30P. Federated Identity Management: Why is Adoption so Low?

Keith Ivy
Allstate Insurance Company, Keith.Ivy@allstate.com

Sue Conger
University of Dallas, Sue.Conger@gmail.com

Brett J. Landry
University of Dallas, blandry@gsm.udallas.edu

Follow this and additional works at: http://aisel.aisnet.org/confirm2010

Recommended Citation
Ivy, Keith; Conger, Sue; and Landry, Brett J., "30P. Federated Identity Management: Why is Adoption so Low?" (2010). CONF-IRM 2010 Proceedings. 34.
http://aisel.aisnet.org/confirm2010/34
Abstract

As enterprises extend internal systems and applications to external users, it is important to ensure that the user experience operates seamlessly between disparate organizations. To meet this challenge, Federated Identity Management (FIM, also single sign-on) provides an economically efficient and convenient way of providing connectivity to customers, partners, suppliers, and others. FIM is a topic of widespread discussion with rapid growth predicted for almost ten years. This growth has not happened. This prescriptive study identifies some key factors contributing to the slow adoption of FIM technology, including technological complexities, lack of trust between partners, and the complications and expenditures involved in establishing and maintaining contractual agreements between partners.

Keywords

Federated identity management, single sign-on, access management, identity management, SAML, WS-*

1.0 Background

Federated Identity Management (FIM) refers to a collection of technologies and solutions that enable organizations to trust each other’s user authentication in a single sign-on (SSO), mainly web-enabled, environment (Kobielus, 2005). FIM simplifies and secures a user’s access to inter-organizational applications and resources through the use of a digital identity stored in a directory service that is the information repository about users, devices, and services, including names, locations, access rights, and authorizations (Loosely Coupled, 2002-2005).

Microsoft was one of the first to conceptualize FIM with a project called code-name ‘Hailstorm,’ which consisted of a Microsoft-controlled database in which users registered their details to seamlessly browse the web. However, Microsoft failed to obtain support because of its proprietary ownership, leading to resistance and ultimate failure of the initiative. (Foley, 2008) Microsoft’s efforts ignited general interest in FIM technology and in September 2001, the Liberty Alliance, a consortium of major companies led by Sun Microsystems, HP, IBM, and others developed the initial specifications for federated identity management (De Clercq, 2006; Vierboom, 2004).
Where SSO technology allows users to log-in and authenticate once in co-located domains (Stallings, 2007), FIM enables enhanced SSO that provides seamless access to systems in autonomous networks across the Internet. Google for example uses SSO for authorization and authentication to Web-based applications such as Gmail and Google Calendar. Google acts as the service provider enabling FIM technology for access to applications it hosts (Google, 2009).

FIM requires both affective and technological trust relationships between the disparate partner organizations (Our federated ID future, 2004). FIM establishes technological trust relationships though a trust service, consisting of the following: Principal, Identity Provider (IdP), and Service Provider (SP) (Bhargav-Spantzel, et al., 2007). A Principal is a primary actor in a federated environment and can be either a person or application identified and authorized to perform business tasks. An Identity Provider (IdP) is a trust service organization that authenticates a Principal’s identity. IdPs can be employer, financial institution, government agency, or some other organization (such as VeriSign) recognized by trading parties as the Principal’s authenticating authority. A Service Provider (SP) is a system entity providing a service (e.g., SaaS) to Principals. A ‘digital identity’ is an electronic representation of a real-world entity, such as a user, represented by a set of attributes stored in a directory. Thus, the trust relationship is a logical connection between autonomous networks (PCMag.com, 2009) provided through an Identity Provider to connect contractually related Principals and Service Providers via a digital identity.

Process flow for identity management begins with an authorized Principal that sends a request from a browser to gain access to a third-party external application (SP) through a web service (Figure 1, Step 1). The web service communicates with the FIM system’s IdP. The IdP finds the Principal’s digital identify and creates an assertion token, which is returned to the Web Service (Steps 2 and 3). Linkage to the external application is established through a redirect sent to the browser from the web service, which is an intermediary in web service-Principal communications (Step 4, repeats until the connection is severed). Thus, federated access is established between the user and the external application (Blakley, Blum, & Gebel, 2008).

FIM includes two methods -- one for Business-to-Business (B2B) processes and transactions and one for Business-to-Consumer transactions (B2C). While this study focuses on the enterprise issues, it is essential to also understand B2C FIM. B2C FIM also consists of two connectivity methods --
relationship and credential-focused methodologies. The relationship-focused approach maintains user relationships with IdPs, and each transaction conveys identity information to a SP via the appropriate IdP. For the credential-focused approach, users obtain long-term credentials from an IdP but store them locally (Bhargav-Spantzel, et al., 2007).

Federation is particularly useful for business processes that span multiple organizations and require interoperability between environments, such as financial services companies, governments, healthcare providers, and telecomm companies (Carr, 2008). FIM offers benefits such as reduced identity management cost and increased identity security. With federation, only the IdP maintains user identities, thus reducing administration and maintenance costs for all principal organizations. Security is enhanced because principals no longer manage identity records (Cser, 2008). Thus, FIM meets requirements for secure inter-organizational access requirements and is amenable to future technology changes (Blakley, Blum, & Gebel, 2008).

Since FIM appears to be a useful, mature, and secure technology, the question then is why is FIM adoption so slow? As of 2007 the FIM adoption rate was less than 5% in the U.S. and lower in other countries (Cser, 2008). This study is important because only in understanding reasons for slow FIM adoption can strategies for increasing adoption be developed. This research evaluates FIM adoption by evaluating the technology challenges relating to key characteristics of FIM's relationships and technology: FIM technology, FIM standards, security/privacy, trust relationship issues, and financial issues.

2.0 FIM Technology

Three basic topologies for linking federated domains are point-to-point, hub, and networked (Figure 2). In a point-to-point topology, two or more domains exchange assertions directly. The number of bilateral trust relationships required is \( \frac{n(n-1)}{2} \), where \( n \) is the number of domains. Because trust relationships are expensive to establish, the number of domains federated in this fashion is usually necessarily small.

In a hub topology, each participating domain (spoke) in the federation connects to a hub domain. Hub topologies are best when there is little inter-spoke communication. In a networked topology, the federation may contain multiple hubs, and spokes may interconnect with more than one hub. While not all networking is direct, large, industry-wide federations have developed features to support networked topologies (Blakley, Blum, & Gebel, 2008).

![Figure 2: FIM Topologies Source: (Blakley, Blum, & Gebel, 2008)](image)

3.0 Standards and Technology

From fiascos like VHS vs. beta formats to the de facto adoption of TCP/IP, we know that adoption of new technology is facilitated with the support of recognized global standards. In this section we
discuss the FIM technology standards, which consist of the Security Assertion Markup Language (SAML), Web Services-Federation (WS-Federation); and open standards for user authentication and access control such as OpenID (Shwartz, 2006). Several organizations are key to FIM standards development including, the Liberty Alliance and Organization for the Advancement of Structured Information Standards (OASIS). Technology challenges relate to the number of federation protocols and incompatibilities primarily between SAML and WS-Federation. In addition, large vendor implementations lack support for all the FIM protocols, for example, Microsoft Active Directory Federated Services (ADFS) lacks SAML support (Scarlet, 2006). The two most important standards – WS-Federation and SAML, are described in more detail to provide understanding of the technology challenges.

3.1 WS-Federation

WS-Federation will be the final element of the Web Services (WS-*) suite of security specifications that was designed by the Liberty Alliance as the basis for secure web services interoperability (Blakley, Blum, & Gebel, 2008). WS-Security, WS-SecurityPolicy, and WS-Trust services are currently operational and provide a basic model for federation between IdP and SP. The fundamental goal of WS-Federation is to complete the WS-* stack and deliver a suite of integrated protocols to address identity and security requirements of both web applications and web services ((Blakley, Blum, & Gebel, 2008). The Liberty Identity Federation Framework (ID-FF) consists of the standards for implementing SSO with federated identities. The framework provides the design for SSO within a Circle of Trust (CoT), a contractual arrangement between a group of organizations to share transaction inter-operability. It accomplishes this by defining protocols for account linking, global logout, and mechanisms for browser redirects (Liberty Alliance, 2003).

3.2 Security Assertion Markup Language (SAML)

SAML is an Extensible Markup Language (XML) standard for exchanging authentication and authorization data between security domains, using standard mechanisms for authentication. SAML allows authentication authorities (IdPs); attribute authorities, and policy decision points to make assertions regarding the identity, attributes, and entitlements of a Principal to other entities, systems, or applications. SAML protocol defines rules for requesting and responding to authentication requests (OASIS Security Services, 2008).

SAML provides SSO and access management for browser requests between organizations with relatively simple trust relationships while the WS-* standards were designed to promote interoperability for all aspects of Web services, such as policy, messaging, transactions, and security. SAML is restricted to inter-organizational applications, while WS-* is devoted specifically to Web-Services Security. Thus, the two standards have some points of overlap but are essentially different (Microsoft, 2008).

Liberty’s ID-FF and OASIS SAML were separate efforts in FIM standards for secure SSO. The two standards intermix a variety of security technologies: Channel security consisting of server-side certificates for identity providers; transport layer security, Secure Socket Layer (SSL), or other channel security protocols, such as Internet Protocol security (IPSec), security tokens with a limited lifetime, cryptographic nonce, and digital signatures for single-transaction integrity (Landau & Le Van Gong, 2008).

To further confuse this business space, open-source middleware, such as Shibboleth grants access rights to multiple systems by the use of a single set of authorization credentials (Gilbert, 2003).
Shibboleth has widespread use and is the foundation of the InCommon Federation used by nearly 100 U.S. universities for, for instance, library database access (Carr, 2008).

There are many other standards that interact with FIM but that lead to complexity and interoperability issues. “The variety of federation use cases and the preferences of different vendor or industry constituencies, […] have led to a […] number of standards, or specifications” (Blakley, Blum, & Gebel, 2008, p. 14). Figure 3 depicts FIM specifications in five core categories: profiles and services; web transport, session and security; Simple Object Access Protocol (SOAP) message security; Web-Services token specifications; and policy management. The most likely core specifications are highlighted in blue (Blakley, Blum, & Gebel).

In addition, WS-* uses multiple token formats used in its assertion process. Other complications are that vendors use cryptography inconsistently in their products and that algorithms and schemas used to support FIM products depend on the identical configuration across member organizations (Grant, 2008).

Most commercial FIM products use SAML-based technologies, and most comply with the Liberty Alliance conformance program to ensure interoperability (Carr, 2003). SAML is more mature than WS-Federation and there are more products based on SAML (Carr, 2003). There are more customer deployments based on SAML 1.1 than for WS-Federation. Also, SAML 2.0 is required by U.S. government initiatives, such as the eAuthentication project (Microsoft, 2008).

To spur momentum in FIM adoption, the Concordia project, a consortium organized by Liberty Alliance, was formed. Its goal is to further interoperability by defining use cases and requirements for interactions among CardSpace, OpenID, WS-Federation, and SAML. The primary objective of Concordia was to accelerate the FIM adoption integrating the current multiplicity of environments (Concordia Project, 2007). To summarize, confusion and inconsistency in commercial offerings is one reason for slow adoption rates.
3.3 FIM Technology

The emergence of trusted identity providers, trusted broker networks, and vendors providing interoperability will be a cornerstone of success for FIM adoption. Vendors have simplified deployment of FIM products by creating lightweight, standalone solutions that do not require large scale Web-based solutions. Table 1 lists most of the prominent FIM vendors and products approved by Liberty Alliance, which conducts rigorous compatibility testing (Brenner, 2005). SAML, OpenID, WS-Federation, and CardSpace not only support producing and accepting tokens, but also provide protocol translation (Cser, 2008). Trusted broker networks and workspaces provide scalable federation technologies to connect organizations reliably.

There is a growing list of choices for organizations looking to federate. Healthcare and financial industries lead in adoption of FIM services to comply with government regulatory requirements and to reduce associated data management costs. Federating access-management environments gives principals a set of tools to facilitate compliance with Sarbanes-Oxley (SOX) (Carr, 2008), the Gramm-Leach-Bliley Act (GLB) (Carr), and other mandates.

4.0 Security and Privacy

Security is a critical concern in managing access to enterprise resources. Most vendors that specialize in the access control domain feel that today’s collaborative and interconnected e-business landscape requires a secure and effective methodology for enterprises to share trusted user identities and entitlements. The ability to federate identity across organizations while maintaining access rights and privileges continues to be a major challenge when securing online business collaboration (Bhatti, Betino, & Ghafoor, 2007).
With increases of data leakages and identity thefts, companies must be certain that federated partners actively practice security control with procedures that ensure compliance with regulatory directives and its own security policies (Carr, 2008). Nevertheless, regardless of policies and procedures, organizations in federated relationships accept equal responsibility in the event of a compromise.

Security concerns with FIM technology relate primarily to the extensive exchange of sensitive information that traverses organizational boundaries. Securing communication channels and encrypting messages helps preserve the privacy of Personally Identifiable Information (PII) and proprietary data, but is not a complete security solution. In a federated transaction, such as a user request to an IdP, inadequate security countermeasures could result in attacks, such as a man-in-the-middle assault, resulting in unauthorized disclosure of information (Ahn & Lam, 2005).

Almost all well-known solutions involve tradeoffs that are application centric and are less useful in a broader scope. Additionally, the development of Web-based federated identity solutions has advanced more rapidly compared to Web-based privilege management mechanisms resulting in a wide gap between the federated identity and privilege management mechanisms. The demand seems to be trending more toward an integrated comprehensive approach to access management. Because of this disparity, the migration of enterprise operations to the Internet demands a significant evolution of traditional access management mechanisms for securing dynamic Web-based resources. Federated identity and privilege management are both critical elements that require equal emphasis (Bhatti, Betino, & Ghafoor 2007).

To achieve comfortable levels of assurance, FIM systems need the cooperation of all three sets of members -- the Principals, IdP, and SP, to establish and manage FIM security. The SP shifts responsibility to the IdP for security assertions made on their behalf. Reluctance to participate in federation occurs when partners lose confidence in the security measures or feel that data is used for other than its intended purpose.

Concerns can be aligned with just about every conventional IT paradigm from compliance, security, and privacy to outsourcing. While privacy drives security and security enables privacy, continual risk reduction against unauthorized disclosure is key to CoT maintenance (Landau, & Le VanGong, 2008). Given the sensitive nature of identity information and the very real possibilities of fraud, financial damage, or privacy violations, organizations will inevitably struggle with security, legality, and liability (Bhatti, Betino, & Ghafoor, 2007).
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Supported Standards</th>
<th>Liberty Alliance Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Associates (CA)</td>
<td>Federation Manager</td>
<td>SAML 1.0, 1.1, 2.0, WS-Federation</td>
<td>Yes</td>
</tr>
<tr>
<td>Hewlett-Packard (HP) (Acquired 2005)</td>
<td>Trustgenix Identity Bridge</td>
<td>SAML 1.0, 1.1, 2.0, WS-Federation</td>
<td>Yes</td>
</tr>
<tr>
<td>IBM</td>
<td>Tivoli Federated Identity Manager</td>
<td>Identity Federation Framework (ID-FF 1.x), SAML 1.0, 1.1, 2.0, WS-Federation, WS-Security, WS-Trust</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Active Directory Federated Services (ADFS) v1</td>
<td>Identity Federation Framework (ID-FF 1.x), SAML 1.0, 1.1, 2.0, WS-Federation, WS-Security, WS-Trust</td>
<td>No</td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Identity Federation</td>
<td>Identity Federation Framework (ID-FF 1.x), SAML 1.0, 1.1, 2.0, WS-Federation</td>
<td>Yes</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>PingFederate</td>
<td>SAML 1.0, 1.1, 2.0, WS-Federation, WS-Trust</td>
<td>Yes</td>
</tr>
<tr>
<td>Sun Microsystems</td>
<td>Sun OpenSSO Enterprise</td>
<td>Java Authentication and Authorization Service (JAAS), Kerberos, Liberty ID-FF, Liberty ID-WSF, Online Certificate Status Protocol (OCSP), SAML 1.0, 2.0, WS-Federation, WS-I Basic Security Profile tokens, WS-Policy, WS-Trust, X.509 Digital Certificates, XML Digital Signature, XML Encryption</td>
<td>Yes</td>
</tr>
<tr>
<td>Symlabs</td>
<td>Federated Identity Suite</td>
<td>Liberty Alliance (ID-WSF 2.0 &amp; ID-FF 1.2), SAML 2.0, WS-Federation</td>
<td>Yes</td>
</tr>
<tr>
<td>Open Solutions</td>
<td>Shibboleth</td>
<td>SAML 1.0, 1.1, 2.0</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 1. FIM Products (Source: Liberty Alliance project, 2003)

5.0 Human Issues

This section discusses the two types of trust required in FIM relationships: Affective relationship trust and technical definitional trust. Both are sources of problems and show that the human aspects are more daunting than technical concerns as more organizations join a CoT, transaction-sharing environment.

5.1 Affective Relationship Trust
Accurately making access control decisions is a critical element in trusting a Federated Identity system. These decisions directly protect the security of the resources involved in federated relationships. FIM must have dynamic controls for managing user lifecycle. Because the role of service providers and identity providers are sometimes inter-changeable in web services, all participating organizations in FIM systems must face the trust decisions implied by all possible cross-organization interactions (Goodrich, Tarmassia, & Yao, 2008).

Some federated relationships could be relatively simple, and as a consequence are easy to govern (Windley, 2006). However, many organizations have complex business processes, and multi-partnership relations that result in a number of factors slowing FIM adoption. FIM implementation requires the mutual cooperation and commitment of all participating partners in order to develop the desired transparency across organizational boundaries.

Building affective trust across autonomous principals is paramount to FIM adoption (Carr, 2008). Before FIM can be realized, business process owners must collaborate and trust each other. An organization must be able to discern whether its CoT partners know about and adhere to their policies, practices, contracts, and those of the organization with the most stringent compliance efforts and mandates in the FIM federation (Tippett, 2006). Principals seeking to initiate federations require documentation, tools, services, and techniques for enabling and encouraging partners to participate. Issues relating to the roles, privileges and access rights for individuals on partner networks must be defined. Policies and procedures used by federated partners for authenticating and assigning roles to users also are required (Smedinghoff, 2008). The various consortia provide support to ease the complexity of adding new members to existing federations (Blakley, Blum, & Gebel, 2008). Yet, different technology and security maturity levels among organizations continue to be a problem (Cser, 2009).

In effect, most existing SSO solutions assume preexisting trust relationship among providers and do not provide adequate mechanisms for the trust establishment between providers. This limitation hinders the wide deployment of SSO in web-service environments, because providers may be unknown to each other. Therefore, flexible, reliable and secure trust establishment mechanisms need to be provided to support federated identity management (Goodrich, Tarmassia, & Yao, 2008). Partners in federated systems are essentially vouching for the identities of their users and their access requirements for hosted externally services. Network principals, roles, privileges and access rights for individuals on partner networks all need definition (Vijayan, 2004). Then, a technology-based CoT between external partners is established to "share linked identities and have pertinent business agreements … regarding how to do business and interact with identities. Once a user has been authenticated by a CoT identity provider, that individual can easily … take part in targeted services from other service providers within that CoT" (Liberty Alliance, 2003, p. 6).

Figure 4 depicts a Venn diagram with proprietary authentication relationships within each circle with shared identity attributes shared among overlapping circles. Attributes from, for instance, a supply chain circle may be shared with the home circle (Liberty Alliance, 2003). An example of such a configuration is an individual who uses an online travel agency both at work and at home. The person can access his attributes regardless of their work location.
The Service Provider must have confidence that the Identity Provider will both manage and authenticate users on behalf of the SP. Trusting a partner to authenticate its own users requires the partner to have solid security and identity management practices (Carr, 2008).

FIM raises critical legal issues that often are ignored because of technology emphasis. Failure to recognize and address the legal contractual requirements can delay or cause failure of FIM adoption partnerships (Smedinghoff, 2008). Federation partners must be able to establish agreements outlining the compulsory assurance of identity information. Contractual agreements cause delays because of their inherent complexity, especially when delineating partner liability (ABA, 2009; Baldwin, et al., 2007).

Hub-and-spoke federations, in which all principals share a hub with a single dominant principal, are a relatively simple FIM organization from a legal perspective. All interaction is between the hub and its spokes, as depicted in Figure 2. For example, Wal-Mart as a strong central principal requires suppliers to adopt its identity management practices to do business. In such a case, the dominant principal dictates the trust requirements to the other principals (Carr, 2008).

5.2 Technological Trust

Once affective trust is developed, it is translated into a technological trust definition. Principals require development of an Identity and Access Management (IAM) framework to which all partners comply before FIM can be fully developed and managed. Good governance and robust implementation of each organization’s internal identity and access management are critical to creating a federated partnership network. Principals need to address internal IAM issues first and agree on the levels of security, privacy, and trustingness. Yet many organizations have not implemented business processes for managing their own internal identities (Cser, 2008). Such organizations would be precluded from FIM networks.

The complexity in managing dynamic federation agreements through technology is another inhibiting factor in FIM adoption (Cser, 2009). Federation advocates say that once the agreements are in place, the technology allows for richer partner integration, faster, cheaper coupling through standards, simplified customer experience, and better protection of customer information (Brenner, 2008).

In recent years, several identity federations have been established in higher education around the world. Typically these institutions systematically establish federations within a national scope, but the need for cross-border collaboration has led to the first interconnects of national federations. The Kalmar Union was established as a cross-federation of the Nordic academic identity federations. Trust
relationships between federated organizations such as education tend to be less problematic. The federation established between Nordic national federations and the Kalmar Union posed few obstacles from a technical perspective due to efforts by the standards committees developing stringent controls.

The reality seems different though as partnership coordination adds significant complexity to contractual agreements. Challenges such as cross-border legislative agreements tend to be problematic and difficult to resolve. In regard to federation agreements, policy makers do not have former precedence to rely on thus resulting in policy versus technological obstructions hampering widespread acceptance (Walter, Ingrid, & Mikael, 2007).

6.0 Return on Investment (ROI)

Cost-effective initiatives are fundamental to cause complex changes, such as FIM, in the business environment (Gebel, 2008). Contrary to initial claims that FIM has many cost reduction benefits, savings can accrue in several areas: Reduced security administration costs, reduced logon times, and reduced help desk call volume associated with password resets. Administrative costs are reduced because identify and access management for the federation partners is outsourced to the Identity Provider. Thus, the costs are shifted to another organization.

Savings from reduced logon times can be significant but are dependent on organization size. If a $100,000 employee has five logon sequences per day that would be replaced by one logon sequence in FIM, huge savings can accrue. For instance, five logons at 30 seconds each over a 260-day year takes 11 man-hours of time and costs the organization about $450/year in lost productivity. In a large organization with, for instance, 10,000 such employees, the increase in productivity is worth about $4.5 million per year and 52 fewer people are required to do the same amount of work for an additional savings of $5.2 million. From this analysis, the potential for significant cost savings, which were doubtful three years ago, have become substantial and attainable with mature identity and access management (Witty, et al., 2006; Perkins, 2009).

A final source of savings is from help desk calls that would be outsourced to the Service Provider. As much as 85% reduction in help desk calls substantially reduces credential management cost for the individual principal organizations (Carr, 2008). Non-monetary benefits accrue from the improvement in user convenience. Convenience is one of the main benefits of FIM (Witty, et al., 2006). To gain these improvements, investments in FIM require solid business process management to ensure the savings (Witty, et al.).

7.0 Discussion

Federated identity is a topic of widespread interest; however, the adoption rate is lower than expected. Some FIM challenges are to integrate business processes across organizational boundaries, simplifying access requirements to disparate systems through the use of a single identity FIM. The reluctance of organizations to adopt the technology relates to interoperability between dissimilar technologies and protocols, delegation of access control management to a third-party provider, uneven maturity of IAM management, reluctance to form trust relationships between partners, and the complexities and costs to establish contractual agreements between organizations that meet required regulatory compliance.

The major reason why FIM adoption remains slow relate to lack of affective relationship trust with reliance on unknown people and processes, legal complications, and technology inconsistencies. Therefore, technology is not the main issue, people are.
Beyond the CoT, affective trust relationships with the intricate legal agreements assigning culpability in the event of a security breach are difficult to attain. Lawyers, by training are untrusting and it is unclear how to define trust in a contract. Bilateral multi-organizational agreements do not scale and are costly and complicated to develop and maintain (Cser, 2009).

CoT relationships require process maturity that is at least similar across all expected federation partners. Organizations at different maturity levels for security and access management have difficulty in arriving at anything other than bi-lateral, hub-spoke relationships because the weakest link in the relationship defines the level of security.

7.1 Recommendations

Enterprises should aggressively investigate the capabilities of FIM. FIM can provide a methodology that can help organizations tighten security, reduce administration costs, and improve the overall IT experience for its users.

Management buy-in and senior leadership support is paramount to the success of any enterprise technology adoption. Executive managers must be convinced that the adoption of FIM technology will facilitate organizational strategy, be cost effective, and benefit the organization. To that extent, deploying federation in multiple organizations requires sponsorship, leadership, and cross-organizational support.

Concerns with the liberal sharing of identity information common in organizations often over unsecure channels require legal and business negotiation and continuous monitoring. Stringent controls that meet all legal and regulatory of the most regulated partner are required by all federation parties to safeguard sensitive information.

Security and privacy management of the Identify Provider must be more robust than that of any of the federation partners. Constant monitoring and management of the on-going FIM relationships and transaction processes is needed. The identity mapping process should be capable of ensuring that identity information is correctly used; that data are verified, updated when information is added or changed; and that data are not retained longer than necessary. The process also should be capable of ensuring IT systems are managed properly, and identity information is not accessible to anyone but federation members (Baldwin, Mont, Beres, & Shiu, 2008).

7.2. Limitations and Future Research

This research evaluates only organization-level FIM. Future work should evaluate user-centric FIM. Technology, in terms of operating environment, was ignored in this discussion. Yet, there is some evidence that new technologies, such as cloud computing, will impact FIM efforts in as yet unknown ways. Future research could evaluate operating environment impacts on FIM adoption by both individuals and organizations.

Further research on vendors such as IBM, Microsoft, and Sun to obtain current FIM technology assessments and evaluate their campaigns on FIM adoption would be highlight industry aspects of FIM. Evaluation of FIM early adopters, such as American Express, Boeing, General Motors, Nokia, and Proctor & Gamble, to define factors leading to their FIM acquisition would provide functional requirements for others to evaluate. Also, by evaluating individual company aspects of FIM, a FIM methodology for access and security management could be developed to aide less mature organizations in making the move to FIM.
Other future research could evaluate financial aspects of FIM to determine the breakeven point for FIM adoption and maintenance versus traditional IAM management.

8.0 Summary

This prescriptive research analyzes the reasons for slow adoption of FIM technology, which has been commercialized for over five years and had high expectations of swift adoption. FIM adoption is slowed primarily by the difficulties in the inter-organizational trust relationships required for FIM but also by uneven organizational maturity, and the plethora of different solutions accompanied by little common knowledge about their differences and similarities.

The financial analysis shows that FIM can be cost-beneficial for large organization but the scale remains unknown. Future research on different types of FIM, different vendor offerings, and the cost dynamics for FIM technology and company demographics all are areas for further research.

Bibliography


Loosely Coupled – connecting with Web Services. URL= http://looselycoupled.com/glossary/directory services


