WHITE PAPER

The Primer: Nuts and Bolts of Federated Identity Management

Overview

For any IT department, it is imperative to understand how your organization can securely manage and control users' identities. With so many employees accessing up to thirty different resources over the Internet to do their daily jobs—often with thirty different usernames and passwords—organizations are struggling to maintain a secure working environment. This white paper provides an introduction to leveraging user credentials securely through federated identity management.

PingIdentity™

Ping Identity™

Background

With employees accessing up to thirty different resources over the Internet to do their daily jobs—often with thirty different usernames and passwords—organizations are struggling to maintain a secure working environment. Due to the complex and fragmented nature of employee identities, the ability to coordinate, interact and control employee identity information has become more difficult.

For any IT department, it is imperative to understand how your organization can securely manage and control users' identities, not just your employees but all digital identities (e.g., customers, trading partners, employees of acquisitions, affiliates, subsidiaries and joint ventures) that access corporate resources over the Internet, including software as a service (SaaS) sites, business processing outsourcing (BPO) providers, managed services and third party industry hubs. Having a clear strategy for distributed identity management is fundamental to ensuring a secure workplace.

Gaining access to resources over the Internet is becoming increasingly vital to performing day-to-day work, and traversing the Internet with highly sensitive information requires that IT organizations effectively and securely manage identities between different security boundaries. As a result of this need, new methods were developed to enable the portability and interoperability of identity information across boundaries and security domains, providing IT organizations with a solution for decentralized identity management.

The Evolution of Identity Management

Organizations have traditionally managed their own employees' identities. With the advent of collaboration and information sharing, however, many users (including employees, partners, suppliers and customers) increasingly require access to resources outside of their own organizations, and their identities are not managed by the external organizations providing these resources. For example, when an organization uses a hosted, software as a service (SaaS) customer relationship management (CRM) solution (e.g., salesforce.com or Siebel CRM On Demand), users who access the application have corporate employee identities. These users only have access because they are employees; should their employment be terminated, so should their access to the SaaS application. With a SaaS provider like salesforce.com, access is often managed by a separate account, which is not connected with their organization's identity management system and thereby represents a significant security predicament.

Identity federation overcomes the issues of securely managing identities, enabling the organization to share its employee identity information with the SaaS provider or any other resource over the Internet. This allows the organization to increase their control over who has access to what information and resources, regardless of where those resources reside (e.g., on salesforce.com's servers).

Introducing Identity Federation

Federated identity management allows organizations like enterprises and service providers to securely exchange user information across partners, suppliers and customers. By utilizing standards-based methods, identity federation can reduce costly repeated provisioning, security loopholes and user inconvenience, which are often the consequences of rigid, proprietary, tightly-coupled application architectures. Organizations that have deployed federated identity management software remove barriers from logging in and improve collaboration with partners, enhance customer service, accelerate partnerships and alliances, reduce

costs associated with integrating to outsourced services and free themselves from large vendor-specific, all-encompassing systems.

Federation bridges segregated silos of identity systems to provide organizations with the ability to secure their cross-boundary interactions—removing friction, improving productivity, efficiency and competitive differentiation. Federated identity management enables:

- Easier access for users to utilize external resources over the Internet
- Improved end-user experience through Internet single sign-on (SSO) and just-in-time account provisioning
- Reduced cost and time to integrate authentication, legacy and target applications
- Elimination of non-scalable proprietary or homegrown SSO applications
- Uninhibited online interaction
- Decreased phishing opportunities
- Reduced sharing and impersonation of usernames

Critical Identity Federation Capabilities

Federated identity management allows local identity credentials and their associated data to stay in place while linking organizations together by distributing validated copies of selected identity information. This allows for efficient management, control and movement in a heavily distributed world. As organizations integrate more tightly with partners, outsourced services and even customers, federated identity management provides flexible mechanisms to authenticate users from external organizations and provide them with direct access to protected online resources.

While many of the early use cases surrounding identity federation centered on individuals roaming between security domains (via their Web browsers), federation is by no means limited to end-user or browser interactions. Application servers, Web services and even mobile transactions all need access to identity information, with security and auditability. For example, when an end-user initiates a series of Web services interactions, the information systems must convey information about the end-user to the Web services.

Profiles of Federation

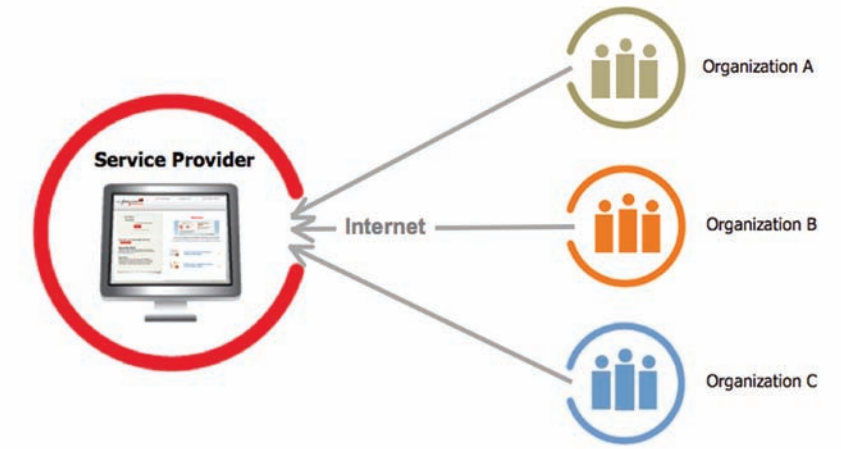
A majority of today's federation activity is described as hub and spoke. Most federation initiatives begin as one of two simple profiles: service provider hub or identity provider hub.

Profile 1: Service Provider Hub

In a service provider (SP) hub, the SP (e.g., Orbitz, Fidelity NetBenefits and salesforce.com) sits in the middle of a number of surrounding identity providers (IdPs). The SP is a relying party for the identity assertions made by its customer. Characteristics of the SP hub include:

- Service providers accept identities of their customers (IdPs)
- Organizations (IdPs) wish to extend their employee identities (login information, policy information and account information) to those entities hosting their SaaS or on-demand services
- Authentication of the employees takes place at the IdP and is propagated via identity federation authentication assertions to the SP

- Roles, credentials or even authorization policies may also be asserted from the IdP to the SP via identity attribute exchange
- New accounts can be provisioned and de-provisioned as an extension of the existing provisioning systems at the organizations (IdPs)

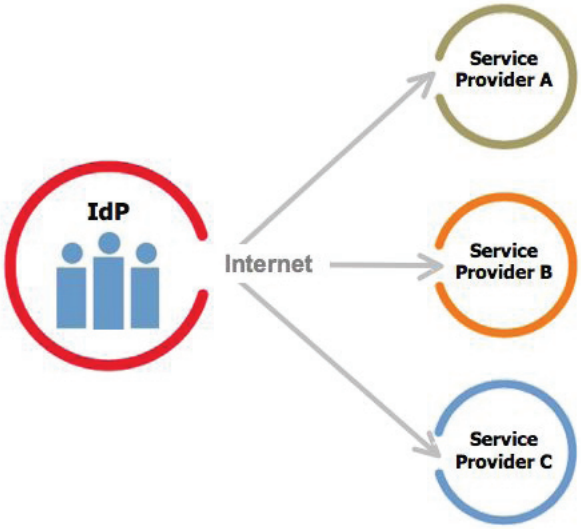


The SP hub is ideal for service providers who want to integrate and connect their managed applications or Web services to external organizations and for organizations who want to enable tighter end-to-end security of their users (employees) as they access remotely hosted services and applications.

Profile 2: Identity Provider Hub

Practically a mirror image of the service provider (SP) hub, the identity provider (IdP) hub is designed to allow central authentication from the IdP in order to pass authenticated users and their attributes to a surrounding number of SPs. Organizations that have a large number of users (such as carriers, very large enterprises with tens of thousands of employees, Internet service providers and customer-facing portals) typically rely on the IdP hub profile. Characteristics of the IdP hub include:

- Centralized authentication
- Varying authentication mechanisms based on the security standards of each service provider
- Service providers occasionally act as their own identity attribute providers, storing and propagating attributes pertaining to their users' preferences and interaction history over time



The IdP hub is ideal for organizations that want to maintain centralized customer relationships and authentication while still enabling a surrounding number of service providers to leverage identity information.

Profile 3: Multi-Provider Cross-Domain

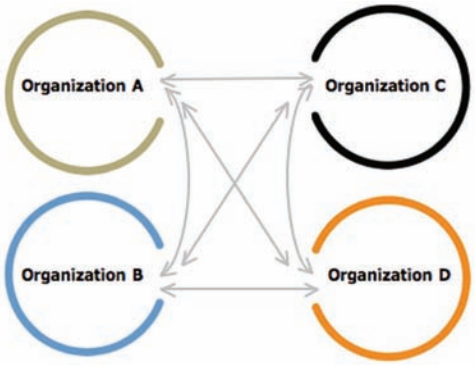
An advanced profile of identity federation is the multi-provider, cross-domain profile, where each entity acts as an issuer of identity assertions (IdP) as well as a consumer of identity assertions (SP).

Many large organizations simultaneously manage numerous heterogeneous security domains, such as affiliates, acquisitions, subsidiaries and joint ventures. This creates both a security challenge in ensuring proper access to resources, as well as a layer of IT and employee complexity in maintaining multiple passwords for each employee. Internal identity federation utilizes standard protocols to link the identities and accounts maintained in the various individual security domains of each organization or sub-organization.

Just as internal identity federation makes identity portable across heterogeneous security domains, so, too, does external federation with companies outside of the corporate domain. Internally–facing, multi-provider identity federation often occurs as a prerequisite to externally-facing identity federation activities. As more organizations implement federation, both SP hub and IdP hub federation profiles will grow into multi-provider federations.

Characteristics of the multi-provider, cross-domain profile include:

- Mature organizations that have internal and external cross-domain authentication requirements
- Multiple entities simultaneously engaging with each another as both IdPs and SPs



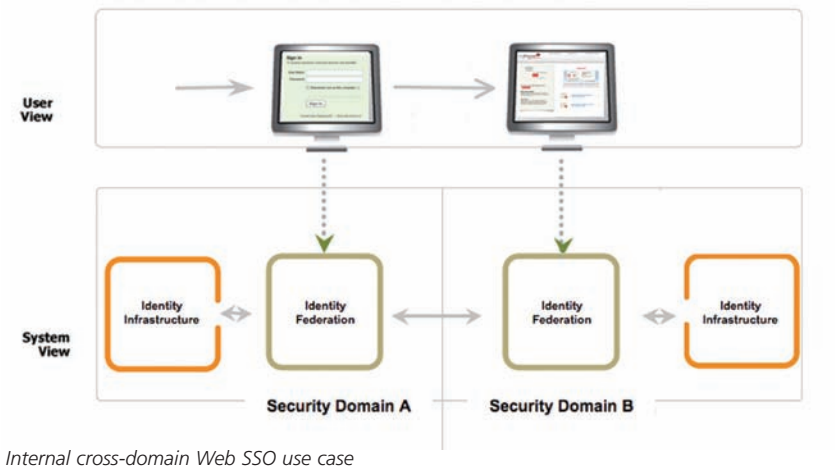
The multi-provider, cross-domain profile is ideal for very large organizations that want to enable a loosely-coupled approach to cross-domain SSO without needing to homogenize systems or authentication approaches.

Federated Identity Use Cases

Many use cases for identity federation exist, but the most commonly-implemented use cases are internal cross-domain SSO, external secure Internet SSO, attribute exchange, federated identity provisioning and federated identity Web services.

Use Case 1: Internal Cross-Domain SSO

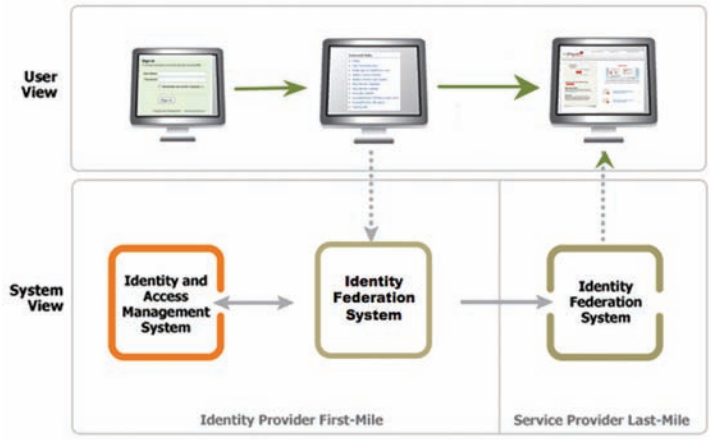
This use case is often used to eliminate redundant logins without the need for proprietary agents or tightly coupled installations of centralized identity management systems. Many times, this use case is associated with intranets or company portals. When a user logs into an application in his security domain that is federated with another security domain, he is automatically logged into the other security domain, thereby giving him direct access to remotely-protected resources.



Internal cross-domain Web SSO use case

Use Case 2: Secure Internet SSO

The secure Internet SSO use case resembles the internal SSO use case, with the exception that the SSO event occurs between organizations. When a user logs into his intranet or home network, his identity is federated over the Internet to an application residing at a different organization. In this use case, federation enables direct SSO over the Internet to an application in another organization. Explicit account linking or a more loosely-defined subject mapping of identities can be used to correlate the user's identity in his security domain (IdP) with his identity or role in another security domain (SP).



External Internet SSO use case

Use Case 3: Attribute Exchange (Browser and Web Services-Based)

In this use case, attributes are provided as part of the initial SSO event (authentication assertion), or the target site (SP) can make a separate request for additional user attributes from the IdP to complete a transaction. These attributes, which are stored at the IdP, may include information such as addresses, contact data or preferences. Identity federation provides the user with a more personalized experience; it can potentially eliminate initial account creation as well.

Use Case 4: Federated Identity Provisioning

Federated identity provisioning is an extension of the attribute exchange use case. By enabling dynamic or batch provisioning of user accounts across domains, the identity federation system assists in the movement of user account information required to create a new account (provisioning) or delete an existing account

(de-provisioning) with a remote security domain. This can be achieved independently or as part of an SSO transaction.

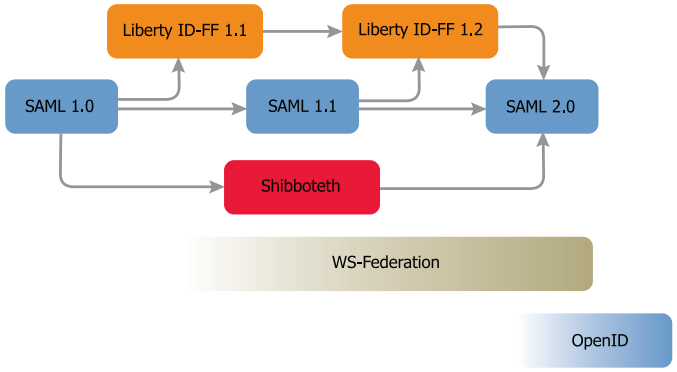
Use Case 5: Federated Web Services

By integrating identity into Web services, we can provide verifiable identities for both the originator of a transaction (such as the user) and the Web service endpoint involved in processing the transaction. When a user initiates a session by logging into a Web portal at a local domain via a Web browser, he is authenticated and the identity federation system creates an authentication token, which can be consumed to continue that session (cross-domain) at a remote Web application. The remote Web application initiates a series of Web services calls (via SOAP), and the end-user's identity is inserted into the SOAP message (via a token) along with the identity of the particular Web service.

Federation Standards Overview

The best way of deploying any identity federation use case is with standards-based identity federation systems. Standards provide interoperability between security domains as well as inherent security due to being peer-reviewed.

Although there are multiple identity federation protocols, the three most widely adopted are the Security Assertion Markup Language (SAML), the Liberty Alliance protocols (ID-FF) and the WS-* ("WS-star") suite of specifications.



The evolution of federated identity standards

SAML

SAML is the foundation for much of the current identity federation activity. It has gone through three releases—1.0, 1.1 and (the most recently ratified) 2.0. SAML 2.0 is seen as a point of convergence, as it incorporates ID-FF 1.1 and 1.2 as well as Shibboleth 1.3 functionality.

Shibboleth

The Shibboleth initiative is being led by Internet2 to provide peer-to-peer collaboration using a federated identity infrastructure based on SAML. Shibboleth has been largely adopted by the university and research communities around the world. Shibboleth 2.0, which went GA in March 2008, is based on SAML 2.0.

*WS-**

The WS-* suite of specifications are driven by a collaborative effort between Microsoft, IBM, VeriSign, RSA Security, Ping Identity and others. Some of these protocols, such as WS-Security, have been submitted to and ratified by existing standards organizations, such as OASIS.

Generally speaking, WS-* can be thought of as a composable suite of specifications for enabling secure Web services. Specifically, this collection of

specifications, including WS-Trust, WS-Federation, and WS-Policy is an evolving set of mechanisms for layering authentication, authorization and policy across both single and multiple security domains.

Liberty Alliance

The Liberty Alliance is an organization of vendors and enterprises that is largely perceived as having formed in response to Microsoft's Passport efforts. Since that beginning, the Liberty Alliance has written several protocols that enable both browser-based identity federation as well as Web services identity federation. The Liberty Alliance protocols include the identity federation framework (ID-FF) and identity Web services framework (ID-WSF). Their ID-FF work, which originally resulted in two versions of the ID-FF specification, has now been incorporated into SAML 2.0.

Liberty Alliance has also taken on the role of certifying conformance and interoperability of vendor products to federation standards. They provide testing services for SAML 2.0 as well as their own protocols.

Deciding Which Standard to Use

When evaluating the various standards, IT organizations should consider the following:

- SAML is the predominant protocol for browser-based identity federation—especially in business-to-business and employee-facing use cases. SAML's market dominance has accelerated as a result of Liberty ID-FF being rolled into SAML 2.0 and the WS-* stack defining SAML security tokens as an accepted format.
- While corporations implemented the Liberty ID-FF protocol for account linking and Web SSO in 2003 and 2004, this early Liberty work has converged into SAML 2.0. As a result, Liberty ID-FF 1.1 and 1.2 have effectively reached end of life. Thus, if you are just now looking to start a project that requires some of the features of the Liberty standards such as global logout, destination-site-first functionality or account linking, a safe bet will be to focus on SAML 2.0.
- Liberty's ID-WSF specifications (which can be subsequently added on to SAML 2.0) focus on enabling identity-based Web services; however, the standards were drafted largely by those looking to implement consumer-facing identity-enabled services; as a result, they may be more comprehensive than is required for some internal deployments.
- The composability of WS-* means that the profiles for interoperability are not as well-defined. If you wish to enable both identity-based Web services as well as browser-based interactions, then some combination of SAML and WS-Trust is likely the right course of action.
- OpenID is a relatively new SSO mechanism that was designed to facilitate blog commenting. Although OpenID provides a decentralized SSO model, it is not secure enough for business-to-business exchanges due to the necessity of relying on a third-party IdP to confirm the identity of the user requesting site access.

Role of Federation in Identity Management

Securing Outsourced Services and Collaboration Platforms

Collaboration is blurring the lines between enterprises and their service providers. With employees traversing the Internet with highly-sensitive data, the connection has to be secure to protect the user, enterprise and service provider. Users are also demanding direct access to external resources and improved ease of use with single sign-on (SSO). Federated identity is being deployed to secure configurations such as:

- Outbound SSO for users to access software as a service (SaaS) and business process outsourcing (BPO) providers, and to connect with trading partners
- Inbound SSO for service providers, such as BPOs and managed services, to access the enterprise's resources
- Internal SSO for the enterprise and its acquisitions, affiliates, subsidiaries and joint ventures
- SSO to a third-party, hosted hub for users to share information among industry organizations

Leveraging Standards to Extend the Reach of Centralized Identity Management

The business value of an identity management solution is directly tied to the number of applications that can be integrated into the solution. Vendor-specific identity management solutions often run into technical, organizational and political barriers that prevent them from being broadly deployed. By introducing standards-based interfaces, identity federation technology makes it easier to integrate identity functionality across disparate vendor products and platforms. Identity management interoperability via federation allows companies to enhance and leverage their existing investments in proprietary authentication and authorization solutions, as well as connect different vendor products.

Federated identity is replacing vendor-specific and proprietary SSO methods for moving authentication, authorization and attributes between security domains. If you have invested in a centralized identity management system, then you will likely use identity federation to enable Internet SSO between security domains. Market research indicates that continued implementation and maintenance of internal proprietary SSO agents is cost-prohibitive when compared to the cost, value, and re-use of deploying standards-based SSO identity federation. Once an internal application is federation-enabled, it is ready to be rapidly repurposed for external federated identity access.

Adding Internet SSO to Provisioning Systems

In cases where an organization has already deployed a provisioning solution, adding identity federation can enable Internet SSO between security domains. Typically, provisioning solutions are used to centralize the administration of users and automate the process of creating, updating and deleting user data across multiple applications. Once a provisioning solution is in place, accurate identity data is reliably loaded into applications and directories. Layering an identity federation solution into this architecture provides users with the convenience of SSO and administrators with the benefit of using standards-based technology.

Designing Modular, Interoperable Architectures

New application deployments, mergers and acquisitions, company restructuring and the evolution of technology platforms all combine to create a constant demand to integrate new systems into existing identity management systems. Identity federation provides a modular approach in which identity functionality

passes through standards-based interfaces.

Federating Virtual Directories

If you have invested in virtual directories and need to leverage the attributes contained in the virtual directories to another security domain, federation can provide standards-based methods for querying and retrieving attributes.

Federated Identity Management with PingFederate

PingFederate is the only standalone federated identity management software to deliver secure Internet single sign-on to all external partner connections including Software as a Service (SaaS) and Business Process Outsourcing (BPO) providers, trading partners, managed services, acquisitions, affiliates, subsidiaries and joint ventures. To learn more about how PingFederate provides federated identity management, visit www.pingidentity.com.

Getting Started

Begin by clearly defining your use case, seek expert advice on solving that use case and choose the solution that best suits your needs, not the vendor's. It is important to identify with which partners you want to federate and that they meet your security, architectural and implementation standards, then properly test with your partner's federation implementation. Be sure to research and trial solutions to simplify your identity federation project, identifying solutions that employ the most widely-used identity federation specifications.

To get started, it is important to identify the various options for your federated identity project. This will give you the basis for determining what kind of identity federation is best for you. Important considerations to determine include:

☑ Profile:
- a. Service provider
- b. Identity provider
- c. Multi-provider cross domain

☑ Use case:
- a. Internal cross-domain SSO
- b. Secure Internet SSO
- c. Attribute exchange
- d. Federated identity provisioning
- e. Federated Web services

☑ Standards applicability:
- a. SAML
- b. Shibboleth
- c. WS-*
- d. Liberty Alliance

☑ SSO configuration:
- a. Outbound
- b. Inbound
- c. Internal
- d. Third-party hosted

Additional Resources

You can find additional information on the topics addressed in this paper at www.pingfederate.com. Relevant resources that may be of interest include:

- Data sheet: PingFederate 5
- White Paper: Secure Internet Single Sign-On 101
- White Paper: Internet-Scale Identity Systems: An Overview and Comparison
- Webinar Archive: Federated Identity Management: What Is It and Why Should You Care?

About Ping Identity Corporation

Ping Identity's dedication to delivering secure Internet single sign-on software and services for over 150 customers worldwide has earned us recognition as the market leader in federated identity management. PingFederate®, the world's first rapidly deployable identity federation software, provides an organization's users safe access to Internet applications without the need to re-login. With PingFederate and PingEnable—Ping Identity's expert support, services, and methodologies—external connections can be operational in less than a week. Download a free trial at www.pingidentity.com.

PingIdentity™