SAML 101

WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

Today's enterprise employees use an ever-increasing number of applications, both enterprise hosted and in the cloud, to do their jobs. What's more, they're accessing those applications from a variety of devices (desktops, laptops, tablets, phones, etc.) and application models (both browser and native). Expecting those employees to remember strong and unique passwords for each and every application is simply unreasonable.

Identity federation solves these challenges by providing a secure, private mechanism for organizations to share user identities, removing the need to maintain separate user profiles for every enterprise application.

The identity federation standard, Security Assertion Markup Language, or SAML, enables single sign-on (SSO) and has a wide variety of uses for businesses, government agencies, non-profit organizations and service providers. The major limitation of SAML is that it was never optimized to enable SSO for the new breed of native mobile applications, or for applications that consolidate data and services through API calls from multiple third-party sources. WS-Trust (for SOAP services), OAuth 2.0, an open standard for authorization, and OpenID Connect, which builds on the OAuth specification, have emerged to meet these needs, providing more value and flexibility for users.

The convenience of identity federation and one-click access to web applications has shown a significant increase in the adoption of applications. Identity federation also enhances security, limits risk and improves compliance by eliminating web application passwords. When it comes to delivering business value, identity federation helps remove business barriers, reduce costs and increase productivity for the entire enterprise.

INTRODUCTION

The web has dramatically transformed the way we conduct business and how people work.

With organizations now able to communicate with one another, in real-time, over the Internet, productivity has soared and new business models have emerged. Simultaneously, the migration from traditional mainframe and client/server applications to cloud applications is occurring at an unprecedented rate.

In addition to the migration to cloud architectures, the way that these these applications are hosted and accessed is changing. Previously, internal teams built, hosted, and maintained business-critical applications. Today's businesses face the daunting challenge of providing seamless, secure access to applications regardless of their physical location and provider, from virtually anywhere, using virtually any connected device (both BYOD and enterprise-provided). In addition to this fundamental change in application architecture and access requirements, maintaining application and data security, ensuring application user adoption, increasing user productivity and containing costs are all still key considerations.

In spite of this, the requirement for applications to reliably identify users and make access and authorization decisions has not changed. Externally hosted applications generally require each user to have their own username and password, forcing them to remember login credentials for each application, and passwords must be changed regularly to ensure security. This diminishes productivity and increases security risks from phishing and hacking as users tend to pick memorable passwords. If an organization attempts to thwart this by establishing strict password policies, users are prone to record passwords offline, leading to further vulnerability. What's needed is a way to eliminate passwords altogether and provide SSO to web applications, while maintaining high security levels.

Standards-based identity federation solves these challenges. This white paper introduces identity federation and the predominant standard, SAML. It describes why standards like SAML are necessary for implementing scalable yet secure federated identity across organizations. SAML use cases are highlighted for enterprise, SMBs and organizations acting as service providers.

Lastly, this paper reviews scenarios where SAML integrates with other key federation protocols and explores the advantages and disadvantages of both WS-Federation and SAML.

SECURITY IN AN INCREASINGLY CONNECTED WORLD

The Internet has become the preferred application platform for a very good reason: the utterly intuitive, universal browser interface.

The point-and-click ease of a webpage makes users more productive, and widespread familiarity with this interface minimizes training and support problems. Despite the rise of native mobile applications, web applications offer undeniable advantages. There's no need to develop applications specifically for multiple mobile operating systems or to distribute new versions.

Behind these user-friendly web applications and services is an extensive set of industry standards that ensure they can seamlessly and securely interoperate. The Hyper Text Markup Language (HTML) and Hyper Text Transfer Protocol (HTTP) are the standards most visible to users, but there is a veritable "alphabet soup" of other protocols that enable effortless navigation among multiple applications from virtually any browser.

Web applications can be located inside of the organization, hosted externally, delivered as a service, or configured as any combination of the three. Security for internal applications is relatively straightforward, provided that all users and applications are in the same security domain, and a central identity management (IdM) system identifies and authenticates users.

All of this falls apart when applications are moved outside of the firewall or another security domain (this includes moving to Software-as-a-Service (SaaS) and Business Process Outsourcing (BPO) vendors). Since these applications don't have access to the organization's IdM system, they must each maintain their own user database for access and authorization purposes. Users sign on to each application with a distinct username and password each time a new browser session is initiated. This may not seem like a major problem, but consider how many logins are required when hundreds or thousands of workers each have to sign on to multiple web applications several times each day.

Business customers and consumers are frustrated by repeated login requests, especially when trying to do business across many products or affiliated services. Employees are keeping password lists that are easily forgotten, lost or stolen.

In addition to becoming an application adoption barrier, repeated logins have a negative impact on an organization's productivity. Remembering all those usernames and passwords is difficult and time consuming, and it's not uncommon for users to choose a memorable, identical username and password for every application. If someone guesses or discovers the username/password combination, they potentially gain access to all of the user's applications.

Equally concerning to IT teams is the common symptom of employees or partners retaining access rights to applications after they've been terminated.

The ideal solution is to eliminate application passwords altogether and provide secure SSO to all web applications using a scalable, cost-effective means. Federated identity was developed by the industry to solve these challenges.

FEDERATED IDENTITY

Federated identity provides a secure, standard, internet-friendly way to share identity among multiple organizations and applications. Users sign on once with a standard network login or hosted authentication service. When they click a web application link, their identity is transparently and securely shared with the application, removing the login requirement. Since the organization authenticates the user and the application provider can verify the authenticity of the provided federated identity, application passwords are not needed and users enjoy “click-and-work” access to applications.

Identity federation is a huge win for users, IT and the business alike. Users love federation because internet SSO enables them to use web applications as easily as internal applications while freeing them from remembering (and resetting) a battery of passwords. IT loves federation because it simultaneously enhances security and reduces the support burden, especially at the help desk. Business leaders love federation because it accelerates application and data sharing with customers, business partners, vendors and subsidiaries while decreasing risk and increasing regulatory compliance.

STANDARDIZING FEDERATED IDENTITY

Federation, by definition, is the process of uniting smaller, localized entities as a single group. When a technology is federated, all participants agree to conduct themselves in an identical, “standard” fashion, playing by the same rules to enable seamless interoperability.

Federated identity would be impossible without standards. Each organization embarking on application sharing would have to spin up an elaborate design and development project, negotiating point-to-point interfaces between each party’s unique infrastructures. Unless each connection was exhaustively tested, security risks or other instabilities could easily result. And imagine conducting such a complicated, collaborative effort each and every time a connection is made with a business partner or vendor. Scaling federation without standards is virtually impossible due to security risks, prohibitive costs and longer time to market.

The need for federated identity was identified in the early 2000s, and several groups began work on creating the necessary standards. Unfortunately, multiple standards can be the same as having no standards at all, when organizations choose to implement different ones. By 2005, after a number of groups consolidated, two major identity federation standards for the enterprise remained: SAML and WS-Federation. (In the consumer world, OpenID 2.0 has been the default SSO protocol, but is now being replaced by the more robust and secure OAuth and OpenID Connect protocols.)

While SAML has emerged as the dominant standard, WS-Federation continues to be found in Microsoft-centric organizations that use Active Directory Federation Services (ADFS) (note: the latest version of ADFS supports both SAML and WS-federation). The existence of two protocols underscores a very important point: identity federation products and services need to support multiple protocols in order to cover all potential use cases and connection types.

SAML enables the secure exchange of authentication and authorization information between security domains (such as separate organizations or company divisions) or even company divisions.

In SAML terms, an “assertion” is made by an identity provider (IdP) who has the responsibility of maintaining and authenticating the user’s identity through a variety of means (usually via an IdM system), including username/password or even “strong authentication” techniques like biometrics.

When a user attempts to access at a service provider (SP), federation software creates a SAML authentication request and delivers that to the user’s appropriate IdP. After the IdP federation software receives and validates the authentication request, the IdP authenticates the user and creates a SAML assertion that represents that user’s identity and attributes. The assertion is digitally signed and encrypted to ensure authenticity and may optionally include other data required by the destination application. The assertion is then securely transmitted back to the SP.

Identity federation software at the SP receives the assertion, verifies its authenticity, decrypts the contents and then shares the information in the assertion (including the user’s identity) with the application. The application then uses the data to sign the user on, enabling SSO. From the user’s standpoint, they click the application link and start working, completely insulated from the federated identity ‘magic’ taking place on their behalf.

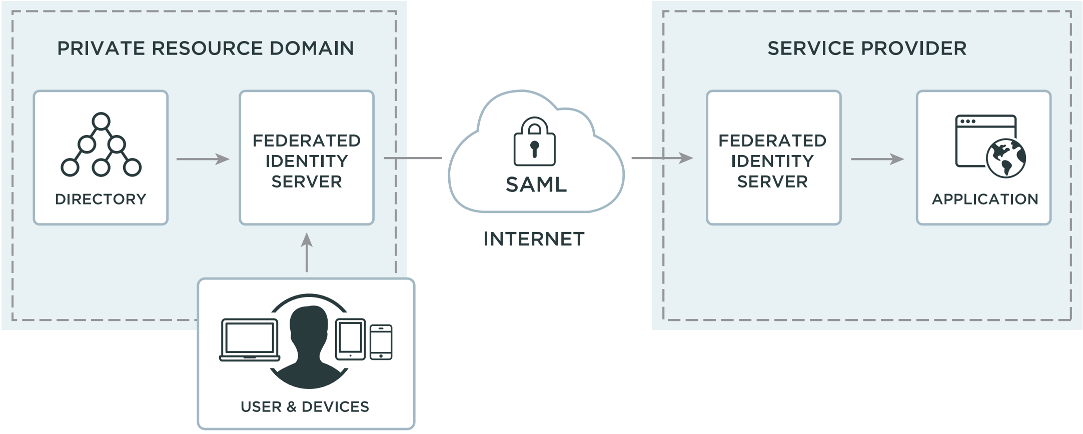

Figure 1: Federated identity software translates the user’s local identity into a SAML assertion, enabling Internet single sign-on

SAML is managed by OASIS (the Organization for the Advancement of Structured Information Standards), which also manages over 70 other web standards. However, SAML has roots that extend far beyond OASIS. Today’s SAML 2.0 is the result of the convergence of three separate standards, which together give SAML its unparalleled market dominance.

SAML version 1.0 was introduced in 2002, with version 1.1 arriving the following year. 2005 would see the full convergence of SAML 1.1 with two alternative forms of SAML: the Liberty Alliance Identity Federation Framework (ID-FF) and Shibboleth, into SAML 2.0, the latest and final version. The Liberty Alliance, which has now been subsumed by the Kantara Initiative, continues to perform a critical role by providing independent SAML interoperability testing and certification.

While SAML has become the identity federation protocol of choice for business-to-business interactions, multiple protocols will continue to exist indefinitely. For example, in the consumer space, OpenID 2.0 emerged to satisfy specific requirements around user-centric social networking, a use case that SAML was never designed to address. OAuth 2.0 is another standard that, while it emerged from the consumer space, shows increasing relevance to both enterprise and the cloud. OAuth 2.0 is now providing the foundation for additional capabilities in OpenID Connect, a standard that adds additional identity capabilities to the OAuth standard. OpenID Connect will become a key standard for (native) applications on mobile devices and tablets, and for machine-to-machine interactions.

Interoperability will be required between standards like these and SAML, and multi-protocol identity federation software will be the glue that makes it happen seamlessly.

SAML IDENTITY FEDERATION USE CASES

This section highlights how various types of organizations typically utilize SAML to enable federated identity for seamless and secure web application access.

ENTERPRISE USE CASES

Virtually every large enterprise has already invested in an IdM system for authenticating users and securing internal applications. Therefore, enterprise SAML identity federation use cases generally revolve around sharing identity between an existing IdM system and web applications.

The following is a summary of typical enterprise use cases:

- Outbound Internet SSO to web-based cloud, business-process outsourcing, partner, vendor or supplier applications
- Inbound Internet SSO to provide secure access to internal web applications for customers, business partners and affiliates/subsidiaries
- Internal web SSO to provide centralized access for the organization and any subsidiaries, acquisitions or joint ventures where enabling web services (SOAP and RESTful) to securely share identity with one another using the WS-Security and OAuth standards

Leveraging SAML to enable these use cases provides the following benefits:

- User passwords never cross the firewall, since user authentication occurs inside of the firewall and multiple web application passwords are no longer required.
- Web applications with no passwords are virtually impossible to hack, as the user must authenticate against an enterprise-class IdM first, which can include strong authentication mechanisms.
- "SP-initiated" SAML SSO provides access to web apps for users outside of the firewall. If an outside user requests access to a web application, the SP can automatically redirect the user to an authentication portal located at the IdP. After authenticating, the user is granted access to the application, while their login and password remains locked safely inside the firewall.
- Centralized federation provides a single point of web application access, control and auditing, which has security, risk and compliance benefits.

A properly executed identity federation layer that satisfies all of the use cases described above, supports multiple protocols and can provide an enterprise-wide, architecturally sound Internet SSO solution.

SMALL-AND-MEDIUM-SIZED BUSINESS (SMB) USE CASES

SMBs can reap many of the same rewards from Internet SSO as large enterprises, but they face additional infrastructure challenges. Many SMBs don't have (and don't want) an in-house identity management system, relying instead on a hosted authentication service like Google Apps. In this case, it's possible to use an on-demand identity federation service that leverages the hosted identity to enable Internet SSO to on-demand business applications.

Most SMBs that do have a directory service use Microsoft Active Directory, which is bundled at no extra cost with many Microsoft Windows Server products and works seamlessly with Microsoft Windows PCs and their peripherals. In this case, an identity federation server or on-demand service can provide Internet SSO capabilities that equal those enjoyed by larger companies.

SERVICE PROVIDER USE CASES

A large number of service providers have realized that federated identity is a business enabler, either as a value-added service or to satisfy customer demand for Internet SSO.

Service provider use cases include the following:

- Inbound connections from customers (acting as the IdP) that wish to enable Internet SSO for their users accessing the SP's applications
- Inbound Internet SSO connections from hosted authenticators like Google Apps
- Outbound connections to other SPs where identity needs to be securely shared in order to leverage third-party, value-added services without requiring additional logins

The benefits of SAML-based federated identity for service providers include:

- The ability to offer secure, scalable, standards-based Internet SSO to customers, either as a value-added service, a competitive differentiator, or to satisfy customer demands
- Decreased administrative overhead due to removal of user password management from the SP's system (password management responsibility is accepted by the customer), including decreased help desk costs
- Ability to federate with other service providers, sharing user identity in order to deliver seamless, transparent, value-added services without requiring an additional login

Service providers need to carefully consider which identity federation platform they deploy, ensuring that it's scalable, cost-effective, multi-protocol and easy to implement and maintain.

SAML OR WS-FEDERATION?

SAML's major advantage is its widespread and growing adoption throughout the industry.

It's commonly used between enterprises and their customers, business partners, and cloud providers. The reason for its popularity naturally derives from its many advantages. As an OASIS standard since 2002, SAML enjoys field-proven security, scalability and dependability in thousands of production deployments worldwide. The Liberty Alliance provides rigorous interoperability certification to minimize problems in situations where prospective partners are utilizing different vendor products, and SAML expertise is readily available in the market. A wealth of SAML deployment choices exist, these include: commercial identity federation software products, open source options and commercial development libraries.

WS-Federation is part of the web services, or WS-* (pronounced "WS star"), suite of specifications created by Microsoft and IBM. The WS-* suite includes numerous specifications for implementing web services in an interoperable and secure fashion.

WS-Federation is the suite's specification for issuing secure tokens (similar to a SAML assertion) that contain the attributes required for federated identity, providing comparable functionality to SAML's Internet SSO capabilities.

WS-Federation is primarily popular in environments dominated by Microsoft Windows servers. WS-Federation was initially the only identity federation standard supported by Microsoft's ADFS, a part of Microsoft's Active Directory family. ADFS was initially used to enable SSO and other forms of federated identity between Windows applications. Recognizing the widespread market acceptance of SAML, Microsoft added support for SAML 2.0 in the second release of ADFS. The addition of SAML to ADFS is significant, as it shows that even Microsoft has acknowledged SAML's dominance in B2B identity federation.

Denmark's National IT and Telecom Agency conducted a thorough evaluation of both SAML and WS-Federation. In every category, SAML was judged to have an advantage over WS- Federation, with only one exception: the fact that Microsoft supports WS-Federation was judged to be an advantage. The report did note, "All other significant suppliers support SAML 2.0 or are planning to do so, and all are expected to support WS-Federation." In other words, the major vendors of identity federation solutions typically support both SAML and WS-Federation.

SAML and WS-Federation are not mutually exclusive. An organization will quite likely need to federate with partners that support one or the other, but rarely both. An enterprise- and service provider-class federated identity solution must therefore support both standards. Implementing both standards ensures the broadest possible applicability across potential partners, and what good is federated identity if it's not fully federated? Support for all three versions of SAML (1.0, 1.1, and 2.0) and WS-Federation (including both generating and consuming assertions) is also required in order to cover all possible scenarios.

SAML AND OTHER IDENTITY PROTOCOLS

While SAML may be a key piece of federation architecture, it's not the only piece; so it needs to "play well" with other federation protocols.

One such protocol, a relative newcomer, is the Simple Cloud Identity Management (SCIM) protocol. SCIM is a lightweight provisioning protocol, optimized for (but not restricted to) enterprises managing user accounts and access for their employees in the various cloud providers and applications they have subscribed. SCIM defines a RESTful API by which the enterprise can directly perform CRUD (Create, Read, Update, Delete) operations to manage accounts for its employees at SaaS provider provisioning endpoints. SCIM also allows for a so-called "Just-In-Time" provisioning model, whereby accounts are not created on the first access by the employee, but rather indirectly via the first SSO operation. To enable this scenario, SCIM defines a binding to SAML, stipulating how to carry SCIM-defined user attributes (profile info, groups, roles, etc.) within the SAML assertion.

OAuth 2.0 is another protocol that was not even a twinkle in its creator's eyes when SAML was first defined. And yet, from an initial focus on the consumer world of shared tweets and Facebook photos, OAuth 2.0 (and, more recently, OpenID Connect, which builds on the OAuth 2.0 specification) is emerging as a key cloud standard because it provides a framework for securing the APIs that are a key underpinning of the cloud.

As an example, Salesforce is moving to using OAuth for its entire set of APIs. These APIs are becoming more and more important, even supplanting the browser as the dominant access channel that Salesforce offers to its customers. Importantly, OAuth can be applied to authenticating mobile native applications to their RESTful APIs–a use case SAML never optimized for. There are many different scenarios or deployment models where OAuth and SAML can be combined. They range from carrying OAuth tokens as parameters on SAML messages, to trading a SAML assertion for an equivalent OAuth token; thereby bridging between the SOAP web services world and the RESTful world.

SUMMARY

In today's web-centric application environment, with its wealth of internal and external web applications and services, federated identity is critical for making access both seamless and secure while ensuring that users adopt applications as quickly as possible. Without the standardization afforded by identity federation, Internet SSO can't be scaled beyond one or two partners in a cost effective manner.

SAML has emerged as the primary identity federation standard, due to its certifiable interoperability, proven security and thousands of production deployments worldwide.

When evaluating SAML solutions, make sure to consider all enterprise use cases, the need for integration with your existing infrastructure and the adherence to all identity standards. Because today's SAML solutions are now fully mature, implementing SAML-based Internet SSO now takes only days (sometimes even minutes) with the right solution.