Case Study: Use of Liberty Federated Network Identity in an Enterprise Outsourcing Environment

Yvonne **Wilson**

Abstract

This paper covers use of federated network identity to solve issues arising in enterprise outsourcing environments.

Table of Contents

1. Executive Summary 3
2. Federated Network Identity in Enterprise Outsourcing Environments 3
3. Liberty Alliance 4
4. Federated Identity Overview 4
5. Business Overview 5
6. Technical Deployment 6
7. Use of XML 7
8. Business Benefits 7
9. Issues Faced 8
    9.1. Account creation (Manual or bulk federation) 8
    9.2. SP identity and password 9
    9.3. Data required for Authorization 9
    9.4. Support Process 9
    9.5. Monitoring 9
    9.6. Logout 9
    9.7. Troubleshooting 10
    9.8. Varied authentication mechanisms 10
    9.9. Time synchronization 10
    9.10. Business Agreements 10
10. Summary 10
11. Glossary 10
Acknowledgements 11
Acknowledgements 11
Bibliography 11

1. Executive Summary

This paper will describe the use of standards from the Liberty Alliance to address issues arising from a typical enterprise outsourcing scenario. Enterprise outsourcing often results in issues for both end users and IT organizations, including proliferation of login passwords and different login solutions for each application service provider. Federated network identity solutions can solve these issues. Use of federated network identity allows an enterprise to outsource applications to various providers while retaining the ability to implement single signon across the outsourced applications and even implement different strengths of authentication mechanisms for low vs high sensitivity applications. Furthermore, federated network identity helps support privacy compliance, reduced application work for authentication, and more up-to-date authorization decisions.

2. Federated Network Identity in Enterprise Outsourcing Environments

The current trend of enterprise outsourcing creates an urgent need for federated identity solutions. With ongoing pressures to reduce costs and focus on core competencies, many businesses have turned to outsourcing IT services and often entire business functions. As a result, enterprise employees need to access business applications hosted by numerous different application service providers (ASP).

Unfortunately, this results in numerous issues for end users. Often, each different application service provider uses its own, proprietary, authentication service. This requires that users remember many different usernames and passwords. This results in passwords being forgotten, which leads to applications that are seldom used (because users can't remember how to log in) or higher help-desk costs for resetting passwords.. Alternatively, in an effort to remember these myriad passwords, users may write passwords down, which compromises security if such notes are found. Either way, the absence of federated network identity in an enterprise outsourcing solution leaves end users with login hassles or compromised security.

The lack of federated network identity also gives rise to significant issues and costs for IT organizations. In the absence of open, industry standard solutions, each outsourcing agreement requires IT staffs from the outsourcing company and the provider company to have lengthy discussions to agree on several facets of custom authentication and authorization solutions. This includes factors such as what to use as an identifier and password for the outsourced application and how to initialize accounts at the application service provider. It also involves designing mechanisms to synchronize account information on an ongoing basis at the application provider as new employees arrive or as employees are terminated. In addition, each custom interface solution adds to support costs and to the work required for subsequent system upgrade projects. As a result, the absence of federated network identity in an enterprise outsourcing environment can leave IT organizations with more work, higher development costs, more difficult upgrades and longer project times.

Fortunately, federated network identity solutions offer a clever solution for enterprise outsourcing. With federated network identity, an enterprise can outsource applications to numerous providers while retaining a single signon capability based on federated network identity. This eliminates the need for users to remember many different passwords. It allows an enterprise to implement several authentication mechanisms of different strengths, in one place, so that low-sensitivity applications can be accessed with a simple password and higher-sensitivity applications can require stronger authentication mechanisms such as token cards and smartcards. Furthermore, this solution can be based on industry standards which reduces project time spent discussing custom solutions for each outsourcing partner. A federated network identity solution allows enterprises to deploy one re-usable single-signon authentication service, based on industry standards, and re-use that service across both internally and externally hosted applications. For each new outsourcing, end users enjoy single signon, applications are easier to access and therefore more widely used, and IT staff work is reduced to a configuration project rather than a custom coding or interface project. As will be shown below, this ends up as a win for both the outsourcing enterprise and their partnering application service providers.

3. Liberty Alliance

The Liberty Alliance is a world-wide consortium of over 150 companies who have banded together to create open standards for federated network identity. The Liberty Alliance organization focuses on technology, public policy, business and marketing, conformance and service development, as related to federated network identity. [1] The technology and standards work of the Liberty Alliance has focused on three phases, or sets of specifications.

These specifications include:

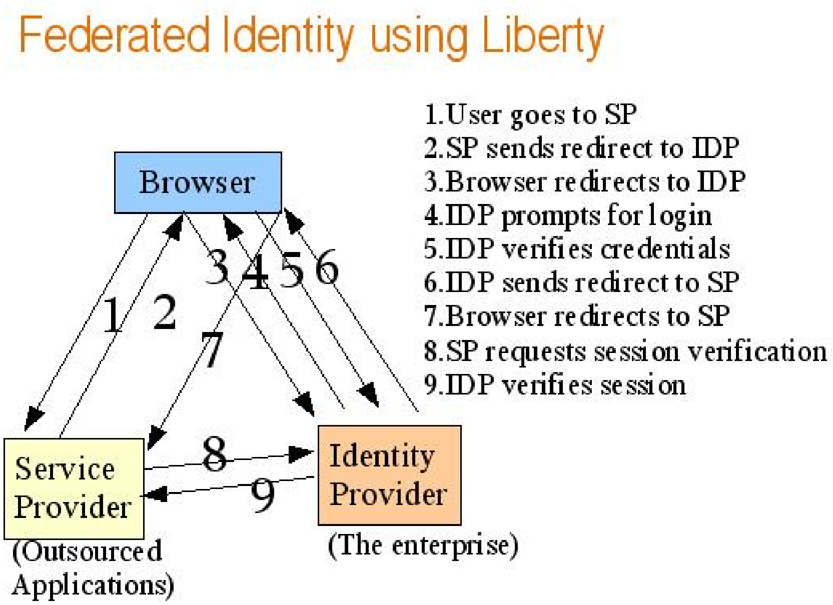
- D-FF: Identity Federation Framework. A framework for account federation and single-signon for end users
- ID-WSF: Identity Web Services Framework. A framework to allow web service clients to discover and securely conduct messaging transactions with identity-based or identity-consuming web services.
- ID-SIS: Identity Services Interface Specifications. A set of specifications for specific, identity-based services. Examples so far include a personal profile service, an employee profile service, a contact service, a geolocation service and a presence service. [2]

In the interest of brevity, this paper will concentrate on the usage of ID-FF, the Identity Federation Framework, in an enterprise outsourcing environment. ID-FF leverages and builds upon SAML1.0 and SAML1.1. SAML, which stands for Security Assertion Markup Language, is defined by an OASIS technical committee[3]. It is important to note that while ID-FF has in turn been incorporated into SAMLv2, and SAMLv2 adopted by the Liberty Alliance as well, the benefits and lessons learned from this early deployment of ID-FF are expected to apply similarly to a SAMLv2 deployment.

4. Federated Identity Overview

The Liberty Alliance's ID-FF specification involves two types of entities, namely service providers and identity providers. A service provider is typically any entity providing a web enabled service, such as a website or application. The identity provider is an entity that agrees to take on responsibility for authenticating users. The ID-FF specification describes a protocol which allows (among other things) one organization, known as a service provider to securely rely upon another organization, known as an identity provider for authentication of users.

In an enterprise outsourcing scenario, the identity provider would typically be the enterprise. The service provider(s) would be the application service providers to which the enterprise had outsourced various applications or business functions. The diagram below illustrates an outsourcing scenario where the enterprise user goes to an outsourced application (service provider) and is redirected back to the enterprise (identity provider) to be authenticated, and only upon successful authentication (and backchannel verification of authenticated session) is the user allowed through to the outsourced application. The sequence below can be repeated with each outsourced application (service provider) redirecting to the same identity provider. Alternatively, multiple identity providers can be implemented with some outsourced applications redirecting to one identity provider and other outsourced applications redirecting to another.


Federated Identity using Liberty
1.User goes to SP
2.SP sends redirect to IDP
3.Browser redirects to IDP
4.IDP prompts for login
5.IDP verifies credentials
6.IDP sends redirect to SP
7.Browser redirects to SP
8.SP requests session verification
9.IDP verifies session
Browser
1
2
3
4
5
6
7
8
9
Service Provider
(Outsourced Applications)
Identity Provider
(The enterprise)

A typical Federated Identity login sequence.

Figure 1. Federated Identity Login Overview

5. Business Overview

The rest of this paper will describe an actual deployment of federated network identity between Sun Microsystems, Inc. and BIPAC. A brief introduction to each company will be given, followed by a description of the project.

Sun Microsystems, Inc. provides products and services for network computing. A singular vision -- "The Network Is The Computer" -- guides Sun in the development of technologies that power the world's most important markets. Sun's philosophy of enabling trust and sharing of innovation and building secure communities is at the forefront of the next wave of computing: the Participation Age. Sun can be found in more than 100 countries and on the Web at http://sun.com <http://www.sun.com/>. [4]

BIPAC provides political insight to the nation's business community and supports candidates for Congress who are committed to free enterprise and minimal government interference - regardless of party. Many Fortune 500 companies use BIPAC's services to educate their employees about candidates, issues and elections, and to get them to the polls.[5]

At the time this project was initiated, BIPAC was already providing an interactive, web-enabled application to Sun employees, to enable them to view information about how their political representatives had voted on issues related to Sun’s business. The application also assisted employees in writing to their political representatives about those issues. These public policy application services were hosted at BIPAC and accessed by Sun employees. Before this project, these employees were authenticated solely by mechanisms such as referring page and client IP address. Nothing in the previous authentication process could individually identify a particular user.

Going forward, Sun wanted BIPAC to provide additional services, but such services required that users be individually authenticated because such services could only be made available to a restricted class of users.

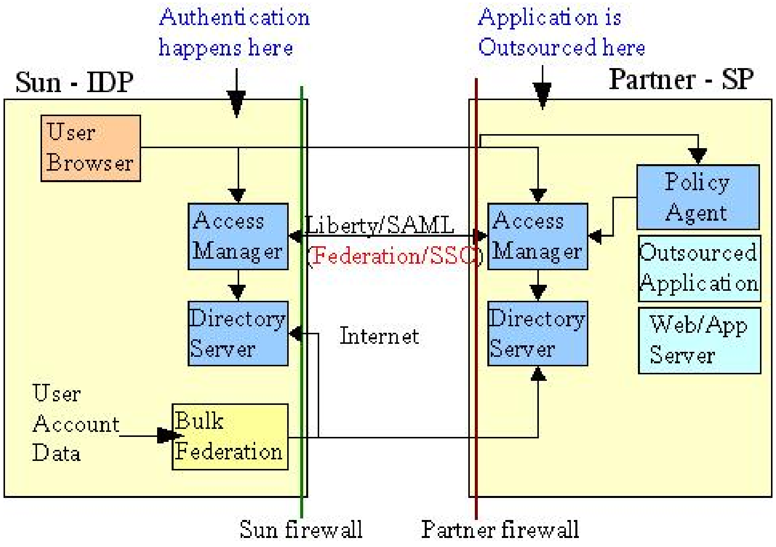
Sun wanted users to be individually authenticated to the outsourced BIPAC application, without adding to the proliferation of usernames and passwords required by previous outsourcing. Sun wanted to realize single-signon, and enable stronger authentication mechanisms without waiting or relying on each ASP to implement such technology. Federated network identity was an obvious solution to these requirements. By deploying federated network identity:

- Sun employees can now access outsourced BIPAC application services using stronger authentication mechanisms than had been previously used.
- Sun employees can enjoy single-signon across outsourced applications and internally-hosted applications (that are of similar sensitivity level).
- Sun can leverage additional services from BIPAC that had to be restricted to certain classes of employees to comply with legal requirements.
- Sun and BIPAC achieved a reference solution which will be used with other partners and customers of Sun and BIPAC.

6. Technical Deployment

This project deployed a Liberty-enabled (Liberty Phase 1 ID-FF) security service at BIPAC and linked it to Sun's employee-facing Liberty-enabled security service.

The project involved the deployment of Sun Java(TM) System Access Manager product at both Sun, the Identity Provider (IDP), and BIPAC, the Service Provider (SP). While this deployment happened to use the Access Manager product on both sides of the outsourcing partnership, any Liberty-compliant products could have been substituted at either or both sides.



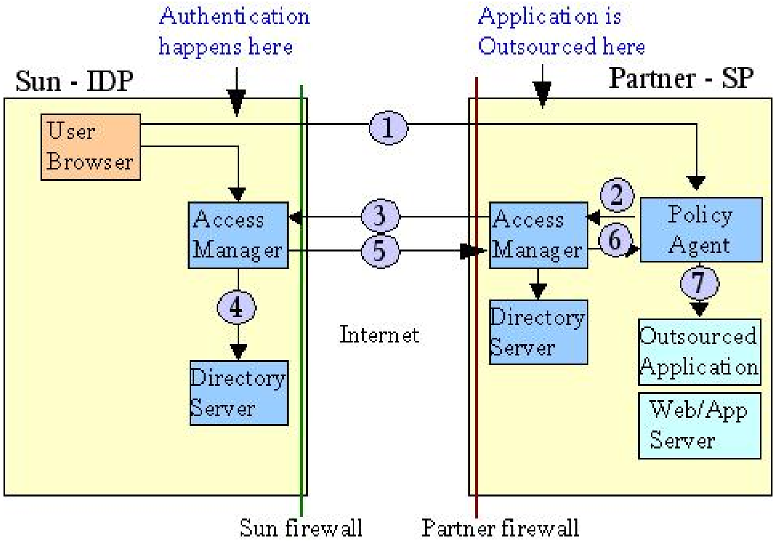
Components deployed at Sun and BIPAC for the project.

Figure 2. Deployment Architecture

Sun's Access Manager product was deployed in an internet accessible location at Sun and configured to serve as an Identity Provider. Sun's Access Manager product was also deployed at BIPAC and configured to serve as a Service Provider. The Sun Java (TM) System Directory Server product provided persistent storage for identity and security policy information managed by Access Manager. In addition, the Sun Java(TM) System policy agent was deployed onto the web server upon which ran the outsourced BIPAC application.

Once the software had been deployed, bulk federation was utilized to pre-initialize accounts at BIPAC for Sun users and pre-federate those accounts back to the account at Sun for each user. This bulk federation step eliminated the need to send instructions to users to self-register at BIPAC and manually federate their account. All accounts were automatically created and federated for the users so that no extra steps were necessary on the part of end users.

With the accounts at BIPAC federated back to Sun, the following login sequence was thus enabled.



Sun employee's login sequence for outsourced applications

Figure 3. Sun-BIPAC Liberty Deployment

A Sun employee, browsing Sun's employee-facing portal, clicks on a link for the outsourced BIPAC application. The user's browser sends a request to the externally-hosted BIPAC application (1) and the policy agent on the application intercepts the request and ascertains whether the user has an existing login session or not. If the user does not have an existing session, the policy agent redirects the user's browser to the BIPAC Access Manager deployment, (2) which in turn redirects the user's browser to Sun's Access Manager deployment, (3) which prompts the user to log in. Sun's Access Manager collects and validates the user's credentials (4) using any of a variety of possible authentication mechanisms, and upon successful authentication, sets an appropriate cookie in the user's browser and redirects the user's browser back to the BIPAC Access Manager (5), which establishes a local session and redirects the user's browser back to the URL for the BIPAC application. (6) This time, the policy agent sees the necessary cookies. The policy agent then checks access control policy to verify the user is allowed to use the application module in question, and if so, allows the request to pass through to the application (7). Of course, if the user had previously established a session by logging into the employee portal or any other application, they would enjoy single signon, and access the outsourced BIPAC application without having to login again.

7. Use of XML

The Liberty ID-FF protocols leverage the work of the OASIS SSTC SAML committee. As such, the communication described above between the service provider instance of Access Manager and the identity provider instance of Access Manager is conducted via SAML, SOAP, and HTTPS.

8. Business Benefits

The project offered several benefits to both BIPAC and Sun.

Benefits to BIPAC:

- Capability to individually authenticate Sun's employees using BIPAC's services
- Ability to offer new services to Sun based on federated identity and authentication
- Ability to offer single-signon capability to Sun's enterprise users
- Ability to delegate responsibility to Sun for authentication of Sun's employees
- Freedom from having to implement and maintain various authentication services (token cards, smart cards etc) demanded by customers
- Compliance with privacy and SEC-related regulations
- An industry-standard solution for authentication in an enterprise outsourcing environment that can now be reused with other customers.

Benefits to Sun:

- Industry standard authentication solution for all outsourcing efforts (no more custom solutions for each outsourcing partner)
- Better ability to implement stronger authentication mechanisms for more sensitive applications
- Potential to use single-signon to reduce support costs from password resets
- Consistency of authentication mechanisms across different outsourced apps
- Facilitation of privacy while outsourcing
- Ability to implement single signon to improve user satisfaction
- Security is enhanced because only Sun's security service is collecting and validating credentials.

9. Issues Faced

This section will describe a few of the lessons learned during the project implementation.

9.1. Account creation (Manual or bulk federation)

In cases where individual users are conducting personal business using internet services, it makes sense for users to self-register and manually federate their accounts to their chosen identity provider(s). In an enterprise situation, however, it is possible and much more efficient for the enterprise to automatically provision ASP accounts for their employees and to bulk-federate those ASP accounts back to the enterprise.

In cases where individual users are conducting personal business on the internet, it is appropriate that users should be in control of federating and defederating their account. In an enterprise outsourcing situation, however, it will often make sense for the user's account to remain federated to the enterprise as long as the user is an employee.

When employees are terminated from the enterprise, their ASP accounts should be de-federated from the enterprise. Whether the account is actually removed from the ASP is a matter of business requirements. For certain HR benefits applications, it may make sense for the user's account to remain at the ASP, without federation. For other applications, it may make sense for the user's account to be entirely removed from the ASP.

9.2. SP identity and password

If an enterprise automatically provisions an account for an employee at an ASP, federates that account back to the enterprise, and requires the account to remain federated for the duration of the user's employment, then the username and password for the ASP will never really be used by the user. Therefore the username and password can simply be generated by the IDP. To maximize privacy, the user identifier at the ASP can be a randomly generated string. Alternatively, if allowed by business and legal requirements, the username at the ASP can be the same as used internally within the enterprise, which can simplify support processes, but decreases the privacy afforded to the individual user.

9.3. Data required for Authorization

In an enterprise outsourcing situation, it is very likely that the outsourced application (service provider) needs trusted user profile information about the user from the outsourcing enterprise (identity provider). This information is needed by the service provider to implement access controls. It is possible that the data needed may come from a variety of applications that have in turn been outsourced to other providers. Furthermore, for privacy reasons, it is possible that the data as stored in such source applications may not be appropriate to share directly with ASPs and may need to be altered or obfuscated in some way in order to provide the ASP with the minimal information needed. In such a situation, it is recommended to collect the data from the disparate applications and store the original user profile attribute value and the altered/obfuscated value in an interim collection point before making it available to the ASP. This interim collection point (with both profile attribute values) can be accessible to support staffs who respond to any questions about inappropriate or denied access based on such data. This will save time over going to each source outsourced system individually.

9.4. Support Process

In any Liberty environment, a user will work with applications provided by the SP and, on occasion, need to contact support for help with such applications. Once a user's account is federated to an IDP, however, the user has little need to use or remember their SP identifier. As a result, they are very likely to forget that identifier. If the identifiers used for the user at SP and IDP are different, (and the user has forgotten their SP identifier) an issue will arise when the user needs support if there isn't an easy way for the user to identify their account to the service provider.

9.5. Monitoring

In general, the service provider can monitor their side of the deployment and the identity provider can monitor their side of the deployment. To monitor the availability of the federated login sequence, synthetic logins can be used. In some enterprise outsourcing cases it may be desirable to restrict access to the identity provider to the corporate intranet. In such cases, the synthetic logins will need to be managed by the identity provider.

9.6. Logout

In a federated network identity environment with single signon, two logout options are possible. A service provider may provide a 'local' logout link, which terminates the user's session in the service provider's infrastructure only. Alternatively, the service provider and/or the identity provider can provide a 'global' logout link, which terminates the user's session in the identity provider's infrastructure as well. Use of local logout may be confusing to users because their identity provider session remains intact, allowing them to access without login an application from which they just logged out. Providing both a local logout and a global logout link may be confusing to users who don't understand the difference between them. Therefore, it is recommended to use only a global logout link.

9.7. Troubleshooting

Troubleshooting of the federated login sequence will frequently need to involve technical staffs at both (all) companies involved in a federated network identity partnership. A process will be needed to make both sides aware of issues requiring troubleshooting and to facilitate communication between both support staffs.

9.8. Varied authentication mechanisms

As more enterprise resources are enabled for single-signon access, it becomes imperative to implement a range of authentication mechanisms and demand that high-sensitivity content require stronger authentication mechanisms for access.

9.9. Time synchronization

The communication between service providers and identity providers leverages SAML assertions, which have a time period associated with them for validity of the assertion. Therefore it is critical that the servers communicating via SAML have their time synchronized via a mechanism such as NTP. If servers are allowed to drift out of synchronization, and a SAML assertion is generated by one machine that is 'behind' time, the SAML assertion may be considered invalid by the SAML consumer machine simply because its clock is ahead. When this happens, failures may occur for authentication and authorization requests. Such issues are avoided by simply keeping all servers in sync timewise and configuring SAML assertion timeouts to a reasonable value for the deployment.

9.10. Business Agreements

It was not necessary to start from scratch when creating business agreements for the Liberty deployment. In an enterprise outsourcing arrangement, there are already a number of business and legal agreements which are created for the outsourcing partnership. As a result, Liberty-specific terms were simply added to documents such as service level agreements. The terms covered issues such as procedures for adding members to, or withdrawing from, the circle of trust. The terms also covered more technical aspects of the deployment such as session timeouts and notification procedures prior to any upgrades.

10. Summary

As enterprises move to more outsourcing to reduce costs and gain greater efficiencies, several issues arise in terms of user login and security. A federated network identity deployment helps solve these issues. Federated network identity, as described by the Liberty Alliance protocols, enables the federation (linking) of a user's account at an application service provider (ASP) to the user's account within the enterprise. This enables the ASP to leverage authentication services within the outsourcing enterprise. This in turn enables single signon (fewer passwords to remember, fewer password resets) and faster deployments (by reusing industry standard solutions rather than custom solutions for each outsourcing). The Liberty Alliance protocols have adopted and leverage the work of the OASIS SSTC SAML standard and have been implemented by numerous industry purveyors of identity management solutions, such as Sun Microsystems with Sun Java (TM) System Access Manager and Sun Java (TM) System Federation Manager product. This means that outsourcing enterprises and their partners can simply choose a Liberty-enabled product, configure it to become aware of their partner's implementations and thereby enable numerous benefits such as industry-standard single signon, a variety of authentication mechanisms, and reduced work for outsourcing projects to implement authentication solutions.

11. Glossary

- ASP - Application Service Provider. An entity that provides and/or operates an outsourced application or service for an enterprise.

- HR - Human Resources. A function within an enterprise that deals with systems and processes to register, track, and manage the needs of human beings working for an enterprise.
- HTTPS - Hyper Text Transfer Protocol. A protocol for transmitting hyper text over a network.
- IT - Information Technology. A function within an enterprise that is responsible for the design, implementation and maintenance of computer systems used to manage the enterprise's business.
- NTP - Network Time Protocol. A protocol used to synchronize over a network the clocks of various computers.
- OASIS - Organization for the Advancement of Structured Information Standards. A not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards. [6]
- SAML - Security Assertion Markup Language. An extension of XML used for transmitting requests and responses for security authentication and authorization.
- SEC - Securities and Exchange Commission. A US regulatory body for some aspects of financial transactions, including the ability of enterprises to solicit funds from employees for Political Action Committees (PACs).
- SOAP - Simple Object Access Protocol. A language-independent mechanism for a program on one computer to invoke an object method (subroutine or function) of another program on another computer.

Acknowledgements

Many thanks for helping make this deployment a reality to team members from BIPAC, ServerVault, and Sun Microsystems Inc.

Acknowledgements

Bibliography

[Project Liberty] *Liberty Alliance website [http://www.projectliberty.org]*.

[ID-WSF] *ID-WSF Whitepaper [https://www.projectliberty.org/resources/whitepapers/Liberty_ID-WSF_Web_Services_Framework.pdf]*

[SAML] *OASIS Technical Committee for SAML* Available at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security .

[Sun Microsystems, Inc.] http://www.sun.com .

[BIPAC] *BIPAC Website*. Available at http://www.bipac.org .

[NTP] *NTP Website*. Available at http://www.ntp.org .

[OASIS] *OASIS Website*. Available at http://www.oasis-open.org .

[SOAP] *SOAP Website*. Available at http://www.w3.org/TR/soap .

Biography

Yvonne **Wilson**
Architect
Sun Microsystems, Inc. [http://www.sun.com]
Santa Clara
California
United States of America

Yvonne Wilson is an architect with Sun Microsystems Inc.