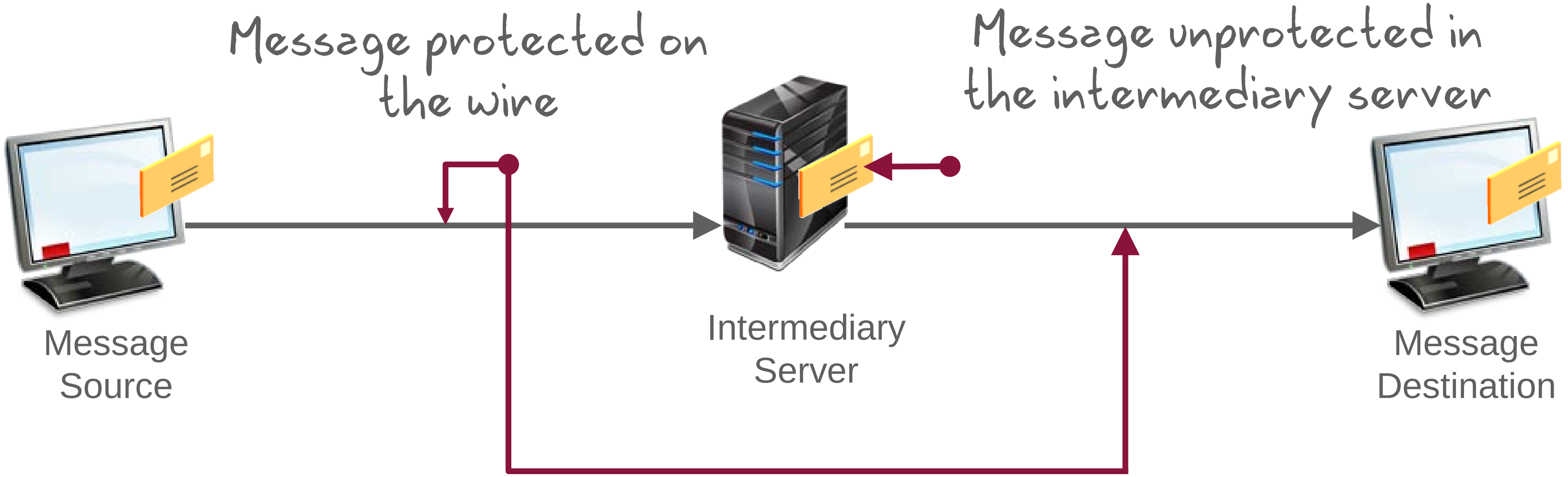
To secure your web service, you need to configure one or two different types of security:

- Transport-level security: Secures connections between service consumer and provider
- Message-level security: Secures a message throughout its journey between the sender and the intended recipient
- Access control security: Specifies which roles are allowed to access what web services

Transport-Level Security

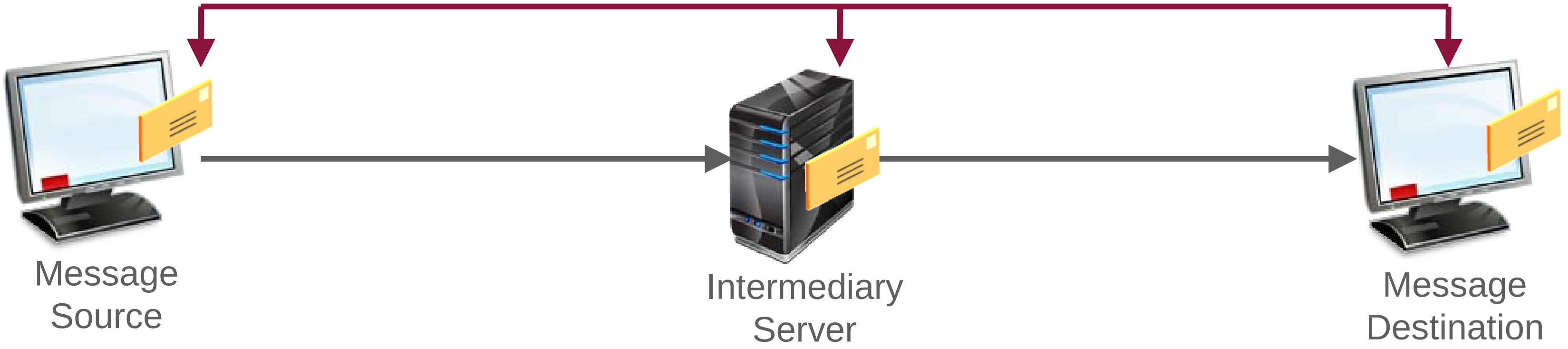
Transport-level security uses protocol-dependent security standards:

- HTTPS (HTTP over SSL)
- JMS over SSL
- SFTP


Message protected on the wire
Message unprotected in the intermediary server
Message Source
Intermediary Server
Message Destination

Message Security

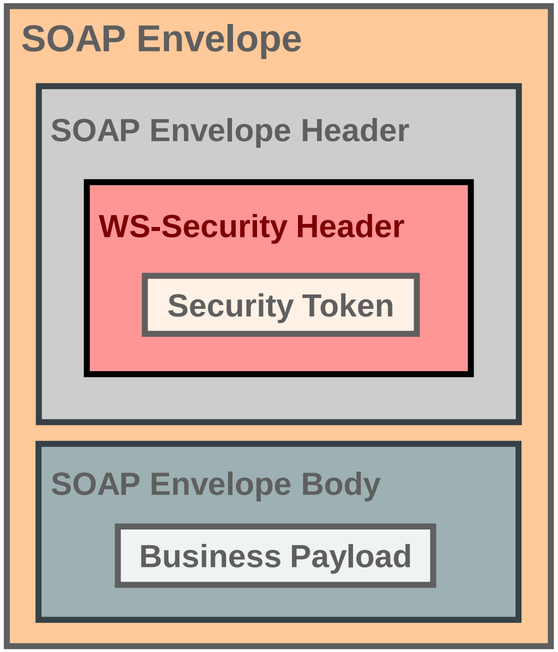
- Uses transport-independent security standards:
  - XML encryption
  - XML digital signatures
  - Web services security
- Has the ability to secure only portions of a message for better performance



Message signed and encrypted, and completely protected on the wire and the intermediaries

WS-Security

- Defines how to attach XML Signature and XML Encryption headers to SOAP messages
- Supports multiple security tokens for authentication:
  - Username/password
  - X.509 certificate
  - Kerberos ticket
  - SAML



SAML

Security Assertion Markup Language (SAML):

- An open framework for sharing security information on the Internet through XML documents
- The dominant standard for federated identity
- A protocol that does not define any new approaches to authentication/authorization (It simply generates appropriate tokens/assertions after authentication occurs.)

SAML Architecture

SAML includes three parts:

- **Assertions:** How you define authentication and authorization information
- **Protocol:** How you ask (SAML `Request`) and get (SAML `Response`) the assertions you need
- **Bindings and Profiles:** How SAML assertions ride “on” (bindings) and “in” (profiles) industry-standard transport and messaging frameworks

WS-Security and SAML

- WS-Security and SAML work together:
  - WS-Security defines how you insert the information into a SOAP envelope.
  - SAML defines what the security information is.
  - WS-Security allows SAML assertions to be placed inside a SOAP header.
- SAML Token Profile 1.1 specifies how SAML assertions can be used for web services security.

WS-Policy: Overview

WS-Policy:

- Provides a model and syntax for describing web service policies
- Enables security policies to be advertised in the WSDL
- Is broken up into several subsidiary specifications:
  - WS-Policy: Defines a grammar that explains web services policies
  - WS-PolicyAttachment: Associates policies to web services
  - WS-PolicyAssertions: Defines a set of general policy assertions

Policy Assertion

- A policy assertion:
  - Is a basic unit representing an individual requirement in a policy
  - Is domain specific (security, reliability)
- Service providers use a policy assertion to convey a condition under which they offer a web service.
- An example of policy expression:

```
<Policy>
  <sp:SamlToken sp:IncludeToken="http://schemas.xmlsoap.org/ws/
    2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
     <wsp:Policy>
          <sp:WssSamlV11Token10 />
     </wsp:Policy>
  </sp:SamlToken>
</Policy>
```

Quiz

Which of the listed options is not correct for the following statement?

“SAML is built upon several existing standards, such as___________.”

a. XML
b. XML Schema
c. XSLT
d. XML Signature
e. XML Encryption
f. HTTP

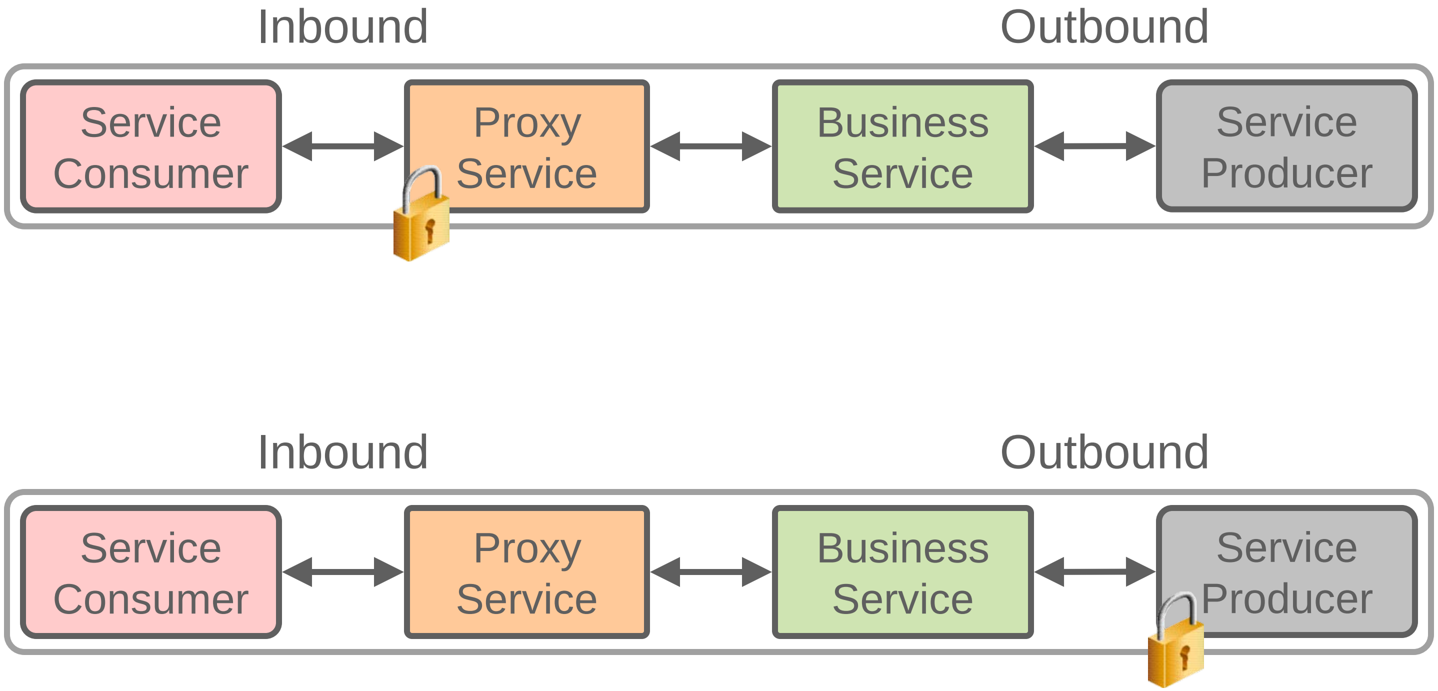
Agenda

- Security concepts
- Oracle WSM security
  - Oracle WSM concepts
  - Securing services with OWSM policies
- Access control policies

SB Security Capabilities

- Integrate with Oracle Web Services Manager (OWSM) and Oracle Platform Security Services (OPSS)
- Enforce transport and/or message security technologies:
  - Authentication
  - Confidentiality
  - Integrity
- Inbound security
- Outbound security
- Propagate security identity
- Bridge different security technologies

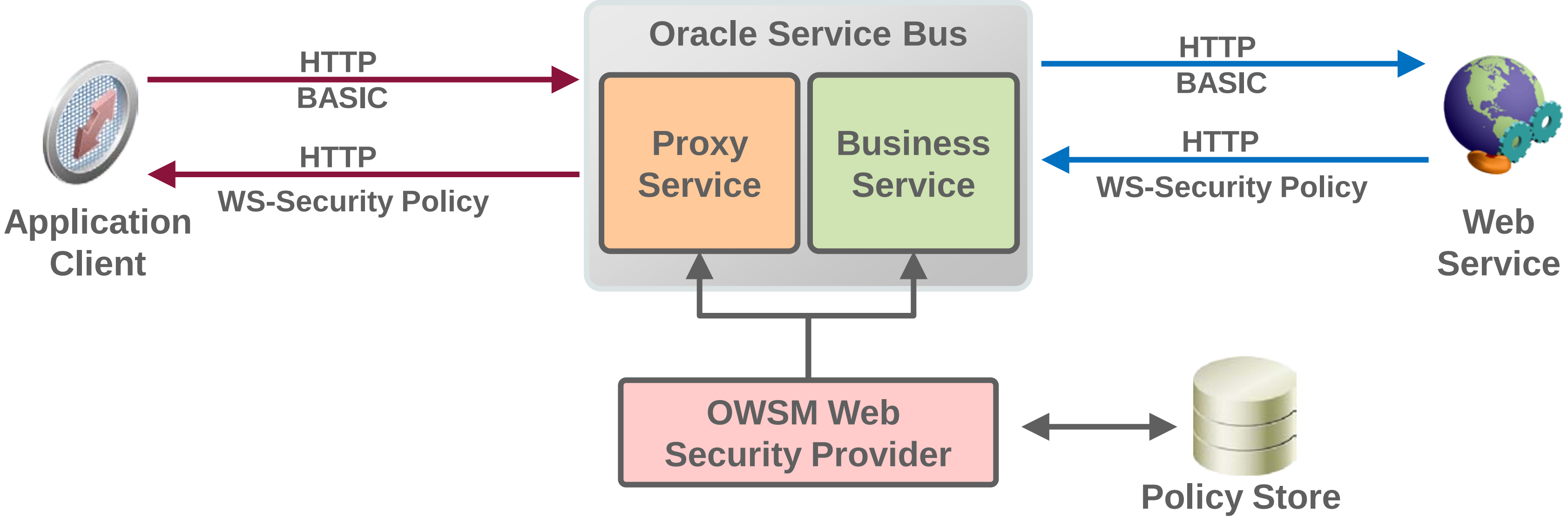
Active and Passive Intermediary



🔒 = Authentication, Authorization, Confidentiality

Securing Services with OWSM Policies

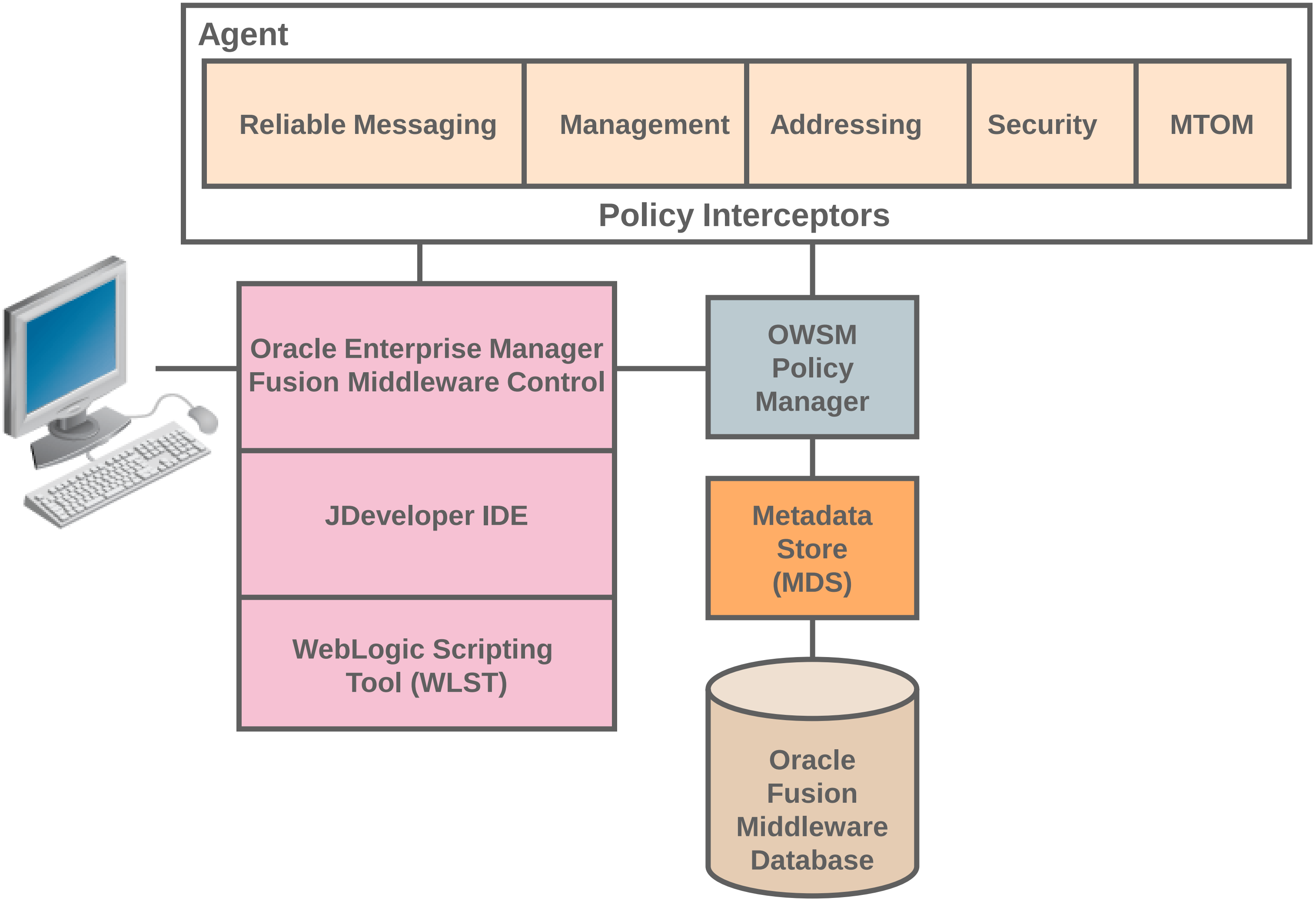
In Service Bus 12*c*, you can secure web services by using OWSM policies.



Oracle Web Service Manager

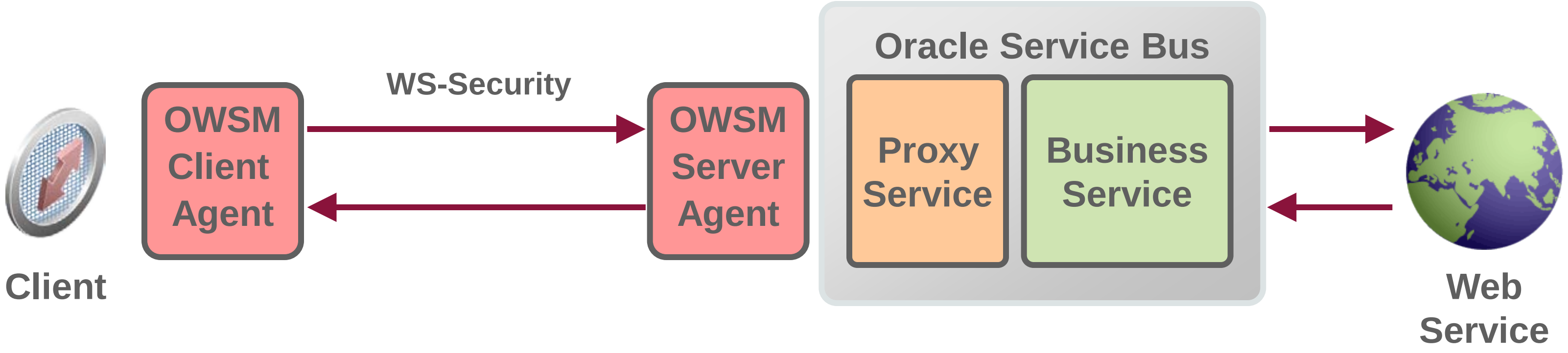
- Oracle Web Service Manager (OWSM) is a security and management system that provides a common security infrastructure for web services applications.
- The Oracle Web Service Manager is based on three main operations:
  - Define
  - Enforce
  - Monitor

Components of Oracle Web Services Manager Architecture



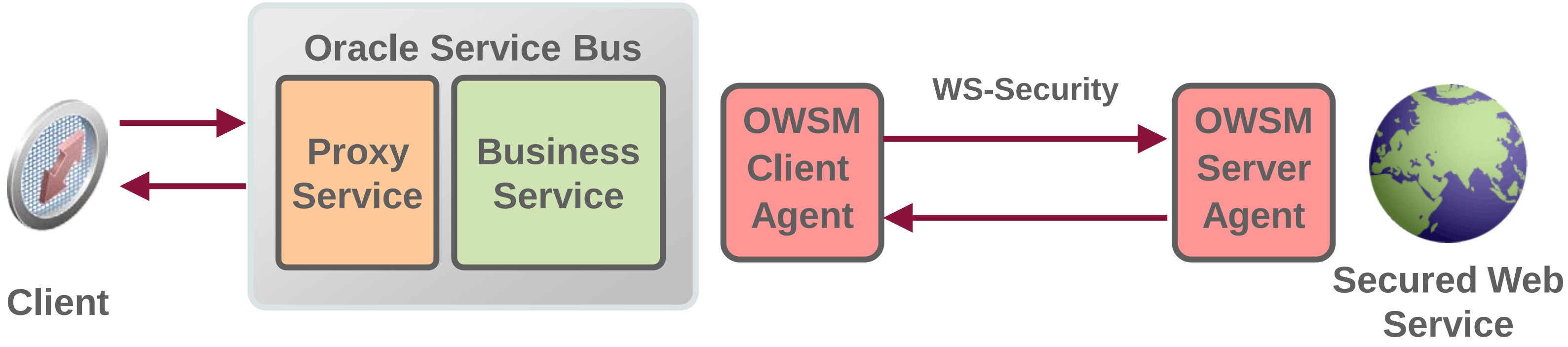
Inbound Security by Using OWSM

A secured communication between a client and a proxy service by using OWSM agents



Outbound Security by Using OWSM

A secured communication between a business service and a web service by using OWSM agents



Policy Support (12*c* 12.1.3.0)

- The following policies are supported:
  - WS-Policy 1.2 (default) and 1.5
  - WS-Security Policy 1.1 (default), 1.2, and 1.3
  - WS-Security: X.509 Token Profile 1.1
  - WS-Security: SAML Token Profile 1.1 (with SAML 2.0)
  - …and more
- The following policies are not supported:
  - Transport policies (HTTPS/SSL, SAML Bearer over SSL)

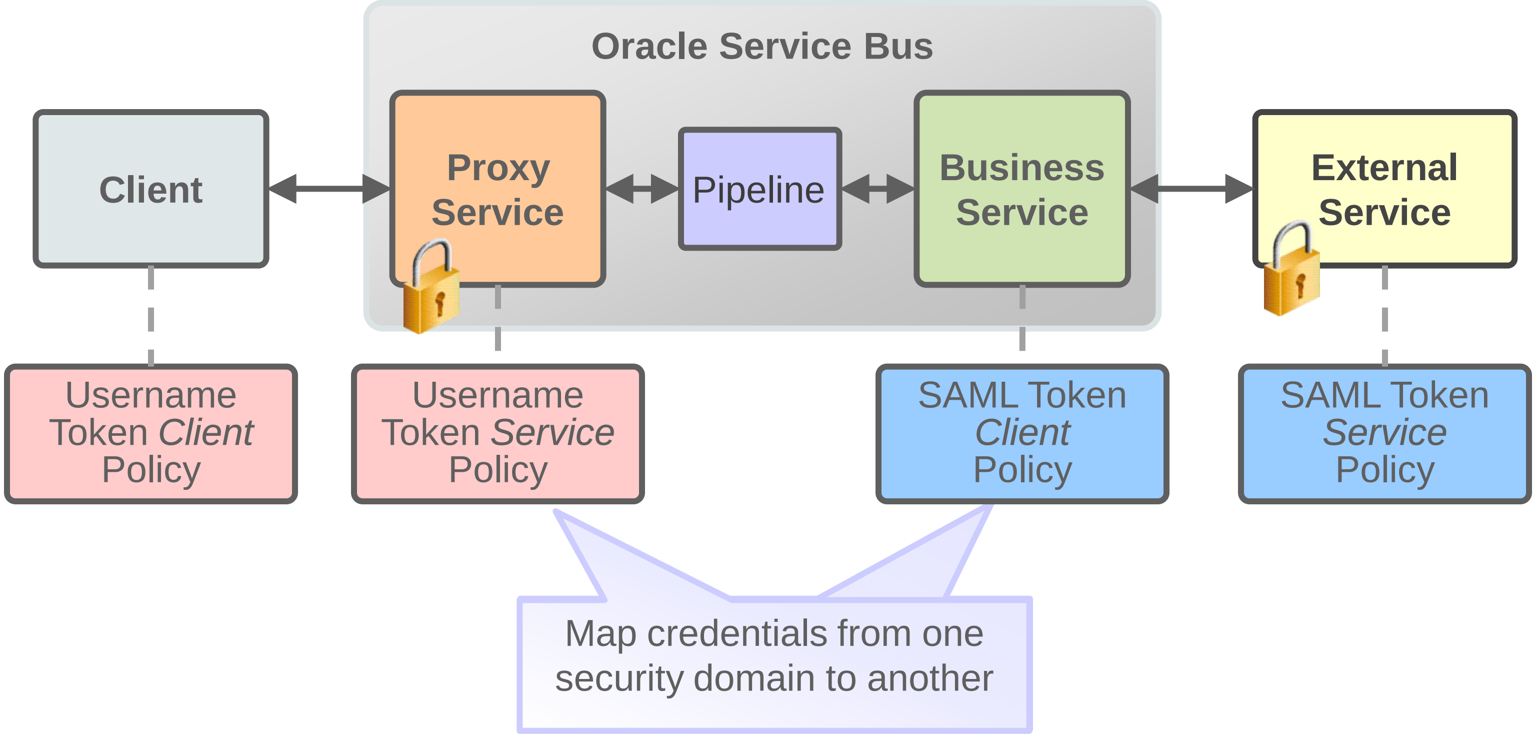
User Interface (UI) Support

Feature	SB Console	JDeveloper	FMW Console
Author OWSM policy			✓
Export custom OWSM policy			✓
Import OWSM policy			✓
Browse OWSM policies from a central policy store	✓	✓	✓
Attach/detach a OWSM policy to/from a proxy or business service	✓	✓	
Set policy overrides/configuration for service	✓	✓	
View currently attached OWSM policy on proxy/business service	✓	✓	
View effective WSDL that embeds OWSM policies	✓	✓	
View security statistics	✓		
View audit logs			✓

Identity Propagation

- Identity Propagation: The mechanism to pass identity in the chain of interacting services.
- Service Bus's support for identity propagation includes:
  - Authenticate and authorize clients of the service bus
  - Pass security context through to service producers unchanged
  - Map credentials from one security domain to another

Identity Propagation: Example

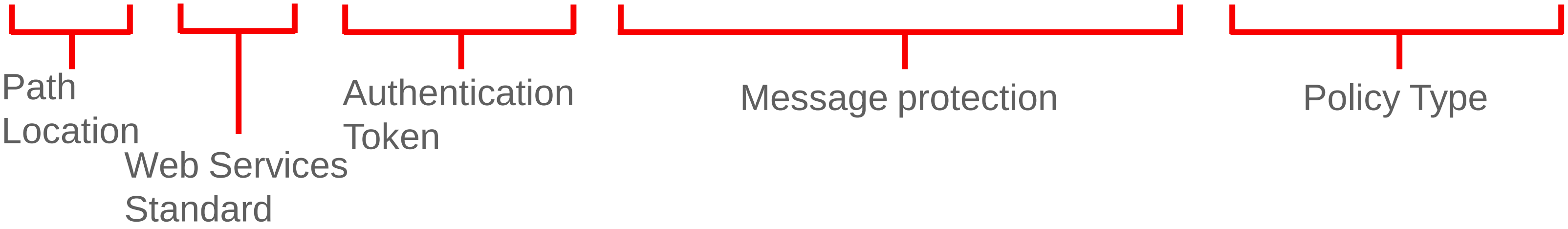

Oracle Service Bus
Client
Proxy Service
Pipeline
Business Service
External Service
Username Token *Client* Policy
Username Token *Service* Policy
SAML Token *Client* Policy
SAML Token *Service* Policy

Map credentials from one security domain to another

OWSM Predefined Policies

- A set of predefined policies are available by default.
- You can directly attach these predefined policies to your web services or clients.
- The naming conventions for security policies:

```
oracle/wss10_saml_token_with_message_protection_service_policy
```



Path Location

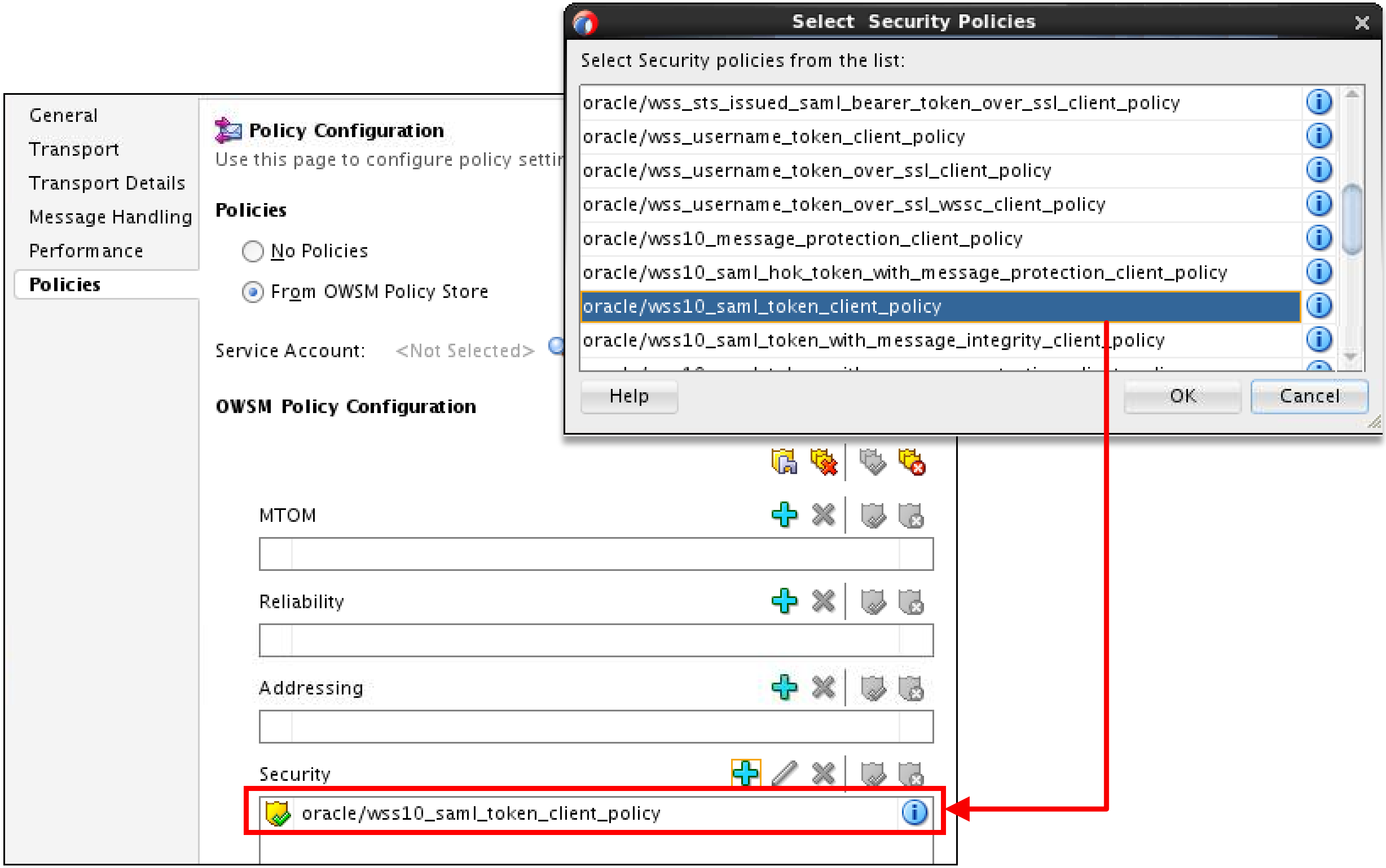
Web Services Standard

Authentication Token

Message protection

Policy Type

Applying OWSM Policies to Services in JDeveloper



Policy Configuration

Use this page to configure policy setti

Policies

○ No Policies

● From OWSM Policy Store

Service Account: <Not Selected>

OWSM Policy Configuration

MTOM

Reliability

Addressing

Security

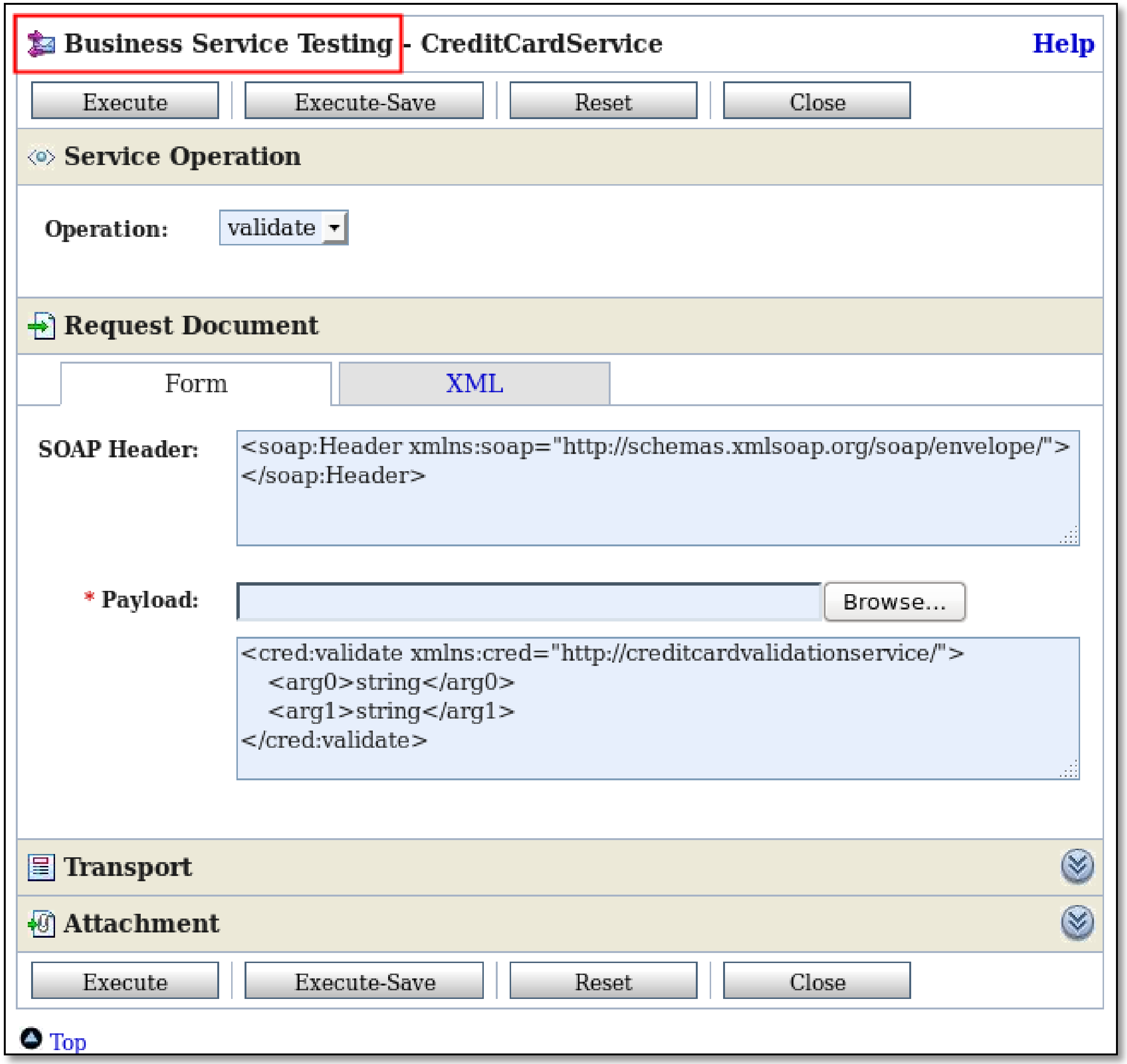
oracle/wss10_saml_token_client_policy

Select Security Policies

Select Security policies from the list:

- oracle/wss_sts_issued_saml_bearer_token_over_ssl_client_policy
- oracle/wss_username_token_client_policy
- oracle/wss_username_token_over_ssl_client_policy
- oracle/wss_username_token_over_ssl_wssc_client_policy
- oracle/wss10_message_protection_client_policy
- oracle/wss10_saml_hok_token_with_message_protection_client_policy
- oracle/wss10_saml_token_client_policy
- oracle/wss10_saml_token_with_message_integrity_client_policy

Test Console Support: Business Service



Operation: validate

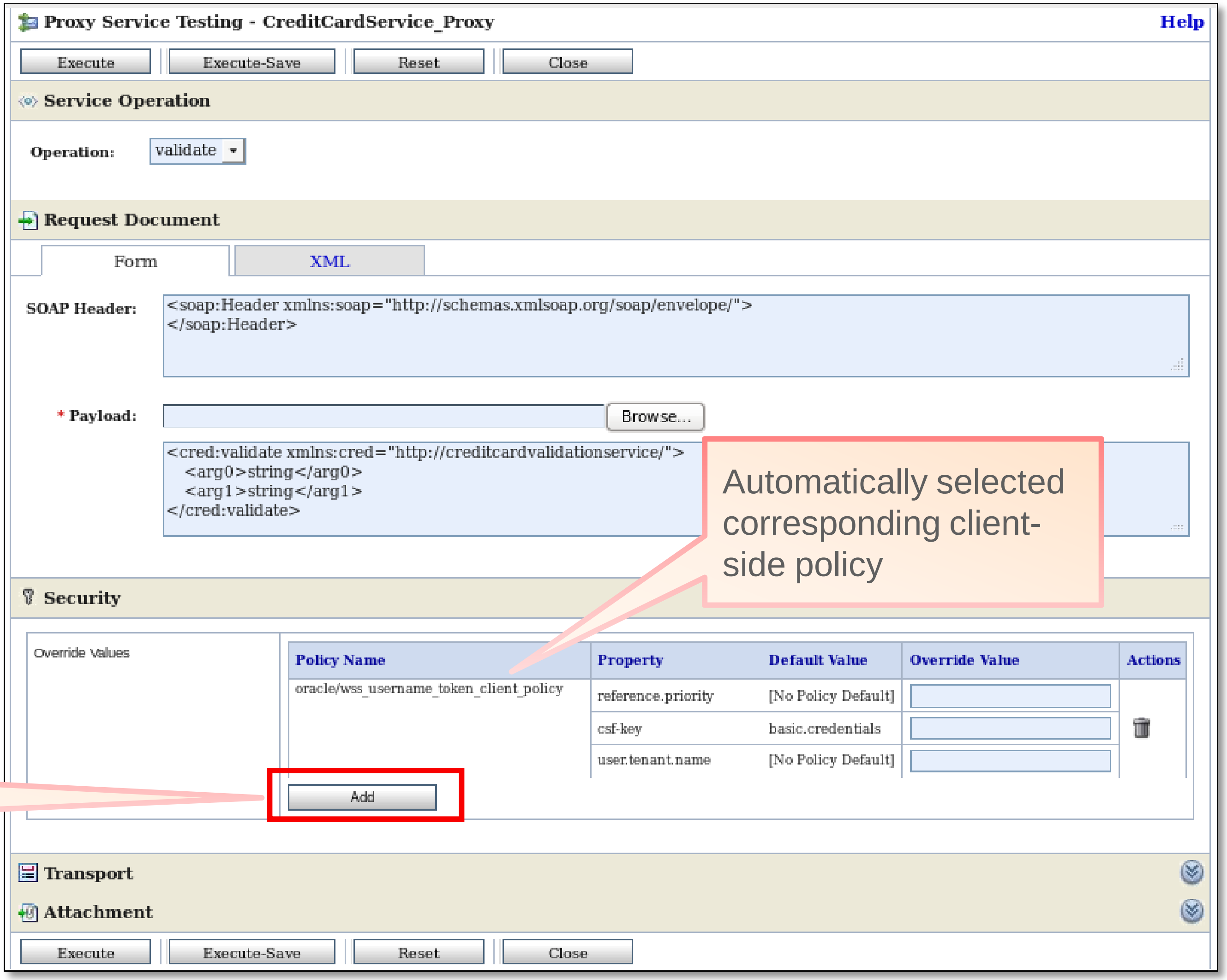
SOAP Header:

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

* Payload:

```
<cred:validate xmlns:cred="http://creditcardvalidationservice/">
   <arg0>string</arg0>
   <arg1>string</arg1>
</cred:validate>
```

Test Console Support: Proxy Service



Proxy Service Testing - CreditCardService_Proxy

Service Operation

Operation: validate

Request Document

SOAP Header:

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

* **Payload:**

```
<cred:validate xmlns:cred="http://creditcardvalidationservice/">
   <arg0>string</arg0>
   <arg1>string</arg1>
</cred:validate>
```

Security

Override Values

Policy Name	Property	Default Value	Override Value	Actions
oracle/wss_username_token_client_policy	reference.priority	[No Policy Default]		
	csf-key	basic.credentials		🗑
	user.tenant.name	[No Policy Default]		

Transport

Attachment

Automatically selected corresponding client-side policy

Click to change the policy

Agenda

- Security concepts
- Oracle WSM security
- Access control policies

Service Access Control Policies

- Policies determine which clients are authorized to access a proxy service, based on:
  - Role membership
  - Any of the conditions available to roles
- By default, all clients are granted access to a service.
- SOAP proxy services also support operation-level access policies if they are active intermediaries:
  - Configured to process WS-Security
  - Assigned a WS-Policy that requires authentication

Role-Based Access: Application Security Roles

Application security roles are divided into three access types:

- Resource Management
- Administration Functions
- Session Management

Summary

In this lesson, you should have learned how to:

- Describe security concepts
- Compare transport-level and message-level security standards
- Describe Oracle Service Bus security features
- Use Service Bus and OWSM to secure web services
- Describe and assign access control policies to services

Practice 12: Propagating Identity from Service Bus to a Web Service

This practice covers the following topics:

12-1: Configuring the Security Environment

12-2: Securing Back-end Web Service and Attaching Security Policy to Business Service

12-3: Applying a Security Policy to Proxy Service