ORACLE

FUSION MIDDLEWARE
ACCESS MANAGEMENT

An Oracle White Paper
Dec 2013

Oracle Access Management Federation 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.

Executive Overview

The Oracle Access Management (OAM) Federation Service is one of the core services of Oracle Access Management. The OAM Federation Service provides a complete, enterprise-level, carrier-grade solution for exchanging identity information securely between partners. With OAM Federation Services, organizations can conduct business online with confidence, by providing to their business partners secure access to protected applications.The OAM Federation Service significantly reduces the need to manage partner identities and lowers the cost of integrating with partners through standards-based federations.

This paper covers the business and technological challenges that drive the need for federated single sign-on, and details how the OAM Federation Service is able to address these challenges.

Business Challenges with Integrating Websites

Cloud and SaaS Adoption

Many IT organizations experience pressure from the business to save costs by outsourcing some functions to cloud and SaaS partners. But the cost savings achieved by leveraging the cloud can be offset by the technology obstacles that cloud integrations create for IT managers. Even though many cloud vendors support federation standards such as Security Assertion Markup Language (SAML), most IT organizations fail to leverage these standards due to the proprietary nature of their own identity infrastructure.

Avoiding standard-based integrations can significantly delay cloud projects, subsequently slowing down cloud adoption and preventing IT from keeping pace with the needs of the business

Today's enterprises are facing some basic business challenges for which identity federation solutions are uniquely suited. As many organizations now outsource important business functions, possibly to a cloud provider such as human resources or employee benefits, there has arisen a need to provide their employees secure access to these services. Increasingly, organizations provide non-employees access to sensitive business applications such as procurement systems. Lastly, companies are aggregating services sourced from multiple organizations and presenting these services to their consumers as a single offering.

There are common business and technical challenges that must be solved in any federated application environment. Organizations must provide single sign-on (SSO) to applications and services across disparate security domains to deliver a compelling user experience. Additionally, organizations must provide these SSO services without having to add large numbers of users to an enterprise directory or having to manage those identities over time. A trust mechanism must exist in order to allow users authenticated in one domain to be trusted in a second domain. Finally, these technical challenges must be managed within the constraints of existing business and legal agreements that define thresholds for

acceptable use, risk and indemnification. Without an effective identity federation strategy and corresponding solution that implements this strategy, organizations face several important operational challenges:

- Delays to adopting cloud, Software as a Service (SaaS) or applications hosted by application service providers
- Recurring identity on-boarding and management costs
- Increased costs and risks associated with identity proliferation
- The inability to quickly address new security threats

Each of these challenges, along with how the OAM Federation Service helps organizations address them, is discussed in the next section.

Recurring Cost of Identity Integrations

The most important promise of federation is interoperability through well-established standards. Historically, federation was viewed as merely cross-domain SSO—a convenience, but not necessarily critical to the business. The utility of federated SSO is now quite obvious and many of the organizations that have adopted federation standards have done so initially to achieve SSO with their partners. However, broader adoption of federation standards combined with innovation within the standards themselves has resulted in higher ROI due to more consistent and reusable identity integrations.

Enterprise-grade, standards-based federation implementations can significantly reduce the ongoing costs of integrating and federating identities across an organization's network of partners. Such implementations can help organizations avoid common pitfalls such as opting for a "quick" or proprietary SSO integration that is not repeatable across partners or choosing a high cost, homegrown implementation of federation protocols using cobbled together toolkits or open source libraries. The early convenience of these approaches is quickly eclipsed by the growing costs and complexity each time a new, one-off partner is added to an increasingly fragmented system.

Proliferation of Identities

Often organizations fail to see federation as an integral part of overall identity management architecture. They approach federation as an isolated task, merely an access control or SSO issue and typically adopt federation protocols such as SAML as a bolt on "extension" to an existing authentication scheme.

This approach ignores the question of how to handle federated user enrollment. While some Service Provider (SP) vendors offer self-registration services for enrolling federated identities, typically identities are exchanged with partners via a spreadsheet sent as an email attachment. This approach leads to loss of productivity, and is prone to human error. But perhaps the most worrisome aspect of this approach is the unnecessary proliferation of user identity information, which can lead to avoidable security and privacy breaches.

A popular alternative is "on-demand" identity creation in the SP domain, which happens upon the first federation, when the user doesn't already have an account with the SP. "On-demand" identity creation claims to improve employee productivity and to improve user experience. But this approach doesn't solve the federation identity management problem. By creating identity without user's consent, it introduces further privacy and compliance issues and further complicates the problem. In essence, both approaches simply place the burden of identity ownership on a SP, who eventually has to deal with orphaned accounts, access violations, forgotten passwords, and various compliance regulations.

The problem of uncontrolled identity proliferation deserves serious consideration. Unnecessary user accounts result in decreased system performance, additional infrastructure costs, and compliance challenges over time. Moreover, this also leads to end user confusion, further increasing service costs via increased administrative and support overhead.

Emerging Security Threats

Security threats to the enterprise are becoming increasingly more sophisticated and harder to discover and deal with. Criminals, who treat identity theft as the lucrative business it has become, are constantly devising new strategies for carefully planned attacks, including social engineering, phishing, pharming, and keystroke logging, to name just a few.

Many organizations find themselves unable to proactively respond to new and emerging security threats because of a lack of attention to them. Paradoxically, those organizations spend their days dealing with symptoms of poor identity integration strategy—adding new infrastructure and new compliance tools and debugging proprietary code.

Oracle Access Management Federation Services: A Comprehensive Solution

For Oracle, identity federation is not a standalone task, but an integral part of overall access and identity management platform. The OAM Federation Service provides an end-to-end, scalable, forward-looking identity federation infrastructure that addresses all needs of modern organizations and their federation partners. It is a complete, enterprise-level and carrier-grade solution for secure identity information exchanged between partners. Irrespective of the protocol used, the OAM Federation Service can be successfully leveraged in both IdP and SP deployments, as shown in Figure 1 below.

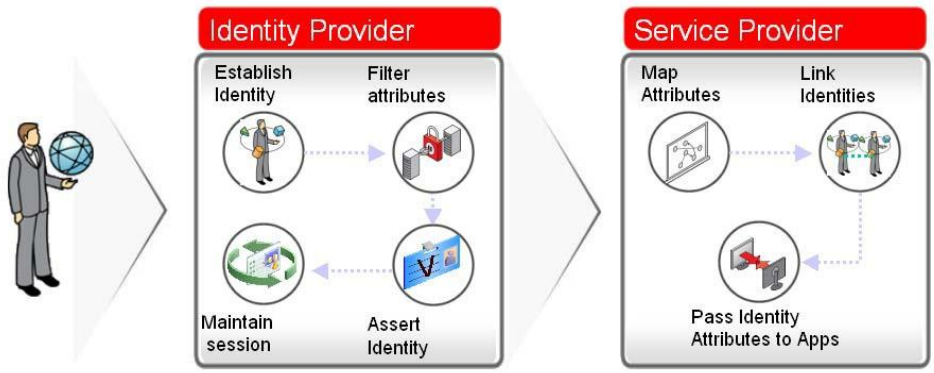

Figure 1: Interaction between identity and service providers

11g R2PS2: Full Convergence within Oracle Access Management

Beginning with the 11g R2 release, Federation services were first converged into the Oracle Access Management product as a shared service of OAM providing Federation Service Provider (SP) functionality. With OAM 11gR2PS2 , Oracle Access Management now includes now both IDP (Identity Provider) and SP(Service Provider) functionality. This integration illustrates Oracle's holistic, platform-centric approach towards identity management, and is driven by the need for a comprehensive identity and access management solution that can deliver long-term return on investment. The convergence of Identity Federation within the Oracle Access Management product lowers risk with centralized policy management and lowers costs with a single infrastructure to stand up once and activate services as needed while leveraging built-in integrations with other OAM services such as OAuth or risk and fraud detection. By taking a broader perspective on manageability, flexibility, and scalability, Oracle is able to offer a comprehensive identity and access management platform that delivers a far stronger and longer lasting value proposition than that of a heterogeneous patchwork of point solutions.

Integrated Administration

Identity federation is now a configurable service of the access management platform with a unified administration console.

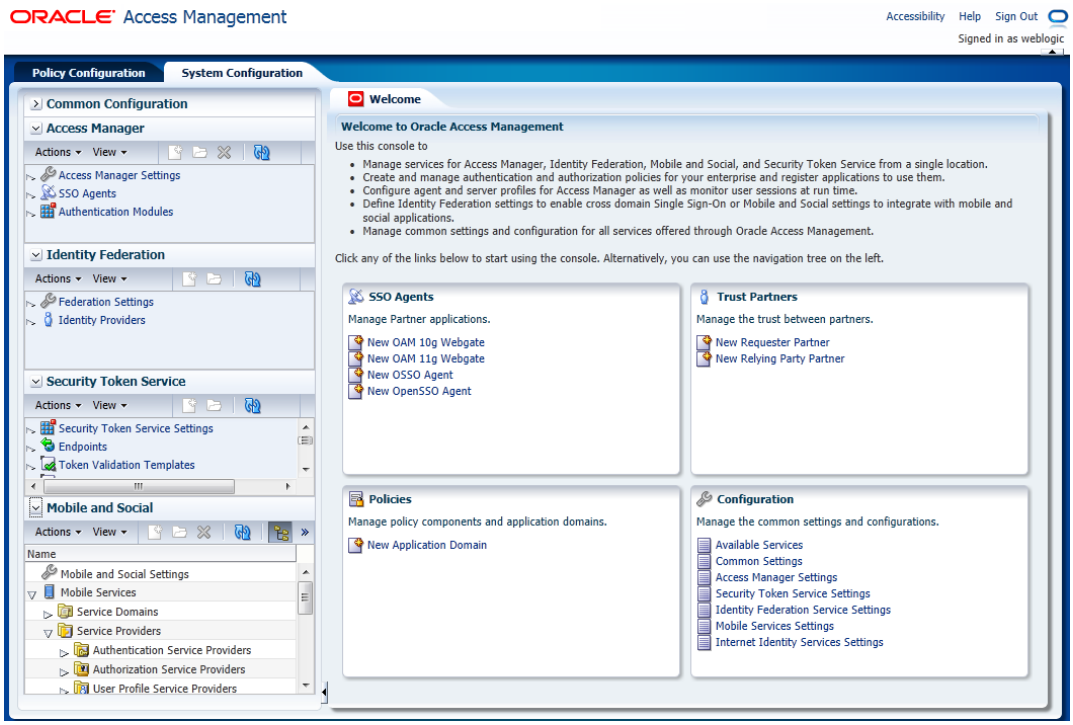

Figure 3: Admin Console Integration

The unified OAM Administration console is used to configure and manage the Oracle Access Management Federation Service

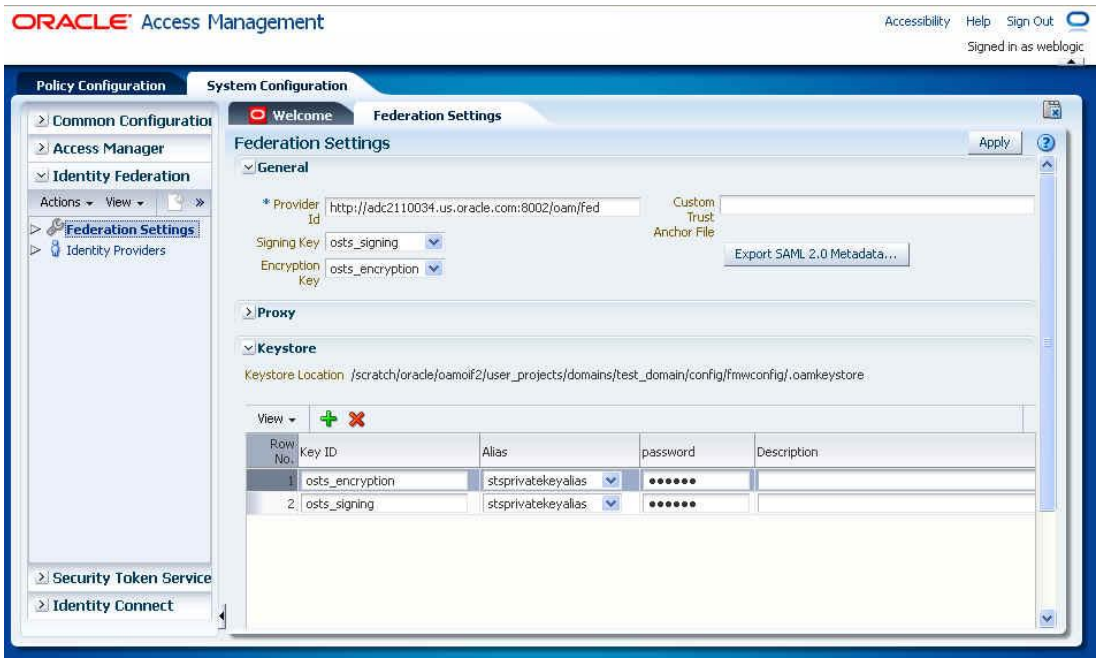

Figure 4: Using the unified admin console to configure Oracle Access Management Federation

Core Feature Set

The key features of the Oracle Access Management Federation Service 11gR2PS2 include:

- Support for multiple federation protocols
- Internet Level Scalability and Availability
- Identity Provider
- Identity Provider Proxy
- Service Provider
- Partner Profiles
- Attribute Sharing
- Identity Provider Discovery
- Provisioning Plug-in Framework
- Social Identity Registration

Each of these features will be discussed in more detail in the next section.

Multiple Protocol Support

Oracle regularly participates in vendor-neutral standards conformance events. In OAM R2SP2, the Oracle Access Management Federation Service is compliant with the following protocols both as an Identity Provider (IDP) and a Service Provider (SP) :

- SAML 2.0
- SAML 1.1
- OpenID 2.0
- FICAM (Federal Identity, Credential, And Access Management):
    - ICAM SAML 2.0 Web Browser SSO Profile - (Level of Assurance 1, 2, non-crypto 3).
    - ICAM OpenID 2.0 Profile (Level of Assurance 1)

The Oracle Access Management Federation Service supports the following attribute provider types:

- SAML Attribute Sharing Profile - SAML provides an Attribute Query/Response protocol for retrieving a principal's attributes.
- OpenID Attribute Exchange (AX) - AX is an OpenID 2.0 extension
- ICAM BAE (Backend Attribute Exchange) Direct Attribute Exchange
- ICAM BAE Broker Attribute Exchange - via an integration with the Oracle API Gateway

Internet-level Scalability and Availability

Oracle Access Management 11gR2 has been architected to provide internet-level performance, scalability, and availability. In support of this claim, Oracle conducted large-scale performance testing that included a database of over 250 million user accounts. The OAM server was able to demonstrate linear levels of performance as the number of access management servers increased, which is shown in the figure below.

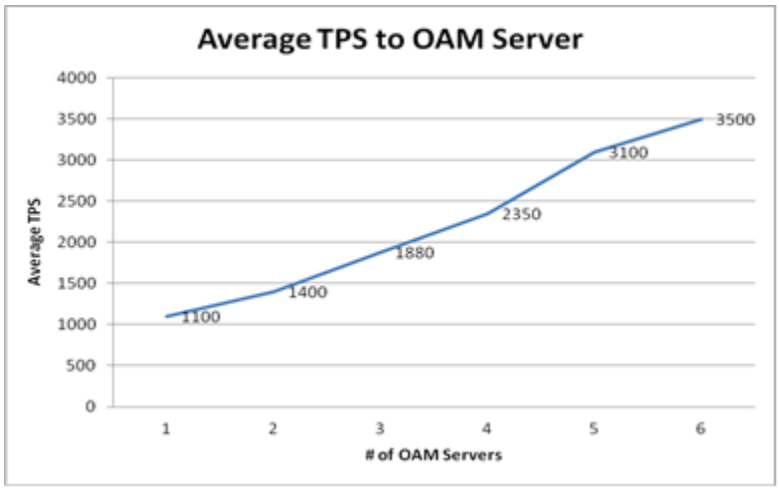

Figure 9: Linear performance improvements

Depending on service level requirements, HA strategies can range from relatively basic standby and active server configurations, up to cross-datacenter, active-active deployments. OAM Federation Services, as a part of Oracle's access management platform, supports the full range of HA topologies.

Identity Provider

When the OAM Federation Service is performing a Federation SSO with an SP partner, OAM Federation Service/IDP always internally forwards the user to OAM to:

- authenticate the user if non authenticated
- ensure that the authenticated user does not need to be challenged because of inactivity
- check that the optional requested federation authentication method specified by the SP partner does not require a challenge, if the requested method/scheme is stronger than the one used to previously challenge the user

The OAM Federation Service/IDP allows the user to leverage the full power of OAM for seamlessly providing flexible and comprehensive authentication mechanisms to authenticate the user. It uses the Federation Authn Method <-> OAM Authn Scheme mappings to determine how to challenge the user or to ensure that the user was authenticated with a scheme/level compatible with what was requested. If the SP partner does not specific a Federation Authn Method, the OAM Federation Service/IdP uses the one specified for the SP partner in:

- The SP Partner configuration entry

- The SP Partner Profile
- The global default scheme. The default is LDAPScheme.

From a logout perspective, the OAM Federation Service supports two flows:

- Logout initiated from OAM
    - User initiates logout by accessing the OAM logout service
    - OAM kills the OAM session
    - OAM displays a logout page that will instruct the various WebGates to remove the user cookies
    - OAM automatically redirects the user to the OAM Federation Service logout service and specifies where the user should be redirected at the end of the flow
    - OAM Federation Service performs the Federation Logout operation by notifying each partner involved in this session by:
        - Either redirecting the user with a Logout Request message via HTTP Redirect or HTTP POST
        - Or directly sending a Logout Request message via SOAP
    - OAM Federation Service kills the Federation session
    - OAM Federation Service redirects to the return URL
- Logout initiated from a Federation partner
    - User initiates logout from one of the partners involved in the federation
    - Partner redirects the user to the OAM Federation Service as part of the Federation logout
    - The OAM Federation Service marks the federated user session as logging out
    - OAM Federation Service redirects the user to OAM for logout
    - OAM kills the OAM session
    - OAM displays a logout page that will instruct the various WebGate agents to remove the user cookies
    - OAM redirects the user back to OAM Federation Service to resume the Federation logout flow
    - OAM Federation Service performs the Federation Logout operation by notifying each partner involved in this session (except the one who redirected the user to it in the first step) by:
        - Either redirecting the user with a Logout Request message via HTTP Redirect or HTTP POST
        - Or sending a directly Logout Request message via SOAP
    - OAM Federation Service kills the federated session
    - OAM Federation Service redirects the user with a Logout Response message to the partner who sent the user to it in the first step

When OAM Federation Service acts as an IDP, it creates or issues an Identity Token that is provided to the SP during the Federation SSO operation. That token contains user information as well as session information that can include any identity attributes known to the sending domain. OAM Federation Services provides the ability for an administrator to define Authorization expressions that can be evaluated during a Federation SSO.

Identity Provider Proxy

OAM Federation Services provides IDP Proxy capability that allows it to leverage a federation partnership itself as an authentication mechanism to authenticate the user. Following outlines the flow when OAM Federation Services acts an IDP Proxy (IDP1):

- IDP (IDP1) Receive an Authn Request from a remote SP Partner (SP1)
- Instead of authenticating the user locally, the IDP (IDP1) becomes an SP (SP2) and starts a second Federation SSO flow with a remote IdP Partner (IDP2)
- The second IDP (IDP2) authenticates the user, creates an assertion and redirects the user to the proxy IdP/SP (SP2)
- The proxy SP (SP2) validates the assertion and identifies the user
- The proxy IDP (IDP1) resumes the first Federation SSO flow, creates an assertion and redirects the user to the original SP (SP1)

OAM Federation Services/IDP supports the IDP Proxy flow by:

- Internally sending the user to OAM for authentication
- Specifying that the user should be challenged via a FederationScheme: that will trigger the second Federation SSO with a remote IDP

Service Provider

OAM Federation Services/SP seamlessly allows building risk and fraud awareness in a federated session. In a Federation world when the IDP authenticates the user via different mechanisms (username/password, X.509, RSA SecurID, fingerprints…) it can indicate so to the SP via the Federation Authentication Method in the assertion (for e.g. AuthnContext in SAML 2.0 or PAPE in OpenID 2.0 etc …). OAM Federation Services/SP provides the capability of providing a way to map Federation Authentication Methods to authentication levels, and at runtime to determine the authentication level from a give assertion (based on the included Federation Authentication Method) instructing OAM to create a session with the mapped authentication level. This allows OAM to create a session with an authentication level that reflects the manner with which the user was challenged at the IDP and thereby seamlessly trigger fraud and risk detection with built-in integrations with OAAM.

OAM Federation Services/SP also supports sophisticated attribute mapping capabilities to:

- Request attributes from the IDP at runtime during Federation SSO flows for protocols that support such a feature (such as OpenID 2.0)
- Map the name of an incoming assertion attribute to a local name (ATTR_NAME for example) that will be available in the OAM session (via the name $session.attr.fed.attr.ATTR_NAME for example)

Attribute Sharing

The OAM Federation Service implements a superset of the X.509 Authentication Based Attribute Sharing Profile (XASP). It provides Attribute Requester (SP) and Attribute Responder (IDP) functionality that is fully integrated with the OAM Custom Authentication Module framework via an Attribute Sharing Plug-in. This allows for seamless back channel attribute sharing while leveraging any of the OAM authentication flows.

Identity Provider Discovery

The OAM Federation Service support Identity provider discovery functionality that enables the selection of an identity provider (possibly through interaction with the user) to use during SSO. While Identity Federation does not itself provide an identity provider discovery service, it provides support for using such a service to select an IDP, if one is not passed in the authentication request to the SP during SP-initiated SSO. When acting as a service provider, Identity Federation can be configured so that if an SSO operation is initiated without the provider ID of the partner IDP, the user is redirected to an IDP discovery service to select the identity provider with which to perform SSO.

Provisioning Plug-in Framework

When a federated SSO transaction is initiated, the processing flows as follows:

- The IDP authenticates a user and sends an assertion to Oracle Access Management Identity Federation.
- Acting as SP, Identity Federation maps the user to the local identity store.
- If the user does not exist in the local store, the mapping fails.

The OAM Federation Service allows resolution of this issue by provisioning the user so that the transaction can continue by providing a configurable provisioning plug-in to provision the user, handle errors as well as provide custom attributes while creating a record for the user in the identity store associated with the IDP partner. The OAM Federation Service also provides a custom provisioning plug-in framework that allows sophisticated workflow and error handling logic to be incorporated while provisioning the user.

Social Identity Registration

For social identities when the Identity Provider is an OAuth (Facebook, LinkedIn) or Open ID Provider (Google, Yahoo), the Oracle Access Management Federation Service allows seamless registration of the social account and provides the ability to automatically trigger a user self-registration flow that creates a local account for the user. Furthermore as shown in Figure 7 below, the Oracle Access Management Federation Service can act as both Relying Party and OpenID Provider in accordance with the OpenID 2.0 specification allowing organizations to start accepting OpenID from leading providers such as Yahoo and Google or to become an OpenID provider themselves. Users can subsequently securely leverage their corporate identity at OpenID-enabled blogging sites or socials networks such as Facebook.

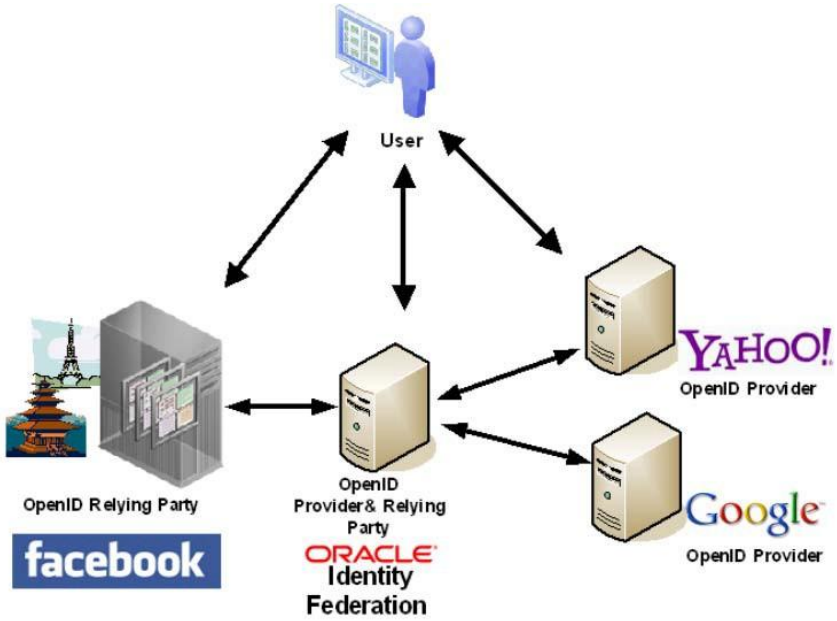

Figure 7: Using OpenID to leverage corporate credentials

Conclusion

Federation standards allow identities to be transferred between domains without content restrictions. A federation request can contain any identity attributes known to the sending domain. The request can include UID, name, address, role, or group membership information. The freedom to include practically anything in the federation message makes federation simultaneously flexible and complicated.

The flexibility of the technology helps organizations implement federation procedures that suit their needs. However, creating trust relationships requires more than technology. To lay a foundation for the use of this type of technology, organizations need to develop a strong understanding of their federation needs and subsequently achieve business agreements with its partners. The Oracle Access Management Federation Service allows organizations to leverage standards and existing identity and access management investments, in order to realize:

- Accelerated SaaS/cloud adoption via streamlined deployment options
- Reduced cost of integration projects through support of industry federation standards
- Greatly minimized identity ownership overhead via elimination of unnecessary user identities in the enterprise directory
- High return on investment resulting from support for a wide variety of data stores, user directories, authentication providers and applications

The Oracle Access Management Federation Service is a core component of Oracle's industry leading identity and access management platform. The 11*g* R2PS2 release delivers a fully converged federation service architecture within Oracle Access Management, enabling several common business scenarios to seamlessly work out of the box. Additionally, a compelling set of new features enable additional scenarios and easier overall management.

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

http://www.oracle.com/identity

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

Oracle Access Management Federation 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

Hardware and Software, Engineered to Work Together