



www.css-security.com • 425.216.0720

Federated Identity in the Enterprise

The proliferation of user accounts can lead to a lowering of the enterprise security posture as users record their account information in order to remember the multiplicity of account names and passwords. In addition, as e-business streamlines processes, the processes increasingly require business partners to access Internet-facing applications. This white paper provides an overview of Federated Identity and looks at a new approach that allows the management of identity to be outsourced to identity providers. This can save costs in maintaining the identity system and allows enterprises with different technology bases to interoperate through a standard set of protocols.

Table of Contents

Introduction	3
Single Sign-On	3
Federation	4
Federated Identity	5
Key Concepts	6
Business Issues	7
Outsourcing Identity Management.....	7
Trust Models.....	8
Standards	9
OASIS Security Assertion Markup Language (SAML).....	9
Liberty Alliance Identity Federation Framework (ID-FF)	9
WS-* Standards.....	10
Solution Models	11
Service Provider Centric Model	11
Identity Provider Centric Model	12
Cross Domain Model.....	12
Operational Considerations	13
Strategic.....	13
Business.....	13
Technical.....	14
Appendix A.....	16

Introduction

Businesses are increasingly moving applications to the Web. Often the applications have their own account databases, and users are faced with having to log in multiple times to access these applications. Additionally, as business processes are streamlined for the Internet, many companies are accessing applications being hosted by business partners; these applications require the user to have additional accounts supplied by the business partner.

The proliferation of account information for accessing applications has led to several cottage industries that concentrate on provisioning user account information from a central authoritative data source, or making multiple data sources appear as a single entity using virtual directory technology. While these technologies help in the overall account-management process, they do not address the fundamental problem that users face with sign-on to multiple independently managed applications.

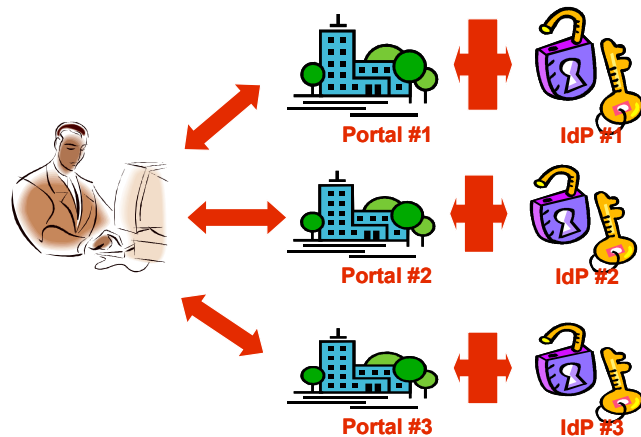


Figure 1: Multiple Identity Systems

Single Sign-On

Single Sign-On has long been the holy grail of authentication; there have been several attempts to provide such systems with limited degrees of success.

Generally, the various approaches involve collecting the user's log-on credentials and storing them in a repository. The single sign-on system then hides the underlying authentication process to each of the applications from the user. More recently, corporations have been attempting to externalize the authentication (and authorization) process

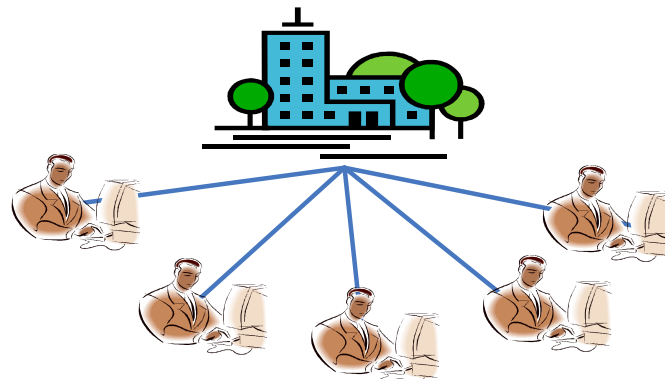
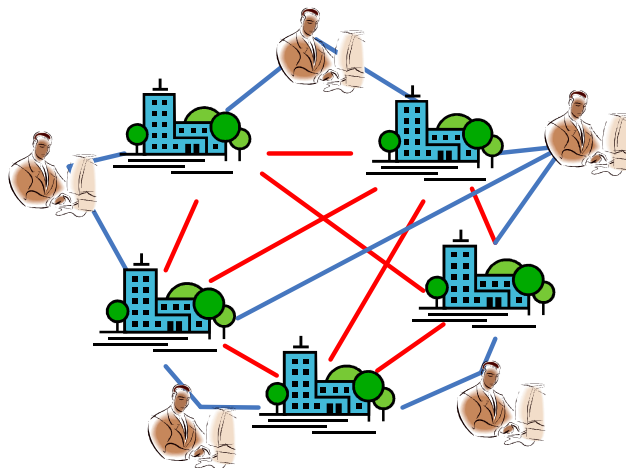


Figure 2: Central Identity Provider

from the application using technologies such as Kerberos and Web-Based Authentication and Access Control.

While these trends are positive, they often result in creation of islands of identity, and for users who need to commute between the islands, the single sign-on problem still exists. This is especially apparent in consumer-based sign-on where sites often require users to register before providing some service. A similar problem can be found in the business world where companies may be limited in their ability to consolidate account information internally both from an organizational and legal perspective. When external partner access is factored into the equation, the problem scope becomes even larger.

Increasingly, businesses are being forced into the realization that in order to get a handle on the issues associated with providing single sign-on to multiple applications they must first address the whole notion of identity and how it is managed. This has led to a move towards loosely coupled identity management systems, which acknowledge that there are multiple jurisdictions that have control over user account information and do not force the participants to utilize common technology.



Federation

In this model the user's identity is **federated** across disparate identity systems and trust relationships between organizations determine whether the assertions about a user identity are honored between identity management systems. The identity information is conveyed between systems using standardized security protocols that do not place requirements on the identity management technology at each end.

Figure 3: Federated Identity Provider

Federated Identity

The concept of federated identity is not new, federated identity is used on a daily basis. For example driver's licenses are issued by each state but are honored by most business for user identification when performing face-to-face business transactions. There is implicit trust that each state verifies the user identity before issuing a license.

Another example are government-issued passports. Every country issues passports, but some countries' passports are more trusted than others. Passports are a security token that can be endorsed with *visas*, which allows a country to qualify the users identity and access rights.

Finally, the most familiar example of federated identity is ATM machines. We take for granted that we can go to almost any ATM machine, both at home and abroad, and use an ATM card to obtain money. Most banks will honor ATM cards issued by other banks because of trust relationships that exist between the banks and *standardized protocols* for performing the ATM transactions.



Figure 4: Network Identity

Historically, as applications proliferate in the enterprise, companies accumulate multiple identity systems. Often new business applications are built around products that have their own identity management, e.g. SAP and Oracle, and in environments where control of the applications is the responsibility of the business segment. Consequently, there may be little incentive to consolidate the identity systems.

There are several solutions in the market that can help with consolidation of user account information, but the process can be expensive, and organizational barriers may limit the overall effectiveness. The enterprise may be able to reduce the number of identity systems but will still be left with several systems, resulting in users having multiple accounts.

In addition, as businesses increasingly build Internet-facing web applications that can be accessed both by internal employees and external partners, users accumulate new accounts for accessing partner web sites. Thus, while it is good practice to consolidate the number of identity systems internally, the net result may not be visible to users who must access external partner sites.

When dealing with internal organizations, there is some expectation that a uniform management model might be obtainable. However, when multiple business partners are added to the equation, this expectation is probably unachievable. Federated Identity provides a mechanism for overcoming these barriers by providing a way for organizations to make use of the identity assertions from other trusted identity systems when a user accesses an application that is outside his/her security domain.

Federation is a loosely coupled system; that is, each identity provider can continue to operate its own identity system without placing specific identity-management-technology requirements on the other parties. In contrast, tightly coupled systems often require a high level of technological compatibility between cooperating partners.

Key Concepts

The terminology of Federated Identity systems introduces a number of key concepts that form the basis of most systems. An *Identity Provider* (IP or IdP) is an entity that acts as an authentication service. An authentication service maintains a list of accounts. When the user authenticates to the service, the identity provider validates the user credentials (typically a password) to substantiate the user's *claim* to the identity.

An Identity Provider is an example of a *Security Token Service* (STS). This is a service that makes assertions about an identity based on evidence that it trusts. Most authentication services are also an STS. For example, the Kerberos authentication system in Windows issues tokens (called tickets) when a user is authenticated. An STS can also be used to translate tokens. This is equivalent to performing a driver's license exchange when moving to a new state. Provided the STS trusts the original token, it will issue a new token of a different type that can be used by the system being accessed by the user.

Organizations that host services are referred to as a *Service Provider (SP)*. A service is typically an application or set of applications, but a web service may also be considered in this context. Web services are typically components of an application. It should be noted that an entity can be both a service provider and an identity provider. When an entity is both, it can consume identity claims from other identity providers as well as produce claims in its own right.

When performing federation, it is highly likely that the user's identity will not be the same in the different systems that the user accesses. This is the case when the user account name is provided to the user by the administrators of the identity system. The *Pseudonym Service (PS)* maintains the alternate identity information that allows the account names to be mapped between the different identity systems being accessed. The pseudonym service is typically part of an STS, so that when a token is exchanged, the new token will have the correct account information for the target system.

Business Issues

As businesses increasingly deploy web applications both internally and externally, authentication and access control to these applications is critical to the overall security of the system. When users are faced with using multiple accounts, the natural tendency is to write the account name and password details down for reference. This lowers the overall security posture of the system and can lead to security vulnerabilities if the information is left in a place where it is accessible to non-authorized personnel.

The traditional approach to this problem is single sign-on. However single sign-on solutions have met with mixed success because of the difficulties in dealing with multiple identity systems. Federation addresses this by leveraging the existing identity systems and providing a mechanism for passing identity claims between systems in a standardized manner so the service provider can utilize the previously authenticated identity.

Outsourcing Identity Management

The ability for a service provider to leverage the identity information supplied by an identity provider allows the service provider to outsource the management of the identity systems to the identity providers and better control the overall management cost involved in maintaining the service provider user account information. In addition, while it is possible to reduce the number of authoritative sources of account information within an enterprise, it can be costly to achieve a single authoritative data source holding all account information. Federation allows an enterprise to go the last leg and provide single sign-on across the

multiple authoritative sources of account information. Finally, the user experience is improved, as the user is no longer required to re-authenticate when moving between applications.

In the following example of federated identity, a financial services company, FinCorp, hosts 401(k) plans for multiple business. Each business supplies a link on its internal portal to the employee 401(k) application hosted by FinCorp. Using a federated identity solution, FinCorp can transparently authenticate users who access the 401(k) web application through the portal sites of its customers using the identity information supplied by the FinCorp customer's identity management system.

In this example, federated identity provides the following benefits:

- ◆ Identity information need not be synchronized across multiple organizational boundaries.
- ◆ Implementation of a centralized identity management system is not required, as each customer manages his/her own account information.
- ◆ The solution can scale to large numbers because systems are loosely coupled.
- ◆ Federation does not force a common identity management system on all customers. Indeed, each customer can run a completely different identity management systems, and it is only necessary to communicate assertions about user identity in a common fashion.

Trust Models

The heart of a federated identity system is establishing trust between the participants. Each participant in a federated identity system must trust that the other participants are adhering to a set of practices that ensure the overall security is not compromised. There are two parts to this process—the business aspects of establishing trust agreements and the technical aspects of implementing those agreements. When dealing with partners, the business aspects of trust agreements must be formalized. This is discussed later under federation agreements. The technical aspects of trust management are generally implemented by exchanging cryptographic keys that can be used to verify the identity of the parties.

The most common form of trust is direct trust. In this model, each party maintains a list of the other participants and only communicates with them. However, there are other trust models, such as brokered trust, where a party that is trusted attests to the validity of a third party that it trusts. Use of these trust models is driven by the overall business requirements. While the underlying technology may support many complex trust models, the business relationships and legal

liability issues associated with the transactions that can be performed ultimately dictate what trust model will be used.

Standards

The purpose of standards is to promote interoperability. In any emerging technology area, there are initially a number of bodies that develop standards to promote specific technologies. There are several bodies promoting standards that address different aspects of Federated Identity.

OASIS Security Assertion Markup Language (SAML)

The OASIS standards body developed the SAML language as a way of expressing security assertions in a standardized manner. Security assertions can express claims to authentication, authorization, and attribute information and are passed between participating parties. SAML assertions are expressed in XML and are extensible. SAML also defines a binding to the http protocol that allows SAML assertions to be passed over an http connection.

Liberty Alliance Identity Federation Framework (ID-FF)

The SAML standard defined a basis for expressing security assertions but did not explicitly deal with federation of user identity. The Liberty Alliance was formed by a group of commercial and product-development companies to define how network identity can be managed across multiple web sites, both internally and externally. Liberty has more than 150 members representing a variety of

Liberty Identity Federation Framework (ID-FF)

Enables identity federation and management through features such as identity/account linkage, simplified sign-on, and simple session management

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile services, contact book service, geo-location Service. Presence services and so on.

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards

(SAML, SOAP, WS-Security, XML etc)

industries from all corners of the globe.

The previous diagram illustrates how the Liberty specifications are organized. From a pragmatic perspective, companies considering federation projects begin by using products that implement the ID-FF specifications. As these projects move into subsequent phases, the ID-WSF and ID-SIS specifications come into play.

WS-* Standards

The WS-* set of standards is often regarded as a set of competing standards to SAML and Liberty. However, a closer look at the technical specifications (rather than the marketing hype) indicates that while there are areas of overlap, the WS-* standards can be regarded as complementary standards in that they primarily deal with securing SOAP messages that are sent between web services.

The Liberty standards primarily deal with the protocols for relaying information via the browser interactions that a user makes between partner web sites. The WS-* standards are complex and require a Web services infrastructure to be deployed. The SAML and Liberty standards have seen more traction in the market, since they require far less infrastructure and are simpler to implement. It should be noted that WS-Security provides for multiple security tokens, and SAML assertions can, theoretically, be encoded in the SOAP header as a security token.

Solution Models

There are several high-level federation models. It is important when considering a federated identity solution to identify the applicable model or models for an organization.

Service Provider Centric Model

This model applies to companies that offer services thru a web site to other companies. A user typically clicks on a link to the service provider from his/her own company's web portal and then is transferred to the service provider web site. Examples include corporate credit card management and a financial service company offering employee 401(k) plan management.

A user generally authenticates at his/her company site (the identity provider), and the company provides assertions to the service provider about the user's authentication along with attribute information that the service

provider uses to identify the user and determine if access is allowed. This model is particularly useful when the service provider has a large number of customers because it allows the service provider to leverage the identity management systems of its customers. Complexity can be reduced (both from the business and technology perspective) by side stepping the issues associated with each customer running different identity management systems.

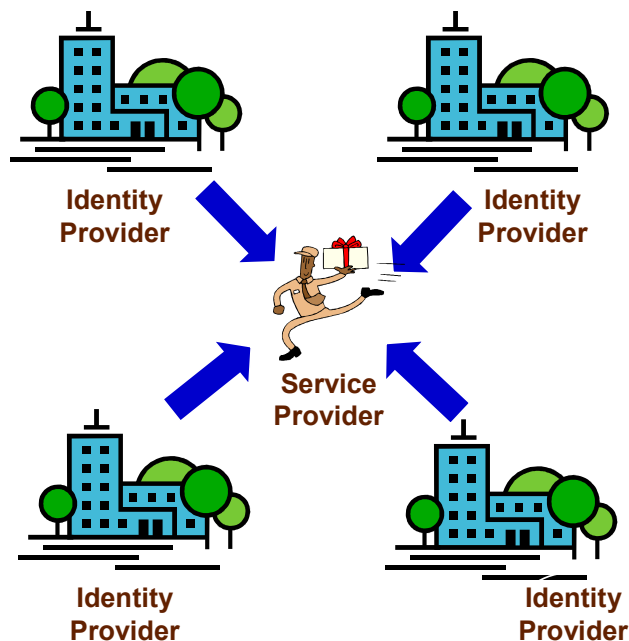


Figure 5: Service Provider Centric Model

In this model all parties must agree on the type of authentication that will be accepted and the attribute information that can be passed. The latter is particularly important when adhering to privacy regulations that may cross boundaries managed by different legal jurisdictions.

Identity Provider Centric Model

This model is more focused on the internal consolidation of multiple identity management systems into a single system which is used by multiple service-provider applications. The typical model for web application development has been that each application has its own identity and authorization system or leverages the identity and authorization system of the underlying framework, e.g. Oracle or SAP. This results in multiple identity-management systems and leads to increased management overhead, necessary to maintain the information about users in multiple data stores.

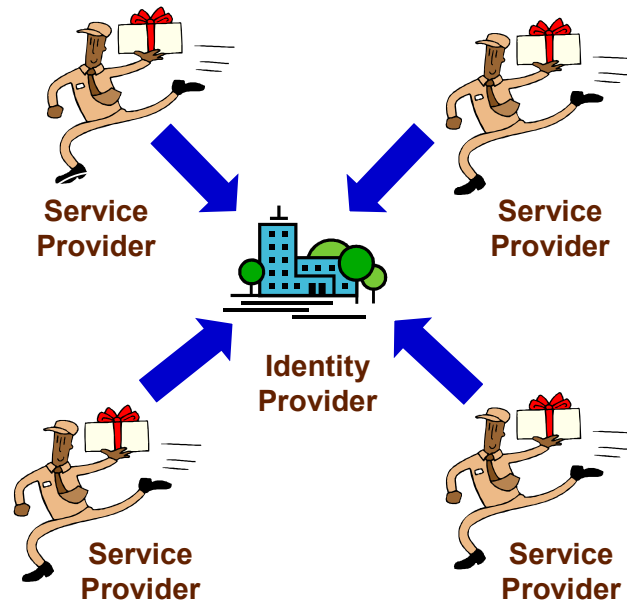


Figure 6: Identity Provider Centric Model

Many companies attempt to consolidate the user account information in a single authoritative data source, typically a directory or meta-directory. Web applications can then leverage a centralized authentication system that utilizes this information.

This type of approach more typically results in multiple islands of service providers clustered around an identity management system. Often this is because organizational boundaries make true consolidation difficult, or legal hurdles exist to consolidating user information into a single authoritative data source.

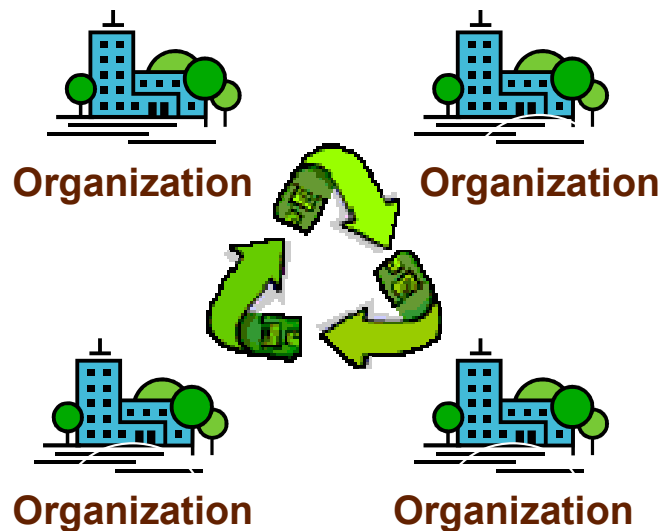


Figure 7: Cross Domain Model

Cross Domain Model

In the cross-domain model, each organization can be both an

identity provider and a service provider. This would be the outcome when an identity-provider-centric model failed to achieve its goal of a single authoritative data source. This model can be used both internally, as just described, and also externally when users must interact with external partner sites.

All companies can be producers and consumers of identity information. In any particular implementation, the company typically plays the service provider or identity provider, but when looking at the larger picture it is likely that all companies will play both roles, although for many the identity provider role may be limited to internal applications.

Operational Considerations

Operational considerations impact the rollout of any system. In the following section we take a high-level look at the strategic, business and technical aspects of a federation project.

Strategic

Federated identity is one component of an overall identity-management strategy that includes provisioning, authentication and authorization. Federation can impact authentication policy because in a federated environment the service provider is accepting authentication assertions produced by an identity provider that operates under a different set of policy rules. It is thus important that the service provider be able to obtain sufficient information about the authentication assertion to determine if it conforms to the local policy.

In a similar way the service provider must be able to determine the access rights of the federated user. This is generally done by mapping the user to a local account that has associated access rights. The account can consist of a one-to-one mapping or mappings based on attribute information passed by the identity provider. An alternative is to explicitly pass authorization assertions, however the lack of standardization in this area makes this approach difficult.

Business

The federation agreement is the contractual obligation between parties when entering into a federation. The federation agreement determines the rules by which the participants operate and is akin to the Certificate Practice Statement (CPS) that governs the operation of a certificate authority. Like any business contract, the federation agreement must lay out what is expected of each party.

When multiple parties are involved, there may be separate federation agreements between various parties or a common agreement to which all parties adhere. Federation agreements can also be used to formalize the operational rules under which internal federations function.

A federation agreement covers (but is not limited to) the following areas:

- Technical Agreements on technology interoperation. These define the technical standards that govern the transfer of information between federation partners. In most instances, an existing technical standard is used, and the technical agreement covers the encoding of information into the various messages that are transmitted.
- Policy agreements that cover authentication requirements and access rights. This can cover requirements regarding the strength of the authentication, e.g. single-factor or two-factor, and may also include minimum requirements on password management.
- Standards for maintaining identity information at the identity provider. These govern the operational parameters around account management and may explicitly stipulate minimum requirements on account management.
- Auditing requirements for traceability. Many companies may be required by regulatory policy to maintain audit trails. The types of transactions that must be logged need to be explicitly called out.
- Business liability issues. In many instances it is possible that one of the parties might sustain a financial loss as a result of a transaction that was unauthorized or performed in error. The federation agreement needs to lay out the legal liability that individual parties incur when these type of situations arise.
- Privacy standards for information shared about users. In some instances it may be necessary to pass information about a user as attributes in an assertion. Generally this is required to identify the user to the service provider or for the service provider to determine the user's access rights. The privacy agreement determines how this information is managed. For example, it can determine whether it is transient or permanent and what, if anything, may be divulged to third parties.

Technical

There are several choices in technology to implement federation. At the time of writing, the primary method for federating between web sites is to utilize the SAML technology to pass authentication and attribute assertions. An out-of-band mechanism is used to pass information that can be utilized for account mapping. As Liberty Alliance product implementations mature, the expectation is that SAML implementations will evolve into Liberty Alliance implementations.

Federated Identity in the Enterprise

The WS-* technologies are still in their infancy and the long-term success of these technologies will be driven by the rate of adoption of web services for componentizing applications both within and across enterprises.

Appendix A

Federation Products

The following list represents a sample of the vendors supplying products for implementing federated identity. There are also several open source toolkits on the market that can be used by companies to implement their own solutions.

1. RSA Federated Identity Manager

This was originally was part of RSA ClearTrust but has been split off into a separate product. It currently implements SAML 1.1, but a new version is expected to provide support for the Liberty protocols.

2. Netegrity SiteMinder

SiteMinder provides SAML 1.1 support for partner and affiliate sites. Netegrity was recently acquired by Computer Associates.

3. Oblix SHAREid

SHAREid provides SAML 1.1 support and, like RSA Federated Identity Manager, is a separate standalone product.

4. Trustgenix IdentityBridge

IdentityBridge is a standalone product that offers SAML 1.1 and Liberty 1.1 & 1.2 protocol support.

5. PingID PingFederate

PingFederate is a standalone product that offers SAML 1.1 support and will soon offer SAML 2.0 and Liberty Phase 2 support.

6. Microsoft ADFS (aka TrustBridge)

Microsoft is revamping its TrustBridge product and re-branding it as Active Directory Federation Services. This is projected to be released as part of Windows 2003 R2 in the second half of 2005. Initial documentation indicates that SAML token will be supported in WS-Security SOAP headers, however at this time no information is available regarding whether it will support the SAML or Liberty protocols.

7. SUN Java System Access Manager

This provides SAML 1.1 & Liberty Phase 2 (ID-WSF) support and is part of a suite of Identity Management products from SUN.