Federated Identity and Super Sign On

Though Single Sign On has been popular on internal networks, extending this concept further has been the focus of Federated Services. With Cloud-based computing gaining popularity, a means of accessing resources across the internet is necessary. The term *Identity Management* is used as a means of coordinating user accounts/traits/attributes/entitlements across multiple organizations or across the web. Users log in once, in their own organization or to their own Identity Provider (ex: GoogleID, Microsoft Passport, aka LiveID, Facebook, Twitter, etc). The username and password are matched with an identity that is

**XML:** Is a common universal format for storing and exchanging information. Most all databases can import and export data to and from XML format. The universal nature of this language eases exchange of information.

**SPML** is an XML protocol for exchanging user and resource information and for controlling identity provisioning operations with heterogeneous systems and resources. It defines an XML-based framework for representing provisioning requests intended for creating, modifying, deleting, enabling/disabling, searching user accounts and associated access control privileges with their target resources. The SPML-based provisioning process may also involve business work flows, designated approval actions based on other user attributes such as roles, permissions and privileges. With SPML, it would be lot quicker to automate provisioning user accounts and associated access rights to multiple resources and integrating different provisioning systems. **As a standard, SPML promotes integration and interoperability between SPML-aware identity provisioning systems and also allows exchanging identity information using standards-based protocols via XML Web services. This markup language allows for the integration and interoperation of service provisioning requests across various platforms.**

**SAML** provides an XML-based framework for exchanging security-related information over networks, and thus over the Internet. SAML does not define newer mechanisms for authentication or authorization. Instead, it defines XML structures for representing information pertaining to authentication and authorization so that these structures can be marshaled across system boundaries and can be understood by the recipient's security systems residing within and across networks. SAML is emerging as a de facto standard for securely exchanging XML-based security information, for enabling single sign-on and identity federation regardless of the underlying security architectures, and for promoting security interoperability. The current specification SAML 2.0 has been ratified as an OASIS standard.

When there is a need to allow a user to log in one time and gain access to different

and separate web-based applications, the actual authentication data have to be shared

between the systems maintaining those web applications securely and in a standardized

manner. This is the role that the ***Security*** *Assertion Markup Language (SAML)* plays.

**It is an XML standard that allows the exchange of authentication and authorization data to be shared between security domains**. When you purchase an airline flight on www.southwest.com, you are prompted to also purchase a hotel room and a rental car. Southwest Airlines does not provide all these services itself, but the company has relationships

set up with the companies that do provide these services. The Southwest

Airlines portal acts as a customer entry point. Once you are authenticated through their

web site and you request to purchase a hotel room, your authorization data are sent

from the airline web server to the hotel company web server. This allows you to purchase an airline flight and hotel room from two different companies through one centralized portal.

**SAML provides the authentication pieces to federated identity management systems to allow business-to-business (B2B) and business-to-consumer (B2C) transactions. In our previous example, the user is considered the principal, Southwest Airlines would be considered the identity provider, and the hotel company that receives the user’s authentication information from the Southwest Airlines web server is considered the service provider*.***