Oblix NetPoint SAML Services: Building Secure Online Partnerships

A Technical Perspective

WHITEPAPER

oblix™

Identity-Based Security Solutions

Printed in the United States of America.
Printing Date: March 2003 **Part Number: obx41b**

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
T 408.861.6800 F 408.861.6810

European Headquarters
Atrium Court
The Ring, Bracknell
Berkshire RG12 1BW, UK
T +44(0)1344 393 054

www.oblix.com
info@oblix.com

Overview

Companies have long ago recognized the advantages of engaging and building strategic business partnerships. In today's increasingly competitive business environment, leading companies are starting to recognize that significant strategic advantages can be gained by moving these collaborative partnerships to the Internet, in which business is transacted online directly with business partners, suppliers, and customers. Although they must do so on tightening budgets and stretched resources, corporations that are able to build collaborative online partnerships reap tangible benefits, including:

- **Reduced operational costs -** by streamlining, standardizing, and even automating cross-business interactions and transactions
- **Improved customer satisfaction and end-user productivity –** by enabling end-users to move efficiently across collaborating partner sites and eliminating cumbersome processes and tasks
- **Improved marketplace presence –** by extending a company's reach as far as that of the partner network

In online collaborative environments, end-users move seamlessly back and forth between corporate Web sites governed by security systems that are not only heterogeneous, but also owned by different corporations each with their own data repositories. Until recently, this has been difficult to achieve, since there was no standard way to pass user security information securely between such sites. Collaborating corporations were daunted by the complexity and cost of setting up the systems and processes to exchange and cross-maintain user security information. And without this framework, users would have to register different identities with redundant information at each site (for example, multiple storage of passwords), which is enough to discourage them from taking full advantage of these partnerships.

The SAML (Security Assertion Markup Language) standard, developed by the Security Services Technical Committee (SSTC) of the standards organization OASIS (www.oasis-open.org), solves an important component of these problems for corporations today. Technically, SAML provides the secure framework to support online partnerships in which a transaction initiated at one site is completed at a different site. It supports transactions initiated by users in business-to-consumer (B2C) scenarios, by XML-based document flows between services in business-to-business (B2B) applications, or by users simply trying to navigate across separately secured domains within a single corporate enterprise.

For example, SAML can enable a B2B Exchange to offer access to additional services through links in the site based on a specific user attribute such as their membership status. These services can be offered transparently to the end user using SAML without requiring re-authentication. Examples of such services might include an

automated credit check prior to completing a transaction or checking the employment status of a user. Using SAML, these transactions can be conducted seamlessly between partners without integrating their respective security systems.

Because SAML is designed to be the industry standard for exchanging authentication and authorization information, and it works with multiple industry-standard transport protocols, such as HTTP, SMTP, FTP, and others, as well as multiple XML document exchange frameworks such as SOAP, companies choosing to implement SAML can be confident they are making the right long term investment.

Oblix has been an active participant in the SAML standardization committee through OASIS, and through its contribution to the definition of SAML, now delivers the most mature SAML solution on the market today in Oblix NetPoint™. The Oblix NetPoint SAML solution is the only solution that provides a market-leading integrated platform that addresses the critical underlying issue of maintaining identity data across partner companies. The real time management of digital identities is necessary in order to implement SAML solutions in a cost-effective and scalable manner.

This white paper first provides an overview of the SAML standard itself. It then discusses NetPoint's out of the box implementation of SAML, how this allows companies to work more closely together across corporate boundaries using the Web, and how this can translate into tangible business benefits for corporations today. Finally, the paper describes how the NetPoint SAML Services™ is the only solution in the marketplace that allows companies to take full advantage of all the business benefits offered by the SAML standard.

Introduction to SAML

Definition and Need for SAML

SAML provides an interoperable secure mechanism for passing credentials and other related information between Web sites each having their own authentication and authorization system. With SAML, a transaction initiated at one site can be completed at a different site, through sharing of security information required to complete the transaction between the two sites.

The traditional way of handling Web-based single sign-on uses transient browser session cookies. Since each security solution uses different cookie security mechanisms and encryption algorithms, an alternate approach is required to allow these systems to interoperate. This alternate mechanism must be able to work with the browsers and Web servers of today and must be able to provide a secure mechanism for communicating credentials and related user information between partner sites.

Before describing the details of SAML, it is important to introduce two important terms:

- **Simple Object Access Protocol (SOAP) -** SOAP is a protocol that is used to exchange structured information between different Web-based systems and/or applications. SOAP provides a way to structure how separate systems are going to exchange infor mation. Also, SOAP is designed to use HTTP as its primary transport mechanism. Thus, two different systems that are talking SOAP to each other can send structured messages over HTTP (using SSL if desired). The SAML standard requires that the separate systems in a SAML-based relationship communicate using SOAP.
- **SAML assertions -** SAML allows for one system to assert characteristics of an entity to another system. SAML assertions can be made in the following forms:
  - Authentication assertion - This assertion indicates the authentication of a specific user. For example, “This user is ‘Lou Reed’”.
  - Authorization assertion - This assertion indicates if the user may perform an operation against a resource. For example, “the user is allowed to GET a specific URL”.
  - Attribute assertion - This assertion passes user attributes. For example, “the user has PLATINUM status”.

These assertions are the way SAML compliant systems tell each other about a given user that is navigating from one site to the next. Assertions are passed between SAML-aware systems using SOAP.

How SAML Works

SAML facilitates online partnerships between secure Web sites through the integration or interoperation of their respective security systems. SAML provides a secure mecha-nism for partner sites to exchange security information about a user transparently.

SAML gives partnering organizations the following capabilities:

- Enables the exchange of authentication and authorization information between sites that have separate user databases and authorization policies in a coherent/uniform manner.
- Supports the distribution of additional information (for example, group information, credit card information, etc.) about the user to partnering sites by using pre-specified structures in the SOAP message.
- Includes the ability for the vendor to include proprietary information. In order for that proprietary vendor information to be useful, both sides of the exchange must know what to do with it.
- Defines the security mechanisms to protect the information that is to be passed between sites, such as protecting the conversations between SAML servers using SSL, preventing replay attacks, preventing SAML memory stores from growing without bound (a type of "denial of service" attack), and preventing third-party theft attacks.

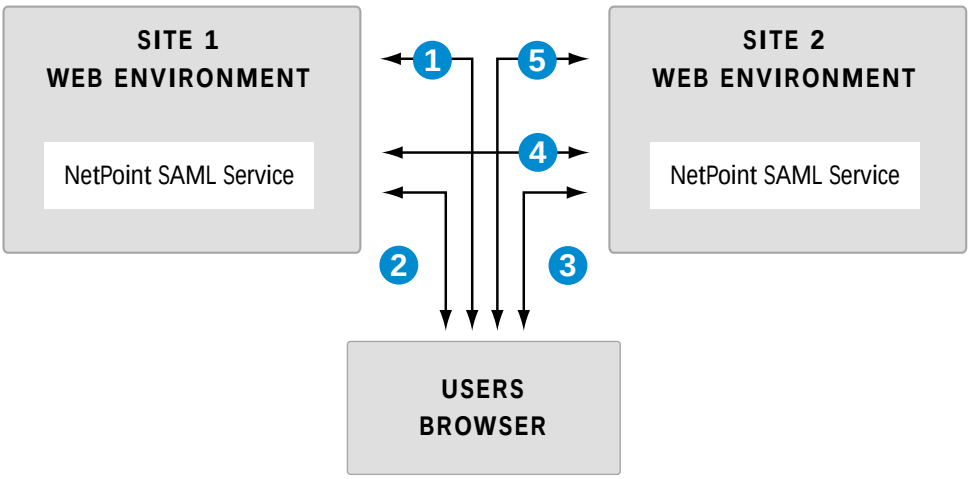

Figure 1: Basic SAML Architecture

Figure 1 shows the basic architecture required for a SAML-compliant site and how such a site interacts with another SAML-compliant site. It illustrates how each Web site that wishes to take advantage of SAML needs a SAML service as part of its architecture.

This diagram illustrates one SAML scenario called the Web SSO Browser Artifact profile, which is perhaps currently the most important, but not the only, way to use SAML.

The steps shown are as follows:

1. The user navigates to and authenticates to Site1's Web environment.
2. The user clicks on a link to transfer her to Site2. The browser is first transparently forwarded to Site1's SAML service. This SAML service generates an assertion with information about the user, and adds an identifier (a source ID) and a handle for the assertion to the link, so that Site2 can retrieve the assertion from Site1.
3. The browser is now redirected to Site2's SAML service, which retrieves the initial link and the additional information. The source ID tells Site2 how to contact Site1 and the handle tells Site2 how to ask for the user's assertion.
4. Site2's SAML service calls back to Site1's SAML service directly, using the source ID, and using the handle created in Step 2, retrieves the assertion for the user from Site1.
5. Site2's authorization solution then decides whether or not to grant the user access to its Web environment.

It is possible in a given environment that there will be a separate Web server and SAML service(s), or the SAML service could be combined with a Web server, or there may be no traditional Web server at all. In the latter case a company might be using an application server or some other software to handle their Web environment.

The information added in Step 2 is a binary piece of data that is fixed in size, called an artifact. The information passed between Site1 and Site2 in Step 4 contains a SAML assertion in XML, encoded using SOAP and layered on top of HTTPS (i.e. HTTP over SSL).

The Oblix NetPoint SAML Solution

Oblix NetPoint Overview

The NetPoint Access System™ and NetPoint COREid System™

Oblix NetPoint is composed of two powerful systems: the NetPoint Access System and the NetPoint COREid System. The NetPoint Access System delivers common security across multiple Web and non-Web servers and applications, and ensures that only authorized users can gain access to information, applications, and resources residing across virtual organizations. Access is controlled by a strict, standards-based authentication and authorization process that protects both Web and non-Web resources residing on companies' servers. The NetPoint COREid System, the market-leading identity management platform, provides powerful self-service security features, multi-step identity workflow, and delegated administration to ensure that user identity information is continually kept current, even in dynamic e-business environments. Because user identities are always up-to-date, Oblix NetPoint increases the effectiveness of security policies, and in turn the security of the overall business network in real time.

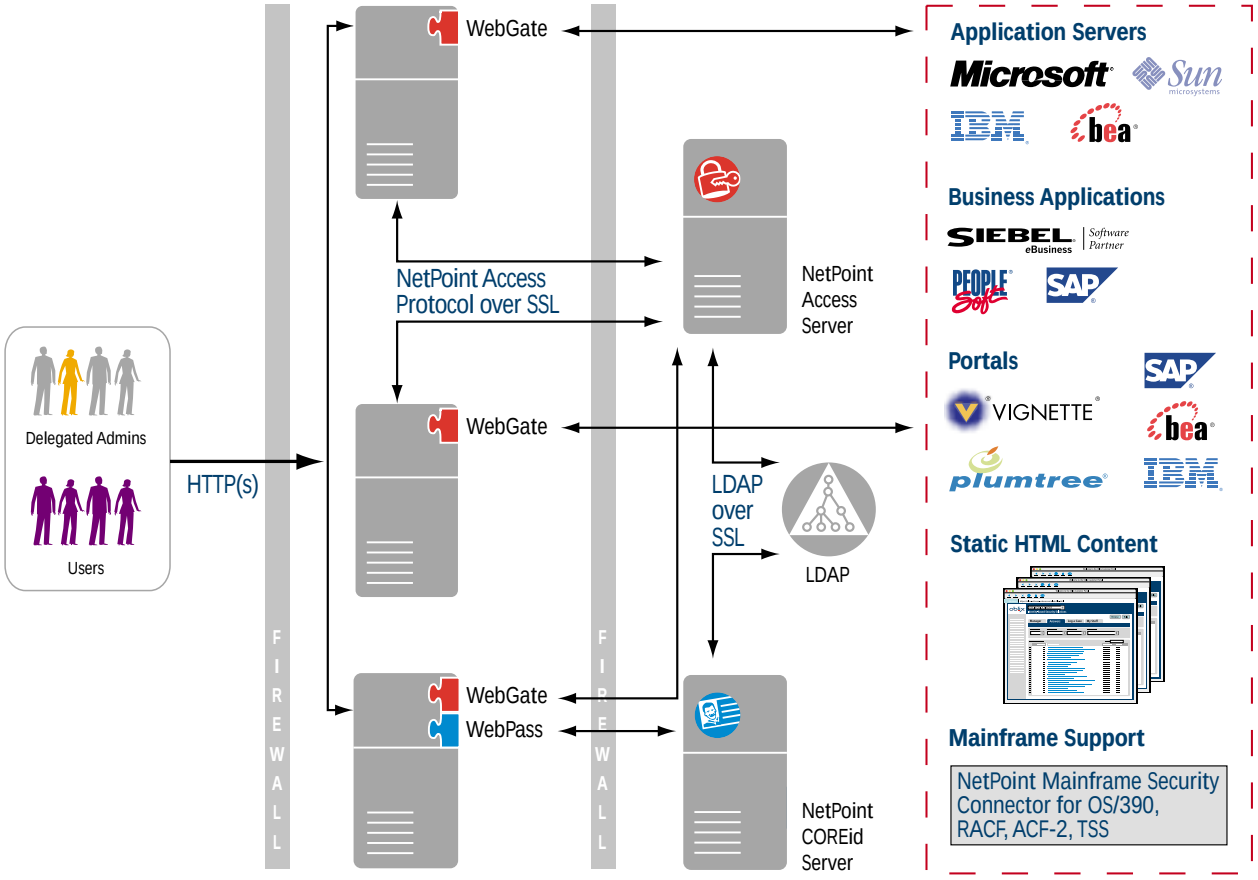

Figure 2: A Typical Oblix NetPoint Deployment

Although replete with the most sophisticated functionality, both systems are designed for use by non-technical business workers—rather than by designated IT professionals alone. This means that the workload of system management and upkeep can be efficiently distributed throughout an e-business environment, giving each typical user and administrator appropriate responsibilities for managing information and thereby eliminating IT bottlenecks.

The basic Oblix NetPoint architecture without its SAML Services is shown in Figure 2.

The NetPoint SAML Services

The NetPoint SAML Services provides complete out of the box support for exchanging SAML authentication, authorization, and attribute assertions. The NetPoint SAML solution sets itself apart from other SAML solutions today by a unique set of differentiators. First, unlike other solutions available on the market today, the NetPoint SAML Services support the full range of abilities to produce, consume, and respond to all SAML assertions. In addition, the NetPoint SAML Services does not suffer the limitations of an "affiliate" model, which can only support one-to-many relationships. Companies hosting "hub" Web sites, which are accessed by many partners, cannot deploy "affiliate" based SAML solutions. The NetPoint SAML implementation can support both one-to-many and many-to-one relationships.

Second, the NetPoint SAML Services is a part of NetPoint Federation Services, a comprehensive set of services that enables interoperability between disparate authentication and authorization services. The NetPoint Federation Services include:

- **NetPoint FEDERATEDid Layer™ –** An integration layer within Oblix NetPoint that allows an enterprise to identify users from any 3rd party authentication source while maintaining tight control over access to Web-based applications and resources.
- **Passport Authentication Plugin –** Native integration with .NET Passport's authentication capability, gives enterprise customers the ability to use their .NET Passport user name and password, or credentials, to gain access to both internal and external applications.
- **Associate Portal Services™ –** Allows customers to protect systems that reside at multiple Web sites and provide single sign-on to multiple sites.
- **NetPoint SAML Services –** A complete out of the box SAML solution that provides enterprises with industry-standardized services through which authentication, authorization, and single sign-on profile information can be exchanged and trusted between multiple policy-based security systems.

This means that users signed onto a SAML-secured site can also have single sign-on to all other Web and non-Web sites protected by Oblix NetPoint, to sites that require Passport authentication, and to any other site integrated under the NetPoint Federation Services umbrella.

Last, and most important, the NetPoint SAML Services is the only SAML solution on the market today that is integrated with a leading federated identity management platform, NetPoint COREid™. Implementing a SAML solution requires synchronization of some information between partner company user directories, which can become expensive and difficult to manage if the number of SAML partner end-users grows large. For this reason, companies looking to implement SAML solutions also need strong federated identity management capabilities. The NetPoint COREid System has a strong track record, both in its market-leading position, and in proven success in large-scale deployments.

NetPoint SAML Implementation Details

The Oblix NetPoint SAML implementation provides the SOAP over HTTP binding of the SAML protocol, including the Authentication, Attribute and Authorization Decision Queries. These queries allow SAML-enabled applications to retrieve SAML assertions with information about subjects in a security domain protected by Oblix NetPoint.

Oblix NetPoint SAML also implements the Web SSO Browser/Artifact and Browser/POST profiles, which allow Web browser users to sign in once to a Web site protected by one SAML-compliant security product and transfer to another Web site protected by a different SAML-compliant product, without having to sign in again. Oblix NetPoint can be used to protect either the originating site (the producer) or the receiving site (the consumer), or both.

Architecturally, the Oblix NetPoint SAML implementation is a set of Web services that use the NetPoint Access Server API to obtain authentication information, user attributes, and authorization decisions from the NetPoint Access Server™. It is comprised of a Responder Service, a Transfer Service, a Receiver Service, and a Requester class:

- **Responder Service -** Processes incoming SAML protocol requests and returns the appropriate SAML protocol response. It constructs new assertions or retrieves previously constructed assertions to satisfy the requests.
- **Transfer Service -** Provides the producer part of the Browser/Artifact and Browser/POST profiles. It is invoked to begin the transfer of a user logged into the local NetPoint-protected Web site to another site.
- **Receiver Service -** Provides the consumer part of the Browser Artifact and Post Profiles. It is invoked when a transfer from an originating site is received.
- **Requester Class -** Can be used by other SAML-enabled applications to send SAML requests and receive SAML responses to a SAML Responder. The Requester methods open HTTP connections to the SAML Responder and send and receive SOAP messages containing SAML requests and responses.

The NetPoint SAML Services Manager, a management console within the NetPoint Access Manager, enables users to easily set up and configure the NetPoint SAML solution, and delegate configuration rights.

How Oblix NetPoint SAML is Secured Against Attacks

The NetPoint SAML Requester and Responder Services can be configured to use SSL to ensure the privacy and integrity of their communications. This is in fact required by the Browser/Artifact profile. The Responder Service does this through its host Web or application server, which must be set up with a public/private key pair and an X.509 certificate. The Responder Service has to be configured to trust the Certificate Authority that issued the server's certificate. Optionally, the Responder Service can also be set up with a public/private key pair and an X.509 certificate for SSL client authentication. Oblix NetPoint incorporates this into the tool to install and configure the Requester Service.

The Oblix NetPoint SAML services can be protected by a NetPoint policy on the service URLs, which is enforced by the NetPoint WebGate component on the host Web server. This policy can require any form of client authentication that may be provided by the SAML requester, including HTTP basic or SSL client authentication. An Oblix NetPoint authentication scheme maps the SAML requester to a NetPoint identity that represents the requester. The policy for the Web services can restrict access to the SAML Services to authorized SAML requesters.

Both the Browser/Artifact and Browser/POST profiles require that SSL communication between the user's Web browser and the Web server's hosting the Transfer and Receiver Services. This prevents interception and replay of the artifact or assertion.

The Browser/POST profile has an additional requirement that the assertion response in the HTML form be signed to protect it from being altered without detection. Oblix NetPoint uses a standard Java keytool program to set up the keys and X.509 certificate required for the digital signature. Additionally, Oblix NetPoint can generate or verify a signed response with a certificate embedded in the signature, or with a certificate that has been previously set up for the signer.

Oblix NetPoint SAML Services implement other security requirements of the SAML protocol and bindings, including randomization of IDs and artifacts, one-time use of artifacts, configurable assertion expiration, matching of artifact requests to the expected requester, and matching of responses to requests.

Real World Examples

Oblix NetPoint Technical Process Flow with SAML

Figure 3, and the corresponding sequence of steps listed below, is from a real example of a customer use case requiring single sign-on between two separate domains and security systems. In this case, separate instances of Oblix NetPoint with different user repositories have been implemented to support each of the sites.

0. Authenticate to Site1 Domain - the browser user accesses a protected resource on Site1, for example, https://host1.site1.com/home/oblix.html. Site1 is protected with a NetPoint WebGate that challenges the user and, upon successful authentication/authorization, sets a single sign-on cookie (called the ObSSOCookie) for the Site1 domain.

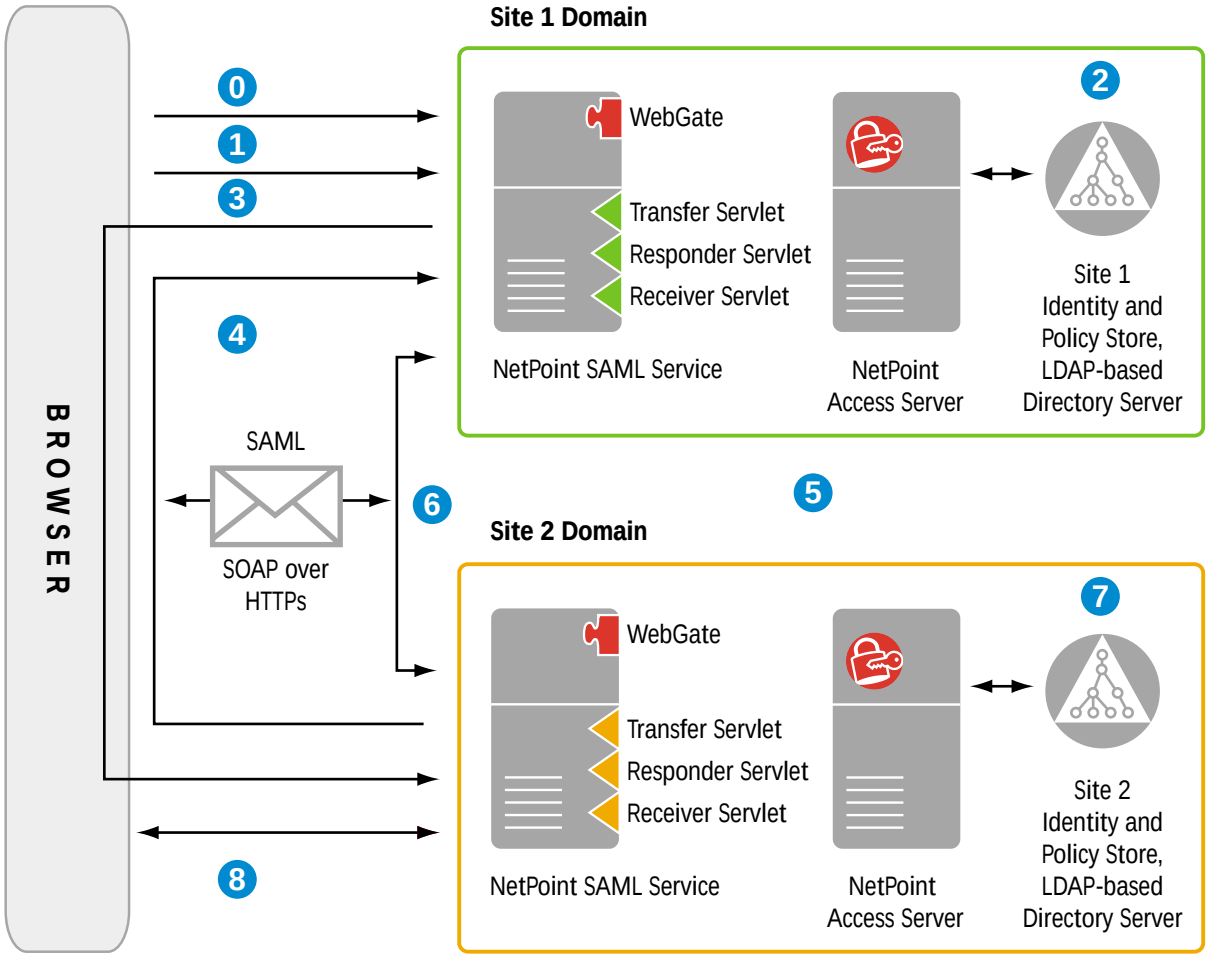

Figure 3. Oblix NetPoint SAML Diagram

1. Request a Site2 Resource – within a single frameset, the browser user is presented with local content from the Site1 Web server and requests a transfer to a protected resource on Site2. The Site2 browser frame is made up of a transfer link that points to a URL on the Site1, called by SAML the Inter-Site Transfer Service, that initiates SSO to Site2 using the artifact profile. Since the Site1 WebGate sets a local ObSSOCookie in Step 0, the browser will send this cookie to the Inter-Site Transfer Service. An example of the Site1 Inter-Site Transfer URL follows:

   https://host1.site1.com/saml/ObSAMLTransferService?TARGET=
   https://host2.site2.com/protected/default.asp;DOMAIN=site2

2. Create and Store Authentication Artifact and Assertion - the Site1 Inter-Site Transfer Service creates an authentication assertion based on its local state – the Site1 ObSSOCookie. The Inter-Site Transfer Service then creates an artifact for the authentication assertion. The artifact contains three fields:

   - a typecode that identifies the structure and use of the artifact (SAML defines a typecode 0x0001 for the Browser Artifact profile)
   - a source ID that indicates Site1. This requires prior agreement between Site1 and Site2 on source ID values
   - an assertion handle that Site1 will use in Step 3 to retrieve the assertion.

   Site1 redirects the user's browser to a URL on Site2, called the Assertion Consumer Service (ObSAMLTransferService). The query string of the redirection URL contains the artifact. An example of this follows:

   https://host2.site2.com/saml/ObSAMLReceiverService?TAR
   GET=https://host2.site2.com/protected/default.asp&SAMLart=artifact

3. Re-direct to Site2 with Authentication Artifact and Target Resource - the Assertion Receiver Service on Site2 receives the redirection, extracts the artifact typecode, source ID, and assertion handle from the URL, and looks up Site1 in a local table of source IDs.

4. Request Assertion with Artifact - the Assertion Receiver Service, as a SAML Requester, sends an assertion artifact request with the artifact to the SAML Responder registered for Site1. In the example, to

   https://host1.site1.com/saml/ObSAMLResponderService

5. Map Artifact to Assertion - the SAML Responder on the Site1 processes the assertion artifact request and maps the assertion handle in the artifact to the original authentication assertion. The SAML Responder sends a response with the assertion back to the Site1. Site1 also removes its mapping of the artifact to the assertion, since the Browser Artifact Profile dictates that the artifact be usable only once to prevent replay attacks.

6. Response with Assertion -the Site1 Assertion Consumer Service receives the response with the authentication assertion.

7. Process Authentication assertion and set Site2 ObSSOCookie, send re-direct back to browser - the NetPoint system on Site1 interprets the information in the authentication assertion. It performs a local login for the subject and sets its own ObSSOcookie for future requests from the browser user. The Site2 NetPoint system evaluates local authorization rules to determine if the user is allowed access to the originally requested target resource.

8. Validate Cookie, evaluate Site2 Authorization rule, serve Site2 content - once the authorization rules are satisfied in Step 7, Site1 redirects the user's browser to the resource.

   While there appears to be a lot going on, note the following:

   - All of the redirects happen automatically and are handled transparently by the system.
   - The user only has to authenticate to the system once.
   - Site1 can determine if its users have access to the SAML link.
   - Site2 can control the user's access to the resources at their site.

Figure 3 illustrates a typical "pull" model for exchanging SAML messages; a model in which the browser passes a URI to a destination (consumer) server and the destination server uses a reference (a SAML artifact) within the URI to retrieve (pull) the assertion message from the message source (producer). The NetPoint SAML Services also supports the "push"-oriented models, typically one in which the browser submits a message directly containing an authentication assertion to a SAML-enabled destination server.

Although Figure 3 shows Oblix NetPoint on both sides of the message exchange (operating in both Site1 and Site2), NetPoint is capable of exchanging SAML messages with any SAML-compliant service as either a SAML assertion producer or a consumer. In other words, Oblix NetPoint does not necessarily have to be deployed at both sites. It is also important to note that SAML enables the exchange of authentication and authorization messages between security domains, and that these domains can exist within a single enterprise or across separate enterprises. Most discussions around SAML focus on single sign-on across corporate boundaries, but SAML can also enable single sign-on across separate domains within a single corporate enterprise that each wish to maintain separate control over their own security data.

Because SAML addresses communication between companies across the Internet, it has some strict security requirements. These have been built into the specification as part of the standard itself. Please refer to Appendix A.

Oblix NetPoint Business Flow With SAML

Now let us examine a scenario based on a real customer use case that shows how the NetPoint SAML process flow may be used to derive real-life business benefits.

Multiple Logins: High Cost, Low User Satisfaction

Consider a scenario in the airline industry, in which a large aerospace corporation builds and sells airplanes to airline corporations. The aerospace corporation has been a close business partner with a particular airline company that buys airplanes exclusively from the aerospace company. In return, the aerospace company allows the airline's mechanics direct Web access to highly sensitive airplane maintenance information through one of its applications.

Both companies face a number of challenges in supporting this access in a secure manner. The aerospace corporation is concerned about the cost of securing outsider access to highly sensitive information. Would this require that it manage authentication information for each of the partner airline's mechanics? For example, would it need to manage a login ID and password for each mechanic, and therefore shoulder the added cost of managing password resets and lost passwords?

At the same time, the airline company faces a different issue: Because the mechanics are highly specialized in repairing airplanes, their union applies a surcharge for any required tasks falling outside of that scope, including a surcharge for every user ID and password the mechanics must remember. So the airline company wishes to minimize the required number of user login IDs and passwords.

SAML Single Sign-on Powered by NetPoint SAML Services

The NetPoint SAML Services meets all of these challenges by enabling the two partner companies to establish a SAML trust relationship. In this relationship, the aerospace company and airline company agree to use a common identifier to mutually and uniquely identify each mechanic – for example, the mechanic's email address. After synchronizing these identifiers across their respective user data repositories, the airline company then configures its corporate portal with a NetPoint SAML-powered link through which the mechanics can access the aerospace company's application.

The system then works as follows: After a mechanic successfully logs in to the airline corporate portal, he clicks on the NetPoint SAML-powered link. This initiates a series of SAML exchanges with the aerospace company, similar to those illustrated in Figure 3. Within these exchanges, the mechanic's authentication is asserted using the common identifier, his email address. Using this common identifier, the aerospace company maps the user within its own local repository, and then applies its own local security policy to evaluate if the mechanic is authorized to access the application. If so, the mechanic is seamlessly granted access to the application.

Lowering Administrative Costs and Maintaining Security

By using only a single common identifier to map users between partner security domains, the aerospace company avoids additional administrative overhead and help desk costs associated with password management and enforcement. In addition, the aerospace company maintains complete control of the authorization policies that protect its highly sensitive information. The airline company also reaps tangible benefits, not only because it avoids union surcharges, but also because the SAML-powered single sign-on experience improves user satisfaction and productivity.

NetPoint SAML Services and COREid

SAML and Identity Federation

Most current discussions around SAML focus on federated single sign-on – that is, on enabling a user logged into one security domain to transparently access resources in another domain protected by an entirely different security system. Federated SSO has a critical underlying requirement, namely that of identity federation. Identity federation is the exchange and synchronization of authentication (and possibly authorization) information about users across security domains. To enable federated single sign-on through SAML, collaborating partners must, at the very least, exchange and synchronize user identification information using a set of common identifiers.

As an example, let us revisit the airline scenario discussed in the last section. Key to this scenario is the sharing and exchange of common identifier information. In this case, a set of common email identifiers were exchanged between partner companies prior to any SAML message exchanges. More importantly, in order to maintain secure access, these identifiers must be kept up to date and synchronized between the two partners at all times. For example, when a mechanic retires or leaves the airline company, his or her access to the aerospace application should be immediately disabled.

If the number of airline mechanics is small, maintenance of common identifiers at the aerospace company may not be big issue. But what if the aerospace company wishes to establish similar SAML partnerships with many other airlines? What if those airlines have hundreds, maybe thousands of employees, as well as a high employee turnover rate? How can one SAML partner accurately track the lifecycle of end-users employed by all of its SAML partners?

The answer is identity federation. The success of a SAML partnership depends upon it, even if SAML itself doesn't address this issue. Customers looking to implement a SAML solution should not look only for a complete and flexible SAML solution, they must also look for a complementary federated identity management solution. Oblix NetPoint is the only platform that provides mature SAML capabilities integrated with COREid, the industry's leading federated identity management platform. NetPoint COREid not only allows partner companies to accurately exchange, synchronize, and manage identity data, it enables these capabilities in a scalable and cost-effective way.

How NetPoint COREid Enables Identity Federation

The innovative NetPoint COREid System not only manages user identities within an enterprise, it is capable of federating identity information across corporate and security systems boundaries. Underlying each of its powerful features are two key principles: first, that accurate management of user identities is a critical underpinning of enterprise security, and second, that today's market demands identity management methods that are cost-effective and scalable. Some key NetPoint COREid features that SAML partners can leverage for identity federation are:

- **Multi-Level Delegated Administration –** Oblix NetPoint provides a unique multi-level delegation model that allows companies to distribute responsibility for maintaining user identity information throughout their networks. In this way, identity data can be entered, approved, and maintained by the individuals who are most knowledgeable about it—whether in internal or external organizations.
- **Self-Registration –** Oblix NetPoint offers a full array of customizable self-registration workflows that enable employees, partners, and associates to fill out personal information about themselves and their organizations.
- **IdentityXML™ –** IdentityXML allows applications and systems to easily access all the NetPoint COREid System functionality programmatically through XML. For example, with IdentityXML, the creation of a new user in an HRMS system can trigger an Oblix NetPoint workflow, or a portal/personalization product can use IdentityXML to find out whether a user is part of a particular group or organization.
- **Attribute Access Control –** With fine-grained access control, companies have complete control over who has the authority to view, modify, create, or delete identity information, down to the attribute level.
- **Group Management –** Oblix NetPoint allows companies to identify dynamic, static, and nested groups of users that need identical access privileges to a specific resource or set of resources.
- **Identity Workflow –** Oblix NetPoint COREid features a multi-step, flexible workflow engine for the automated management of user identity, group and organization information.

Leveraging the airline industry scenario outlined in the previous section of this paper, let's now take a look at some ways in which companies could implement these features to enable cost-effective and scalable identity federation.

Delegating Administration to Partner Help Desks

Probably the simplest method for identity federation, customers can deploy delegated administration initiatives through Web browsers. For example, in revisiting the aerospace and airline company scenario, the aerospace corporation can deploy a portal site through which airline help desk administrators have the authority to view and modify specific user attributes for each mechanic. The aerospace corporation can apply attribute access control to specifically limit which attributes the partner administrators may view or modify, and can also implement approval-based workflows for added control over specific requests to modify sensitive user data.

Automated Provisioning Through XML

Over time, SAML partners will no doubt shift certain administration tasks to automated provisioning services over the Web. For example, when new mechanics join the airline company, they should have immediate access to the aerospace company's airplane maintenance application. This can be enabled by configuring the airline's HR system to send IdentityXML messages to the aerospace's NetPoint system upon "new employee" events. Approval-based workflow enables the aerospace company to maintain control and visibility over user entry creations within its own repository, and attribute access control limits which directory tree elements may be modified, thereby disallowing one partner airline from modifying employee data belonging to another partner airline.

Portal Self-Service

Self-service portal inserts empower end users to keep their identity data up to date. For example, airline mechanics can click on a "My Identity" NetPoint portal insert in the airline corporate portal, through which mechanics can directly view and maintain specific elements of their user profile, as it exists in the aerospace company's repository.

Dynamic Group Management for Multi-Tiered Access Control

Features such as dynamic group management enable companies to provide secure sophisticated multi-tier SAML-based access. For example, to meet regulatory requirements, the aerospace corporation can implement security policies and dynamic groups that allow only mechanics with U.S. citizenship to access the more sensitive areas of the aerospace company's application.

Automated Self Registration

Companies can build self-registration on top of SAML services to support automated self-registration. For example, when a "partner end-user" is transferred from a partner site, this triggers the creation of a local user based on attributes contained in the user's assertion. Additionally, SAML services can obtain additional attributes about the user as needed for the registration. In subsequent visits, that user would be mapped to his corresponding local user profile.

Summary

Oblix has provided clear leadership in the definition and delivery of the SAML standard and will continue to play a leadership role in the ongoing development of SAML and other related standards activities such as WS-Security and Liberty Alliance. This strategy enables Oblix to deliver a solution customers can deploy today to take advantage of interoperability standards.

Oblix ships the most mature SAML solution on the market today. Enterprises that adopt Oblix NetPoint SAML today to secure online partnerships can take advantage of a range of deployment options. Oblix NetPoint can support both one-to-many and many-to-one relationships. SAML offerings limited to "affiliate" support can only support one-to-many relationships. Companies hosting B2B applications accessed by numerous partners cannot deploy an "affiliate" based solution. The wide range of options supported by NetPoint SAML allows companies to deploy a cost effective security model that will drive customer satisfaction and competitive advantage.

Appendix:

Security Notes

The SAML standard has built-in security requirements to ensure the privacy of the information exchanged between partnered sites. Some of these guidelines are outlined below:

1. All SAML server connections are supported over SSL (between the user and other SAML servers). The Browser Artifact and POST profiles mandate SSL connections between the browser and the Transfer and Receiver Services and between the Receiver and Responder Services.
2. The source ID is used to look up the address of the partnering SAML server from a local database. This ensures that a SAML server is always going to a known address to do its communications.
3. SAML servers will ensure that the correct server has connected to them and that they are passing assertions only to the server that they were generated for.
4. With NetPoint as a part of SAML, enterprise infrastructure users are properly authenticated and authorized each step of the way even if they are not physically queried for the information.
5. All SAML assertions identify the issuer, so the site receiving the data can verify that the issuer is allowed to make assertions about the role in question and not roles related to other issuers.
6. The data cached by a SAML server, data created as a result of a user clicking on a transfer link, must have a limited lifetime. This helps to prevent theft and denial of service attacks.
7. Handles that allow one SAML server to get information from another SAML server may only be used once. This prevents replay attacks.
8. A SAML server must only give information about a user trying to access resources to the site for which the handle was generated. Thus if Site1 generates a handle for Site2 and Site 3 queries Site1 for the information, Site1 should not pass the information to Site 3. This requirement prevents a third site from being able to get the SAML assertions that are meant to go to a legitimate partner site.