

An Oracle White Paper
April 2011

Qualcomm Case: Supporting User Federation using 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.

Introduction	2
Challenges	2
Oracle Identity Federation (OIF)	3
Solution	3
Benefits	5
Conclusion	5
About Qualcomm	5

Introduction

With the growth of e-business, organizations are struggling with the challenges of managing secure access to information and applications across a wide range of internal and external computing systems and users. Additionally, organizations have to manage identities and profiles to an ever changing number of employees, customers, providers, systems and business partners without diminishing security or exposing sensitive information. What's even more overwhelming to organizations today is to manage multiple user identities across multiple applications? All these challenges add to a great deal of cost of ownership.

Another common business needs in the current world is that vendors and service providers need to establish secure virtual communities, where customers and partners can visit and conduct business on different websites with a single log-in for their end-users. The technology that facilitates this is the Federated identity management solution through Federated Single-Sign-on (SSO) process that allows users of business partners to automatically access each other's applications without requiring multiple layers of passwords.

Federated SSO can help improve user productivity, reduce help desk calls for forgotten passwords, and improve identity lifecycle management between organization and partners.

In this case study we would like to highlight how we have helped our customer, Qualcomm to overcome the federation SSO challenges through Oracle Identity Federation (OIF) product and its benefits.

Challenges

Oracle customer Qualcomm, which is an American wireless telecommunications research and development company, as well as the largest fabless chip supplier in the world, is based in San Diego, California. Qualcomm designs, manufactures and markets digital wireless telecommunications products and services based on its code division multiple access (CDMA) technology and other technologies. With multiple divisions and thousands of employees, Qualcomm needed a way to manage identity in a heterogeneous environment of "in-house" developed and "off the shelf" systems and applications. The enterprise application deployment environment spanned across many platforms and involved different types of application environments (such as Web applications, EJBs, Web Services, Fusion Applications, etc.). Increasingly users are accessing these applications through the extranet and the Internet.

The company on a day-to-day business activity has to deal with both customers who they serve, at the same time interact extensively with 3rd parties, such as vendors, suppliers, and contractors who offer their services to Qualcomm.

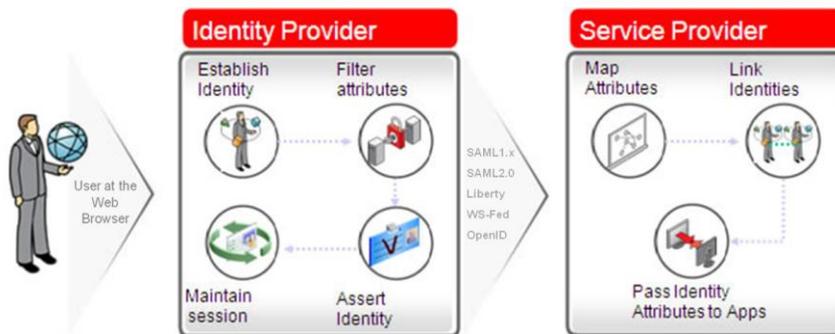
To support such a business model sharing internal Qualcomm applications and resources is a must. At the same time they have to support the needs of their internal users to interact with these external resources, without having to remember separate identity credentials for all these applications that these users need to access on a daily basis.

To overcome these challenges the Qualcomm's IT identity management team had to standardize their process to integrate with their business partners, which could enable managing application user accounts across the business-to-business boundaries in a seamless way there-by saving cost in the long run, at the same time meet their company's growing business needs.

Oracle Identity Federation (OIF)

Oracle Identity Federation (OIF) is an enterprise level Federated identity management solution from Oracle which simplifies the process of enabling Federated Single Sign-on (SSO) for users coming through a web browser to access resources across different security domains or across administrative boundaries through various federation protocols like SAML, WS-Federation, Liberty or OpenID.

Regardless of the protocol used, a single instance of OIF can be successfully leveraged both in Identity Provider (IDP) and in Service Provider (SP) deployments.



With OIF, organizations can do more business online by helping their business partners to get started on federation and quickly achieve SSO without the extensive knowledge of the protocols that they will have to leverage for their Federation process. Thereby OIF significantly reduces the need to create unnecessary identities in an enterprise directory and lowers the ongoing costs of partner integrations through the support of industry federation standards.

Here are some of the highlights of OIF

- Complete, end-to-end, enterprise-level federation solution for any company
- Standard-based cross-domain authentication and SSO
- Standard-based attribute exchange
- Advanced identity attribute mapping and filtering
- Comprehensive support of industry standards (SAML, WS-Federation, Liberty, OpenID)
- Flexible framework to support customization and integration

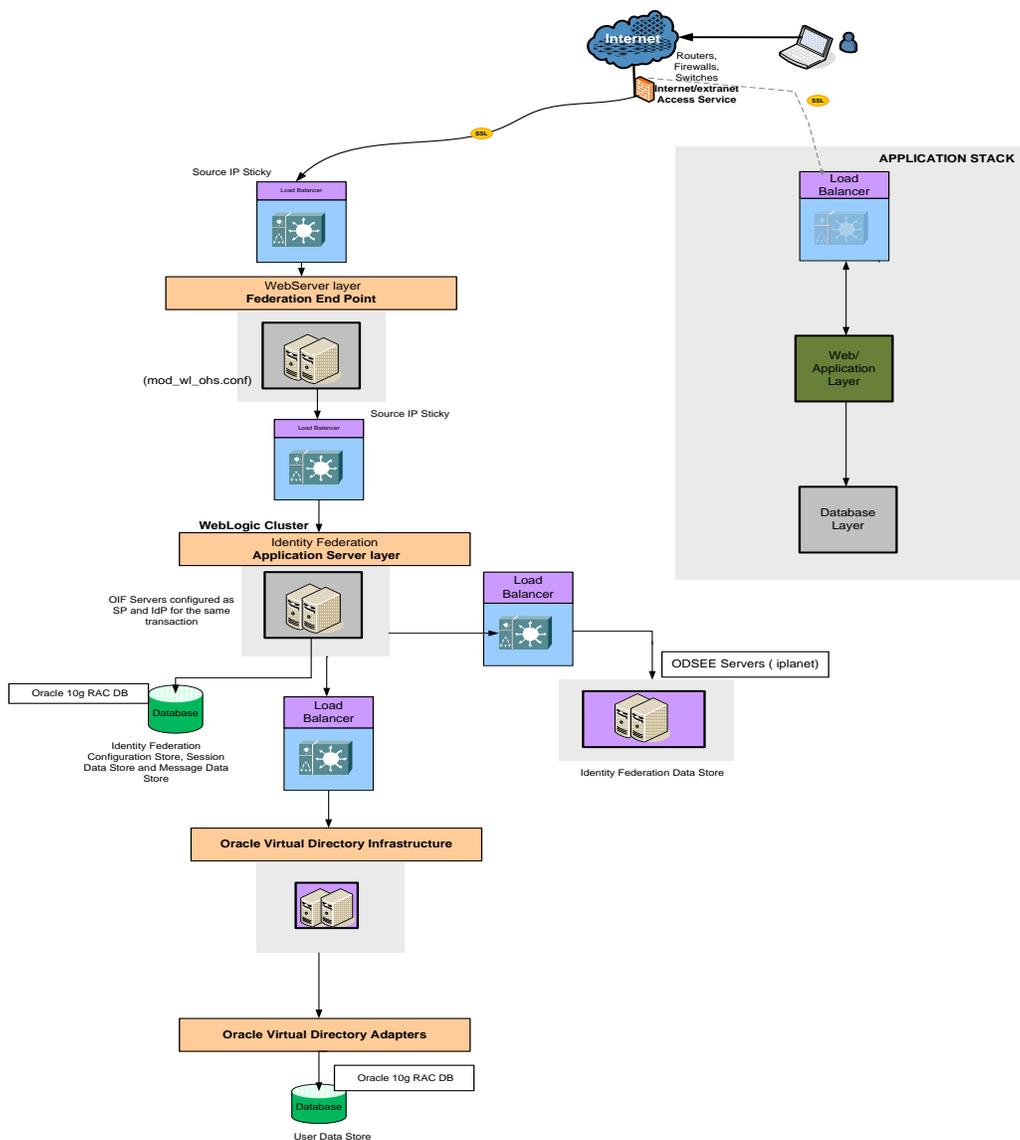
Solution

One of the noticeable challenges which Qualcomm faced during OIF deployment was to make sure that OIF sessions were sticky to one application server in a cluster during federation transactions. As the required functionality involved OIF to be the an identity provider and a service provider for a single transaction, Qualcomm Identity Management team had to configure the OIF web layer infrastructure to interact with a load balancer (with sticky sessions set) which had OIF application servers under it.

As the business use case required us to integrate with a home grown single sign on solution, this implementation required us to make use of OIF's custom authentication scheme functionality which provided cookie orchestration between domains which were independent of each other.

Below is the deployment diagram of how Qualcomm has deployed OIF in their IT environment.

- Qualcomm is using OIF instances both as an IDP and also as an SP for federating their users who are trying to access their services.
- They standardized on SAML 2 as their federation protocol to send their user assertions across the security domains and with their business partners.
- Uses Oracle 10g RAC DB as the OIF Configuration, Session and Message Data stores
- Uses ODEE as the OIF Federation Store
- The user store is in a Oracle 10g RAC DB
- OIF is deployed on WebLogic Server clusters to support HA and Failover scenarios
- OHS acts as the proxy for the Cisco Load balancer which is front ending the Weblogic clusters hosting the OIF instances.



Benefits

Here are some of the benefits that Qualcomm was able to get through OIF.

- Overall cost reduction through centralized administration of circle of trust between Qualcomm and its business partners
- Increased end-user productivity through Single Sign-on automation capabilities
- Improved security through better trust enforcement through standards
- Reduced Total Costs of Ownership through task and process automation
- Minimizing unauthorized access to sensitive systems through audit and logging.
- Ease of integration with our home grown single sign on solutions through orchestration between independent platforms.

Conclusion

Sharing applications and resources over the Internet to external divisions and partners and users interacting with different applications that are hosted in different security domains through a web browser is becoming a common scenario in the current business world. The common challenges that any organization faces today includes establishing trust between these different business entities so their employees can operate between these security boundaries effectively at their same time protect their company assets without compromising security.

A product like OIF which leverages standards and existing user identity information, facilitates customers like Qualcomm to adopt and deploy solutions and services to meet their business needs quickly at the same time simplifies their IT environment to meet the needs of the business by replicating and reusing the infrastructure to add additional business partners or services without adding additional cost.

About Qualcomm

QUALCOMM Incorporated is a leader in 3G and next-generation mobile technologies. For 25 years, QUALCOMM ideas and inventions have driven the evolution of wireless communications, connecting people more closely to information, entertainment, and each other. QUALCOMM technologies power the convergence of mobile communications and consumer electronics, making wireless devices and services more personal, affordable, and accessible.



Qualcomm Case Study
April 2011
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 © 2011, 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. 1010

Hardware and Software, Engineered to Work Together