

An Oracle White Paper
August 2010

Oracle OpenSSO Fedlet

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.....	2
About Oracle OpenSSO Fedlet	3
Key Features.....	4
Deployment Architecture	4
Deployment Assumptions and Constraints	7
Understanding Typical Business Use Case	8
Evaluating Benefits and Tradeoffs	9
Conclusion	11

Executive Overview

Over the past several years, innovations to Internet technologies and federation standards helped enterprises and business partners to achieve unprecedented levels of online collaboration, primarily because they are now able to implement business and legal agreements through simple, technical integrations. Federation standards have gained broad acceptance, and commercial products that implement those standards have become cost effective not only for large corporations, but also for midsize and small organizations. Where before IT organizations had to materialize their federation vision through in-house development, now they can choose from a range of interoperable, enterprise-grade, standards-based products, which substantially lowers the costs, reduces the time required, and minimizes the risks of setting up point to point and multi-partner federation projects. As a result, exposing business functions to partners over standards-based, federated trust relationships is no longer an innovation but rather a norm for any company doing business online.

Most enterprises however still experience difficulties with their federation projects when they encounter small partners who have not yet adopted a federation standard such as Security Assertion Markup Language (SAML). The most common reasons for resisting a federation protocol adoption are:

- **Avoiding costs.** Adopting a federation standard would require investments in hardware, services, and human resources that your partner cannot afford or justify.
- **Lack of confidence.** The partner doesn't have experience implementing identity federation protocols and/or trained workforce.

Without the benefit of standard protocols and the products that support them, partner integration projects can be significantly delayed. In order to meet deadlines, companies often resort to developing proprietary one-off integration solutions. This approach introduces unnecessary security risks and higher implementation and maintenance costs.

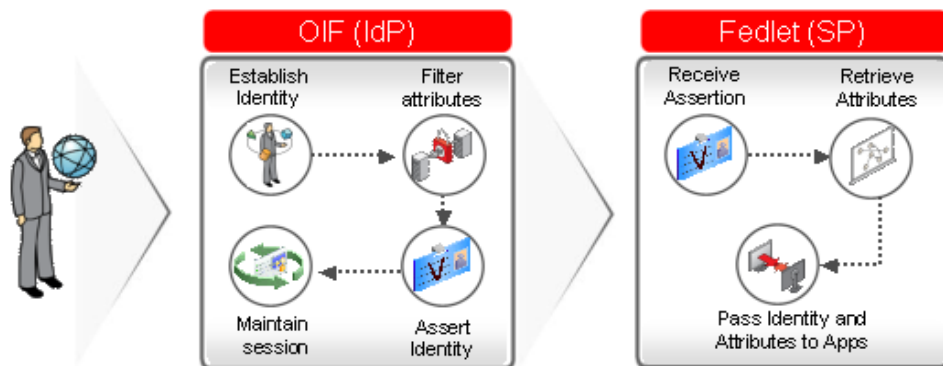
Oracle solves the problem of complex partner integrations with a simple, innovative solution: Oracle OpenSSO Fedlet. Oracle Identity Federation and Oracle SSO Fedlet together comprise a complete, enterprise-level, carrier-grade solution for secure identity information

exchange between partners. Using Oracle OpenSSO Fedlet organizations can quickly and easily set up standards-based federations with Service Provider partners, create a standard integration pattern for additional partners, and achieve secure sign-on across partners in a matter of hours, not days or weeks.

About Oracle OpenSSO Fedlet

Oracle OpenSSO Fedlet (Fedlet) is a compact, easy to deploy SAMLv2 Service Provider implementation. It includes a small software package and a simple file-based configuration, embeddable into a Service Provider's Java EE or .NET application. Fedlet establishes SSO between an Identity Provider instance and the Service Provider application without requiring a fully featured federation product on the Service Provider side.

Organizations that use Oracle Identity Federation as a SAMLv2 Identity Provider, can distribute Oracle OpenSSO Fedlet to their partners. This gives the Identity Providers a way to retain control over security settings, configuration, and distribution mechanism of the Service Provider federation components. This approach not only accelerates deployments but also enables better ongoing management of federation interactions between partners.



Service Providers also can get Oracle OpenSSO Fedlet directly from Oracle. Once deployed, Oracle OpenSSO Fedlet can accept SAMLv2 assertions from any SAMLv2 Identity Provider and retrieve user attributes to accomplish single sign-on (SSO) and content personalization. Fedlet can be configured to communicate with any number of Identity Providers. It also can leverage an external Discovery Service to find the preferred Identity Provider.

Key Features

Oracle OpenSSO Fedlet is available in Java and .NET versions. The following table lists the key features for each version.

Feature	Java	.NET
SAMLv2 Single Sign On (Post, Artifact)	Yes	Yes
SAMLv2 Single Logout (Post, Redirect, SOAP)	Yes	Yes
Attribute Query	Yes	
Signing of Requests and Responses	Yes	Yes
Encryption/Decryption of Attribute, Assertion, and NameID elements	Yes	Yes
Export of SP Metadata	Yes	Yes
Discovery Service with Multiple IDPs	Yes	Yes
External IDP Discovery Service	Yes	Yes
Bundled IDP Discovery Service (Reader service only)	Yes	

Deployment Architecture

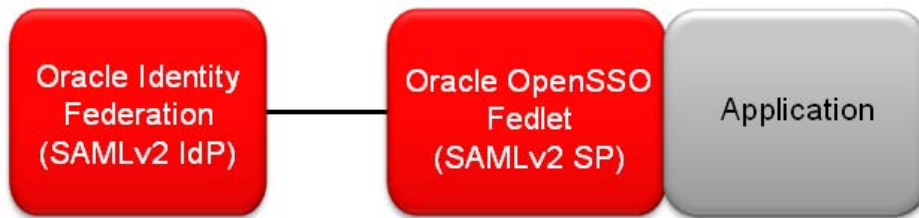
This section describes typical deployment scenarios for Oracle OpenSSO Fedlet. In the most commonly used deployment, Oracle Identity Federation plays the role of Identity Provider, while Oracle OpenSSO plays the role of Service Provider.

Deployment options

Each Service Provider application requires its own Oracle OpenSSO Fedlet instance. The deployed Fedlet instance acts as an independent Service Provider endpoint and can be configured to exchange SAMLv2 messages with one Identity Provider or with a few Identity Providers.

Oracle OpenSSO Fedlet with a single Identity Provider

Deploying a separate instance of Oracle OpenSSO Fedlet per each Identity Provider is the simplest deployment option. It is a common deployment scenario for organizations that have only one partner. It is also useful in SaaS multi-tenant deployments, where each SaaS customer acts as an Identity Provider (IdP). Then each of the tenant applications authenticates remote users coming from its' own IdP. In such environments, each Oracle OpenSSO Fedlet instance is configured to always communicate with the same IdP.



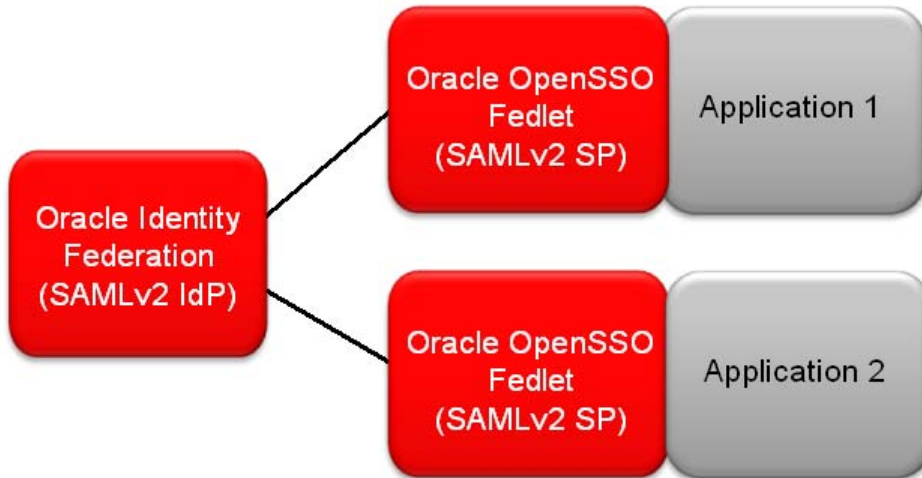
Oracle OpenSSO Fedlet with Multiple Identity Providers

Frequently organizations need to deploy an application instance and enable that application to receive identity data from multiple Identity Providers. This is an important requirement for organizations with many partners who need to access the same application.

Allowing an organization to dynamically add new Identity Providers and allow them to authenticate users or provide additional attributes about those users to an already deployed application - without having to add more application instances - provides a tremendous business advantage in terms of shorting the time to deployment and increasing value to end users.

In this case, a single instance of Oracle OpenSSO Fedlet can be used to authenticate users against more than one Identity Provider. The Fedlet also can be deployed in conjunction with an Identity Provider Discovery Service to allow users to select a preferred Identity Provider. When configured this way, the Identity Provider Discovery Service remembers the user's preferred Identity Provider information, and communicates it to Oracle OpenSSO Fedlet. Oracle OpenSSO Fedlet can leverage Oracle Identity Federation instance as an Identity

Provider Discovery Service or any 3-rd party Identity Provider Discovery Service present in your environment.



Integrating Oracle OpenSSO Fedlet with Service Provider Application

Oracle OpenSSO Fedlet includes a sample JSP module. It can be used to simply and quickly integrate Oracle OpenSSO Fedlet with any application. The following outlines the typical ways to integrate Oracle OpenSSO Fedlet with a Service Provider application:

Embedded Application

This option is useful for testing and training purposes or to jumpstart new development. Developers can use the Oracle OpenSSO Fedlet sample JSP module as a template for a brand new Service Provider application.



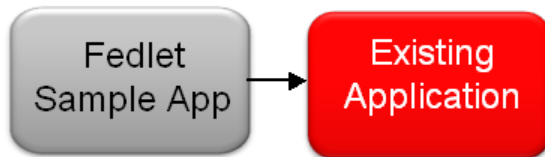
Embedded Oracle OpenSSO Fedlet

The embedded Oracle OpenSSO Fedlet sample option offers a simple way to add SAMLv2 features to applications that need to be deployed in a number of multiple locations. The integration is done only once during development. Once the development is completed, the Oracle OpenSSO Fedlet is packaged with an application, and is fully embedded in it.



Request Forwarding

This option is designed for situations when an already deployed business application needs to be SSO-enabled with minimal disruption to an existing service. The Oracle OpenSSO Fedlet sample can be deployed in front of an application to forward the HTTP traffic to/from the business application (remember that data security between the Oracle OpenSSO Fedlet sample and the business application is typically the responsibility of the application developer).



Deployment Assumptions and Constraints

- The configuration files and SAML metadata for Oracle OpenSSO Fedlet are stored in a flat file at the Service Provider.
- For Single Sign-on Fedlet supports SAMLv2 HTTP POST and Artifact bindings.
- For Single Logout Oracle OpenSSO Fedlet supports HTTP Post, Redirect, and SOAP bindings.

- Oracle OpenSSO Fedlet supports verification of the XML signature carried in the SAML Assertion from an Identity Provider. XML signature verification is done using the Identity Provider's public certificate included in the Identity Provider metadata XML file. If the Identity Provider signing certificate changes, the Identity Provider metadata in the Oracle OpenSSO Fedlet configuration directory must be updated to include the new signing certificate information.

Understanding Typical Business Use Case

The following example illustrates how organizations can take advantage of Oracle OpenSSO Fedlet. SmartPhones Telecom, a large telecommunications company, uses Oracle Identity Federation to implement a SAMLv2 Identity Provider service. Subscribers of SmartPhones Telecom use a custom user portal to receive personalized content, which is delivered by business partners of SmartPhones Telecom: StockService.com and Weather.com. StockService.com and Weather.com already have a federation solution in place.

OnCast.com, a new partner of the SmartPhones Telecom, doesn't have skills to implement a full-featured federation product. SmartPhones Telecom decides to help the new partner by providing a lightweight Service Provider federation component - Oracle OpenSSO Fedlet.

A security administrator at SmartPhones Telecom follows four simple steps to complete the project:

1. Export Oracle Identity Federation metadata
2. Generate Oracle OpenSSO Fedlet metadata and configuration files
3. Import Oracle Oracle OpenSSO Fedlet metadata
4. Create a distribution package and give it to a contact person at OnCast.com

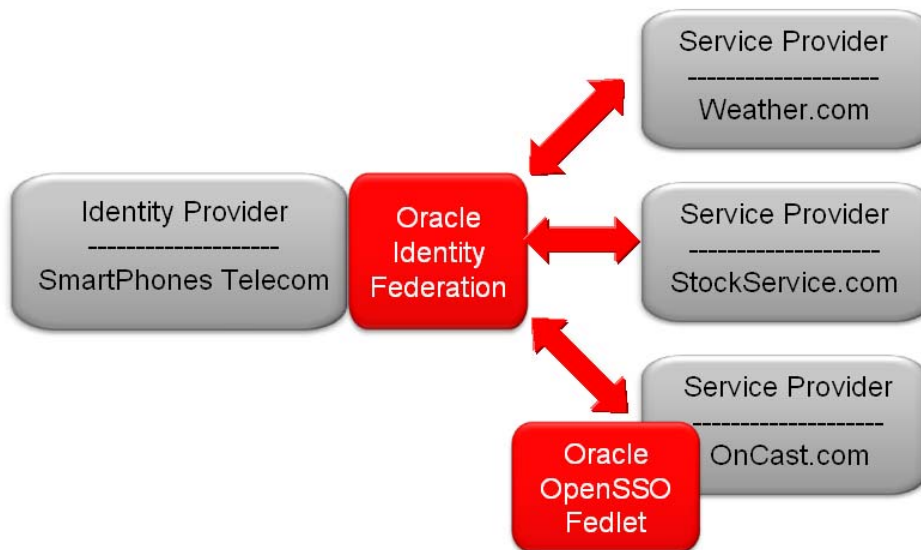
An application developer at OnCast follows three simple steps to complete the project:

1. Receive and open the distribution

2. Integrate Oracle OpenSSO Fedlet with OnCast content service
3. Deploy Oracle OpenSSO Fedlet

The project is completed. The partners are now ready to test their federation.

Using Oracle OpenSSO Fedlet, OnCast retrieves specific user attributes over SAMLv2 from SmartPhones Telecom. OnCast uses the user attribute data to customize its content delivery to the subscribers of SmartPhones Telecom, creating value for both companies and enhancing the experience of their subscribers.



Evaluating Benefits and Tradeoffs

As you design your deployment architecture, consider the benefits and tradeoffs of Oracle OpenSSO Fedlet. This section can help to determine if Oracle OpenSSO Fedlet meets your business needs.

Benefits

- **Simplicity.** Oracle OpenSSO Fedlet is simple to understand and use. It was designed by developers for developers, and does not require any new knowledge or skill that your development organization does not already have.
- **Infrastructure reduction.** Oracle OpenSSO Fedlet does not require additional hardware thus reducing the cost to the Service Provider and increasing the return on investment on existing hardware.
- **Ease of deployment.** Oracle OpenSSO Fedlet is easy to deploy and to embed into the Service Provider's application. Configuration of Oracle OpenSSO Fedlet, if needed at all, requires modifying only a few parameters. This shortens deployment time for the application.
- **Reduced training time.** Oracle OpenSSO Fedlet does not require the Service Provider to install any full-featured federation software. This reduces the amount of training required, thus reducing training costs for the Service Provider.
- **Reusability and consistency.** Oracle OpenSSO Fedlet is compliant with SAMLv2 standards. Because Oracle OpenSSO Fedlet can be reused for multiple projects across your organization, it provides consistency of architecture and protects yours and your partner's existing technology investments.

Tradeoffs

- Oracle OpenSSO Fedlet does not perform session management on the Service Provider; an application or container is responsible for session management.
- Oracle OpenSSO Fedlet supports SAMLv2 protocol only; other federation protocols such as Liberty ID-FF, WS-Federation, and SAML 1.x, are not supported.
- Oracle OpenSSO Fedlet is designed to be a simple and lightweight federation component. Some advanced features, available in Oracle Identity Federation, are not supported by Oracle OpenSSO Fedlet:

- SSO Proxy
- Account Linking
- Advanced Attribute Mapping
- Integration with Information Cards
- Centralized administration, logging, reporting, and operational monitoring

Note: If Oracle OpenSSO Fedlet doesn't meet your organization's business needs, consider using Oracle Identity Federation as your federation solution.

Conclusion

Oracle OpenSSO Fedlet is a simple and lightweight option for quickly and easily creating SAML federations with your Service Providers. It allows Identity Providers to control security settings, configuration, and distribution mechanism of the Service Provider federation components. Oracle OpenSSO Fedlet accelerates deployments and enables better ongoing management of federation interactions between partners.

Oracle OpenSSO Fedlet helps to significantly simplify the environment and deliver on the IT promise of making solutions standards-based and reusable, achieving infrastructure rationalization, and realizing cost reduction. Oracle Identity Federation and Oracle OpenSSO Fedlet together provide a complete, end-to-end, enterprise-level and carrier-grade federation solution for you and your business partners.

For further information on Oracle Identity Federation and Oracle OpenSSO Fedlet please visit:

<http://www.oracle.com/identity>



Oracle OpenSSO Fedlet
August 2010
Author: Sophia Maler
Contributing Authors: Eric Leach, Resha
Chedda

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

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0410

SOFTWARE. HARDWARE. COMPLETE.