An Oracle White Paper
July 2012

Oracle Identity Federation

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

Oracle Identity Federation (OIF) is one of the core services of Oracle Access Management Suite Plus. OIF provides a complete, enterprise-level, carrier-grade solution for exchanging identity information securely between partners. With OIF, organizations can conduct business online with confidence, by providing to their business partners secure access to protected applications. OIF significantly reduces 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 detail how OIF is able to address these challenges. The functional capabilities described span both the 11g R1 and R2 releases; release-specific functionality will be explicitly called-out as such.

Business Challenges with Integrating Websites

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 OIF helps organizations address them, is discussed in the next section.

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 cause significant delays in to cloud projects, subsequently slowing down cloud adoption and preventing IT from keeping pace with the needs of the business.

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.

OIF: A Comprehensive Solution

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

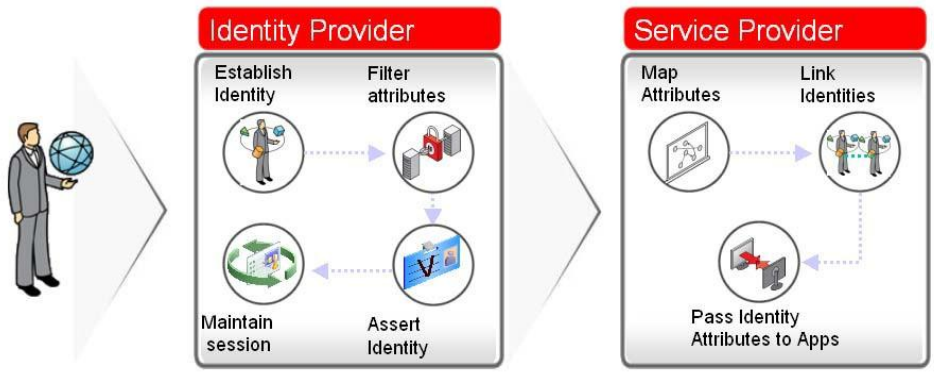

Figure 1: Interaction between identity and service providers

With OIF, organizations can do more business online by helping their business partners to get started on federation and quickly achieve single sign-on without extensive knowledge of SAML. OIF significantly reduces the need to create unnecessary identities in an enterprise directory and lowers the ongoing costs of partner integrations through support of industry federation standards.

OIF protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications. Using its extensive and flexible integration framework, it can be rapidly deployed in any multi-vendor environment.

11g R2: Convergence within Oracle Access Management

Beginning in the 11g R2 release, OIF is converged into a shared service of OAM. 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. 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.

As an example, by moving to a converged architecture, OAM policies can now leverage OIF SAML attributes for authentication and authorization workflows out-of-the-box. Previously, this scenario would require custom integration in order to implement.

Shared Service Architecture

OIF is now a converged service of the Oracle Access Manager (OAM), as shown in Figure 2 below. There is a single, unified WebLogic managed server and installation happens via a single EAR file. OIF can leverage the OAM identity store and/or multiple LDAP stores.

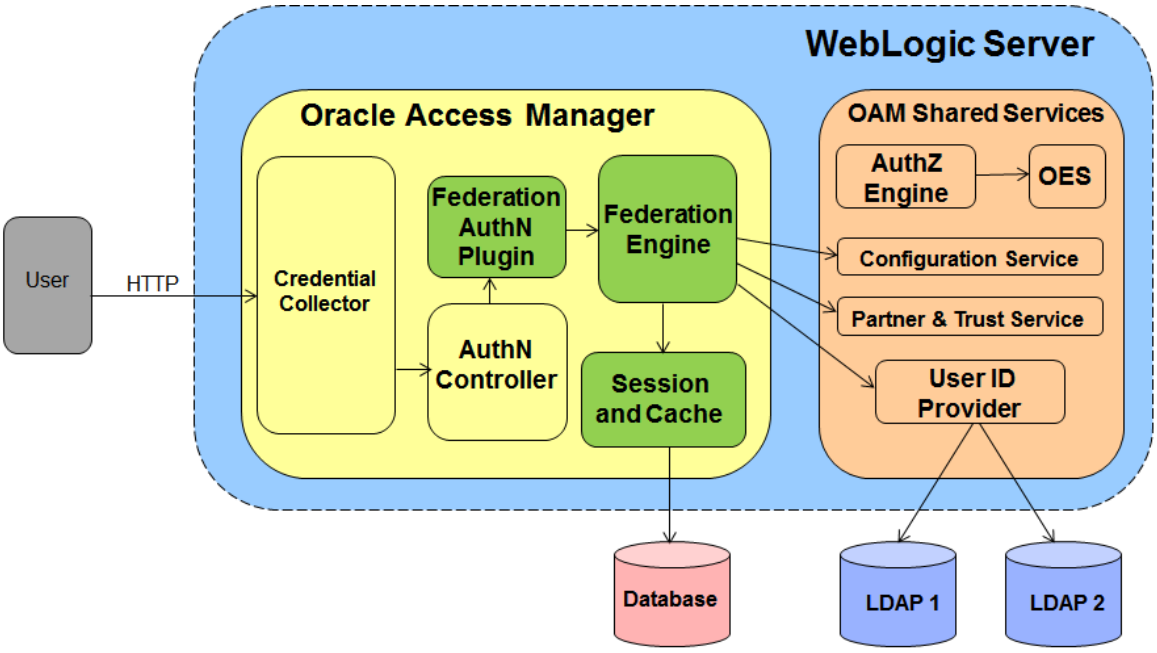

Figure 2: Convergence of OIF Service Provider within Oracle Access Manager

As of the initial R2 release, only service provider capabilities are converged with OAM. Still, the OIF 11g R1 and 11g R2 releases can be used in conjunction with one another as business needs dictate. When the time comes to upgrade R1 instances to R2, this can be accomplished in a seamless fashion.

Integrated Administration

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

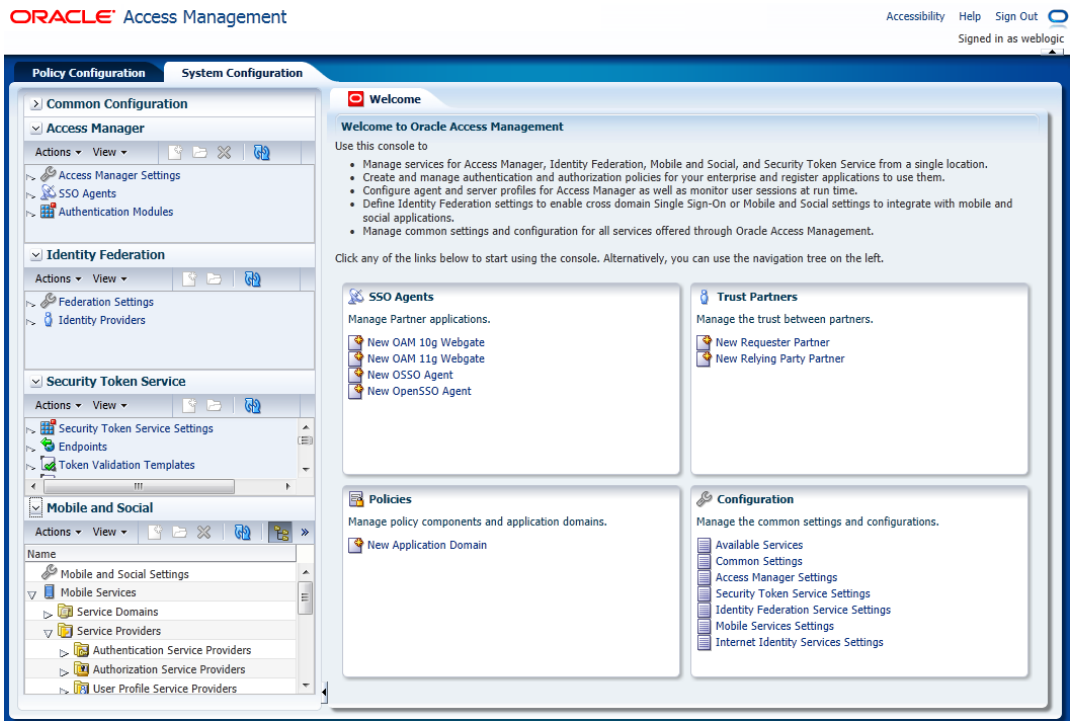

Figure 3: Admin Console Integration

Both the OAM admin console and WebLogic Scripting Tool (WLST) can be used to configure and manage OIF.

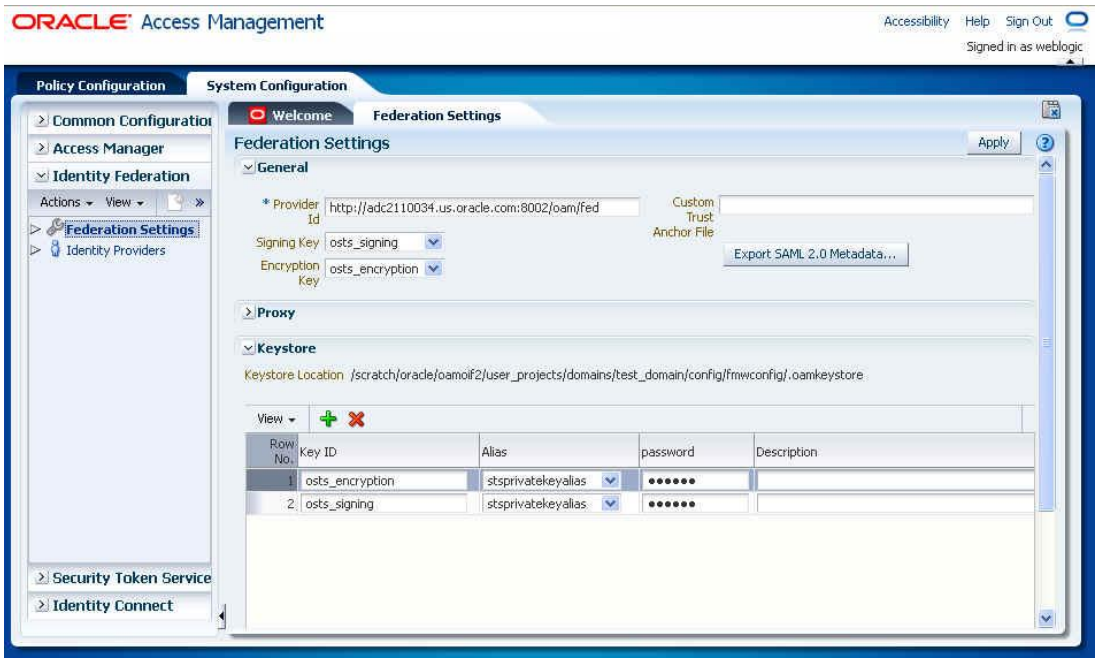

Figure 4: Using the unified admin console to configure OIF

Business Value

OIF is a core pillar of Oracle Access Management Suite. Adoption of an enterprise class federation solution such as OIF, results in meaningful value for the business. Several examples illustrating this business value are detailed below.

Accelerated SaaS Adoption

With OIF, IT organizations can respond to the growing needs of the business. OIF supports all the leading federation standards, enabling organizations to federate with virtually any SaaS or cloud vendor in the market regardless of the protocol versions used. This increases the flexibility to choose different service providers, avoids costly, proprietary lock-ins, and gives customers the ability to source the services that best meet their business-specific needs. In addition, by using OIF, customers gain the flexibility to quickly replace SaaS vendors if needed.

OIF offers a lightweight service provider deployment option. This capability helps customers acting as identity providers quickly achieve cross-domain SSO with their partners who don't have extensive federation infrastructure or knowledge. With this option, service providers can quickly stage a production deployment on their side without getting trained on OIF or the intricacies of SAML.

OIF also delivers enterprise-class partner management capabilities for service providers who need to interact with multiple identity provider (IdP) partners using different single sign-on protocols. With OIF, new partner endpoints can be configured and tested in a matter of minutes.

Reduced Cost of Integration Projects

OIF saves time and money associated with building and maintaining of proprietary and homegrown federation solutions. Once implemented, OIF allows customers to federate with all their partners via industry standards and to add new partners without needing to fund new IT projects.

Elimination of Identity Ownership Burden

OIF offers a sophisticated and flexible way of managing federation agreements. This makes it possible for identity providers to share much less information about the user and yet achieve the required behavior in the receiving application. With OIF it's possible for the identity provider to communicate user attributes to the federation partners on an as-needed basis. This allows the service provider to store only necessary information and often eliminates the need to have a local identity for each individual user.

In cases when a local identity is still required, OIF reduces cost of audit and compliance by providing complimentary enterprise-grade audit and compliance features.

Long-Term Return on Investment

OIF protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers, and applications. With OIF, organizations are able to leverage their existing identity infrastructure, avoiding the need for costly additional technology investments. Moreover, OIF

is very simple to install and configure. New server instances can be deployed and in production in a matter of days. The user interface is streamlined to make common tasks, such as adding new partner endpoints, achievable in a matter of minutes.

Core Feature Set

The key features of OIF include:

- Support for multiple federation protocols
- Support for heterogeneous architectures
- Lightweight deployment option for service providers
- Support for external authentication and authorization
- Support for Microsoft Windows CardSpace authentication
- Support for OpenID
- Custom actions
- Simple administration and management
- Enterprise scalability, availability and manageability

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. OIF has achieved both the Liberty Alliance certification for Liberty ID-FF, and the Kantara certification for SAML 2.0.

OIF supports the following protocols:

- SAML 1.0 / 1.1 / 2.0
- Liberty Alliance ID-FF 1.1 /1.2
- WS-Federation
- OpenID 2.0
- Logout (SAML 2.0)
- IdP/SP-initiated SSO

Support for Heterogeneous Architectures

OIF bundles all the required components necessary for a complete implementation without creating external dependencies or additional operational footprint. The service exposes a set of simplified programmatic interfaces for seamless integration with any application or identity and access management solution that an IT organization may have in place.

Lightweight Deployment Option for Service Providers

OIF includes Oracle OpenSSO Fedlet, a lightweight service provider implementation of the SAML2.0 single sign-on protocol. Fedlets enable quick, cross-domain single sign-on by providing a significantly simplified deployment option, which does not require extensive knowledge of SAML. With Oracle OpenSSO Fedlet, service providers can consume identity assertion and receive user attributes from OIF as shown in Figure 5.

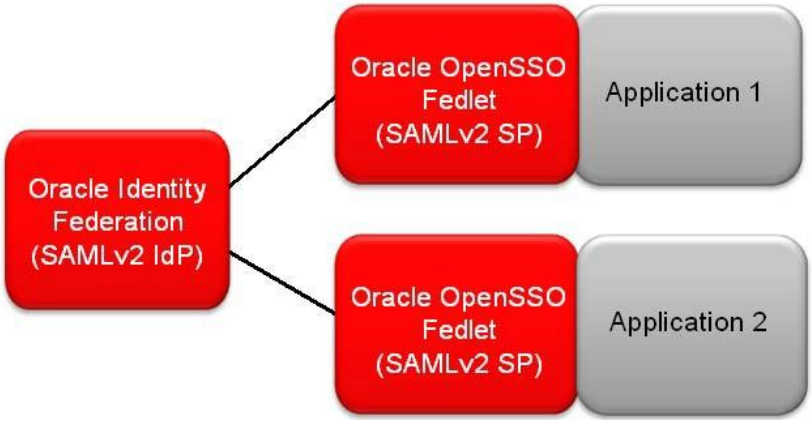

Figure 5: Service provider consuming OIF identity assertions via Fedlets

External Authentication and Authorization

OIF natively supports a wide variety of authentication providers, which can be as simple as a user directory or as feature-rich as OAM. In the environment where an authentication or authorization system is deployed, OIF can leverage these providers in two ways:

- OIF acting as a service provider: Receiving identity assertions and authenticate users locally based on the information sent by an identity provider partner.
- OIF acting as an identity provider: Authenticate users and retrieve user attributes or entitlements. Subsequently generate identity assertion and pass these on to service provider partners.

OIF also includes a set of integration modules for communicating with a variety of external applications and access control systems, as illustrated in Figure 6. Partnering applications can use this information to determine access privileges of federated users for auditing purposes, personalization, or any other business-specific logic.

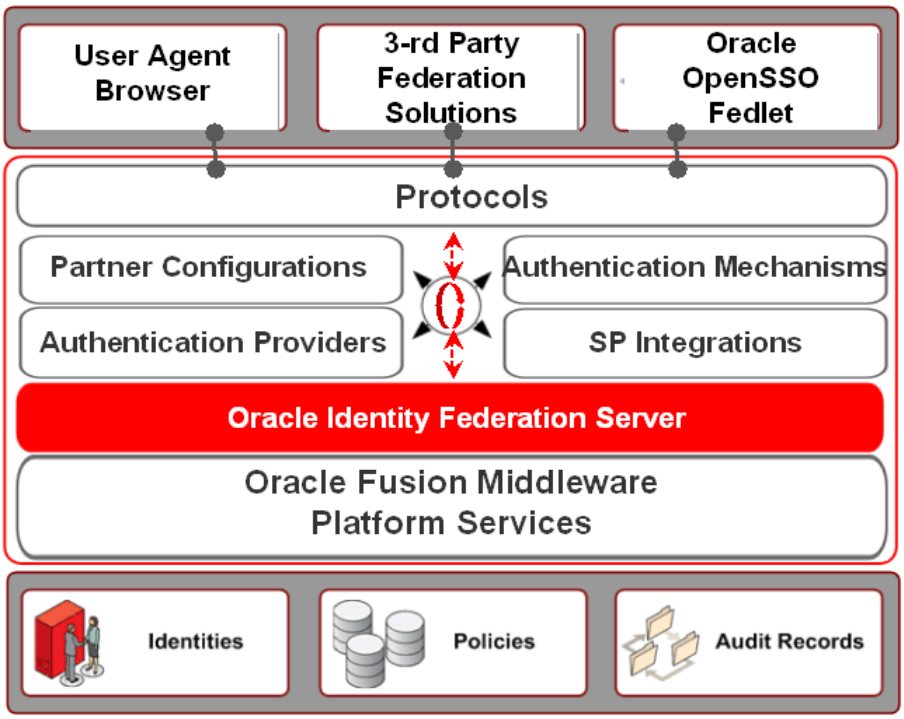

Figure 6: OIF integration points

OpenID 2.0

OIF can act as both Relaying Party and OpenID Provider in accordance with the OpenID 2.0 specification. OIF enables organizations to start accepting OpenID from leading providers such as Yahoo and Google or to become an OpenID provider themselves. Users can subsequently leverage their corporate identity at OpenID-enabled blogging sites and socials networks such as Facebook.

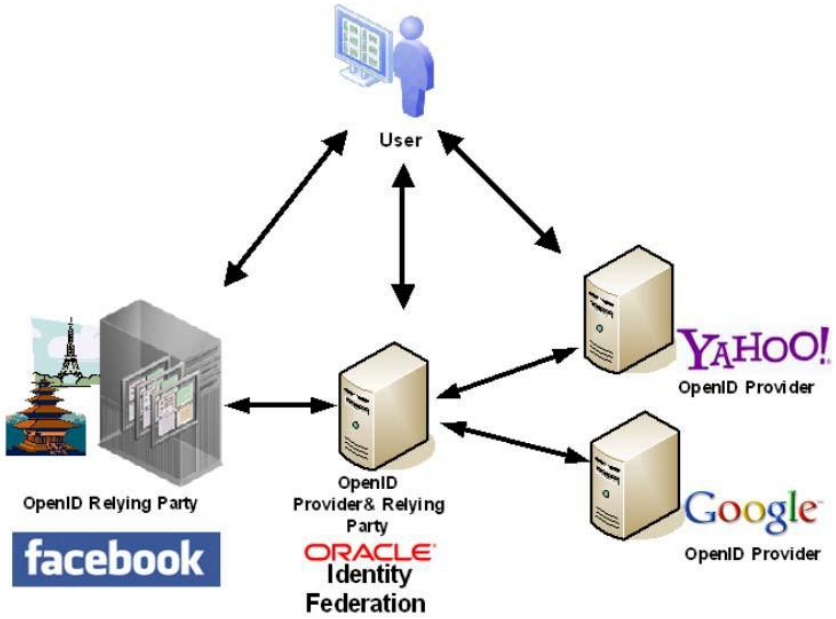

Figure 7: Using OpenId to leverage corporate credentials

Custom Actions

OIF custom actions enable site-specific operations to be executed during federated authentication. It gives organizations additional flexibility to implement an authentication process that meets their specific security and business needs. Custom Actions help both identity providers and service providers streamline integrations and reduce application deployment time. For example, an identity provider can use a custom action to dynamically generate additional user attributes, without storing them in a directory or a database. The generated attributes can be then added to an attribute statement that is then sent to a service provider. A service provider can implement a custom action to manipulate identity data received from identity providers and prepare it for consumption by existing applications or internally developed security tools.

OIF makes development of custom actions straightforward and does not require extensive knowledge of federation protocol as they are exposed as simple J2EE modules. Once developed, a single custom action can be leveraged to customize authentication flows irrespective of the protocol choice.

Simplified Administration and Management

OIF provides simple, easy to master interfaces for common management and administration tasks. The key interfaces are:

- The Access Manager console for UI-based administration and management tasks
- Command-line scripting via the WebLogic Scripting Tool (WLST)
- Oracle Enterprise Manager (OEM) for monitoring and troubleshooting

OIF is the only federation product on the market that comes with enterprise-grade operational management out-of-the-box. OEM adds the following features to OIF:

- Federation Administration console for configuring protocol settings, partner endpoints, metadata, authentication providers, account mapping, and performing other administration tasks as shown in Figure 8 below.
- Operational monitoring of server status, adapter status, system status including CPU & memory utilization
- Single dashboard view of entire deployment topology and server status including all Oracle Fusion Middleware components, databases, and applications.
- Trigger enterprise alerts via SNMP or email
- Integration with Fusion audit and logging viewers enables both a single view of both OIF logs and end-to-end tracing of a transaction across the full application stack
- Built-in standard reports via out of the box integration with Oracle BI Publisher

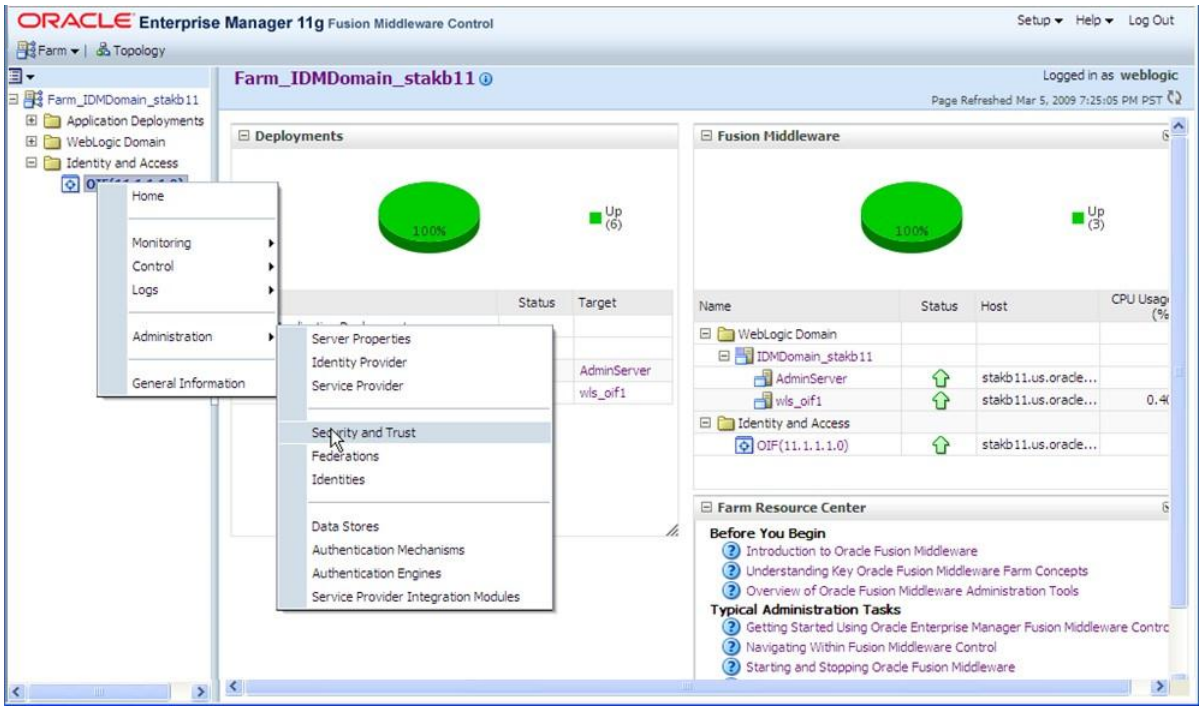

Figure 8: Integrated monitoring and troubleshooting via Oracle Enterprise Manager

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.

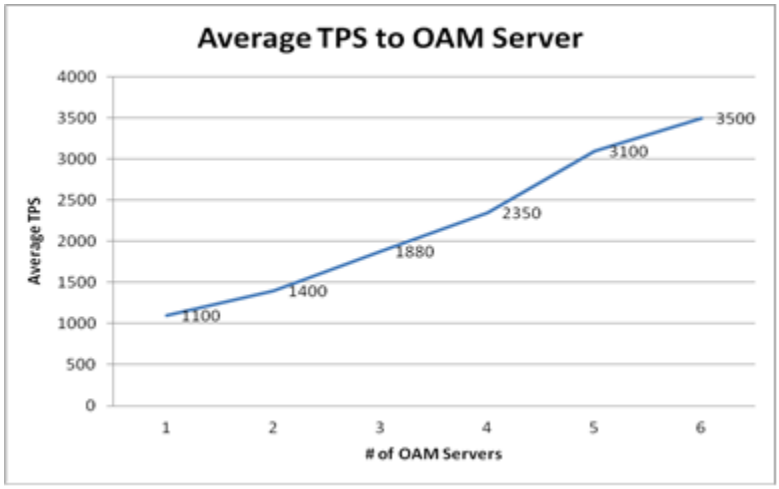

Figure 9: Linear performance improvements

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

Federation Methodologies

Three common federation methodologies will be introduced in this section, along with a corresponding discussion of how OIF can be used to implement each in practice.

Transient Federation

The key in transient federation is trust. Only the user session is transferred from one domain to the other. No additional identity data is sent between domains, and all authentication and authorization happen in the sending domain. Consequently, the receiving domain must trust (and be able to trust) the information sent by the initiating domain.

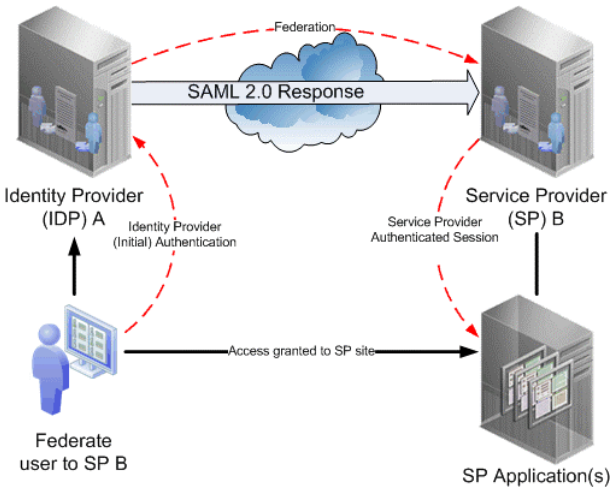

Figure 10: Transient federation

Transient federation is one of the simplest ways to implement federation. Owing to this simplicity, the configuration efforts in both federation domains are easy, and once accomplished, don't have to change over time. The major benefit of transient federation is its ease of use. Users don't have to know that they have been federated. Federations can be presented as a simple link in the sending domain, and then by clicking the link, the user is automatically and transparently redirected to the receiving domain as an authenticated user.

OIF for transient federation on an identity provider often implement this in conjunction with Oracle Access Manager, though this is not a requirement.

Account Mapping

As transient federation sets certain restrictions on trust relationships and information confidentiality, more secure methods are often required if domains participating in a federation do not completely trust one another, or if there are some constraints on the information that federated users can access. Account mapping requires federated users to have accounts in the respective domains and some agreed upon basis for mapping accounts.

From a technical perspective, account mapping is a bit more complicated than transient federation, but it provides much more control for the receiving domain. The receiving domain is able to receive messages from the sending domain that includes an agreed upon element, such as a user ID. The value of this element is then checked against an existing identity in the receiving domain, and if a valid identity is found, the user session is transferred and access to applications or services in the receiving domain is granted. .

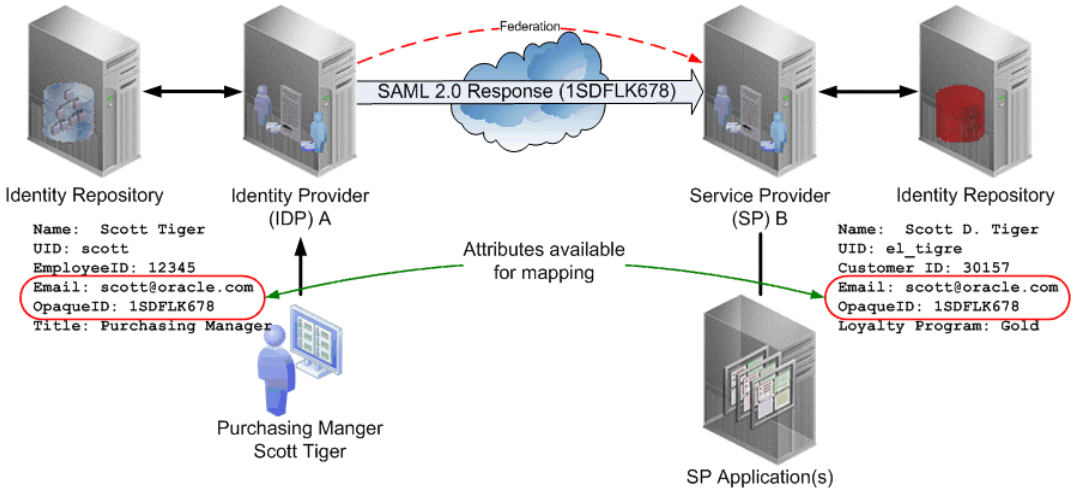

Figure 11: Federation via account mapping

Account Linking

Yet another option is accounting linking, which is really an extension to the account mapping process. The idea behind account linking is that existing user accounts in the receiving domain are updated with the identity information from the sending domain upon first federation.

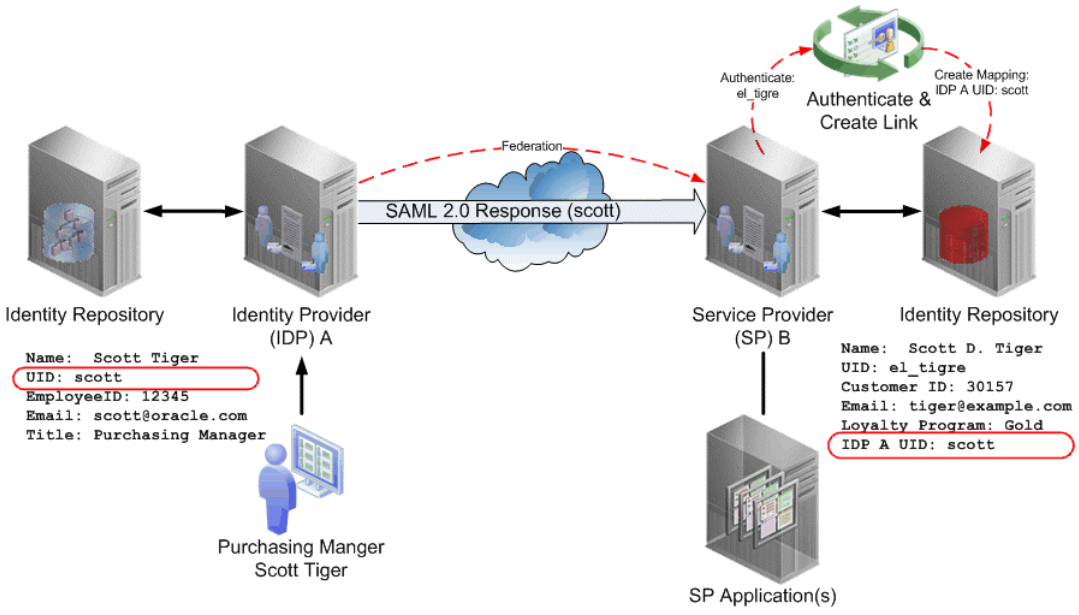

Figure 12: Federation via account linking

As shown in Figure 12, the receiving domain will require user authentication when it gets a federation message from the sending domain, and cannot find the user identity in its own identity store based on the identity attribute it received from sending domain. If the user is successfully authenticated in the

sending domain, the receiving domain updates a local user identity with new information. This information links the two identities to enable account mapping in the future.

Customers, who use OIF for attribute mapping and attribute linking, often implement it in conjunction with Oracle Access Manager, Oracle Directory Services, and Oracle Identity Manager.

Additional Considerations

Identity federation technology exists in two closely related forms: browser-based or document- based. Document-based federations are focused on the use of XML documents transported between two security domains leveraging web service standards.

Document-Based Identity Federation

With document-based federation, the underlying applications can be either invoked by a human user or an application in the absence of direct human involvement. Document-based federation requires the definition of XML document structures, definitions of credential representations, and locations of credential information among other things. Ultimately, document-based federation allows systems to communicate via SOAP or other APIs, using a shared authentication token.

Browser-Based Identity Federation

Browser-based federations are focused on live, interactive application users manually providing credential information on one security domain and subsequently being authenticated in another domain.

A Complete Platform

Both modes of federation rely on standards to simplify how applications residing in two independent security domains can work together for the benefit of common users or shared business processes. Standards such as SAML and WS-Federation define mechanisms of sharing authenticated browser sessions across domains of control. In practice, most IT organizations start with one model, but eventually need to support both.

Oracle offers a solution for both browser-based and document-based federation. Browser-based federation is provided by the OIF service. Document-based federation is provided by the Oracle Web Services Manager product.

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, the organization needs to develop strong understanding of its federation needs and subsequently achieve business agreements with its partners. OIF 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

OIF is core component of the Oracle's industry leading identity and access management platform. The 11*g* R2 release moves toward a converged architecture with 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.

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 Identity Federation and the Oracle Identity and Access Management platform, please visit:

http://www.oracle.com/identity

Oracle Identity Federation
July 2012
Author: Robert Zare

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