

White Paper



The Business Value of Identity Federation

January 2007

Table of Contents

Introduction	3
Federation and Business Value	3
Securing Federation	3
Federation Requirements	3
Federation Use Cases	4
Browser-Based Scenarios	4
Federation Based On Account Linking	4
Federation Based On Roles	5
Document-Based Scenarios	5
Chained Web Services	5
Key Federation Business Issues to Consider.....	6
Federation Standards	7
Security Assertion Markup Language (SAML)	7
Liberty Alliance	7
ID-FF	7
WS-Federation	8
WS-Security	8
Conclusion	8

Introduction

Efficiently coordinating and integrating business processes with trading partners in an increasingly dynamic business environment is a complex dilemma faced by most large enterprises. Identity federation and the industry standards that comprise it were invented to address this cross domain, application interoperability challenge. This paper introduces and defines identity federation; the benefits that companies can reap by leveraging it, some use cases that can be enabled by it, the most relevant industry standards and specifications that underlie it and the business issues that must be addressed for identity federation to be successfully delivered at scale.

Federation and Business Value

Basic access to applications and data over the Internet has existed for years. However, the ability of a user to easily and securely access services that are housed in multiple security domains within an enterprise or from multiple organizations has remained a challenge. Twenty years ago many pinned their hopes on electronic data interchange (EDI), which has been used successfully in the automotive, retail and manufacturing industries, but has generally failed to reach broader corporate use primarily because of its cost, inflexibility and proprietary nature. In addition EDI has not provided any direct benefit to consumers or other classes of end-users.

Today, the Internet, Internet-compliant technology and standards have matured to the point that effective coordination and mass integration between trading partners is now achievable and affordable. Moreover, the advent of standards is easing the extension of today's enterprises by lowering the barriers to connecting disparate business applications both within and across corporate boundaries. This enables businesses to substantially reduce costs, create new revenue opportunities, and provide greater convenience, choice and control for its users.

By integrating applications and business processes across corporate boundaries, trading-partners, business customers and outsourcers can automatically link processes and take part in transactions across multiple companies—eliminating the business interruption associated with traditional means of information exchange, such as phone, fax and email—or traditional (custom) means of application integration. The ubiquitous network (the Internet) and high-scale transactional applications already exist at most organizations. Federation standards and the security systems that implement them were invented explicitly for the purpose of securely tying distributed applications together to accelerate business.

Securing Federation

However, the aforementioned gains can fail to materialize if the system-level information exchange is not conducted securely. For example, a government agency could risk damage through a leak of a citizen's private information. A financial institution might incur financial penalties or brand degradation due to an unauthorized trade or withdrawal. A health care firm might suffer damaging lawsuits with the release of personal health information to the wrong parties. In addition a breach of security might put regulated organizations out of compliance with various related data privacy or IT control regulations and thus put them at risk of government enforcement actions. With federation, as really with most IT efforts, organizations need to have security as a front-of-mind item. In the end though, a balance must be found between letting business in and keeping risk out.

In a federation scenario the way to address these security challenges is to integrate partnering companies' security systems so that user, security and entitlement information can be shared in a defined and controlled way between partners in a trusted business relationship. The sharing of digital identities to enable applications in different security domains to work together, securely, is defined as "identity federation". Federation enables users and applications to work across autonomous internal business units, external business partners and other third-parties seamlessly as if they were part of the same security domain, while in fact the domains remain largely independent.

Since cross-company federation is the ultimate goal, the only way to effectively accomplish this is through the development and use of open standards. Fortunately, many standards and specifications have and are being developed to address various aspects of identity federation (single sign-on (SSO), trust, attribute sharing, authorization, Web services security, privacy etc.). These standards, when combined, provide the basis for identity federation, supporting different requirements and use cases.

Federation Requirements

Given the intense focus on personal privacy and control of digital identities, the existing identity infrastructures that can be found in today's organizations and the high-value of customer information that is often housed within them, it is virtually impossible to expect organizations to collaborate on creating and maintaining a universal, shared point of identity information. Requiring organizations to first merge and centrally manage their user's digital identities as a prerequisite to federating their applications for use by those users, is a non-starter. This is one of the basic requirements driving federation standards and why the term "federation" (implying collaboration between loosely coupled sovereign organizations) is used in the first place.

Companies involved in identity federations establish trusted relationships allowing their respective users or systems to access resources operated by their business partners. To do this companies issue “security tickets” for their users that can be processed by relying business partners. Essentially, to oversimplify, federation standards boil down to defining these security tickets; what their structure is, what is in them, how they are passed, how they are administered, how they are validated and what services they can and should enable.

Federation Use Cases

There are many potential federation use cases. The use cases presented in this paper are not intended to cover all the potential scenarios, but are intended to be generically illustrative of typical federation use cases to get the reader thinking about federation and how it might be leveraged by their organizations.

Identity federations can be conducted in two basic and closely related forms, **browser-based** or **document-based**. The browser-based mode of federation is focused on supporting live users that are using Web applications presented to them via standard Internet browsers. Federation in this case enables an authenticated user to move from one web security domain to another without needing to provide credentials again. Browser-based federations essentially provide the user with SSO between two sets of applications or portals that live in two separate security domains, without requiring the synchronization of the user’s digital identities in the two domains. Essentially the user authenticates in one domain and can use the applications in the other domain without needing to first re-authenticate.

By contrast, document-based federations are based on the use of XML documents transported between two security domains leveraging Web service standards. With document-based federations the activity is driven either by a live user sitting on some “client” application or by some client application operating in the absence of direct human involvement. Federations in document-based scenarios involve defining XML document structures, locations and definitions of credential information and other factors, that are required to enable requests of services from particular Web services offered by a given partner organization.

Both modes of federation, browser-based or document-based, nonetheless hinge on the development and use of standards to simplify how applications residing in two independent security domains can work together for the benefit of their common user or shared business process.

Browser-Based Scenarios

The following use cases demonstrate different ways of using user identities to provide browser-based, end-users with SSO across multiple companies involved in a partnership.

Federation Based On Account Linking

In this use case, Workplace.com contracts the management of its employees’ health benefits to a partner company called Health.com. To access her account, an employee of Workplace.com authenticates at the employee portal (www.workplace.com) and clicks on a link to view her health benefits at www.health.com. The employee is taken to Health.com’s website and presented with all of her personal health benefit information without having to sign-on to Health.com’s website. Her accounts are automatically linked at the time of browser redirection.

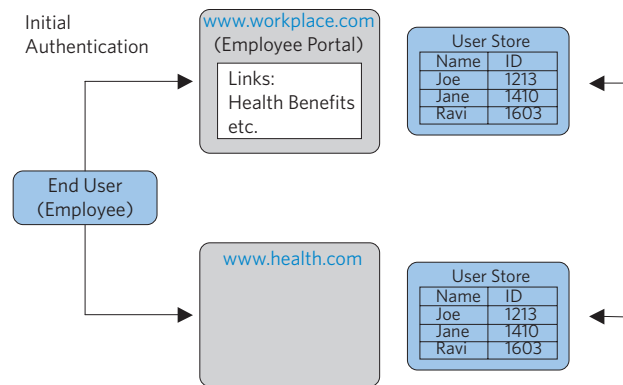


Figure 1: Federation Based On Account Linking

Health.com maintains all health-related information for the employees at Workplace.com. Health.com thus maintains user identities for every employee of Workplace.com a priori. When an employee of Workplace.com accesses Health.com as part of the federation, an identifier for the employee is passed from Workplace.com to Health.com in a secure manner. This identifier allows Health.com to determine who the user is and thus indirectly what access to provide them. The security systems at Workplace.com and Health.com are loosely linked (federated) to provide a SSO experience to their shared users.

Account-linking is the most typical browser-based use case. However, the following additional use case is illustrative of another important browser-based federation scenario that is useful in some situations.

Federation Based On Roles

In this use case Workplace.com buys parts from a partner company PartsSupplier.com. An engineer of Workplace.com authenticates at the employee portal (www.workplace.com) and clicks on a link to access information at PartsSupplier.com.

Because the user is an engineer (has the role of engineer) at Workplace.com, he's taken directly to the technical documentation and troubleshooting portion of PartsSupplier.com's website without having to sign-on.

In contrast when a purchaser for Workplace.com authenticates at Workplace.com and clicks on a link to access information at PartsSupplier.com they are taken directly to the order portion of PartsSupplier.com's website without having to sign-on. In either case, PartsSupplier.com's website can be personalized with information such as the user's name, leveraging whatever information is sent over from Workplace.com in the security ticket.

In this role-based scenario PartsSupplier.com does not need to maintain user identities for all of Workplace.com's employees. However, PartsSupplier.com must still control access to sensitive portions of their website. To do this, PartsSupplier.com maintains a limited number of profile identities (mapping to job functions/roles) for Workplace.com's users.

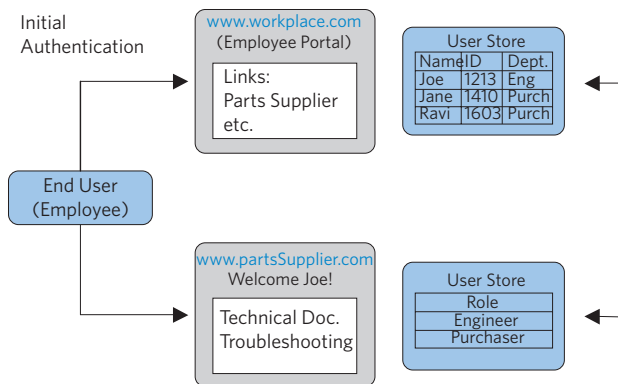


Figure 2: Federation Based On Roles

In this case, one profile identity is maintained for engineers and one profile identity is maintained for purchasers. When an employee of Workplace.com accesses PartsSupplier.com, user attributes are sent from Workplace.com to PartsSupplier.com in a secure manner, leveraging federation standards. These attributes define the role of the user and determines what profile identity is used to control access at PartsSupplier.com.

While there are a number of other potential use cases of browser-based federation and many other industry-specific scenarios, the two just described above should give the reader a good idea of what is possible.

Document-Based Scenarios

Document-based federations are realized using Web services flows. As with browser-based federations there are many possible usage scenarios. For this paper one is highlighted to convey the basic concepts that are involved.

Chained Web Services

In this use case, Workplace.com has a purchasing agreement with PinSupplies.com and PinSupplies.com has a business relationship with E-Ship.com.

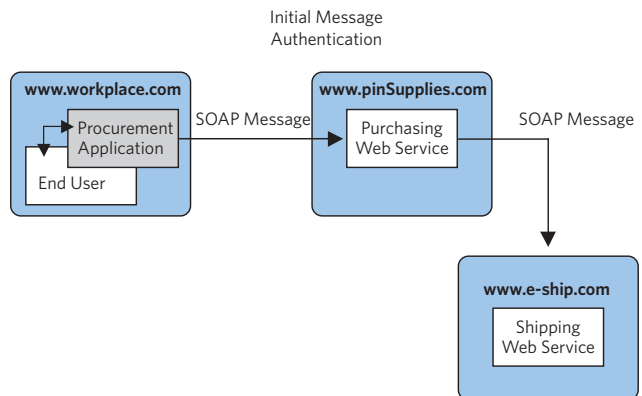


Figure 3: Chained Web Services

The end-user logs-on to her procurement application with her username and password. The procurement application provides a list of Workplace.com's various suppliers. The end-user clicks on the PinSupplies button and is presented with a purchase order in an HTML page. She fills out the purchase order and then clicks the submit button on the HTML form.

The procurement application turns the HTML form into an XML/SOAP document that it inserts in the envelope body of a XML-based message. The procurement application then inserts the end-user's credentials in the envelope header of the message, together with Workplace.com's organizational identity.

The procurement application posts the message to PinSupplies.com's purchasing Web service. The Purchasing Web service (or a security application on its behalf—the more scalable and manageable solution) authenticates the incoming message and processes the request. When the purchasing process is complete, the Purchasing Web service makes a request to E-Ship.com using another XML/SOAP message. This message includes a PinSupply.com security token in the envelope header and the list of items to be shipped as well as the end-user's shipping information in the envelope body. The Shipping Web service (or a security application on its behalf) authenticates the request and processes the shipment order.

One of the keys to creating federated applications, as with any application really, is to think in terms of the users, what experience you are trying to provide them and how best to accomplish it, given your current infrastructure. When thinking about potential federated applications thinking in terms of browser-based versus document-based federations should help focus your thinking.

Key Federation Business Issues to Consider

While identity federation holds the promise of delivering significant benefits to users and organizations alike, the reality is that industry standards and specifications, such as SAML, Liberty Alliance and others (discussed briefly below) can only go so far in resolving issues that are inherent when two or more organizations attempt to integrate their systems and business processes. The standards introduced briefly later in this paper go a long way to make organizations' security infrastructures work together, but do not by themselves resolve the business issues inherent in federation. Early federation adopters will need to resolve the following issues and probably others, in a form satisfactory to the federating partners, before they can launch their federation projects and scale them in any significant way.

- **Legal and Contractual Issues Around Trust.** Since federation implies that one-party depends at least in part on the security systems and practices of another party, any enabling contract needs to define what is required, what is expected, how liability is dealt with, what service levels are promised, what happens if and when there is a security breach, what controls does the partner have on issuing user credentials, etc.
- **What Happens When Things Go Wrong, Who Does the User Call?** If a user can't get what they need for whatever reason, there needs to be a call-center or helpdesk that is equipped to help them and a process for managing customer issues that might originate with a federation partner. In addition, there must be an agreement on committed service levels.
- **What Government Regulations May Apply? How Can the Partners Ensure That They Are Complying?** Depending on the industry, region of the world and the personal data involved, different government regulations may apply. Which regulations apply and how to meet their requirements needs to be addressed as part of any identity federation.
- **Who Pays For the Federation?** Given that by definition federated applications are shared and both sides often gain some benefit, it is not unreasonable to expect that both sides might need to pay for the federation to occur. How this gets sorted out depends highly on the existing economic relationship between the parties. It is certainly possible that one side or the other might handle all the federation costs, but this is clearly a non-technical issue that must be resolved before the federation can occur.
- **Privacy Policy Compliance.** In most scenarios for federation to occur some amount of personal data about the user will need to be "shared" with the federation partner. Not only does this sharing need to be legal, but it also needs to comply with the privacy policies of both federating organizations. In addition every organization needs to ask whether or not user consent is needed.
- **Technical Infrastructure/Savvy of the Federating Parties.** For two organizations to federate they need to integrate their security infrastructures using a standard of their mutual choosing. This assumes that both sides understand what that means and have the ability to acquire or build the required systems. Like any new technology, it is certainly recommended to start with the highest priority business partners that also have the highest level of IT and security expertise.
- **Scaling of the Federation Deployment.** While system scaling is certainly a technical issue, the engineers who are tasked with designing and deploying the federation infrastructure, on both sides, will need to be provided the business requirements regarding how many counter-parties will need to be supported, what the estimated transaction rate will be and a number of other factors. The bottom line is this; the federation system that is built to support one federation partner might be dramatically different from that which would be required to simultaneously support 100 federation partners. The planned growth of federated services will thus need to be addressed as part of the initial federation system design so that this system can scale to meet the organization's business needs.
- **Administration of the Federated Users.** Federation generally does not eliminate completely the need to administer the digital identities of the federated users on both sides of the federation. This administration requires more than a technical solution; it requires that organizations somehow create a cross-company process, perhaps enabled by identity management tools, that supports the digital identity data management. Said another way, organizations need to supply some process that supports the lifecycle of the user identity, from creation, modification, to ultimate deletion, for the federated applications of one or both parties.

- **Rights to Audit Federation Partner.** Auditing and security systems naturally go hand-in-hand. Shouldn't one assume that this applies to federated security systems as well? However, given that one-half of the security system (and associated processes such as initial identity proofing) of a federated solution is housed at a business partner, getting access to their IT audit data (assuming they have it) is something that would have to be negotiated up-front.

The listing of the above business issues was not intended to scare the reader off from considering identity federation projects. It was provided to help set the right expectations for all participants. It is important to understand what business issues will have to be faced with identity federation in addition to the technical issues. Going into a federation project without addressing the business issues is a recipe for a disaster.

Like any new IT initiative in most organizations, effective execution of the first project is critical to making usage grow over time. Success breeds more demand, more funding, more attention and hopefully growth of the initiative over time. The best advice is to pick your best, most motivated partner first. Get all aspects of your federation, both business and technical issues, right with them and then expand to more partners as time, demand and resources allow.

Federation Standards

There is no single industry standard that meets all federation requirements, whether browser-based or document-based. As mentioned in this paper, federation involves description of identities (i.e., security tokens), protocols for exchange security tokens, and methods for the establishment of trust, among other issues.

This section briefly describes four standards and industry initiatives are most immediately important to identity federation initiatives:

- SAML
- Liberty Alliance
- WS-Federation
- WS-Security

Security Assertion Markup Language (SAML)

SAML is an open, application-level, framework for sharing security information on the Internet through XML documents. In January 2001, a division of Computer Associates, along with other companies, created the OASIS Security Services Technical Committee (SSTC) which culminated in the adoption of SAML as an industry standard in November 2002. SAML 2.0, the current version of SAML, was approved by the OASIS SSTC in March 2005.

SAML is probably the single most important, supported and implemented federation standard currently in existence. In particular the SAML Assertion (security ticket) portion of the standard is widely supported among the other standards discussed below. SAML is used to enable browser-based federations.

Liberty Alliance

The Liberty Alliance Project (loosely referred to as Liberty Alliance or Liberty) is an industry organization started in September 2001 that currently includes over 150 member companies worldwide, including Computer Associates. The purpose of the Liberty Alliance is to create a set of specifications for identity federation.

The ID-FF (Liberty Identity Federation Framework) module is the foundation of the Liberty architecture and is the most commonly used portion of Liberty.

ID-FF

A basic ID-FF environment minimally includes three parts: an identity provider (e.g., a telecommunication company), a service provider (e.g., an online retailer, a financial institution, a government agency) and a user agent. The user agent is a thin client (e.g., a standard browser) or a Liberty-enabled client or proxy (LECP), e.g., a wireless (cellular) telephone handset. Use cases under ID-FF fall into the Federation Based on Account Linking use case described in the Browser-Based Scenarios section above.

With ID-FF, upon successful authentication of the principal, the identity provider produces a SAML Assertion including an authentication statement describing the principal's security context, together with a name identifier (or "handle"). Importantly with the release of SAML 2.0, Liberty and the OASIS SSTC have merged ID-FF and SAML. Liberty will no longer iterate on the ID-FF portion of their specification independent of SAML.

WS-Federation

Web Services Federation Language (WS-Federation) is a specification jointly developed by IBM, Microsoft, BEA, Verisign and RSA Security. WS-Federation will no doubt be of interest to most readers since Microsoft has recently shipped a WS-Federation supporting product called Active Directory Federation Service (ADFS). Microsoft includes ADFS as part of the Windows Server 2003, R2 Update. ADFS implements the Passive Requestor Profile of WS-Federation and thus enables browser-based federation.

WS-Security

The Web Services Security specification (WS-Security) was originally developed by IBM, Microsoft and Verisign. It became an official standard in March 2004 and is now managed by the OASIS Web Services Security Technical Committee (WSS TC). The current WS-Security standard is 1.0.

WS-Security specifies SOAP security extensions providing data integrity and confidentiality and is thus useful in the context of document-based federation scenarios. WS-Security defines how to attach signature and encryption headers to XML messages. It also provides profiles that specify how to insert different types of binary and XML security tokens into WS-Security headers.

Conclusion

Enterprises are faced with an increasingly complex set of challenges as they balance the need for security and the growing requirement for seamless access to information from a large and diverse set of users. Integrating partners and their heterogeneous security systems and infrastructures to securely share and administer user information, profiles and entitlements requires a solution that supports scalable, inter-enterprise security that stretches across many partnerships. Federation standards and the security products that implement them are focused on providing exactly these services.

Today, the Internet, Internet-compliant technology and federation standards have matured to the point that effective coordination and mass integration between trading partners is now achievable and affordable. The immediate benefits of this are available to those organizations with the vision and the focus to take advantage of the building blocks and make it happen for their organizations. The question to the reader is how are you going to let business in while keeping risk out? Identity federation provides one such mechanism for this to happen in a standards-based, scalable, and efficient manner.

