

Securing Composite Applications and Invoking Secured Services

Objectives

After completing this lesson, you should be able to:

- Describe Web Service Security
- Describe Oracle Web Services Manager and its use in securing SOA composites
- Discuss security and identity propagation in SOA composites
- Attach security policies to endpoints at design time and run time



Agenda

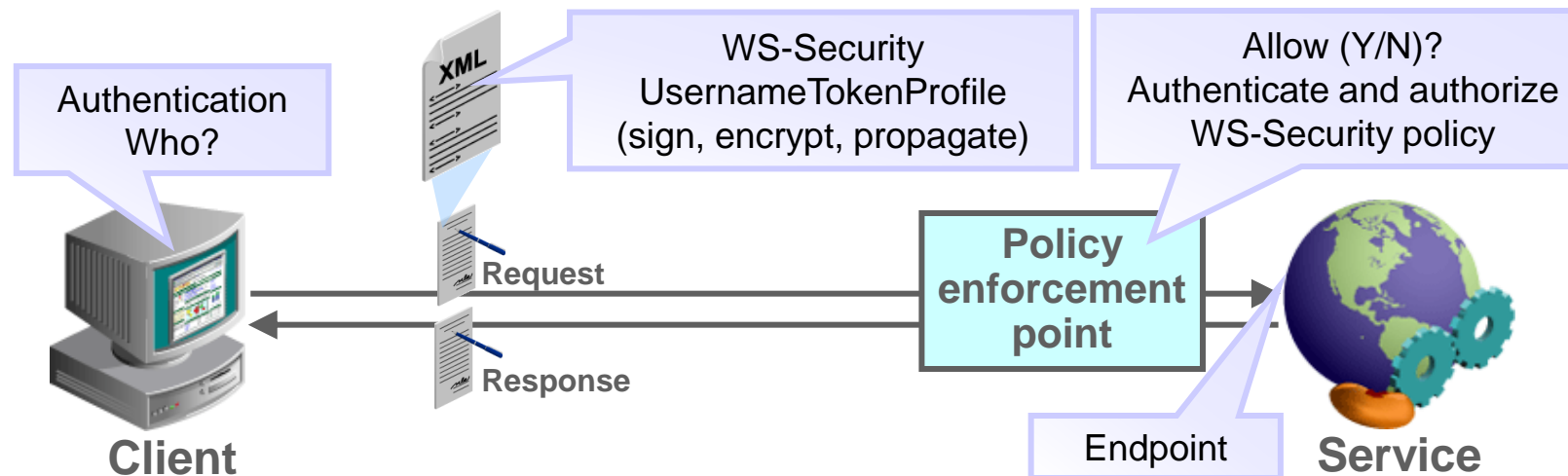
- Web Service Security
- Oracle Web Services Manager
- Securing Composite Applications



Web Service Security: Introduction

Securing web services by using WS-Security standards:

- Supported by WS-Security policy standards, among others
- Applied to service endpoints to provide:
 - Authentication and authorization
 - Signing and encrypting the whole message or parts thereof
 - Integrity (reliable messaging), confidentiality, and propagation of credentials



Web Service Security: Introduction

WS-Security (WSS) 1.0 and 1.1 standards enable:

- Authenticating in multiple ways with security tokens
- Associating different identities with service requests
- Signing or encrypting the whole message body, or a single XML element of the body payload
- Adding credentials in the SOAP header, as in this example:

```
<soap:Envelope xmlns:soap="..." xmlns:wsse="...">
  <soap:Header> ...
    <wsse:Security>
      <wsse:UsernameToken>
        <wsse:Username>jcooper</wsse:Username>
        <wsse:Password>welcome1</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security> ...
  </soap:Header> ...
</soap:Envelope>
```

Security
token

Securing Endpoints: Examples

Policy name is used to enforce assertions.

```
<service name="receiveOrder" ui:wsdlLocation="receiveOrder.wsdl">
  <interface.wsdl interface=".../receiveOrder#wsdl.interface(execute)"/>
  <binding.ws port=".../receiveOrder#wsdl.endpoint(receiveOrder/execute)">
    <wsp:PolicyReference URI="oracle/wss_username_token_service_policy"
      orawsp:category="security" orawsp:status="enabled"/>
  </binding.ws> </service>
```

In composite.xml, security policies are attached in the bindings of service endpoints.

Security policies are also attached in the bindings of external reference endpoints.

```
<reference name="getCreditCardStatus" ... >
  <interface.wsdl interface=".../getStatusByCC#wsdl.interface(execute)"/>
  <binding.ws
    port="... /getStatusByCC#wsdl.endpoint(getStatusByCC/execute_pt)"
    location="... /validationForCC/getStatusByCC?WSDL">
    <wsp:PolicyReference URI="oracle/wss11_saml_token_client_policy"
      orawsp:category="security" orawsp:status="enabled"/>
  </binding.ws> </reference>
```

Quiz



Authentication can be incorporated by using _____ .

- a. Signature
- b. Security tokens
- c. Encryption



Agenda

- Web Service Security
- **Oracle Web Services Manager**
- Securing Composite Applications

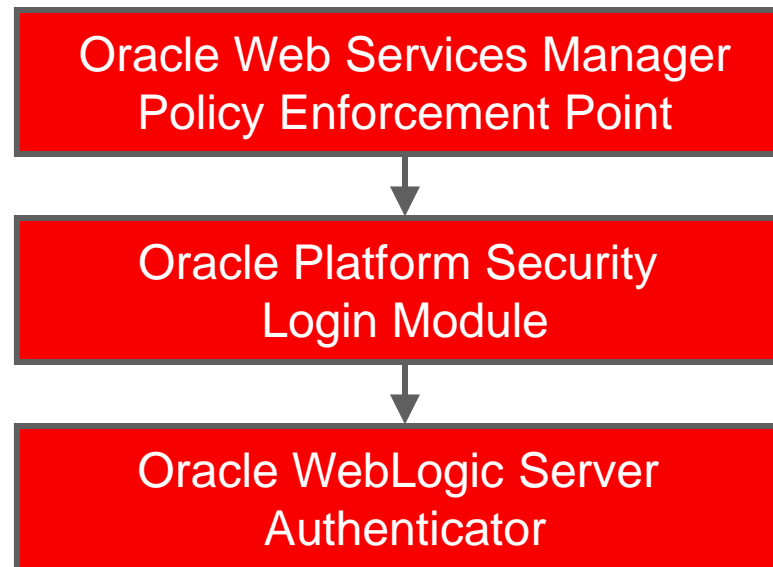


Oracle Web Services Manager

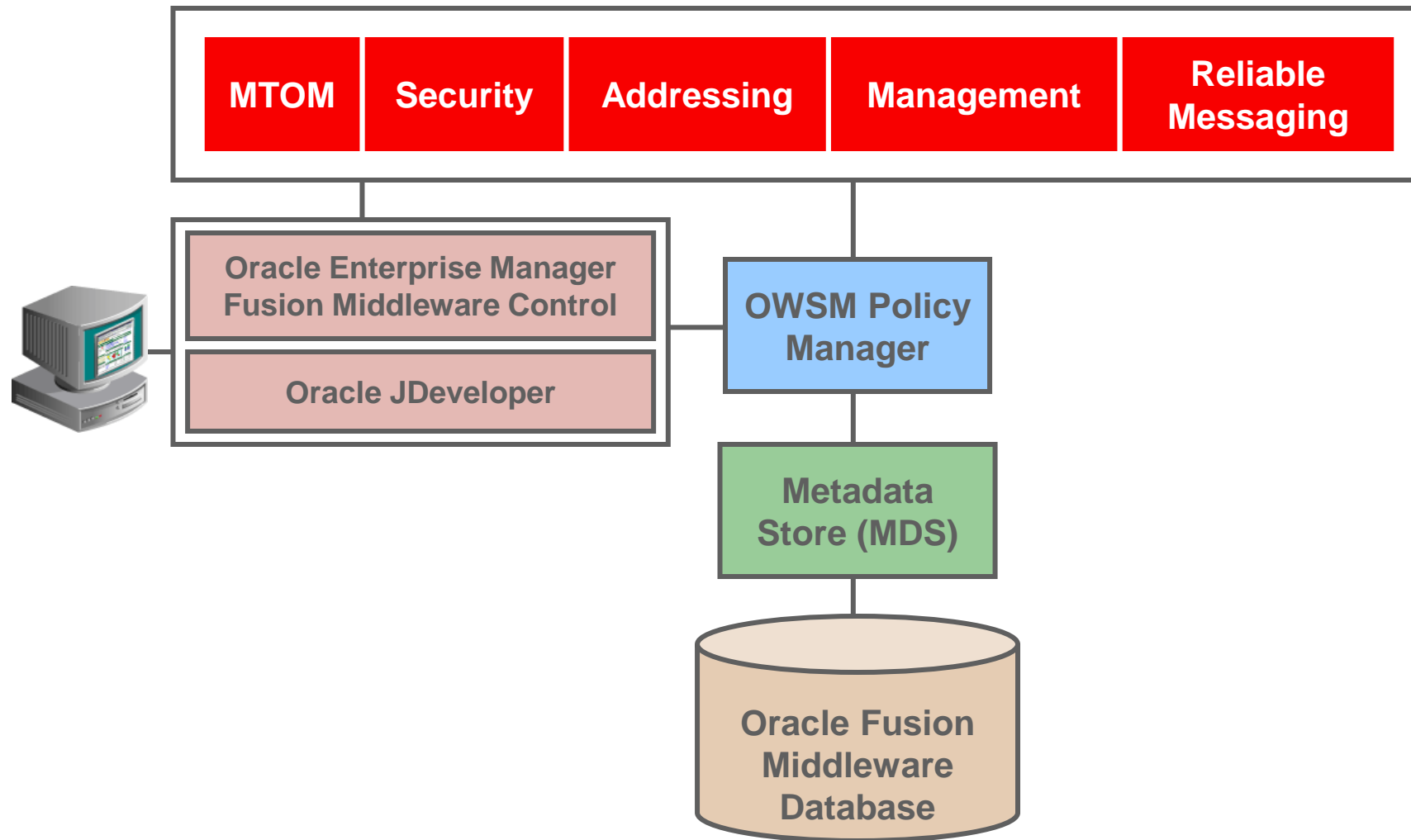
- Oracle Web Services Manager (OWSM) is a security and management system that provides a common security infrastructure for web services applications.
- OWSM is based on three main operations:
 - Define
 - Enforce
 - Monitor

OWSM Policy Framework

- Provides a policy framework to manage and secure web services consistently
- Is built by using the WS-Policy standard and leverages the OPSS Login Module and the Oracle WebLogic Server authenticator for authentication and authorization



Components of Oracle Web Services Manager Architecture



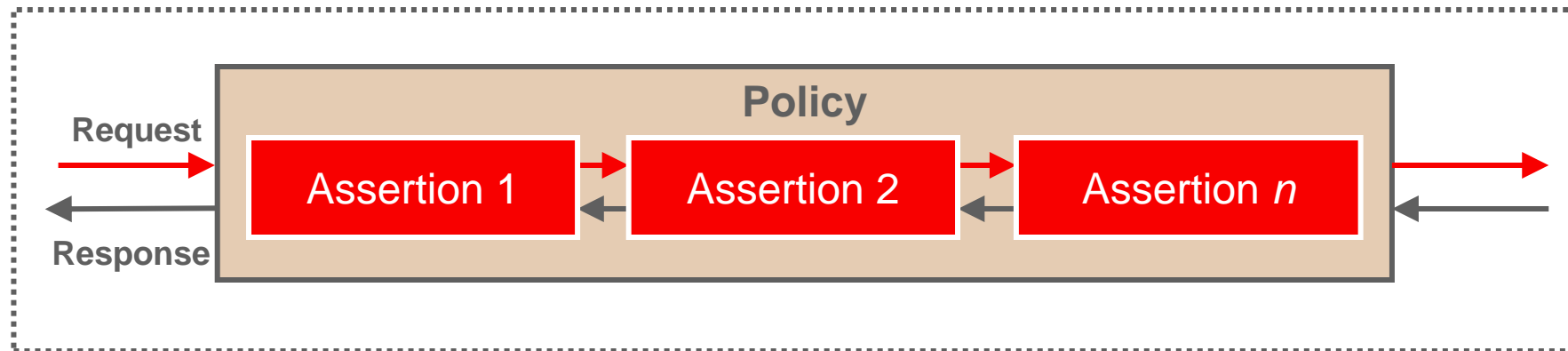
Policies: Introduction

Policies describe the capabilities and requirements of a web service. The different types of policies that are supported in Oracle Fusion Middleware 12c are:

- WS-ReliableMessaging
- Management
- WS-Addressing
- Security
- Message Transmission Optimization Mechanism (MTOM)

Policy Assertions

- OWSM policies contain one or more assertions that exhibit a particular behavior.
- Assertions are executed in the order in which they are listed in the policy.



Types of Security Tokens

Security tokens are used to convey credential information to services. The security tokens that are supported are:

- UsernameToken: With plain type and digest password
- BinarySecurityToken: For embedding certificates
- EncryptedData: For representing a SOAP node or attachment, which is encrypted

Note: SAML is used to exchange authentication and authorization data, such as sending security tokens between security domains.

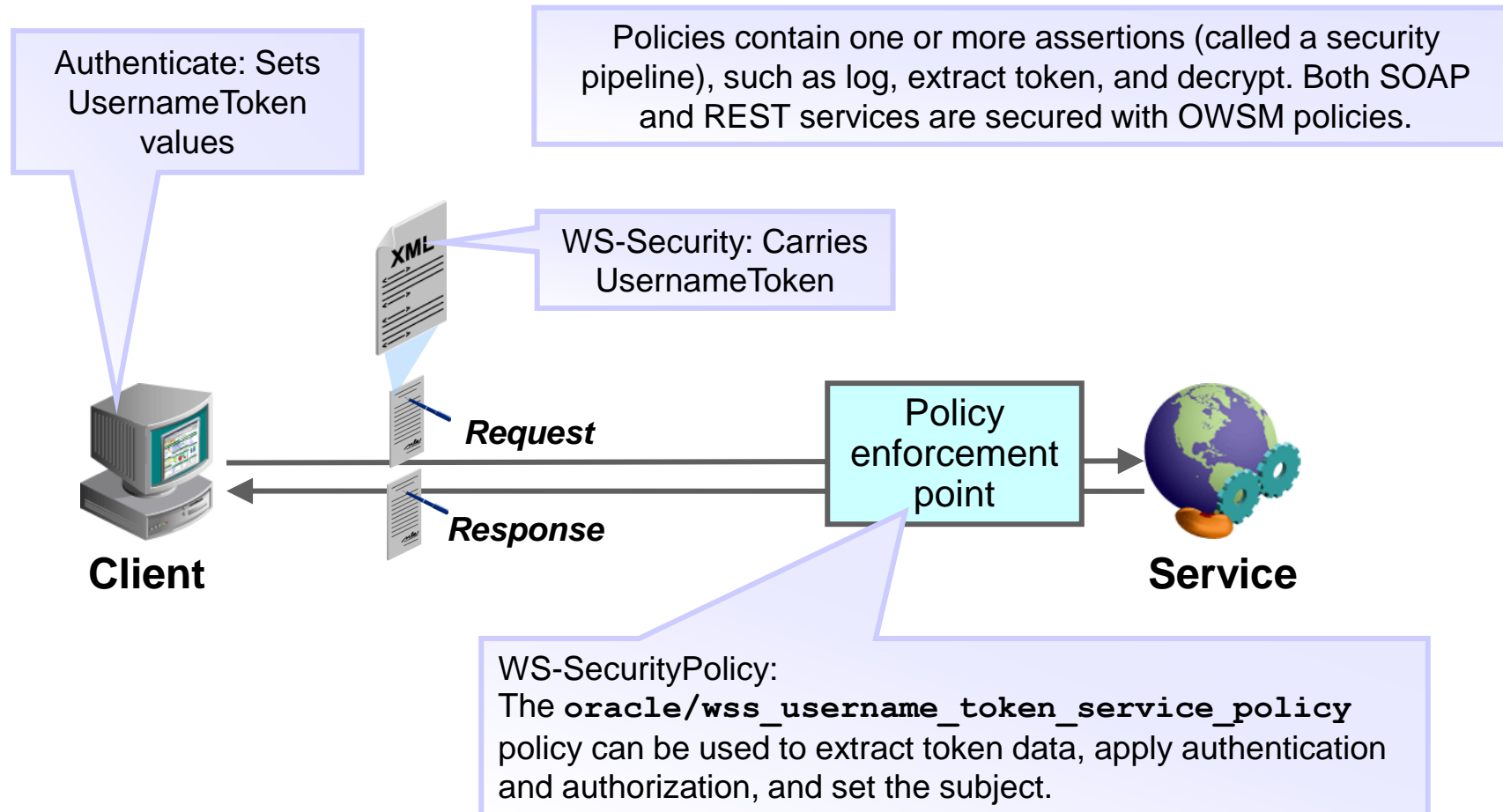
Example: UsernameToken in plain text (in a SOAP header):

```
<wsse:UsernameToken>  
  <wsse:Username>jcooper</wsse:Username>  
  <wsse:Password>welcome1</wsse:Password>  
</wsse:UsernameToken>
```

Security Assertion Markup Language (SAML)

- Exchanges security information between different parties
- Conveys information about subjects, human users, or any entities with the following types of “assertions”:
 - An authentication assertion
 - An authorization assertion
 - An attribute assertion

Security Policies: Introduction



Quiz



Policies are made up of one or more _____ .

- a. Tokens
- b. Protocols
- c. Assertions

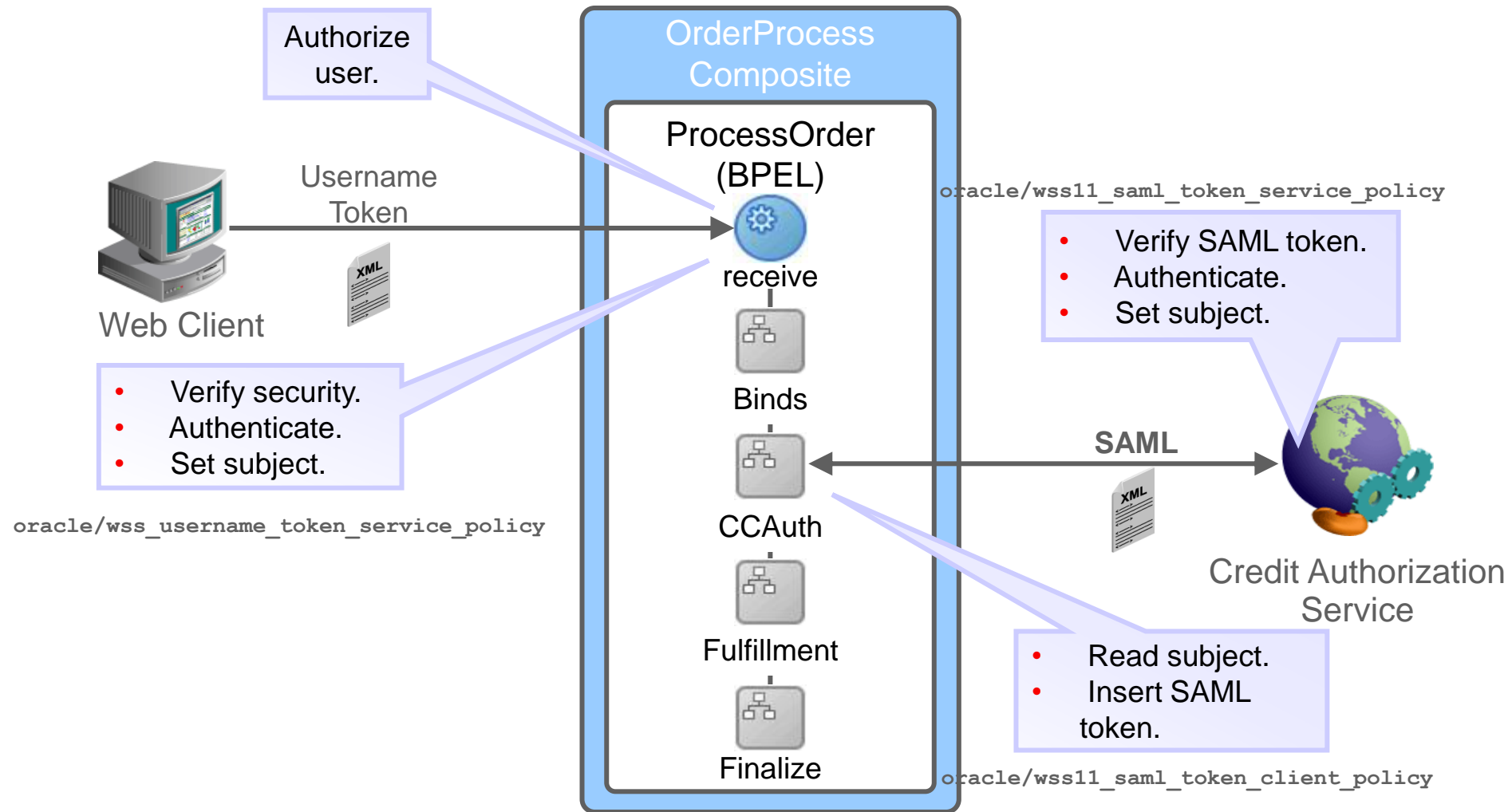


Agenda

- Web Service Security
- Oracle Web Services Manager
- **Securing Composite Applications**



Securing SOA and Identity Propagation



Attaching a Policy to an Inbound Request

Scenario: UsernameToken-based identity authentication

Policy: oracle/wss_username_token_service_policy

```
<service name="Enroll" ui:wsdlLocation="Enroll.wsdl">
  <interface.wsdl interface="../../../Enroll#wsdl.interface(execute_ptt)"/>
  <binding.ws port="../../../Enroll#wsdl.endpoint(Enroll/execute_pt) ">
    <wsp:PolicyReference URI="oracle/wss_username_token_service_policy"
      orawsp:category="security" orawsp:status="enabled"/>
  </binding.ws>
</service>
```

The attachment is added to the service (entry point) in **composite.xml**.
Result: The user is authenticated, and the subject is associated with the current thread.

Attaching a Policy to an Inbound Request by Using Oracle JDeveloper 12c



Attaching a Policy to an Outbound Request

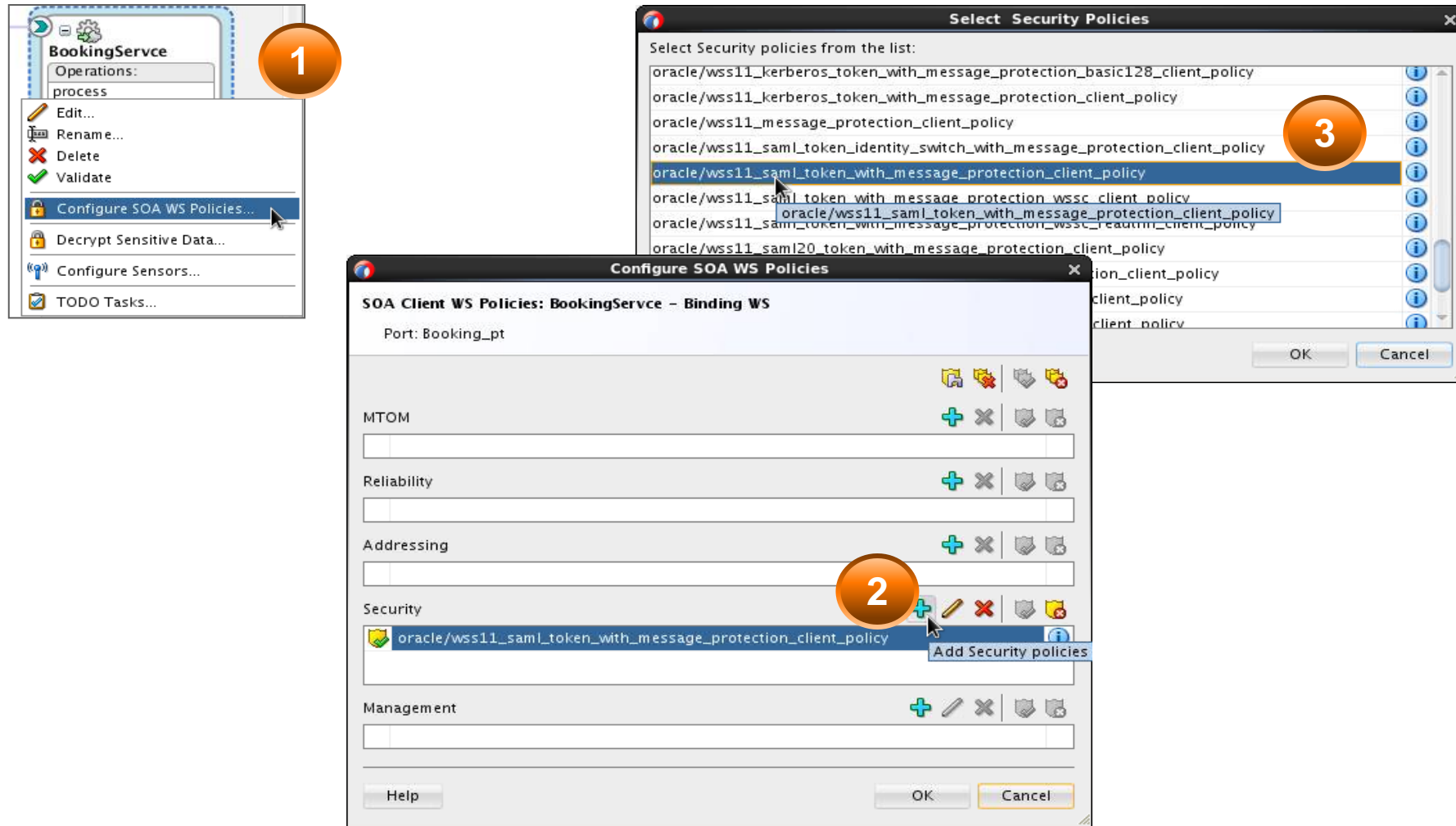
Scenario: SAML-based identity assertion

Policy: oracle/wss10_saml_token_client_policy

```
<reference name="BookingService"
           ui:wSDLLocation="../../../Booking.wsdl">
  <interface.wSDL interface="../../../Booking#wsdl.interface(Booking)"/>
  <binding.ws port="../../../Booking#wsdl.endpoint(booking_client_ep/Booking_pt)"
             location="../../../BookingSystem/booking_client_ep?WSDL"
             soapVersion="1.1">
    <wsp:PolicyReference URI="oracle/wss10_saml_token_client_policy"
                       orawsp:category="security" orawsp:status="enabled"/>
  </binding.ws>
</reference>
```

The attachment is added to an external reference in **composite.xml**.
Result: Identity is propagated, and the payload is encrypted.

Attaching a Policy to an Outbound Request by Using Oracle JDeveloper 12c



Managing SOA Composite Application Policies

Policies page

Dashboard Composite Definition Flow Instances Unit Tests Policies

You can view and manage the list of policies attached to the web service bindings and components of this SOA composite application. Click 'Attach To/Detach From' to update the list of attached policies.

View ▾ Attach To/Detach From ▾

Policy Name	Attached To	Policy Reference Status	Category	Total Violations	Security Violations		
					Authentication	Authorization	Confidentiality
oracle/http_v	ReceiveData	Enable	Security	0	0	0	0

Specify the component to which the policy is to be attached.

Choose From Available Policies

Available Policies

View Detach

Name	Category	View Detail
oracle/atomic_transaction_policy		
oracle/binding_authorization_denyall_policy		
oracle/binding_authorization_permitall_policy		
oracle/binding_oes_authorization_policy		

Columns Frozen 1

- All
- Security
- MTOM Attachments
- Reliable Messaging
- WS-Addressing
- Management
- Atomic Transactions
- Configuration
- SOAP Over JMS Transport

View available policy categories

Click View Detail icon to see details about the policy.

Policy: oracle/binding_authorization_denyall_policy

Category Security

Local Optimization off

Enabled ☒

Description This policy is a special case of simple role based authorization policy based upon the authenticated Subject. This policy denies all users with any roles. This policy should follow an authentication policy where the Subject is established. This policy can be attached to any SOAP-based endpoint.

Assertions

Name	Category	Type	Advertised	Enforced
Log Message1	security/logging	Logging		
J2EE services Authorization	security/authorization	binding-authorization		<input checked="" type="checkbox"/>
Log Message2	security/logging	Logging		

Managing SOA Composite Application Policies

Policy Attachment - Oracle Enterprise Manager

Attach/Detach Policies(RouteData) Constraint: None [OK] [Validate] [Cancel]

Globally Attached Policies

Name	Enabled	Description
No rows yet		

Directly Attached Policies

Name	Category	Enabled	Description	View Detail
Managem...		✓	This policy causes the req...	

[Attach] [Detach]

Available Policies

View Detach

Name	Category	Status	Description	View Detail
oracle/component_authorization_denyall_policy	Security	✓	This policy is a special c...	
oracle/component_authorization_permitall_policy	Security	✓	This policy is a special c...	
oracle/component_oes_authorization_policy	Security	✓	This policy does user aut...	
oracle/component_permission_authorization_policy	Security	✓	This policy is a special c...	

Information [X]

Validation is successful! [OK]

Execute the validation test. Remember to click **OK** to apply the policy change.

Attach (or detach) the policy.

Search for, select and attach the policy.

Summary

In this lesson, you should have learned how to:

- Describe Web Service Security
- Describe Oracle Web Services Manager and its use in securing SOA composites
- Discuss security and identity propagation in SOA composites
- Attach security policies to endpoints at design time and run time



Practice 15 Overview

