

MICROSOFT® “GENEVA” SERVER AND SUN OPENSFO

ENABLING UNPRECEDENTED COLLABORATION ACROSS
HETEROGENEOUS IT ENVIRONMENTS

White Paper
May 2009

Abstract

Interoperability between applications in heterogeneous technology environments is essential to successful collaboration between organizations today. Sun and Microsoft are taking interoperability to a new level by utilizing the SAML federation standard in both the Sun OpenSFO Enterprise federation solution and the forthcoming Microsoft “Geneva” Server federation solution.

By standardizing on SAML for federation, Sun and Microsoft enable organizations to deliver collaborative services with ease.

Table of Contents

Executive Summary	1
The Business Challenge: Working Together When Technologies Don't	2
The Need for Federation	2
The Need for Standards	2
Federated Identity Solutions from Sun and Microsoft	3
Sun OpenSSO Enterprise.....	3
Microsoft "Geneva" Server.....	3
Sun and Microsoft Federated Identity Interoperability.....	4
.NET Integration to OpenSSO Enterprise	4
SharePoint Access from OpenSSO Enterprise	4
Federation Scenarios with OpenSSO Enterprise and "Geneva" Server	5
Use Cases 1, 2, 3: Initiating SSO from a Service Provider	5
Use Cases 4, 5, 6: Using the Fedlet for Lightweight Federation	7
Conclusion	10
Useful Links	11

Chapter 1

Executive Summary

Today’s IT environments are often heterogeneous—perhaps more so than ever, as organizations make divergent choices from an abundance of technologies that are available to meet many different specific needs.

It’s not uncommon to see heterogeneous environments, whether within a single organization that runs both Microsoft® .NET and Java applications or across multiple organizations that seek to collaborate with each other. A classic example of the latter would be a bank that wants to give customers easy access to check imaging services that have been outsourced to a third party, or an airline that wants to allow flyers to go directly to a car rental company’s reservations application without having to sign on again. In cases like these, if both .NET and Java are involved, interoperability between the two kinds of applications is essential to enable the single sign-on (SSO) capability required for secure collaboration across organizational boundaries.

This paper focuses on two solutions for identity federation—Sun OpenSSO Enterprise and Microsoft’s forthcoming “Geneva” Server—specifically, on their common support for the Security Assertion Markup Language (SAML) federation standard as a basis for interoperability and ease of collaboration. The paper will:

- Present an overview of each solution and its capabilities, both as individual and as interoperable solutions
- Describe the business benefits of interoperability between the two solutions
- Share detailed use cases demonstrating the solutions’ proven interoperability in real-world federation scenarios

Together, OpenSSO Enterprise and “Geneva” Server enable businesses to easily achieve SSO for heterogeneous applications across domains.

Identity federation responds to the need to share resources across heterogeneous environments by making identities portable, so that they can be shared with and leveraged by trusted partners.

Sun OpenSSO Enterprise and Microsoft “Geneva” Server are federation solutions that both support the Security Assertion Markup Language (SAML) standard for exchanging authentication and authorization data between domains.

Chapter 2

The Business Challenge: Working Together When Technologies Don’t

Growing demand for online services requires that partners join forces to deliver what customers want in every area of consumer activity—from banking to travel. The challenge is providing users with secure access to multiple types of applications in heterogeneous IT environments without requiring them to sign on to applications multiple times. This need to securely share resources, particularly heterogeneous resources, beyond traditional boundaries drives the need for identity federation.

The Need for Federation

Identity federation responds to the need to share resources across heterogeneous environments by making identities portable, so that they can be shared with and leveraged by trusted partners. It streamlines and simplifies the process of sharing the identity data that’s associated with users. By making it possible to extend those users’ credentials and authorizations across traditional organizational boundaries, federation eliminates the major logistical obstacles to collaboration.

Federated solutions overcome the technical challenge of working together without forcing users to remember multiple passwords for different applications and without requiring administrators who are authenticating user identities to deal with multiple types of identity information for a single user. A federated solution makes identity information portable across security domains and enables SSO access across applications in multiple domains.

The Need for Standards

Federation standards are essential to the exchange of identity information across heterogeneous systems. For example, if one domain uses a password-based authentication system, and another uses a different type of authentication, how can they exchange the information to authenticate users across the domains? The answer is in establishing a standard for exchanging abstracted information about the authentication that was performed. If two domains can agree on that standard, they can interoperate regardless of differing authentication technologies.

Sun OpenSSO Enterprise and Microsoft “Geneva” Server are federation solutions that both support the Security Assertion Markup Language (SAML) standard for exchanging authentication and authorization data between domains. SAML is an XML-based standard that directly addresses the issue of SSO for Web-based access to applications.

Sun OpenSSO Enterprise is a next-generation federated access management solution that provides secure and centralized access control and SSO for internal and external applications and Web services security—all in a single, self-contained Java application.

Chapter 3

Federated Identity Solutions from Sun and Microsoft

Sun OpenSSO Enterprise

Sun OpenSSO Enterprise is a next-generation federated access management solution that provides secure and centralized access control and SSO for internal and external applications and Web services security—all in a single, self-contained Java application. The solution specifically:

- Enables centralization and enforcement of SSO and security policy for internal and extranet authentication
- Offers a truly lightweight means of federating: the Fedlet, a .NET and Java-compatible package that enables service providers to easily federate with online business partners
- Supports interoperability through the SAML federation standard (as well as WS-Federation and other standards)

OpenSSO Enterprise is a commercial offering based on OpenSSO, the world’s largest open-source identity management project providing highly scalable SSO, access management, federation, and secure Web services.

“Geneva” Server is the next release of Microsoft’s Active Directory Federation Services (ADFS), which supports browser-based federation using the WS-Federation standard.

Microsoft “Geneva” Server

Microsoft “Geneva” Server provides a security token service (STS) that enables organizations to collaborate securely across domains using identity federation. The solution specifically:

- Can be used by any identity provider whether inside an organization, exposed on the Internet, or both
- Allows identity federation for both passive clients (i.e., Web browsers) and active clients
- Supports interoperability through the SAML federation standard (as well as WS-Federation and other standards)

“Geneva” Server is the next release of Microsoft’s Active Directory Federation Services (ADFS), which supports browser-based federation using the WS-Federation standard. It is a component in the larger “Geneva” identity platform that also includes “Geneva” Framework, which helps developers create claims-aware applications, and CardSpace “Geneva,” which enables users to convey claims via Information Cards.

With SAML-based interoperability between Sun and Microsoft federated identity solutions, organizations can easily achieve SSO for heterogeneous applications across domains. Examples include:

- .NET Integration to OpenSSO Enterprise
- SharePoint Access from OpenSSO Enterprise

Chapter 4

Sun and Microsoft Federated Identity Interoperability

With SAML-based interoperability between Sun and Microsoft federated identity solutions, organizations can easily achieve SSO for heterogeneous applications across domains. Examples include:

.NET Integration to OpenSSO Enterprise

With support for the SAML standard in both OpenSSO Enterprise and “Geneva” Server, .NET-connected applications can be integrated to OpenSSO. This means that .NET-connected applications that authenticate end users are able to securely pass their attributes to OpenSSO, and applications that require user attributes are able to securely receive them from OpenSSO.

.NET support of OpenSSO Enterprise enables an SSO solution that works across both Microsoft .NET-connected enterprise applications and Java applications. It allows federation-enabled .NET applications to be hosted not only in Microsoft environments, but also in heterogeneous IT environments that include both .NET-connected applications and Java applications.

SharePoint Access from OpenSSO Enterprise

Many organizations use Microsoft Office SharePoint Server to provide access to information and facilitate collaboration within an organization. OpenSSO helps provide both internal and external users with direct access to SharePoint sites and linked Internet resources—without the need for re-authentication.

By using OpenSSO Enterprise to share credentials and attributes for SharePoint-related authentication and authorization, organizations reduce the need to maintain user profiles in multiple systems. This reduces costs by streamlining password management and decreases security risks by centralizing access management.

With both OpenSSO Enterprise and “Geneva” Server on the SAML federation standard, users can access services being offered from outside their identity provider’s site without having to sign on again to another site.

Chapter 5

Federation Scenarios with OpenSSO Enterprise and “Geneva” Server

There are a number of federation scenarios in which OpenSSO Enterprise and “Geneva” Server can work together to achieve the interoperability that is required to deliver services collaboratively. For example:

- A bank can use federation with these two technologies to provide customers with online access to a check imaging service operated by a third party.
- An airline Web site can use the same technologies to offer direct access to a car rental company’s reservations page.
- A company’s HR department can give employees a way to look up policy information from an insurance company.

With both OpenSSO Enterprise and “Geneva” Server on the SAML federation standard, users can access services being offered from outside their identity provider’s site without having to sign on again to another site.

The following use cases illustrate different deployments in which Sun and Microsoft have demonstrated the interoperability that enables federation.

Use Cases 1, 2, 3: Initiating SSO from a Service Provider

In federated relationship, the SSO can be initiated by either the identity provider or the service provider:

- In the first case, the user comes first to SharePoint, and then is redirected by “Geneva” Server (the service provider), to OpenSSO (the identity provider) for authentication.
- The second case demonstrates exactly the opposite: The service provider is using OpenSSO as its SSO infrastructure, and “Geneva” Server is acting as the identity provider.
- The third case illustrates identity federation between JavaEE applications (with OpenSSO in the role of service provider) on one domain and “Geneva” Server (in the role of identity provider) on another domain.

In federated relationship, the SSO can be initiated by either the identity provider or the service provider.

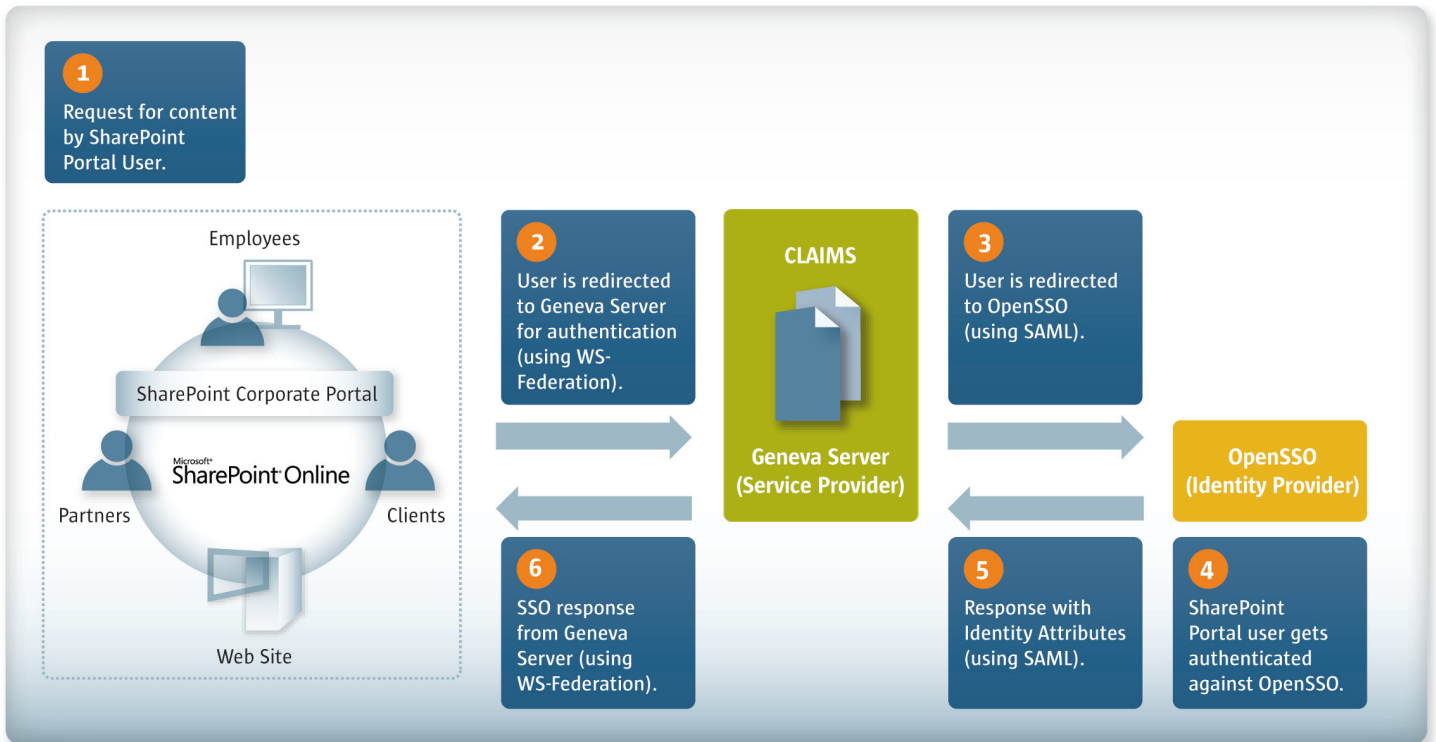


Figure 1. Use Case 1

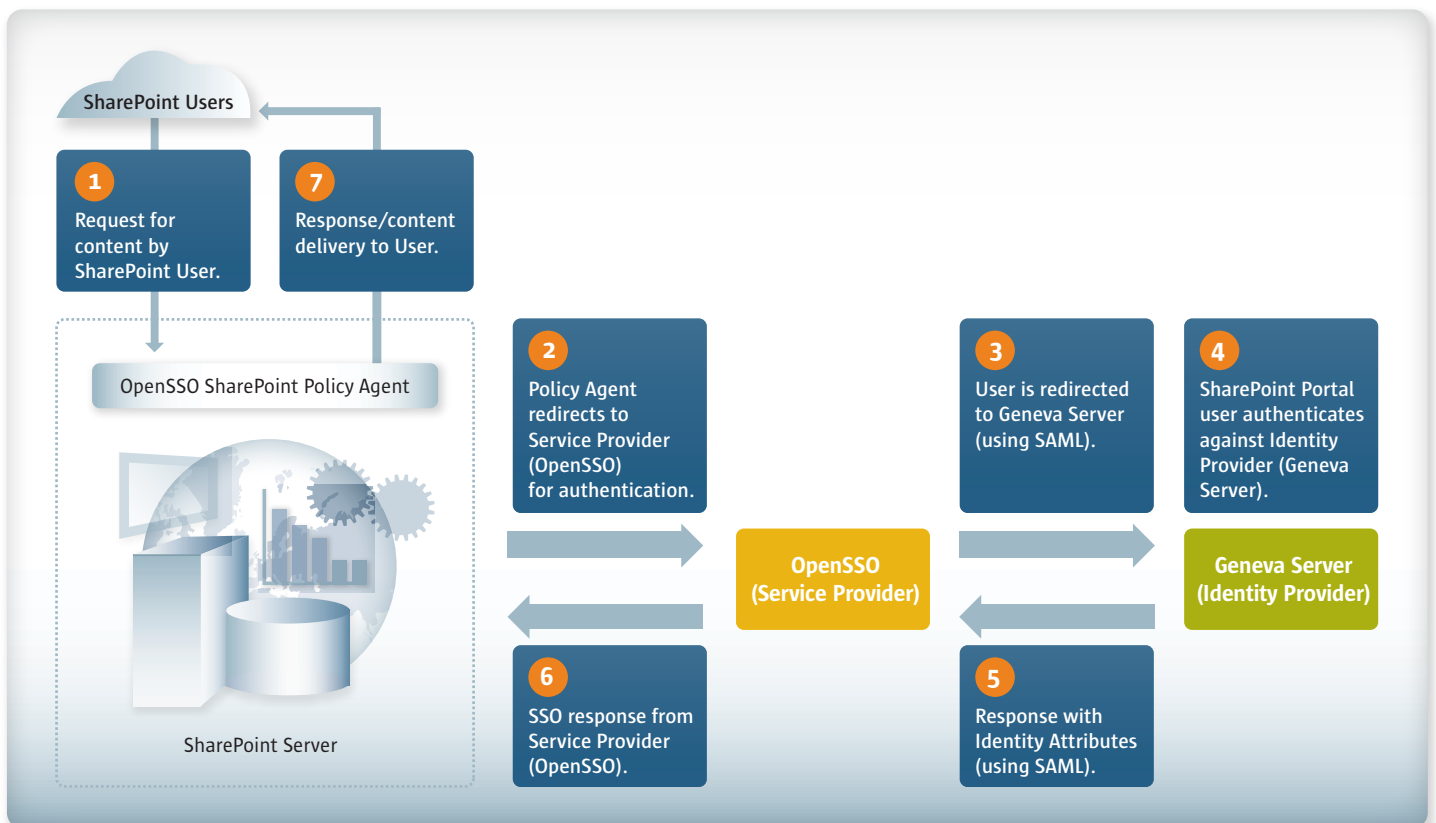


Figure 2. Use Case 2

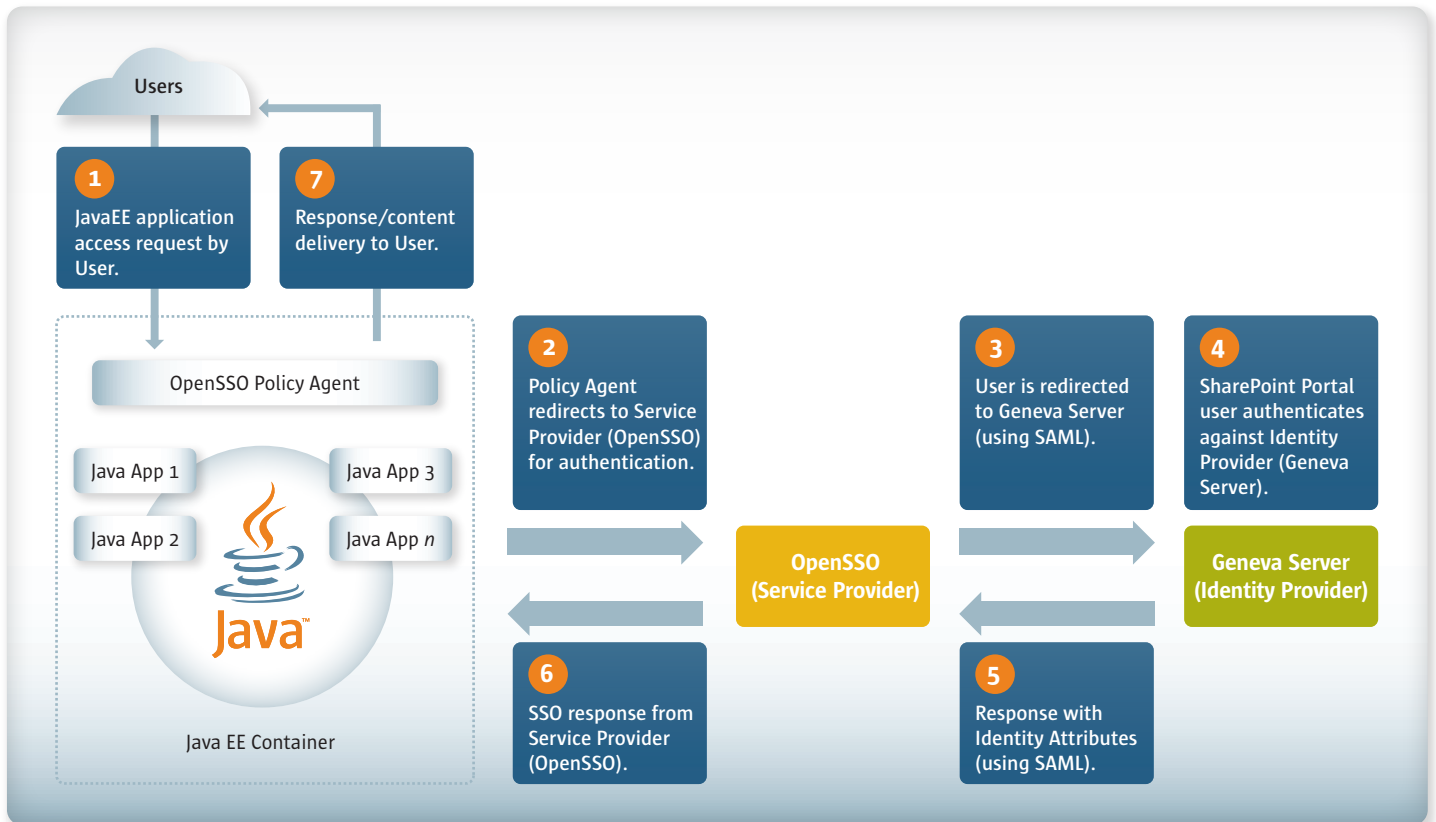


Figure 3. Use Case 3

Use Cases 4, 5, 6: Using the Fedlet for Lightweight Federation

These cases illustrate how the service provider can use the OpenSSO Fedlet capability to have users authenticated remotely by the identity provider:

- In the first case, the user requests content hosted by the service provider, which responds via the Fedlet.
- In the second, the user requests .NET application access and the application uses the Fedlet to make the SSO request to the identity provider.
- The third case illustrates identity federation between .NET applications with OpenSSO Fedlets (in the role of service provider) on one domain and “Geneva” Server (in the role of identity provider) on another domain.

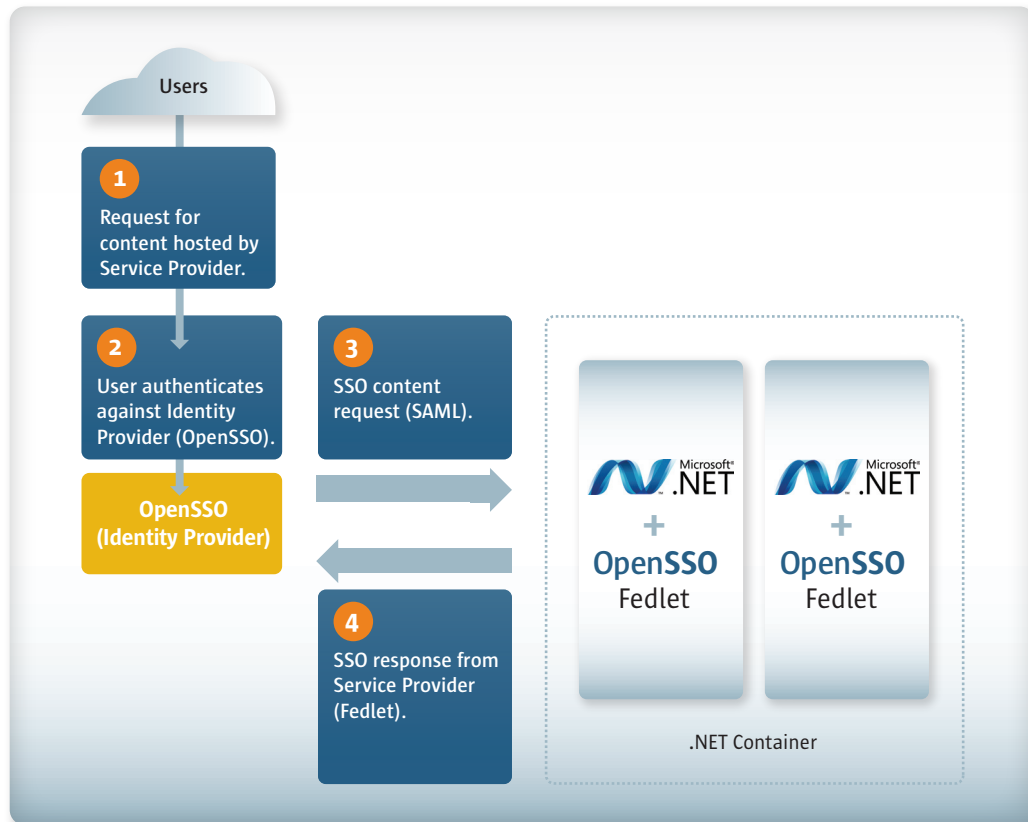


Figure 4. Use Case 4

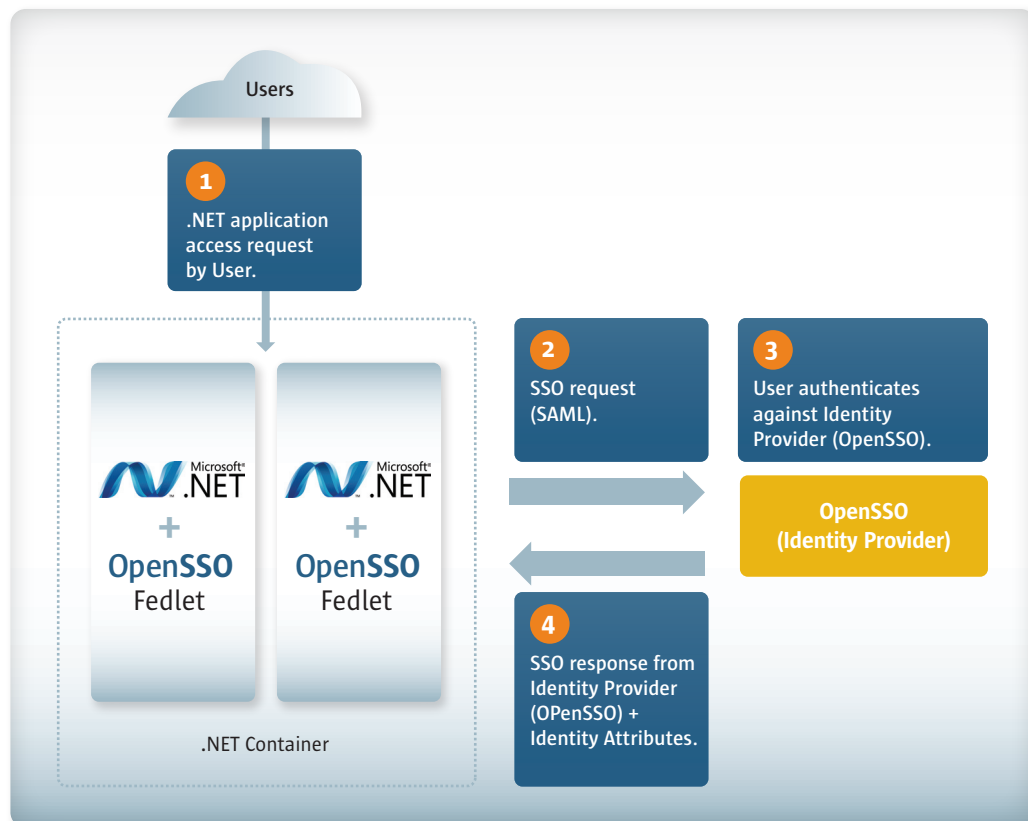


Figure 5. Use Case 5

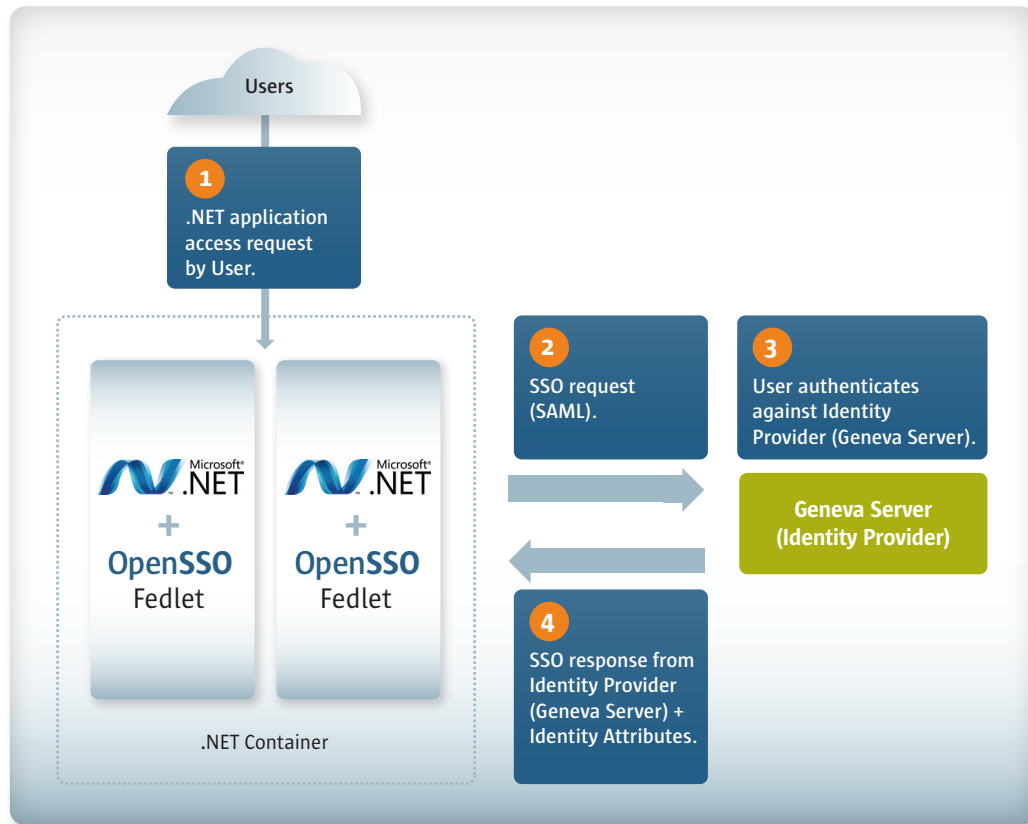


Figure 6. Use Case 6

Chapter 6

Conclusion

Interoperability between heterogeneous technologies is becoming increasingly important as organizations that run different kinds of applications seek to collaborate with each other. Sun and Microsoft are addressing this issue with solutions for identity federation that support the SAML federation standard.

The presence of a common industry standard in the Sun OpenSSO Enterprise and Microsoft “Geneva” Server solutions allows organizations to easily, freely, and securely share resources across heterogeneous applications. The interoperability enabled through these two solutions has been amply demonstrated in a variety of real-world deployments.

Chapter 7

Useful Links

1. *Microsoft “Geneva” Server*
<https://www.microsoft.com/geneva>
2. *OpenSSO Project*
<http://www.opensso.org>
3. *SAML*
<http://saml.xml.org>
4. *Sun OpenSSO Enterprise*
<http://www.sun.com/identity>



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN (9786) Web sun.com

© 2009 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries.
© 2009 Microsoft Corporation. All rights reserved. Printed in USA 05/09 #562889

