# Federated Identity: A Fairytale or Reality?

## Identity and Access Management

**Is sharing trusted identity online a future or just a dream?**

## The Introduction

When business was not done online a decade ago, most companies would accept your driver license, or personal identification card as the proof of your identity. However, in this new cyber age with minimum face-to-face interaction, digital identity is used by many companies to authenticate users when doing business on the Internet.

In order to identify the parties involving in an online transaction, a company usually first registers its users by storing their basic information such as name, address, username, and password in a local database and then authenticate them by confirming their credentials when they login. Unsurprisingly, since most user databases are not connected or shared on the Web, a typical user may have 10 or more digital identities, usually in the form of username and password pair, provided by different unrelated companies. Without integrating or sharing identities among companies and applications, many users on the Web are facing an identity crisis of having an unmanageable numbers of digital identities.

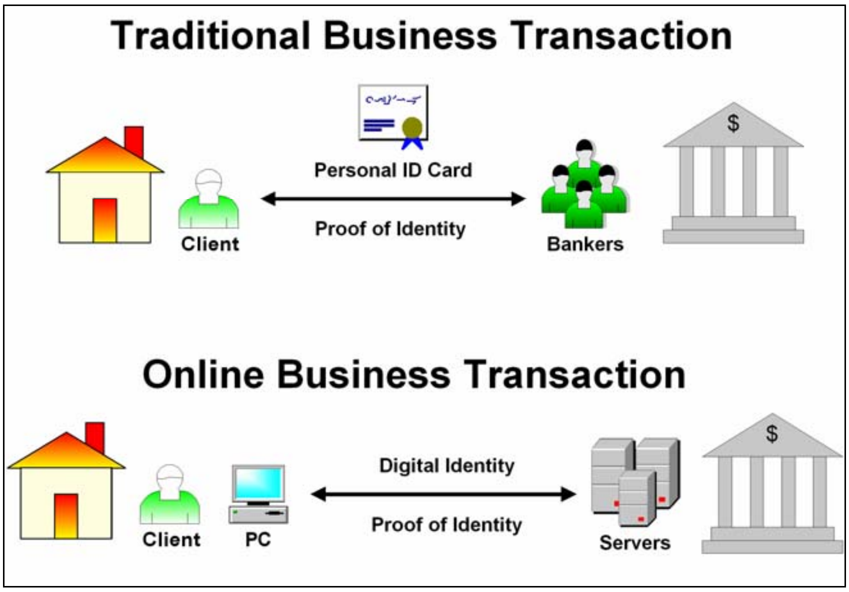

Diagram 1: Traditional vs. Online Business Transactions

## What is FIM?

According to Burton Group, an IT infrastructure research company, federated identity management (FIM) is *the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.*

Using your bank card to get cash in any ATM machine around the world is an example of the federated identity concept. No matter which bank you belong to, you can get money from almost any bank by inserting your card and entering the pin. Since most banks had already agreed to use the same standards for user authentication and mutually trusted each other, your identity can be shared by most banks and authorize the cross-domain transaction smoothly.

Traveling with your passport is also another example of FIM. By only validating the authenticity of your passport, other countries will have a level of confidence in your identity provided by the issuing country if they had already agreed to trust the passport as the proof of traveler's identity aboard.

Similarly, on the Web, FIM is a solution to share user identities across trusted domains. With FIM, a user can first login to a domain or Website and the digital identity can then be shared by other trusted domains. Instead of creating and maintaining yet another user profile in a local database, a company may now reuse and rely on the identity provided by another trusted company or entity without re-authenticating the same user. It allows a user to use the federated identity to logon to multiple sites without being re-challenged again.

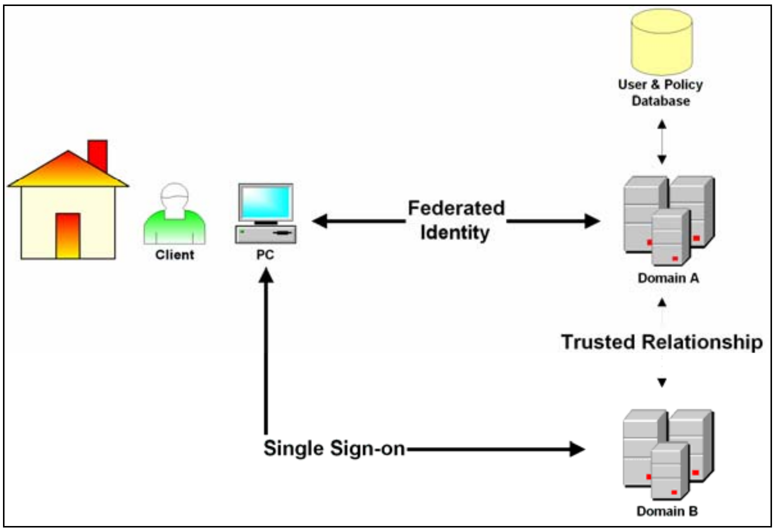

Diagram 2: How FIM works?

## FIM and Users

Many Web applications now have security mechanisms to safeguard valuable information and require users to login before use. While more and more transactions are done online, users are often required to remember more and more sets of username and password in order to access email, handle online banking, shop at e-retailers, and login to company's applications, VPN, Unix systems, time tracking site, and HR portal, etc.

In addition, many digital identities on the Web are protected by poor security systems. Those systems usually use weak password policy and single-factor authentication, depending only on a simple password. User writing down credentials on paper and system allowing the usage of a very simple password are two common examples of the security problems. Stronger authentication methods such as security token, digital certificate, or fingerprint scanning are more secure, however, the costs of those methods are relatively higher for companies to implement and more difficult for users to be accustomed to.

Why FIM is beneficial to users? One of the key advantages of FIM is to reduce digital identities for the same user in related applications and companies. Consolidating identities by FIM will improve user convenience and help users better remember and manage their credentials.

Also, FIM infrastructure may potentially encourage companies to implement stronger authentication mechanism in their applications because the costs can be shared by multiple applications and the ROI can be substantial. From the users' perspective, using a stronger authentication method in a FIM solution can be more secure, practical, and convenient than using a traditional single-factor authentication. For instance, using a shared fingerprint recognition system to single sign-on to 5 different applications is a more feasible and secure solution than logging into those applications with 5 different sets of login ID and password separately.

## FIM and Enterprises

Frequently, users on the Web are anonymous since they can hide behind a computer and access many information on the Web without telling who they are. As more and more sensitive and private information is accessible on the Web, it becomes more and more critical for companies to securely deliver information only to intended users. Many companies had realized the importance of fulfilling security responsibility and managing employees, partners, and clients effectively to the success in this Internet-based economy. As a result, many enterprises have already been developing identity and access management(IAM) infrastructure to manage users within their own organizations.

In the new business world, acquisitions and strategic partnerships are common ways for enterprises to reduce costs, increase revenues, and created new business opportunities and relationships. Companies now demand more than an internal IAM system to do business with their partners and subsidiary companies on the Internet. Sharing user information securely and providing services to a greater population of clients are extremely critical to enterprises. Thus, companies are in need of enhancing communication with business partners and entities by integrating not only applications but also user communities. That is why FIM is one of the hottest topics in IT security today.

Why FIM is beneficial to Enterprises?

To employees: A FIM solution may enhance their interaction and productivity. For example, the employees of a partner can use their federated identities to access real time information about the products in another company and co-market those products to their clients.

To clients: FIM can reduce the number of login attempts and improve their experience in affiliated sites by reusing federated identities. For example, a client can login to one company and gain instant access to another application on a partner’s domain effortlessly.

To Enterprises: Reducing costs by combing identity management services into a trusted entity, FIM can minimize the number of user identities and cut help desk calls in managing those identities. Again, FIM may also provide a better ROI for companies to implement stronger authentication methods and policies, and ultimately, provide better security to companies and their users.

## The Reality

In fact, federated identity management is not a dream or just a diagram on paper anymore. Major software companies, businesses, and organizations have put in serious efforts and investments in developing new federated identity systems and standards to connect their employees, business partners, and clients on the Internet.

According to American Express's Vice President of Internet Strategy, Michael Barrett, " *What you have [today] is an approach where the system is constructed of a series of components that run on different platforms, so its more of an orchestration approach to systems architecture. The difficulty is that you have to move the identities seamlessly across those platforms as the transaction itself flows across them. That exposes you almost immediately to the vagaries of the island of identities that companies like ours tend to have".*

We actually start to hear some successful stories about sharing trusted identity across the Web. Companies like AOL, Fidelity, and European telecom giant Orange have also been planning and implementing federated identity solutions to improve user experience and security.

Although federated identity management is a new concept and technology in IAM, it seems to gain traction quickly in IT security and it may impact the way how we manage our digital identities very soon.

## A Closer Look

The technology for FIM is rapidly changing and improving. However, the main concepts in the federated identity management are single sign-on, identifier mapping, attribute profile sharing, and user management:

- Single sign-on is achieved by the communication of authentication information of a user across multiple domains. After a user login to a domain, the authentication information, or authentication assertion, can be passed to other trusted domains and the user can then access resources on the trusted domains without re-authentication.

- Identifier mapping provides the linkage of different user identifiers for the same user in multiple domains. For example, a user can be johnsmith in one domain but jsmith in another and both names are linked by identifier mapping in FIM. The same user can be accepted in different applications even though the identifiers are different.
- Attribute profile sharing allows user information to be accessed by different domains. The basic information of a user such as names, address, security role, and other attributes can be retrieved by the trusted applications according to the agreed privacy and security policies.
- User Management includes the creation, modification, provision, and deletion of federated identity. Because a FIM solution will service multiple domains and applications, a user may be first created by a federated identity provider and then will require access to another domain, a federated identity consumer. Thus, user management is a very important piece in FIM.

## The Standards

Without generally accepted standards, it is very difficult for companies with different IAM technologies to share federated identity on the Web. In a heterogeneous architecture, companies need to agree on standards to share identity without using the same technologies for directory services, security policies, and methods of authentication. So far, there are some efforts in reaching that goal by the industry such as the Liberty Alliance, the internet2 Shibboleth project, and the OASIS (Organization for the Advancement of Structured Information Standards) Web Services Security (WS-Security). Currently, the most successful and established standard in federated identity is the Security Assertion Markup Language (SAML).

SAML is developed by the Security Services Technical Committee of the OASIS. It is an XML-based framework for the communication of user authentication, entitlement and attribute information among different domains. According to OASIS, *SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.*

SAML V1.0 was an OASIS standard in November 2002. In September 2003, SAML V1.1 was released and gained significant support from the industry. In March 2005, SAML V2.0 was approved as an OASIS standard. At the 2005 RSA Conference in San Francisco, the OASIS SAML Interoperability Lab, sponsored by the US Government's GSA, had demonstrated the interaction of federated identity among multiple sites of government portal, content, and service companies.

It is believed that SAML V2.0 will be a major step towards full convergence for federated identity standards in the FIM industry.

## The Challenge

While enterprises are busy developing IAM infrastructure, building or joining a large federated identity community may not be an easy task for CTOs or CSOs. Before companies can trust each other to provide and consume federated identity, all companies are required to have sophisticated and reliable IAM infrastructures and security policies. Without resolving the business issues related to business relationships, security roles and access rights, introducing FIM to an unprepared company will only cause more chaos and security problems.

In additions, the standards and commercial products in identity federation are still evolving. Although SAML V2.0 will be the critical convergence of all major standards, it may take a while before software vendors can develop products to support the newer version of SAML. Therefore, it may take an enterprise a few years to fully utilize the technology and standards before realizing the benefits of FIM.

## The Conclusion

With the Internet, sharing information anytime and anywhere has never been easier. However, sharing user identity securely on the Web is still a huge challenge for enterprises. Indeed, federated identity management is believed by many analysts, software vendors, companies, and IT organizations to be the future direction of identity and access management.

If FIM is done right, both users and enterprises can be benefited from the enhanced security and simplicity of the solution. Sharing federated identity across the boundaries of enterprises will not only reduce costs but also increase revenue by creating business opportunities.

With the establishment of more interoperable standards, the implementation of stronger authentication methods, and the maturity of more sophisticated federated identity products, enterprises will be able to fulfill the mutual responsibility and commitment to share trusted identities on the Internet.

Handling digital identity on the Web securely and easily may soon be a reality instead of a fairytale.