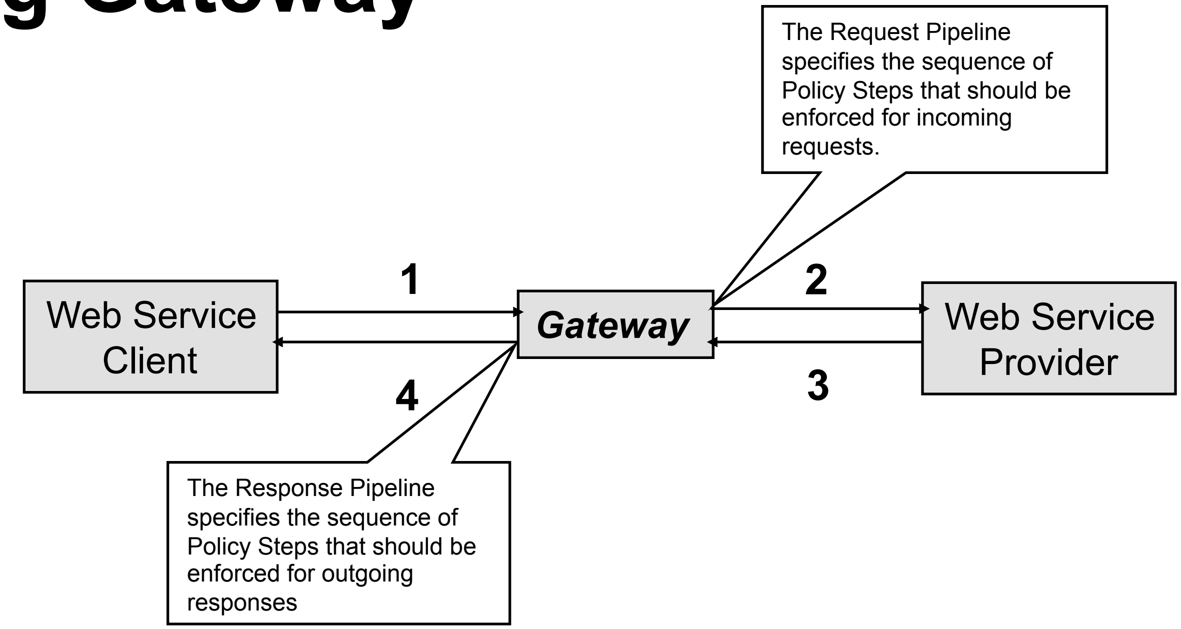
Oracle Web Services Manager (WSM) 10g: Use Case Scenarios

Marc Chanliau, Dir. Product Management
Oracle Fusion Middleware

Agenda

- Generic Oracle WSM Use Cases
- Identity Propagation Leveraging Oracle Access Manager (OAM)
- BPEL Process Support
  - SAML Token Propagation
  - Securing Asynchronous Service Calls
- Miscellaneous
  - Securing Oracle Database PL/SQL Web Services
  - Last-Mile Security
  - Limiting Extranet Access to Web Services

Protecting Access To Web Services Using Gateway

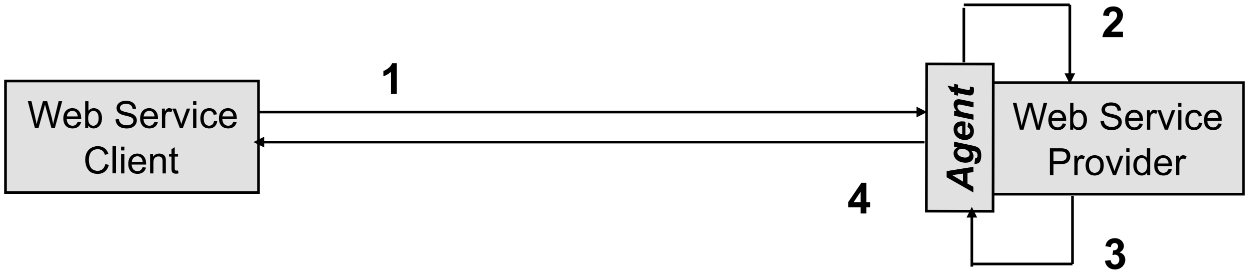


The Request Pipeline specifies the sequence of Policy Steps that should be enforced for incoming requests.

The Response Pipeline specifies the sequence of Policy Steps that should be enforced for outgoing responses

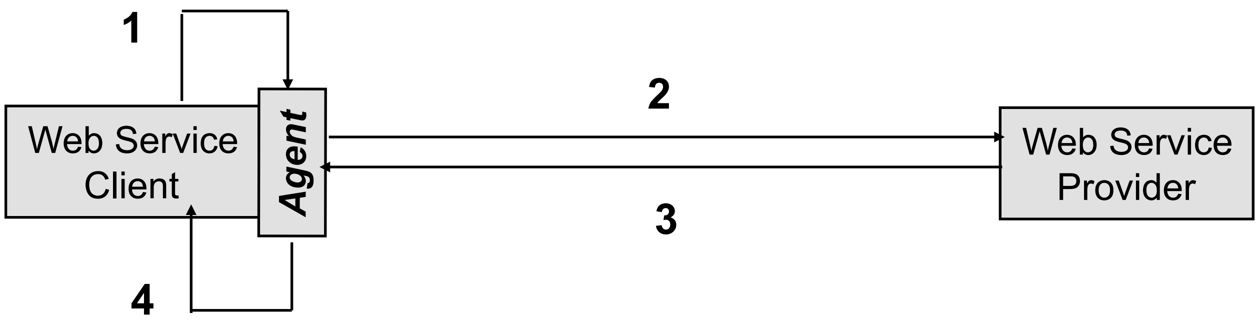
- The Gateway secures access to one or more web services at the web service provider site
  - Step1: The client posts a request to a web service
  - Step2: The Gateway intercepts the request, applies security policies (e.g., decryption, signature verification, authentication, authorization), and forwards the request to the web service
  - Step3: The web service returns a response
  - Step4: The Gateway intercepts the response, applies security policies (e.g., encryption), and forwards the response to the client

Protecting Access to Web Service(s) Using Server-Side Agent



- The OWSM Agent protects access to a web service at the web service provider (server-side Agent)
  - Step1: The client posts a request to a web service
  - Step2: The Agent intercepts the request, applies security policies (e.g., decryption, signature verification, authentication, authorization), and passes the request to the web service
  - Step3: The web service returns a response
  - Step4: The Agent intercepts the response, applies security policies (e.g., encryption), and passes the response to the client

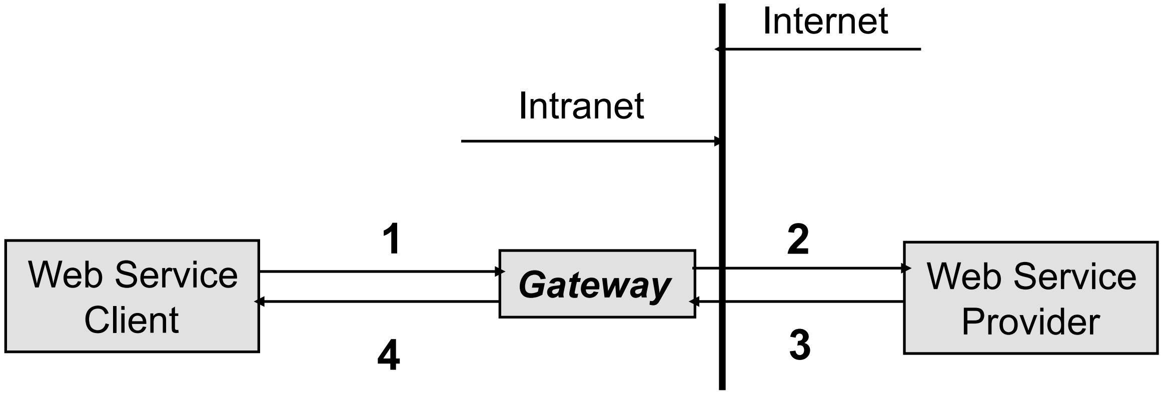
Requesting Access To Web Service(s) Using Client-Side Agent



- The OWSM Client-Side Agent enforces web services policies from within the same web application as the service client
  - Step1: The client posts a request to a web service
  - Step2: The Agent intercepts the request, applies security policies (e.g., encryption, etc.), and passes the request to the web service
  - Step3: The web service processes the request and returns a response
  - Step4: The Agent intercepts the response, applies security policies (e.g., decryption), and passes the response to the client

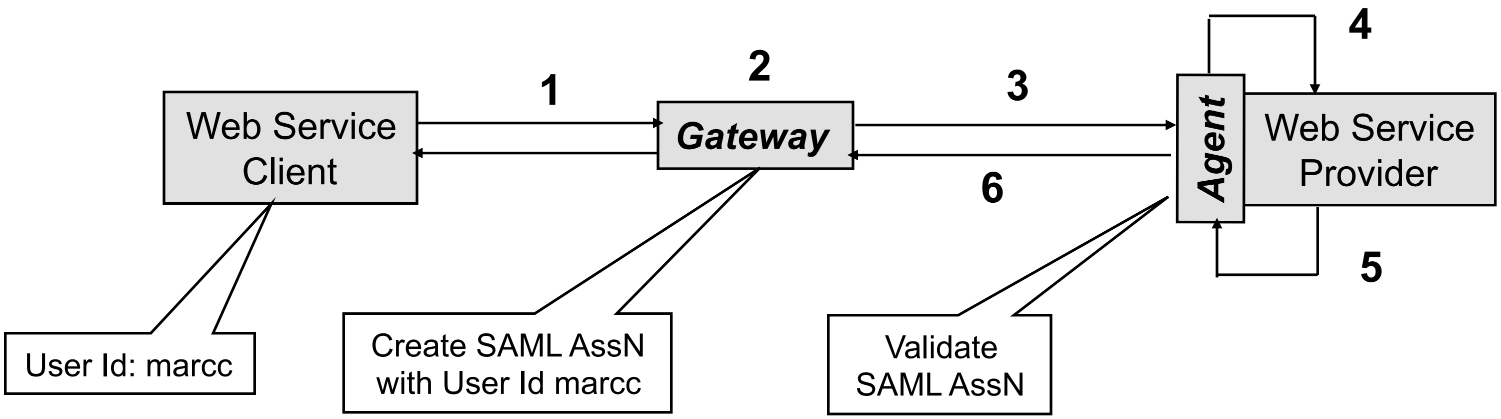
Accessing External Web Services

Using Gateway as a Proxy Server



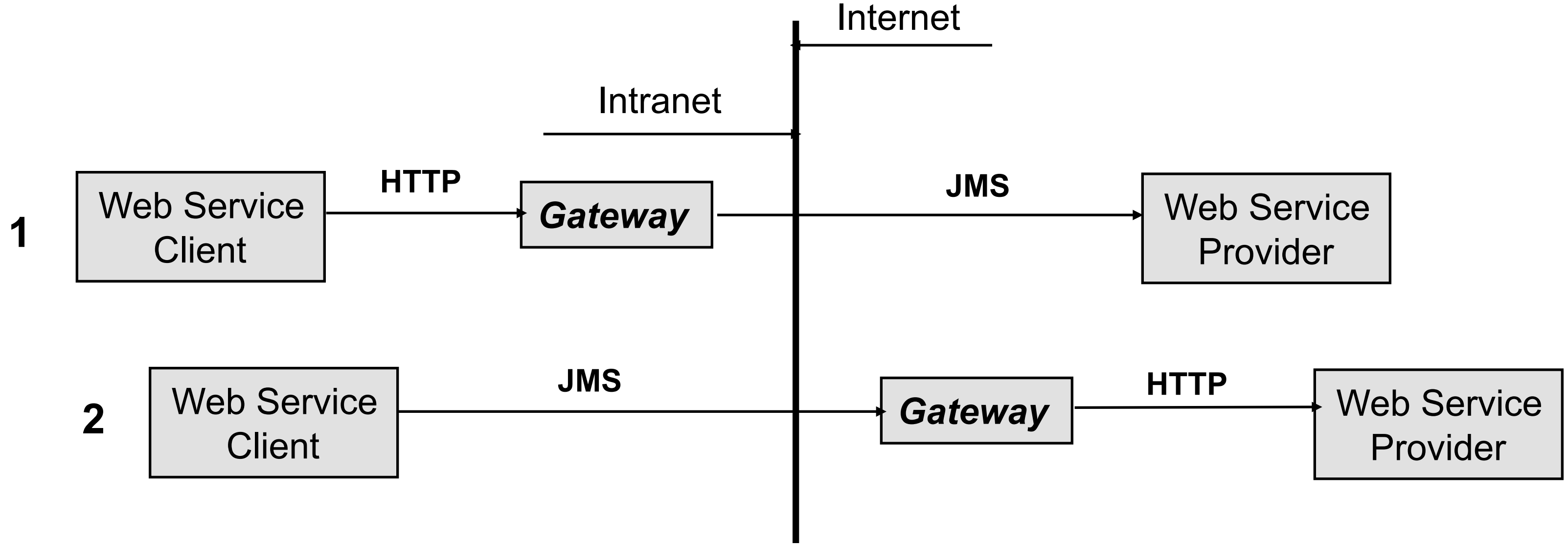
- The purpose is to allow access to external web services only to specific web service clients making a request from within the corporate intranet
  - Step1: The client (within the corporate intranet’s boundaries) posts a request to an external web service
  - Step2: The Gateway intercepts the request, applies security policies (e.g., authentication, authorization), and forwards the request to the web service
  - Step3: The web service returns a response
  - Step4: The Gateway intercepts the response, applies security policies, and forwards the response to the client

Mapping Credentials Using Gateway and Server-Side Agent



- The web service client and the web service provider don’t support the same type of credentials
  - Step1: The client makes a web service request using basic credentials (“marcc”)
  - Step2: The Gateway intercepts and authenticates the request
  - Step3: Upon successful authentication, the Gateway inserts a SAML assertion in a WS-Security header that it posts to the web service provider as part of a SOAP message
  - Step4: The Agent validates the SAML assertion and passes the request to the web service
  - Step5: The web service returns a response intercepted by the Agent for security
  - Step6: The Agent returns the response to the web service client directly or via the Gateway

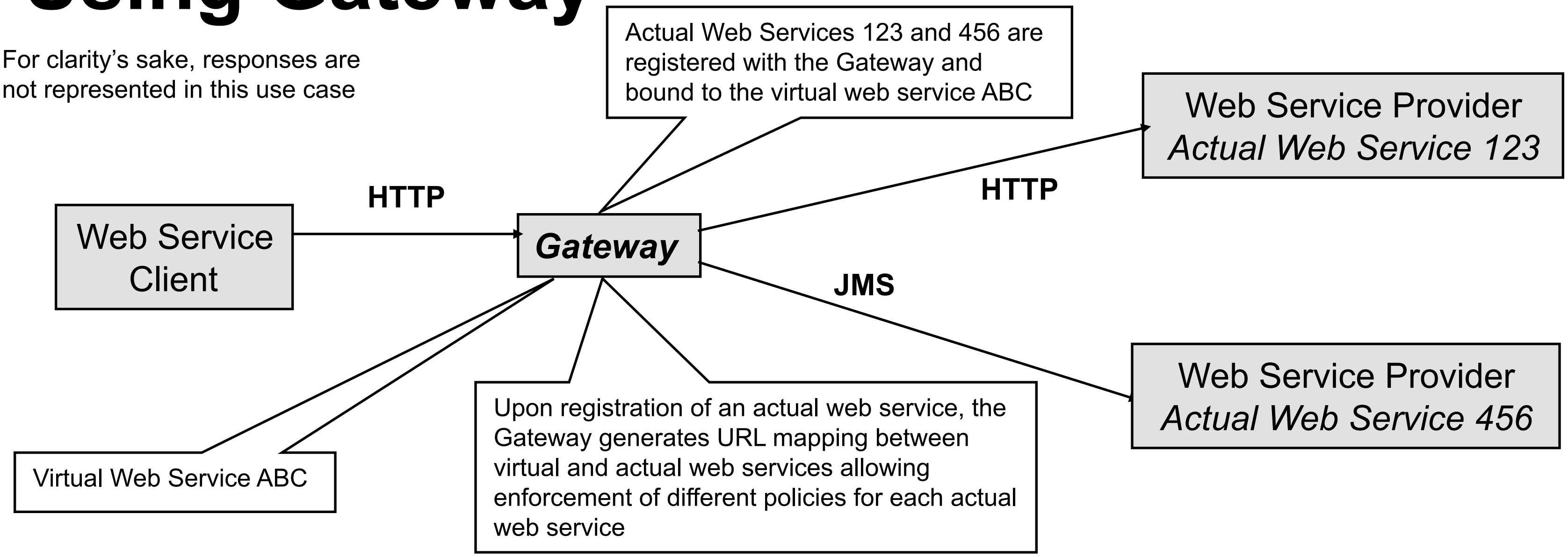
Mediating Heterogeneous Protocols Using Gateway



- The web service client and the web service provider don’t support the same protocol
  - In case 1, the Gateway resides within the Intranet and translates an outgoing HTTP request into JMS
  - In case 2, the Gateway resides outside the Intranet and provides access to HTTP-based web services from JMS-based requests

Virtualizing Web Services Using Gateway

Note: For clarity's sake, responses are not represented in this use case



Actual Web Services 123 and 456 are registered with the Gateway and bound to the virtual web service ABC

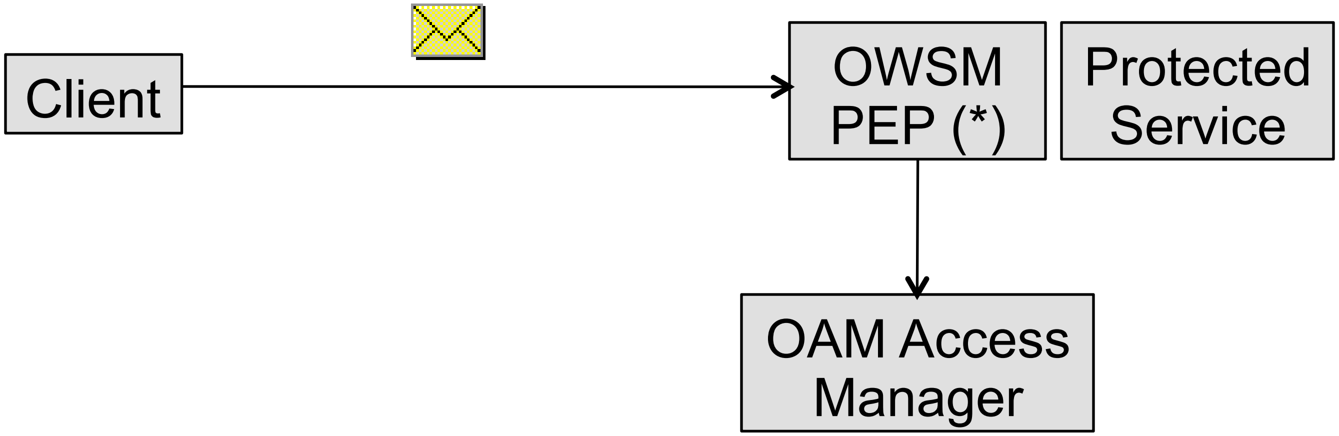
Upon registration of an actual web service, the Gateway generates URL mapping between virtual and actual web services allowing enforcement of different policies for each actual web service

- The OWSM Gateway provides web services virtualization
  - Actual web services are bound to a virtual service (the Gateway)
  - Users first access the virtual web service and based on their roles, users may access selected actual web services
  - The transport protocol can also be virtualized, for example, all users access a virtual web service through one protocol (e.g., HTTP) and the virtual service can pass the request to an actual web service using a different protocol (e.g., JMS)
  - Users can create multiple versions of a virtual web service and redirect an older version of the virtual web service to a new version

Agenda

- Generic Oracle WSM Use Cases
- Identity Propagation Leveraging Oracle Access Manager (OAM)
- BPEL Process Support
  - SAML Token Propagation
  - Securing Asynchronous Service Calls
- Miscellaneous
  - Securing Oracle Database PL/SQL Web Services
  - Last-Mile Security
  - Limiting Extranet Access to Web Services

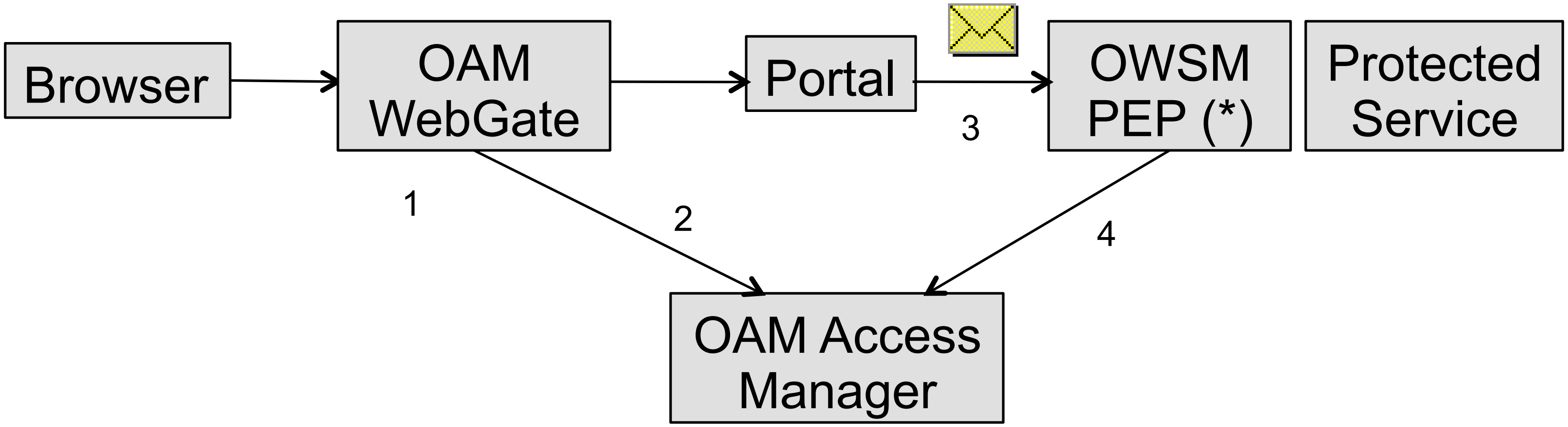
AuthN / AuthZ Using Standard OAM Step



(*) OWSM PEP can be a Gateway or an Agent

- Client sends user credentials in HTTP or SOAP header
  - Credentials can be ObSSOCookie, username/password, SAML assN, x509 cert, 2 way SSL cert
- PEP authenticates/authorizes using these credentials against OAM's Access Manager

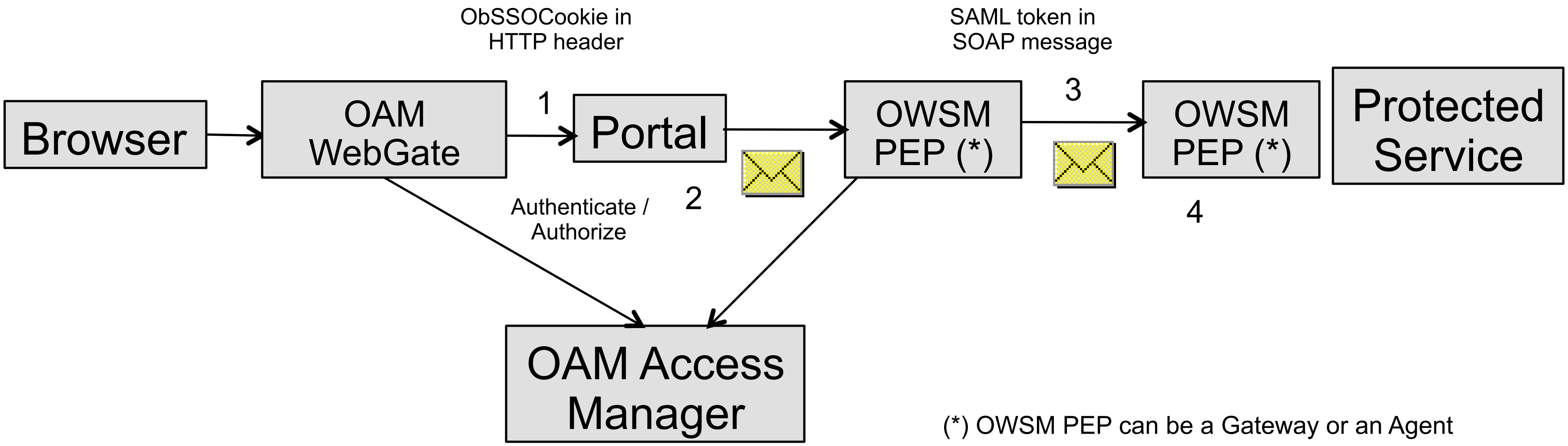
From Web Application to Web Service
Same Security Domain



(*) OWSM PEP can be a Gateway or an Agent

1. Browser user logs into a portal web application protected by OAM’s WebGate
2. OAM authenticates user and creates session cookie (ObSSOCookie)
3. The portal app needs to be customized to read the ObSSOCookie and insert it into a SOAP header
4. OWSM’s PEP verifies ObSSOCookie against OAM’s Access Manager, and authorizes access to web service endpoint

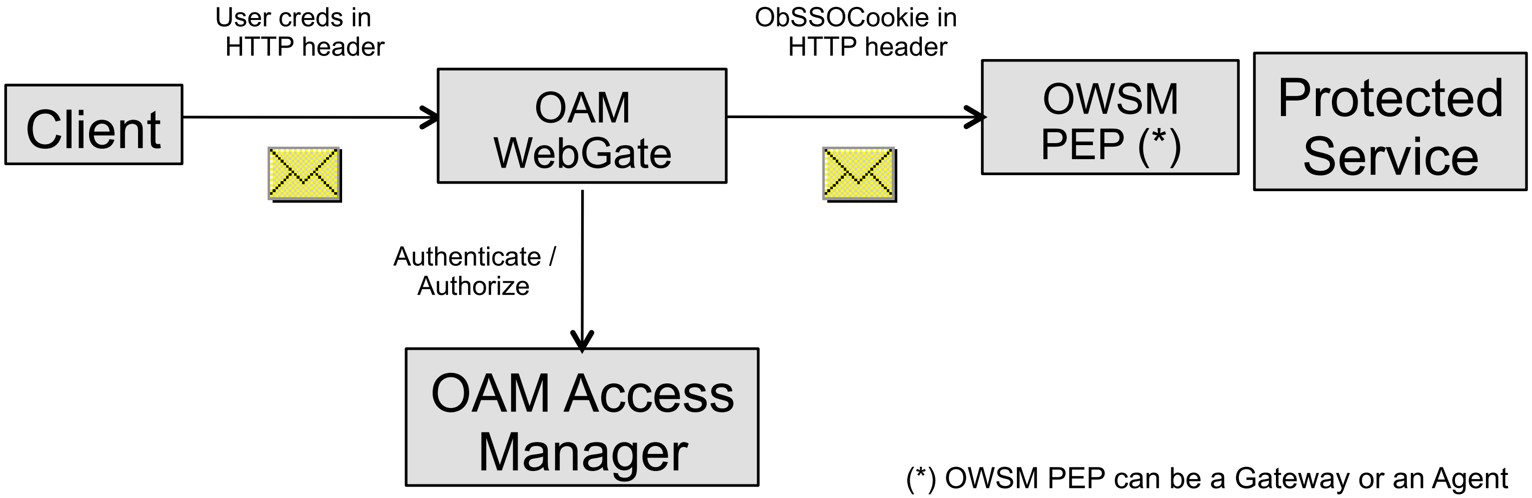
From Web Application to Web Service Different Security Domains



(*) OWSM PEP can be a Gateway or an Agent

1. Browser user logs into a portal web application protected by OAM's WebGate
2. When Portal calls an external web service, the portal app needs to be customized to read `ObSSOCookie` from the portal session and insert it into a SOAP header
3. OWSM PEP reads `ObSSOCookie` from the SOAP header, converts it into a SAML assN, and inserts the SAML assN into SOAP header
4. OWSM PEP verifies SAML token and allows access (instead of OWSM, another PEP could be used)

OAM (WebGate) for Access Control, WSM for Decryption, Sig. Verification, Monitoring



(*) OWSM PEP can be a Gateway or an Agent

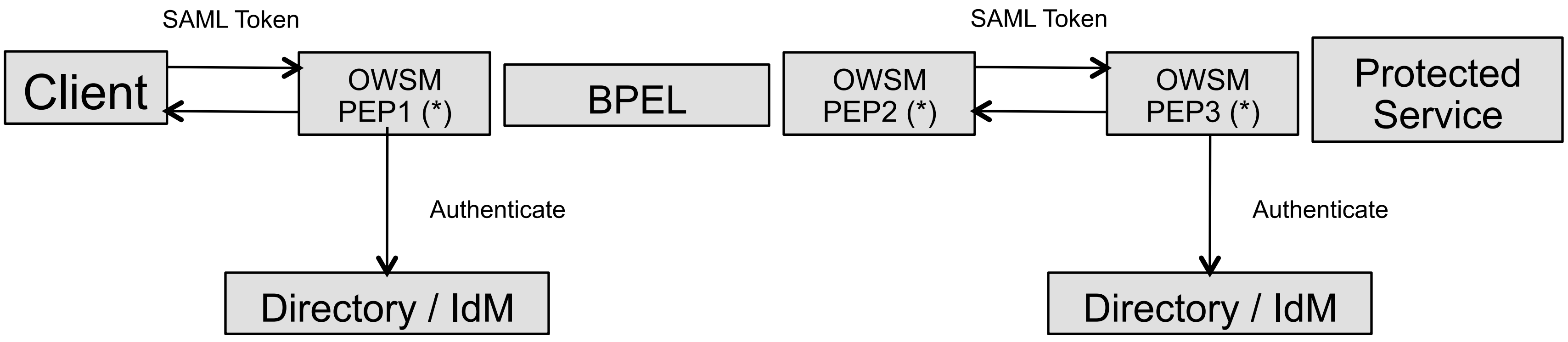
- Client sends SOAP message with username/password in HTTP header
- OAM Webgate intercepts SOAP request, and authenticates/authorizes user access
- OWSM PEP decrypts the message, verifies the signature, and performs monitoring

Note: `?wsdl` should be unprotected in OAM

Agenda

- Generic Oracle WSM Use Cases
- Identity Propagation Leveraging Oracle Access Manager (OAM)
- BPEL Process Support
  - SAML Token Propagation
  - Securing Asynchronous Service Calls
- Miscellaneous
  - Securing Oracle Database PL/SQL Web Services
  - Last-Mile Security
  - Limiting Extranet Access to Web Services

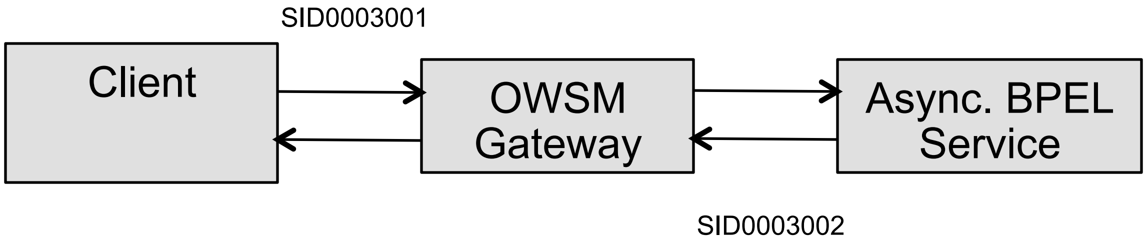
SAML Token Propagation



(*) OWSM PEP can be a Gateway or an Agent

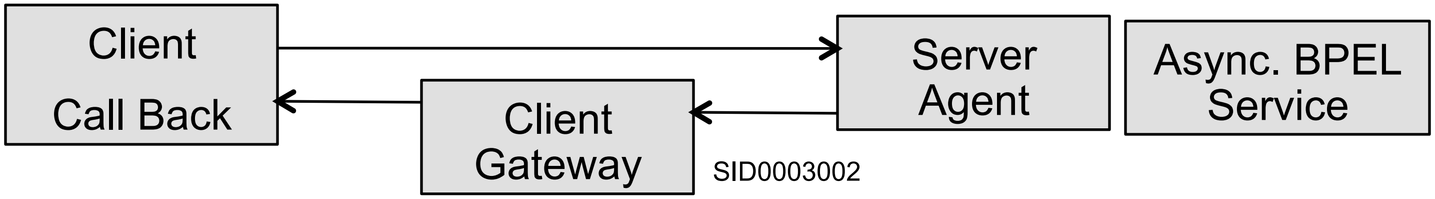
- OWSM PEP1 validates SAML token, and inserts a custom SOAP header with user information extracted from SAML token, through a custom step
- BPEL process reads the custom SOAP header, and assigns it to a global variable for propagation
- Before BPEL calls out an external web service, it reads the global variable, and inserts it as a custom SOAP header into the outgoing message
- OWSM PEP2 reads the custom SOAP header through a custom step, and then uses “Insert SAML token” step to generate and add SAML token to SOAP header
- OWSM PEP3 validates the SAML token

Securing Asynchronous Service Calls Using Server-Side Gateway Only



- Register web service in the gateway, e.g. SID0003001 (SID is the service Id)
- Register callback in the gateway, e.g. SID0003002
- Add XML transform step in policy pipeline for SID0003001 that transforms ReplyTo WS-Addressing header to SID0003002

Securing Asynchronous Service Calls Using Server Agent and Client-Side Gateway

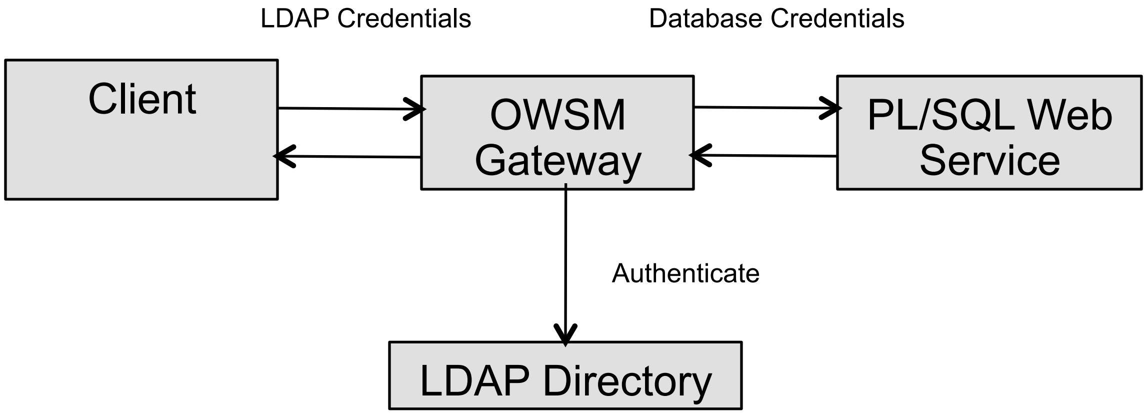


- Register callback in the client gateway, e.g. SID0003002
- Add XML transform step in request policy pipeline for server agent to transform ReplyTo WS-Addressing header to SID0003002

Agenda

- Generic Oracle WSM Use Cases
- Identity Propagation Leveraging Oracle Access Manager (OAM)
- BPEL Process Support
  - SAML Token Propagation
  - Securing Asynchronous Service Calls
- Miscellaneous
  - Securing Oracle Database PL/SQL Web Services
  - Last-Mile Security
  - Limiting Extranet Access to Web Services

Securing Oracle Database PL/SQL Web Services



- Client sends credentials with the request to the Gateway
- Gateway authenticates the user against LDAP or any other authentication source
- Once the user is authenticated, Gateway inserts fixed database credentials into HTTP header of the outgoing request

Last-Mile Security

- Last-mile security can be achieved through one of the following
  - Gateway and server agent combination
  - 2-way SSL (client-authentication) between gateway and service
  - Network access control such that only the gateway machine can talk to the web service machine

Limiting Extranet Access to Web Services

- Virtualize the web service using gateway
- Front end gateway with OHS
- Restrict access to the virtualized service by
  - Controlling access in OHS

    or
  - Using OAM Webgate

More Information

- OTN
  - http://www.oracle.com/technology/products/webservices_manager/index.html
- Internal Wiki
  - http://aseng-wiki.us.oracle.com/asengwiki/display/ASPMOWSMJPS/OWSM+PM
- Blog
  - http://ws-security.blogspot.com