ORACLE

FUSION MIDDLEWARE

ACCESS MANAGEMENT

An Oracle White Paper
Dec 2013

Oracle Access Management Security Token Service

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Introduction

In today's world, the enterprise application deployment environment is comprised of heterogeneous platforms, multiple application tiers, and different types of application environments (Web, EJBs, Web Services, etc…). The users who are accessing these applications originate from both intranet and extranet environments. An environment such as this necessitates the propagation of identity and security context of the user. This paper will focus on how to create and maintain a single 'thread of identity' using Oracle Access Management Security Token Service in order to meet the security and reliability requirements of an enterprise.

Oracle Access Management Security Token Service

The Oracle Access Management Security Token Service (OAM STS) is a service component of Oracle Access Management platform that also includes Access Manager, Identity Federation, Mobile Security etc. These Access Management services are fully converged into a platform with the same administration console, run-time server, and backend data stores. The Oracle Access Management Security Token Service provides an enterprise-level solution to enable the creation of a consistent and streamlined model for token acquisition, validation and renewal; these capabilities are both security infrastructure and protocol agnostic. The STS is a WS-Trust- based token service that allows for a policy-driven trust brokering and secure identity propagation and token exchange between web services. It provides a security and identity service that greatly simplifies the integration of distributed and/or federated web services within an enterprise and its service providers.

OAM STS offers the following benefits for applications and web services:

- Decouples applications and web services from the authentication mechanism.
- Enables applications and web services to support multiple credential types for authentication through token translation.
- Supports federated scenarios by establishing trust between each domain's STS instance.
- Facilitates identity propagation scenarios where the authenticated user is granted access to downstream services.

OAM STS augments OAM Federation Services, which facilitates federated (cross-domain) single sign-on (SSO) and single logout (SLO) and Oracle Web Services Manager (OWSM) and Oracle Application Gateway (OAG), which secure service-oriented architecture (SOA) deployments.

How OAM STS Works

OAM STS leverages the WS-Trust standard protocol to manage token exchange between the web service consumer and the web service provider. WS-Trust provides a standard mechanism to send security token requests to any security token service. This specification can be used to manage token transformation when crossing the various security boundaries of the information ecosystem. Figure 1 below shows an example of how an OAM STS implementation can facilitate interaction between a web service consumer and provider through brokered authentication.

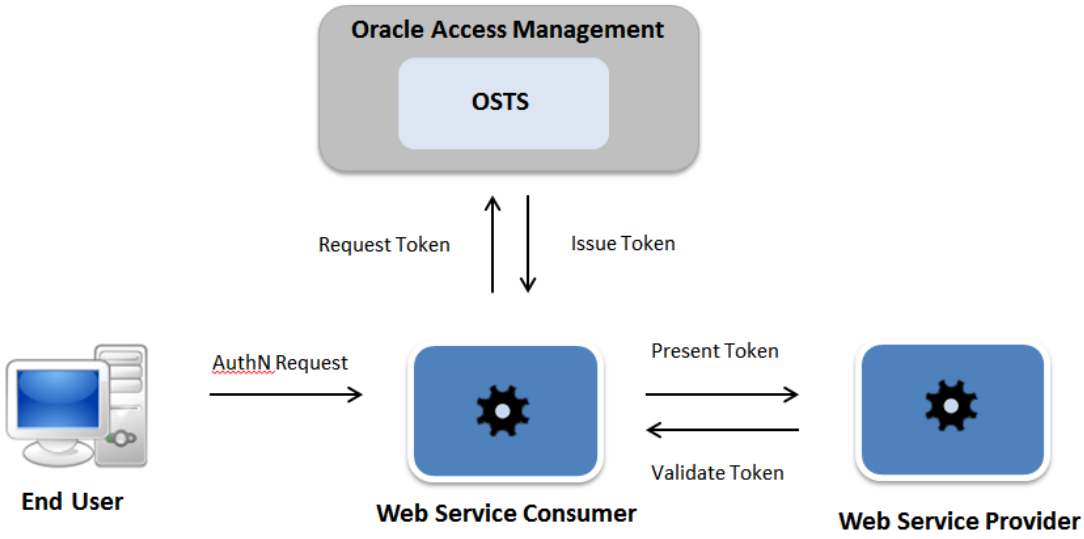

Figure 1: Brokered authentication through OAM STS

1. A user authenticates to a web service consumer. The inbound token types could be a username token with password, an X.509 token, or a Kerberos token.

2. The authenticated web service consumer then requests a token needed to access a web service provider. The request sent to OAM STS will be a WS-Trust request, which is called a Request Security Token (RST). OAM STS verifies the credentials presented by the client and responds with a SAML security token. The SAML token provides proof that the client has authenticated. The response from the OAM STS instance is known as the Request Security Token Response (RSTR).

3. The web service consumer presents the SAML security token to the web service provider in header of a SOAP message. The web service provider then verifies that the token that was issued by a trusted STS before allowing the client is then allowed to interact with the service.

There are two additional points worth noting:

- A multilateral trust relationship must be established between the web service consumer, the OAM STS instance, and the web service provider. Returning a token implies that the OAM STS instance trusts the requesting system to authenticate the users.

- The identities that are propagated between the respective web services by OAM STS should either leverage the same user repository or otherwise be kept in sync.

Web Services Security

As previously illustrated, OAM STS facilitates security token exchange between two web services where one service is a client and the other is the provider. Web services security encompasses multiple functional imperatives, including: authentication, authorization, confidentiality, privacy and integrity, and non-repudiation. Oracle addresses the need for web services-based security and management with a standards-compliant solution, Oracle Web Services Manager (OWSM). OWSM also support the WS-Trust specification and therefore can be leveraged as an optimal client to interact with Oracle STS. That said, any WS-Trust trust-based client that meets the web services security standards can interoperate with OAM STS.

Figure 2 below shows an illustration of a scenario in which OAM STS is used for identity propagation from a web service consumer called 'StockClient' to a web service provider called 'StockService.'

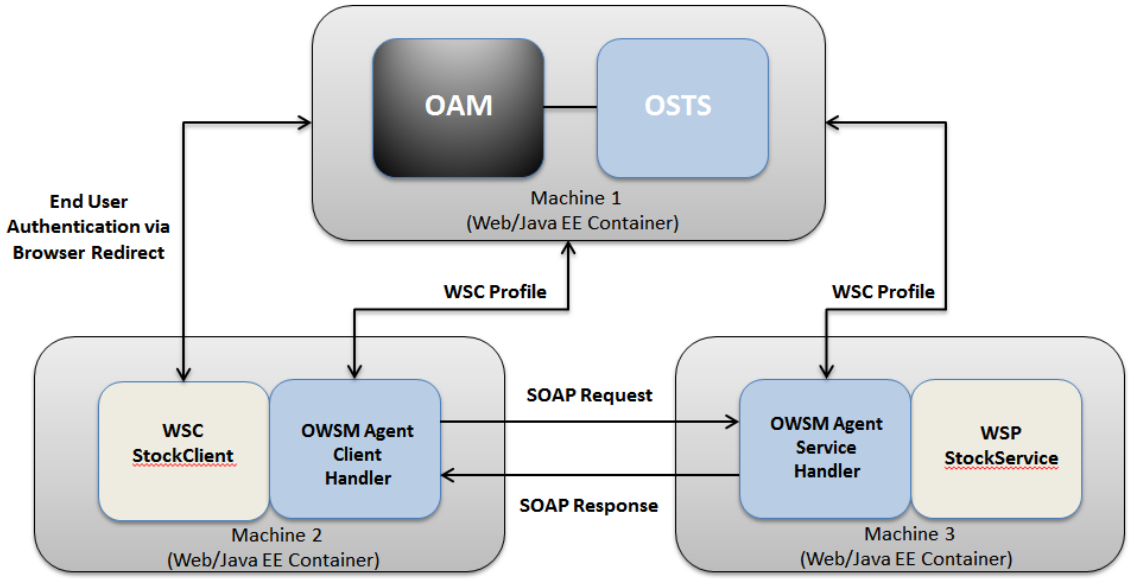

Figure 2: Using Oracle STS for identity propagation

The initial authentication of the end user can be handled through Oracle Access Manager (OAM) via a browser redirect by the OAM WebGate. In this scenario, the web service consumer and the web service provider are both protected by the OWSM agent. The OWSM agent on the client side acts as a WS-Trust client to interact with OAM STS.

The OWSM agent intercepts requests and responses and subsequently executes the policies that are attached to each. Additionally, OWSM agents are capable of looking up the policy definition details from the OWSM Policy Manager and then caching the policies in order to increase performance. Any policy changes are dynamically updated by the OWSM Policy Manager, which propagates the changes to the agents. The agents then refresh the policy cache and thereafter apply the update policy to subsequent requests.

Architecture

OAM STS is a centralized token service that supports the WS-Trust protocol. This protocol defines extensions to the WS-Security specification for issuing and exchanging security tokens and establishing trust relationships. OAM STS is hosted as a web service endpoint and coordinates security-based interactions between web service consumers and providers as shown in figure 3 below. All communication with OAM STS must be via a WS-Trust client.

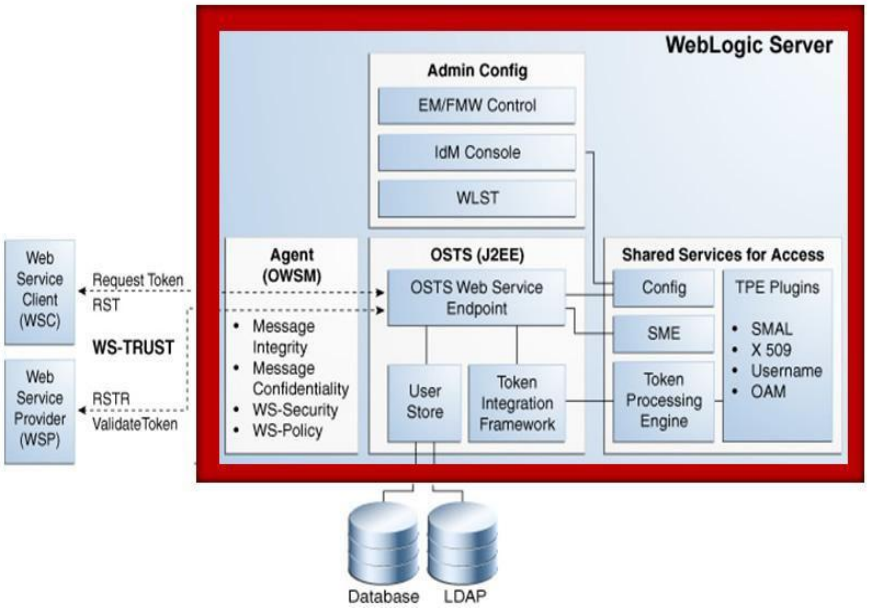

Figure 3: OAM STS architecture

When a web service consumer makes a call to a web service provider, it receives the WS-Security policy indicating that a security token issued by OAM STS must be presented. The policy will contain the location of the OAM STS instance, and the client will subsequently use this location to request the token expected by the web service provider. Alternately, the web service provider could register its acceptable security mechanisms with the OAM STS instance, and prior to validating the incoming SOAP request issue a query to determine the client security mechanisms.

When an authenticated web service consumer (carrying credentials that confirm either the identity of the end user or the application) requests a token for access to a web service provider, the Security Token Service verifies the credentials, and in response issues a security token that provides proof that the client has been authenticated. The consumer presents the security token to the provider which then verifies that the token was issued by a trusted security token service.

OAM STS supports the following token formats:

Requester	"On Behalf Of" (end user tokens)	Output Token
• UserName • X509 • Kerberos • SAML 1.1 • SAML 2.0	• UserName with password • UserName without password • X.509 • Kerberos • SAML 1.1 / 2.0 • OAM Session Propagation token • Custom token	• Username without password • SAML 1.1 • SAML 2.0 • Custom token

Deployment Scenarios

The two most common deployment scenarios for OAM STS are web service identity propagation and token exchange.

Scenario: Web-to-Web Service Identity Propagation

In this scenario a user's identity information needs to be propagated from a web application to a web service provider. For example, a user logs onto an OAM-protected enterprise portal and clicks the purchase order application to make a purchase via web services. The web service provider could reside in the same security domain as the web application or in a different security domain altogether.

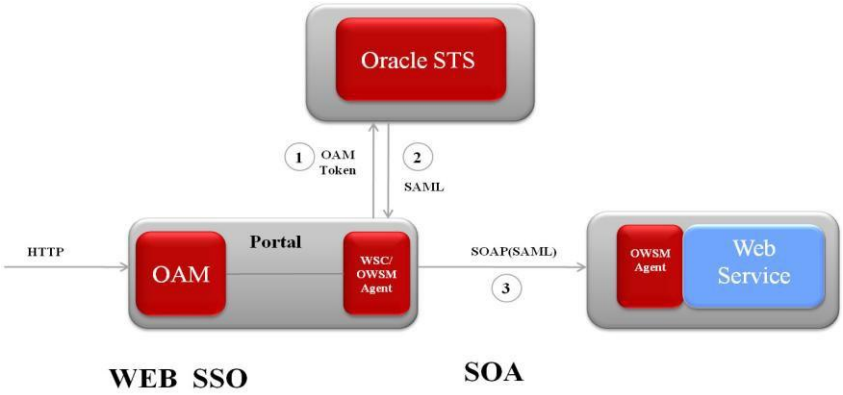

Figure 4: Identity propagation between web services

Scenario: Web Service-to-Web Service Token Exchange

Using the purchase order web services, the user completes an order, but the seller needs to call a shipping service for shipment. The purchase order web service was authenticated using username and password while the shipping web service provider requires a SAML token.

In cases such as this, OAM STS can facilitate token exchange from one standard token format (e.g., username, certificate, SAML or Kerberos) to another (e.g., SAML 1.x or SAML 2.0). Once again, the web service provider could reside in the same or different security domain as the web service consumer.

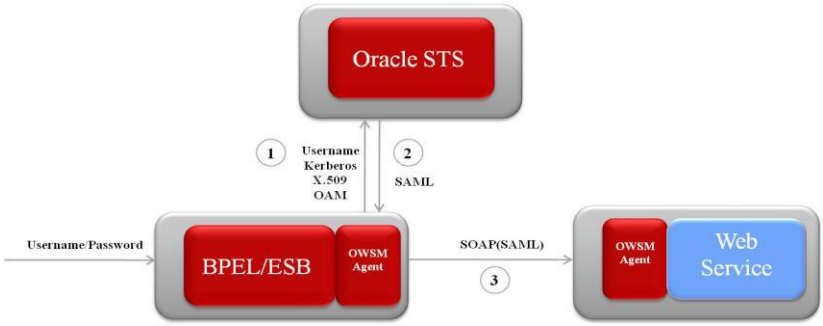

Figure 5: Token exchange between web services

Identity Propagation

OAM STS can be configured to support scenarios that include both identity propagation and token translation between web services deployed in the same security domain. SOAP messages are used to transfer the security tokens and communicating between web services clients and providers.

To further illustrate the use cases of token exchange services between web and web services, below is an identity propagation scenario that covers a case where OAM is used for the initial end user authentication and OWSM is used as the security provider between the web service consumer and provider. OWSM illustrated here can be replaced with either an Oracle (WLSClient or MetroClient) or third party WS-Trust client. This client will then communicate with OAM STS on the web service consumer side and use OWSM on the web service provider side.

In the scenario illustrated in figure 6 below, the portal application, web service consumer, and web service provider are all deployed in the same security domain.

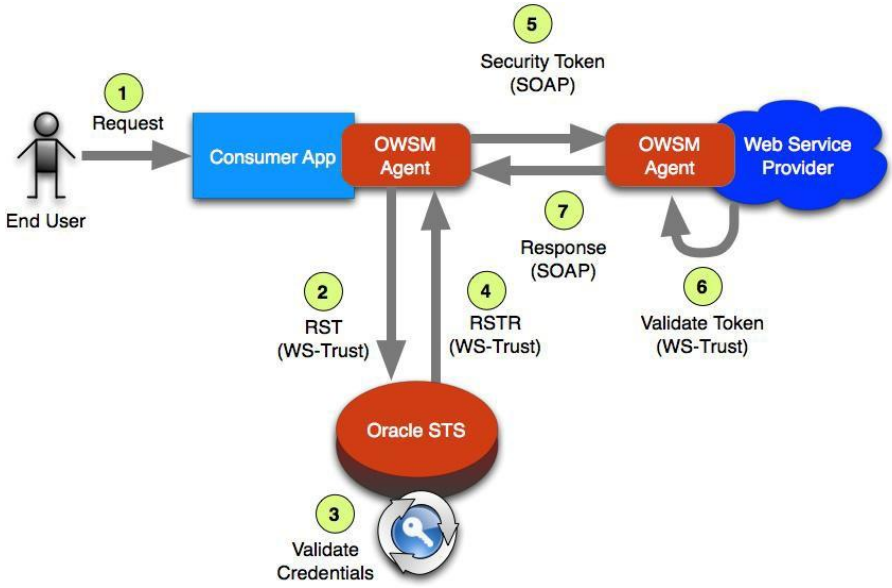

Figure 6: Identity propagation within a security domain

The scenario breaks down into seven logical steps as detailed below:

1. An end user accesses a web application through the company portal that is protected by Oracle Access Manager (OAM).
   a) The end user is first authenticated by OAM and subject to the authorization policy in OAM, is subsequently allowed to access the portal.
   b) The application then next makes a web service call (through a web service consumer) on behalf of the user to the web service provider.

2. The OWSM agent protecting the web service consumer intercepts the application's request. The OWSM client determines from the web service provider's policy that a token issued from Oracle STS is required. The OWSM client then sends a request to OAM STS.

3. OAM STS verifies the user's credentials (via the OAM cookie) presented by the web service consumer. It also makes an authorization decision about whether the consumer is authorized to request a security token to access the provider.

4. OAM STS responds by issuing a security token that provides proof that the web service consumer has authenticated with STS.

5. The web service consumer sends the security token to the provider via a SOAP message.

6. The OWSM agent protecting the web service provider intercepts the response from web service consumer and helps to validate the security token. The web service provider then verifies the security token that was issued by the Oracle STS, which proves that the client has successfully authenticated with STS.

7. The web service provider responds to the client request, granting it access to the application.

Web Service Federation

As in the earlier use case examples, the user can be an employee at company A that made a purchase from company B while the shipment is handled by company C. OAM STS can support this scenarios where a web service consumer needs to communicate with web service providers that operate across organizational boundaries or multiple security domains. In these types of scenarios, there will be two Oracle STS instances deployed, one in each security domain. Moreover, the instances will have a trust relationship established between them in order to enable brokering the trust between the web service consumer and provider. The web service consumer is authenticated in the security domain in which it operates but needs to propagate the identity of the user to the web service provider, which resides in a different security domain. This propagation is done through the help of the second OAM STS instance residing in the web service provider's domain.

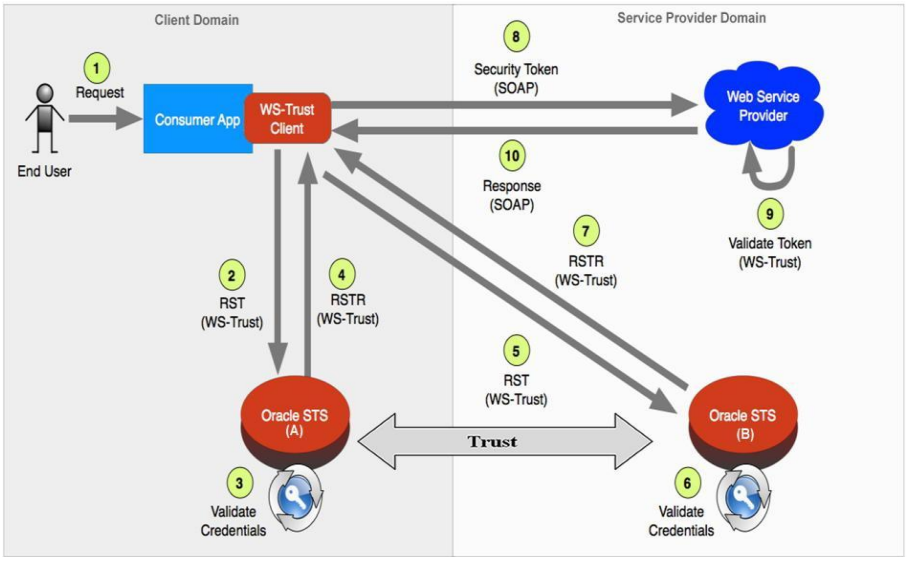

Figure 7: Identity propagation across security domains

A typical OAM STS web service federation scenario involves two Oracle STS instances, one in the client domain (OAM STS (A)) and one in the service provider domain (OAM STS (B)) as shown above in figure 7.

1. An end user accesses the consumer application; the end user is authenticated in the client domain. The consumer application in turn makes a web service call through a web service consumer on behalf of the user to the web service provider. A WS-Trust client at the web service consumer side intercepts the request, and determines from the web service provider policy that a token issued from OAM STS (B) is required. The WS-Trust client sends a request to the OAM STS (A).

2. The web service consumer requests a security token on behalf of the user to communicate with the OAM STS (B) in the service provider domain. The web service consumer subsequently presents the authenticated user credentials.

3. The OAM STS (A) in the client's domain verifies the credentials presented by the WSC

4. The STS in the client domain responds, it issues a security token that provides proof that the web service consumer has been authorized to use the token issued by OAM STS(A)

5. The web service consumer now requests a security token from OAM STS (B) in the service provider domain. It then presents the token issued by the client domain Oracle STS (A).

6. OAM STS (B) verifies that the token presented by the web service consumer originated from an OAM STS instance in a trusted security domain. After OAM STS (B) validates the security token, it then makes an authorization decision about whether the web service consumer is authorized to request a security token to access the web service provider.
8. The web service consumer sends the security token to the web service provider via a SOAP message.
9. The web service provider verifies the security token that was issued by the OAM STS (B), which proves that the web service consumer has successfully authenticated with the Oracle STS (A).

10. The web service provider responds to the request of the web service consumer, granting access to the application.

Oracle Application Gateway

In the earlier use case example, the shipping company exposes their shipment application through web services to vendors selling products. Their application is facing potential security threats such as denial of services, XML injection attacks, etc. Oracle Application Gateway (OAG) is a software solution that provides XML firewall security to protect web services exposed externally. It also provides application-level routing (based on source, target, sender identity, and XML message type); XML conversion, validation and threat scanning; XML acceleration; security (selective encryption and signature of XML messages, decryption and signature validation); monitoring (response time, logging, and alerting); and governance (service access and usage).

Oracle Application Gateway is tightly integrated with Oracle Access Manager, Oracle Entitlements Server, Oracle Web Services Manager, and the Oracle SOA Suite to provide transport and application-level security across all layers involved in web services requests.

OAG can act as a WS-Trust client to OAM STS or any other third-party STS as shown in figure 8 below. All communication between OAG and OAM STS will be WS-Trust-based. A trust relationship between OAG and the web service will be brokered by OAM STS to facilitate identity propagation from the client side to a web service.

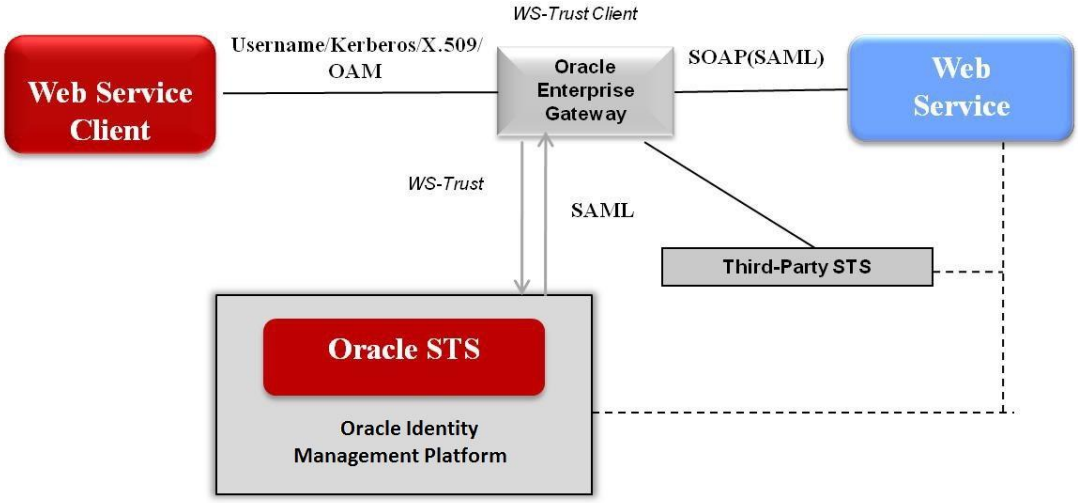

Figure 8: Identity propagation using Oracle Application Gateway and OAM STS

A typical scenario involves a web service consumer that uses a standard security token to access the web service provider which requires a SAML token for authentication:

1. The web service consumer sends an initial request to the web service provider. The SOAP / WS-Security message includes a standard security token (e.g., username, Kerberos, X.509, or OAM token) and uses an XML Signature to establish the identity of the client.
2. Oracle Application Gateway recognizes that the client is using a standard token and that the service provider is expecting a SAML assertion, so OEG sends a WS-Trust request to the OAM STS including an RST element. Included in the RST element is the token type requested by the service provider, which in this case is SAML.
3. OAM STS sends back a message including an RSTR element with an embedded RST element included in the SAML assertion.
4. Oracle Application Gateway forwards the service provider a request that includes the SAML assertion inserted in a WS-Security header (the SAML assertion is signed by Oracle STS).
5. The web service provider verifies the security token that was issued by the trusted Oracle STS instance.
6. The service provider can now accept the request from the web service consumer and responds to the request.

Conclusion

Enterprises today have heterogeneous environments with many systems and applications using their own tokens for security and session management. Achieving interoperability between the applications and propagate user identity for end-to-end security and auditing is a significant challenge. The problem becomes even more difficult when application interactions cross security domains as they often do when working with external partner organizations and service providers. The OAM Security Token Service provides a secure and standard based solution to the problem.

The OAM Security Token Service offers the following benefits for enterprise deployments:

- **Improved application security** – Decouples applications and web services from the authentication mechanism, ensuring better security, increased compliance, and lower costs
- **Rapid deployment** – Offers standards-based token transformation that enables identity propagation between applications and modern web services
- **Lower Cost of Ownership** – Lowers the cost of ownership by integrating out of the box with Oracle Access Manager and centralizing the brokering of trust between applications in different identity domains
- **Part of a Complete Access Solution –** OAM STS is core component of the Oracle's industry leading identity and access management platform. Oracle Access Management 11*g* R2 represents a major milestone in access management technology, unique in the industry for both the completeness of vision and level of integration. Oracle's access management platform provides innovative new services that complement traditional access management capabilities, all of which can be enabled as required to meet the specific needs of your organization.

For further information on Oracle Access Management Secure Token Service and the Oracle Identity and Access Management platform, please visit:

http://www.oracle.com/identity

Oracle Access Management
Security Token Service
Dec 2013
Author: Kanishk Mahajan

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together