Journal of Information Assurance and Security 3 (2008) 244-256

Dimensions of Identity Federation: A Case Study in Financial Services

Manish Gupta and Raj Sharman

School of Management, State University of New York
Buffalo, NY, 14260, USA
{mgupta3, rsharman}@buffalo.edu

***Abstract*:** In the networked economy, strategic partnerships and collaboration are an important way to develop and maintain competitive advantages. At the same time, enterprises also need to reduce costs, increase revenues and seize new business opportunities. This demands enterprises to enable convenient and secure business interactions with internal and external stakeholders, and create relationships to trust the electronic identities to access critical information resources. Federated identity management (FIM) is a system that enables individuals to use the same credentials or identification data to obtain access to the networks of multiple enterprises to conduct business transactions. FIM has demonstrated huge potential in providing reliable and scalable solutions to problems in systems security and access management. SAML (Security Assertion Markup Language) is the dominant web services standard for FIM. The objective of the paper is to present an *exploratory case study based research* to investigate implementation challenges, outcomes and federated identity management opportunities using evidence from a complex implementation of Identity Federation using SAML at a mid-sized north-east US bank. The SAML integration was achieved using a commercial off the shelf product, by Computer Associates, eTrust® that also leverages SAML as web services standard for federated identity management. Discussion in the paper presents common obstacles, opportunities, motivations and future directions in the realm of identity federation based on evidence from extensive project and product documentation provided by the financial services institutions team and on interviews with six team members of the case study project, including one senior information security manager.

Keywords: Identity federation, Security Assertion Markup Language, Identity Management, Single Sign On, Federation Web Services, SAML, Federated Identity Management, case study.

1. Introduction

Enterprises are increasingly focusing on extending their operational and technical resources to greater numbers of entities, including partners, suppliers and customers. On the other hand, they are faced with the critical need to survive and compete by streamlining operations and reducing costs. Many enterprises are finding the management of large numbers of external identities difficult and risky, and would like to develop and maintain a trust relationship with a partner, or a third party, as a way of managing identity-related risks. Federated identity management offers a standards-based means of achieving this goal, by allowing one organization (the identity provider) to provide information about a managed identity to another organization (the identity consumer, service or resource provider). Once individuals have been authenticated by their own organizations, they can access other organizations' resources without re-authentication being required [27]. SAML (Security Assertion Markup Language) is the dominant web services standard for federated identity management. It defines a set of XML formats for representing identity and attribute information, as well as protocols for requests and responses for access control information.

The objective of the paper to present an *exploratory case study based research* to investigate implementation methodologies, challenges, outcomes and federated identity management opportunities using evidence from a complex implementation of SAML at a mid-sized US bank. The SAML integration project was achieved using a commercial off the shelf product, by Computer Associates, *eTrust® SiteMinder* that also leverages SAML as web services standard for federated identity management. The project extensively employs federation security services components and technologies as they relate to cross-enterprise identity management. A discussion on motivations, requirements and opportunities of the integration is presented. The case study presents functional architecture, components and technical architecture and topology of the implementation. The case study also discusses real-world challenges and outcomes with specifications of this implementation and recommendations at a holistic level regarding federated identity management initiatives in conjunction with opportunities and challenges. Detailed discussions on motivations, expectations and challenges before and after the project are captured and presented as cases (propositions).The case study is based on extensive documentation provided by the team at the financial institution (Identity provider) and on interviews of 6 information security team members at the financial institution, including one senior level information security manager. The documentation included project plans, technical and information architectures, topologies, use cases, business cases and *eTrust® SiteMinder* product documentation. Any financial services institution specific sensitive information has been masked.

The case study can be used by access managers or information security managers to guide them with the selection of the methodologies, technologies and architecture for implementing a federated security services framework. This case study will equip them with in-depth understanding of real-world challenges and requirements for any similar sized federated identity management initiative. The case

Received September 19, 2008

study will indicate the aspects of federated identity management that are feasible and better choices in a particular context. This will endow the decision makers with more confidence to embrace web services for access management and enhanced security. The major focus of the design of the case study will be to illustrate key aspects of a real-world federated identity management implementation using SAML and not on any vendor specific technology or implementation.

Contributions of the paper are two-fold. First, the paper discusses, in form of an exploratory case study, details of a real-world successful complex implementation of OASIS-SAML based identity federation project. The details include the technical and functional architectures, business motivations and opportunities, use cases and process flow. This will be of immense aid to professionals and academicians interested in understanding requirements, technologies and workings of a real-world identity federation implementation. Secondly, the paper presents key findings of the implementation and analyses of key expectations of the financial institution before and after the implementation. The analyses are supported by evidence from the financial institution's documentation and interviews and on industry best practices.

The remainder of the paper is organized as follows. In this section we continue to present brief literature review of related work and background on identity federation. Section 2 introduces key concepts and definitions pertaining to digital identity federation, used throughout the paper. In Section 3, we present the case study at the financial institution where a project was undertaken to set up identity federation with a third party service provider. This section will cover, in detail, the process flow, the infrastructural components, technical and logical architecture, use cases and key expectations, presented in forms of cases. Section 4 discusses different security issues faced and considerations made throughout the execution of the project. The last section concludes the paper with discussions on analyses of expectations of the project, key findings and recommendations on the particular case study project and identity federation initiatives in general.

Background and Related work

Identity and access management systems are used by online service providers (SP) to authenticate and authorize users to services based on access policies. With the advent of distributed computing models such as web services, there are increased inter-dependencies among such SP's. As a result, the current trend [9][8] is to focus on inter-organization and interdependent management of identity information [18] rather than identity management solutions for internal use. This is referred to as *federated identity management*. Federated identity is a distributed computing construct that recognizes the fact that individuals move out of the corporate boundaries to access external applications. Practical applications of federated identities are represented by large multinational companies which have to manage several heterogeneous systems at the same time [18]. An effort in this sense is represented by the notion of *Single Sign-On (SSO)* [20], which enables a user to login to multiple organizations or SP's by using the same username and password. This approach increases usability and adds security by reducing the number of passwords that need to be managed. Emerging standards [9][8] are currently extending the notion of federated identity to other user information referred to as *identity attributes*.

2. Preliminaries and Key Concepts

This section presents key concepts and terminologies used throughout the paper.

Federated Identity

A federated identity is a single user identity that can be used to access a group of web sites bound by the ties of federation. Without federated identity, users are forced to manage different credentials for every site they use. This collection of IDs and passwords becomes difficult to manage and control over time, offering inroads for identity theft. A federated identity makes it possible for the end-user to use this same trust relationship to access information with another, related company without establishing new credentials. Ultimately, federated identity offers businesses, governments, employees and consumers a more convenient and secure way of accessing distributed resources without losing control over sensitive identity information, and is a key component in driving the use of e-commerce and personalized data services, as well as Web-based services.

Federated Identity Management

Federated Identity Management is a system that allows individuals to use the same user name, password or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions. Partners in a Federated Identity Management (FIM) system depend on each other to authenticate their respective users and vouch for their access to services. This enables companies to share applications without needing to adopt the same technologies for directory services, security and authentication. Within companies, directory services such as Microsoft's Active Directory or products using the Lightweight Directory Access Protocol have allowed companies to recognize their users through a single identity. But asking multiple companies to match up technologies or maintain full user accounts for their partners' employees is unwieldy. FIM allows companies to keep their own directories and securely exchange information from them.

Single Sign On

Single sign-on (SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems. Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

Received September 19, 2008

Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) is the dominant Web services standard for federated identity management, developed by the Organization for the Advancement of Structured Information Standards (OASIS). It defines a set of XML formats for representing identity and attribute information, as well as protocols for requests and responses for access control information and provide an XML framework for exchanging authentication and authorization information. SAML defines assertions as a means to pass security information about users between entities. An assertion can contain several different internal statements about authentication, authorization, and attributes. SAML defines two browser-based protocols that specify how SAML assertions are passed between partners to facilitate single sign-on. The two profiles are browser/artifact profile, that defines a SAML artifact as a reference to a SAML assertion and browser/POST profile that returns a response that contains an assertion. SAML documents can be wrapped in a Simple Object Access Protocol message for the computer-to-computer communications needed for Web services. The Figure 1 shows a SAML assertion from the case study project. The figure also shows different identity attributes, for example – "ROLE" being sent as part of assertion to the service provider application.

OASIS and Liberty Alliance

The Organization for the Advancement of Structured Information Standards (OASIS) is a global consortium that drives the development, convergence and adoption of e-business and web service standards. OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The OASIS SSTC (Security Services Technical Committee) has defined SAML as a framework for expressing authentication and authorization information using XML syntax [14][3]. Liberty Alliance is a global identity consortium with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trusted Internet by addressing the technology, business and privacy aspects of digital identity management [7][26]. The Liberty Alliance's ID-FF architecture built heavily on earlier version of SAML. Recognizing the value of convergence, the Liberty Alliance contributed ID-FF as input to SAML 2.0, the most recent version of SAML [3]. The Liberty Alliance has defined technology specifications based on three frameworks; these are ID-FF (Identity Federation Framework), ID-WSF (Identity Web Services Framework), and ID-SIS (Identity Service Interface Specifications) [12].

3. The Case Study

The goal of the project was to provide federated single sign on between the financial institution application, code named *Compass*, and an application at third party service provider. The application at service provider is a brokerage

```
<saml:Assertion
        xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
        xmlns:SM='http://www.somevendor.com/product'
                MajorVersion="1"
                MinorVersion="0"
                AssertionID="10.97.2.112.22912829339"
                Issuer="http://www.aBank.com"
                IssueInstant="2008-08-28T16:39:33.332Z"
        <saml:Conditions NotBefore="2008-08-28T16:34:33.332Z"
                        NotOnOrAfter="2008-08-28T16:43:33.332Z"/>
        <saml:AttributeStatement>
                <saml:Subject>
                        <saml:NameIdentifier
                        nameQualifier=www.aBank.com
                        Format="urn:oasis:names:tc:SAML:1.0:assertion">
                        Uid=oneloginID
                        </saml:NameIdentifier>
                </saml:Subject>
        <saml:Attribute AttributeName="ROLE"
                AttributeNameSpace="http://www.test.com">
                <saml:AttributeValue>ABC</saml:AttributeValue>
        </saml:Attribute>
        </saml:AttributeStatement>

        <saml:AuthenticationStatement
                AuthenticationMethod="Unspecified"
                Authentication Instant="2008-08-28T16:41:33.332Z">
        <saml:Subject>
                <saml:NameIdentifier
                        nameQualifier=www.aBank.com
                        Format="urn:oasis:names:tc:SAML:1.0:assertion">
                        Uid=oneloginID
                </saml:NameIdentifier>
        </saml:Subject>
        </saml:AuthenticationStatement>
</saml:Assertion>
```

Figure1: SAML Assertion from the ID Federation project

application, code named portfolio manager, for commercial investment management. Hereafter in the paper, the internal application at the financial institution will be referred to as *Compass* and the application at trade partner as *portfolio_architect* (denoting portfolio Architect application). The information regarding the identity federation project and the case study in this paper is based on extensive documentation provided by the financial institution on the project and the product and on 2 round of interviews conducted with six team members of the project at the financial institution, including a senior information security manager. There are several common pitfalls that the bank must consider if they are to make the most of its first federation project. Bank's managers understand that there is far too much emphasis on the technology issues as opposed to business factors. They believe that while technology is the key, the business benefits must be the main thrust. They wanted to avoid '*if we build it, they will come*' strategy. Given the relative immaturity of identity federation, they believe that efforts need to be taken to ensure that business units, partner and employees understand the potential benefits and risks of the federation projects. The strategy was well laid out: "*Decisions need to be taken in conjunction with clear understanding of the benefits and evidence that the advantages outweigh potential risks.*"

Overview of Application and roles

Compass is a financial application for managing customers and client relationships. Specifically, financial institution's

Received September 19, 2008

Investments Group uses the application to manage clients trades. The trades are done using an external trading vendor. The Compass application defines several roles. These roles determine the user rights in the Compass application and in the *portfolio_architect* application. There are eight roles in use with the integration described here, each denoting specific access rights for content and functionality. Figure 1 shows how a SAML assertion serves as vehicle for "ROLE" information flow. At the time of Single Sign On, there are other information specific to the transaction is also passed on to the *portfolio_architect* application. The following sections describe the process flow, key expectations (cases), architectures and topology of the infrastructure.

3.1 The cases (*propositions*) for Identity Federation at the financial institution

These days regulatory and security requirements signify not just authentication, but also fine-grained authorization and accounting. Federated identity management technologies improve security by controlling access on an operation-by-operation basis and providing a detailed audit trail while enabling access for partners and customers. Below, we present cases that we determined based on interviews and review of other documents provided by the financial institution. Members of the IAM team and a senior manager (Information Security) were interviewed to understand motivations and expectations of the project. The documents shared with us included project plan, project charter, license agreements, product documentation, technical and information architectures and business cases, amongst others. Interviews were conducted at the premises of the financial institution. In total 6 people were interviewed. The information obtained during interviews serve as basis for cases (propositions) presented below and also basis of analysis in a later section of this paper.

i) Case for improved accountability

Accountability is the ability to associate a consequence with a past action of an individual [17]. Integrations using SAML assertions provide for the complete evidence chain that is used to make the access control decision. The evidence chain serves basis for legal records of who accessed what data at what time, why and on whose authority. This is especially important for asynchronous and automated transactions, which are increasingly carried out using components of Web services. This requirement has never been more important for financial services institutions such as one in the case study, more so in light of newer and stricter regulations for customer and financial information safeguards.

ii) Case for Strong Authentication and Federated Single Sign On

Though strong authentication and federated identity can be implemented without each other, they provide a much more powerful defense against identity theft together as compared to just one in isolation. Federated identity makes strong authentication more accessible/realistic for many sites by shifting the burden of the technology onto dedicated providers whose business model can more easily support the infrastructure costs.

iii) Case for user convenience

The other chief motivation of FIM is to enhance user convenience and privacy as well as to decentralize user management tasks through the federation of identities among business partners. As a consequence, a cost-effective and interoperable technology is strongly required in the process of federation. Web Services (WS) is a good candidate for such requirement as it has served to provide the standard way for enabling the communication and composition of various enterprise applications over distributed and heterogeneous networks [23][24].

iv) Case for reduced costs and increased productivity

Organizations considering federations should analyze potential cost savings related to reduced help desk calls, user provisioning labor avoidance, and directory implementation and maintenance elimination. The financial institution was aware of the fact that most the savings will accrue to the identity consumer; they still believed that they are going to see cost savings in other areas after the project is implemented. Strong authentication, if implemented by each service provider, implies sending hardware tokens or key fobs to a large number of customers (even if not to the complete set), and so may be prohibitively expensive. Rather than each service providers having to implement strong authentication systems (with the likely implication of multiple tokens for the user to manage and carry), in a federated model a typical provider can 'outsource' the authentication to a dedicated 'strong authentication identity [13].

v) Case for IAM readiness for adoption of industry standards

One of the other concerns at the time the project was in *initiation* phase was need to select a product or technology that is most compliant with the industry standards for security information exchange in the identity federation area. CA's *eTrust® SiteMinder* was compliant with SAML in both tokens and protocols that lent advantage to its selection. Most cases of single-sign-on use are implemented using Web access management tools that, in turn, can be augmented with federated identity gateways provided by the Web access management (WAM) vendor or an independent vendor. Most of the industry has converged on SAML as the identity federation protocol of choice.

vi) Case for commercial products against open source solutions

The financial institution wants a product suite that is

Received September 19, 2008

reliable and dependable that comes from a commercial software model. This is more so important for identity federation where dependence on partner's technologies weighs heavily. Arguments posed for commercial products was that they are standards compliant that would make federation integrations easier and scalable; and that savings from open source are not real and not meant for mission critical applications where security counts more than technological savings.

vii) Case for opportunities for increased revenues

The financial institution anticipated that the deployment of Web services-based identity federation technology helps to bridge the cross-enterprise environments, enabling new business opportunities and ways to offer a stronger mobile enterprise solution. This infrastructure would be scalable with lesser cost for any new additions of partners to the federated enterprises list.

3.2 The process flow

This section describes the workings of the designed SAML SSO Architecture being deployed at the financial institution. We do so by describing the behind the scenes actions generated by typical use cases. Figure 2 illustrated the information flows in the SSO process.

Initial Sign On to Compass Application

Compass application is a web application used, at the financial institution, by internal users to manage customer relationships. The application is developed in java and HTML. The web application is protected by Computer Associate® product called eTrust® SiteMinder which primarily performs front door authentication and

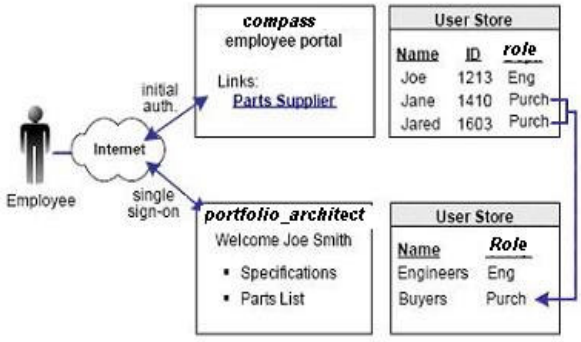

Figure 3. A use case for SAML credential exchange between the financial institution and the service provider

authorization. Once the user is authenticated and authorized to the Compass application, SiteMinder product passes on authorization information to the Compass application that uses that information to decide the functionalities of the application that will be available to the user. The information is retrieved from LDAP directory where authorization information for the user is maintained as an attribute within *Orgperson* object class. Depending on the authorization information, the user may be presented with a link to the *portfolio_architect* application. If the user stays within the *Compass* application and does not access the *portfolio_architect* link, the operation is as simple as accessing any other *eTrust® SiteMinder* protected web application or other resource in the financial institution's intranet, i.e., the *eTrust® SiteMinder* agent checks resource protection and challenges the user for credentials as necessary, and if the user authenticates and authorizes, a browser based *eTrust® SiteMinder* session is issued. By design, no SAML or web services component is invoked in such a use case. Figure 2 above shows the end-to-end SSO process that is implemented for the project.

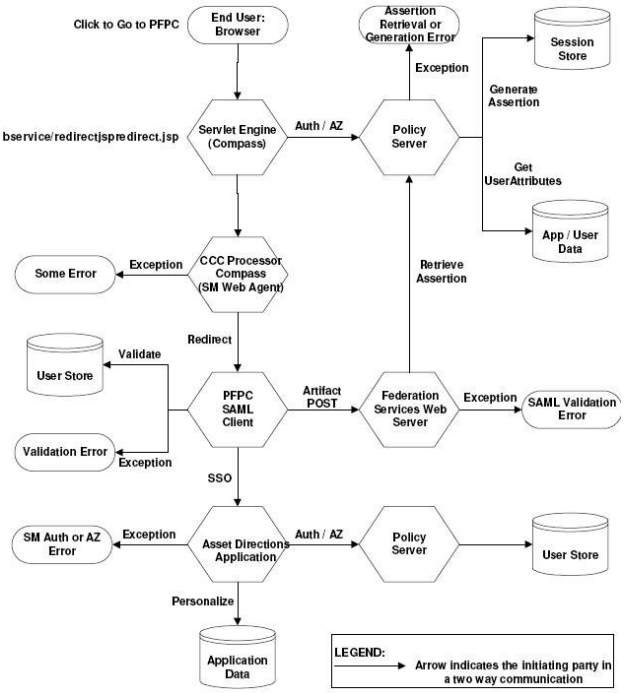

Figure 2. Functional Overview of the SSO Process

portfolio_architect SAML Single Sign On Process

When an authenticated Compass application user accesses the *portfolio_architect* link, a sequence of events leading to the generation of a SAML assertion occurs. These events are designed to simulate and short circuit the *eTrust® SiteMinder* SAML Affiliate Agent function since the integration does not contain a *eTrust® SiteMinder* SAML Affiliate Agent, yet the Web Agent Option Pack expects one to exist. First, the *portfolio_architect* link on Compass application actually points to a resource local to the application. This resource is a JSP application installed on the web server hosting the application.

(a) Application Session Management

eTrust® SiteMinder has its session management process that is well documented by the vendor, Computer Associate. The portfolio_architect application creates its own SiteMinder session based on the SAML Assertion it receives from the financial institution; a user who logs into Compass

Received September 19, 2008

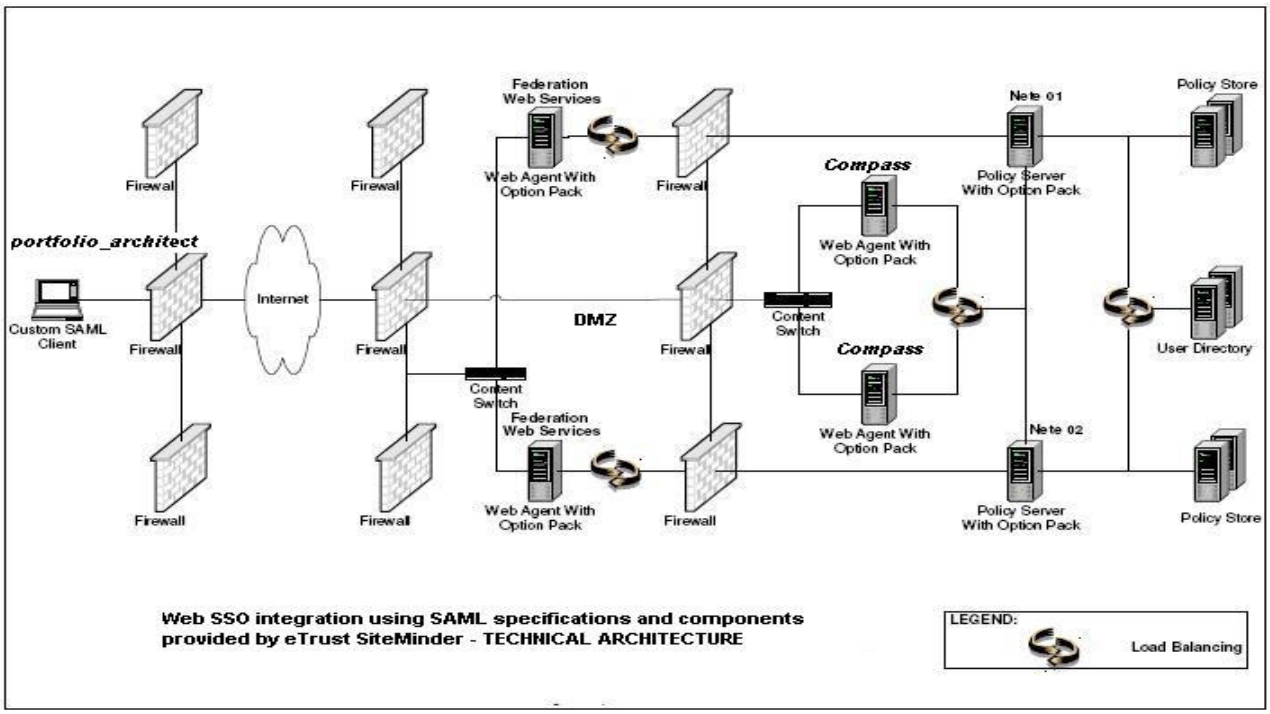

Figure 4. Technical Architecture of Web SSO Integration

application and SSO's to portfolio_architect application will have two independent sessions. The two sessions are independent and maintained using encrypted cookies. This scenario posed some problems from a user experience perspective since each application session may terminate before the other. If, for example, the user session at Compass application times out, it would be natural to assume that the portfolio_architect session would be terminated as well since the Compass session is the session of origin. Even worse, a user who terminates her session at Compass without terminating their *portfolio_architect* session will remain logged in at *portfolio_architect* application contrary to natural expectations. The SAML standard anticipates these issues by defining notification and session management services. The SAML Assertion Producer is responsible for providing a service that SAML Clients may query to find out whether a particular originating session is valid or not.

3.3 Federation Use Case and Information Architecture

A use case is a technique for capturing functional requirements of systems and systems-of-systems. According to Bittner and Spence [2], "Use cases, stated simply, allow description of sequences of events that, taken together, lead to a system doing something useful". Each use case provides one or more *scenarios* that convey how the system should interact with the users called actors to achieve a specific business goal or function. A typical use case for an employee at the financial institution trying to SSO into *portfolio_architect* application is described below. A user authenticates to the financial institution's compass application and clicks a link to access *portfolio_architect* application at the service provider. Because the user is an employee at the financial institution, they are taken directly to the specific module of the *portfolio_architect* application depending on user rights/roles of the user in the *portfolio_architect* application and the context or function he/she was using within the *compass* application without having to sign in.

When an employee of the financial institution authenticates to *compass* and clicks a link to access *portfolio_architect* at the service provider. Additional attributes, such as user name are passed from the financial institution to the service provider (also called trade partner) to personalize the interface for the individual user. The service provider does not want to maintain user identities for all employees at the financial institution, but access to sensitive portions of the *portfolio_architect* application must be controlled. To do this, the service provider maintains a limited number of profile identities for users within

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
        <ns1:Request IssueInstant="2005-04-28T16:39:35Z"
                MajorVersion="1" MinorVersion="0"
                RequestID="NXwkgSFUK+U0JvSobrw5Jf8OZ0w="
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:schemaLocation="urn:oasis:names:tc:SAML:1.0:protocol
                http://www.oasis-open.org/committees/security/somedoc.xsd"
                xmlns:ns1="urn:oasis:names:tc:SAML:1.0:protocol">
        <ns1:AssertionArtifact>AAFafJoGMG5pOAf8lJ/HFl7JeDYA7T
                VFQUlaRFNyNWpGemNVL0xsZGxMUjJjRUFaND06NWZlMzI
                3MDhiNWJkODBhOQ==</ns1:AssertionArtifact></ns1:Request>
   </soapenv:Body>
</soapenv:Envelope>
```

Figure 5. Sample SOAP request for SAML assertion (Artifact)

Received September 19, 2008

portfolio_architect application. Figure 3 illustrates the simple use case. One profile identity is maintained for employees at the financial institution for compass application and the other profile identity is maintained at service provider. When an employee of the financial institution accesses *portfolio_architect* from within compass, user attributes are sent in a secure manner to *portfolio_architect*, which uses them to determine what profile identity should be used to control access.

3.4 The Infrastructure and Technical Architecture

This section of the paper describes the technical components of the *eTrust® SiteMinder* product that has been leverage by the financial institution for Federation Security Services solution for the case study as mentioned in section 4.1, above. Here in discussion in this section, IdP (for Identity Provider) site is the web application that initially authenticates the user and asserts security information, such as role information, personalization parameters and authorization levels, of the user to the application (this target application is referred to as SP – Service Provider) that user single signs on to. The IdP site is also the SAML producer (*Compass application in this case study)* and SP site SAML consumer (*portfolio_architect*). This section also provides an overview of the system architecture of our model for ontology-based management of knowledge artifacts using a P2P approach. Figure 4 illustrates the different layers illustrating different technical components and their placements in the whole layout. The following sub-sections describe the particular layers and components in more detail.

3.4.1 SAML Assertion Generator

The SAML assertion generator creates an assertion for a user who has a session at a producer/IdP site - *Compass*. When a request for a SAML assertion is made, the *eTrust® SiteMinder* Web Agent invokes the SAML assertion generator, which creates an assertion based on the user session and information configured in the policy store. The assertion is then handled according to the authentication profile or binding configured. The 2 profiles are *SAML artifact profile/binding,* where an assertion is placed in the *eTrust® SiteMinder* session server and a reference to the assertion is returned to the *eTrust® SiteMinder* Web Agent in the form of a SAML artifact; and *SAML POST profile/binding,* where an assertion is returned via the user's browser as a SAML response embedded in a HTTP form.

3.4.2 SAML Authentication Schemes

SAML specification has support for three authentication schemes: SAML 1.x artifact, SAML 1.x POST and SAML 2.0. Each *eTrust® SiteMinder* SAML authentication scheme enables a site to consume SAML assertions. Upon receiving an assertion, the authentication scheme validates the SAML assertion, maps assertion data to a local user, and establishes a session at a consumer/SP site. One of the critical features of the SAML authentication schemes is to map remote users at a producer/IdP to local users at the consumer/SP.

3.4.3 Federation Web Services

The *eTrust® SiteMinder* Federation Web Services (FWS) application is installed on a server that has a connection to a *eTrust® SiteMinder* Policy Server. The Federation Web Services and the *eTrust® SiteMinder* Web Agent support the standard SAML browser artifact protocol and the SAML POST profile protocol. The Federation Web Services application includes services as detailed in the Table 1, for SAML 2.0 specification support.

3.4.4 SAML Affiliate Agent

The SAML Affiliate Agent enables businesses using the *eTrust® SiteMinder* Policy Server and *eTrust® SiteMinder* Web Agent to act as a main portal and share security and customer profile information with affiliated partners. The affiliated partners use only the SAML Affiliate Agent. The *eTrust® SiteMinder* SAML Affiliate Agent only supports SAML 1.0. The SAML Affiliate Agent is a stand-alone component that provides single sign on and session management capabilities to a consumer site that does not use the SiteMinder Policy Server and Web Agent. The consumer site, or affiliate, does not maintain identities for users at the producer, or portal, site. The affiliate site can determine that

Service	Description
Artifact Resolution Service (SAML 2.0)	An Identity Provider-side service that corresponds to the SAML 2.0 authentication using the HTTP-artifact binding. This service retrieves the assertion stored in the SiteMinder session server at the Identity Provider.
Assertion Consumer Service (SAML 2.0)	A Service Provider component that receives a SAML artifact or an HTTP form with an embedded SAML response and obtains the corresponding SAML assertion
Single Sign-on Service (SAML 2.0)	This service implements processing for an Identity Provider to process an AuthnRequest message and gather the necessary SP configuration information to authenticate the user, redirect the user to the Web Agent to authenticate, and invokes the assertion generator to obtain an assertion that is passed back to the Service Provider.
Single Logout Service (SAML 2.0)	This service implements processing of single logout functionality, which can be initiated by an Identity Provider or a Service Provider.
Identity Provider Discovery Service	This implements SAML 2.0 Identity Provider Discovery Profile and sets and retrieves the common domain cookie. An IdP requests to set the common domain cookie after authenticating a principal.

Table 1. eTrust® SiteMinder Federation Web Services

Received September 19, 2008

the user has been registered at the portal site, and optionally, that the user has an active SiteMinder session at the portal site. Based on affiliate policies configured at the portal, information can be passed to the affiliate and set as cookies or header variables for the affiliate web server. The SOAP request for assertion from the affiliate agent is done using the received artifact. Figure 5 shows a typical SOAP request for the assertion to the identity provider.

Figure 6 shows how different technical components as covered in this section interact with one another. In the figure, we see that both the ends – SAML producer and consumer – use *eTrust® SiteMinder* components for Identity federation which provides for seamless and easier integration due to the product design. Though, the SP uses on SAML affiliate agent of the product suite that comes cheaper than having to buy the whole suite like IdP did.

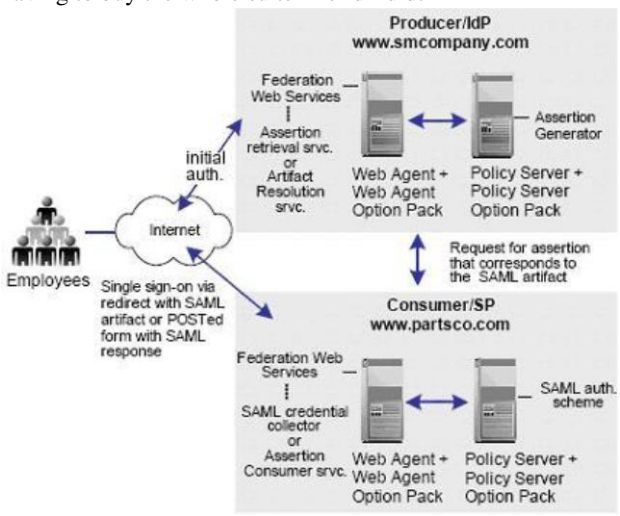

Figure 6. Interaction amongst technical components

4. Security and Privacy Considerations

The potential benefits of the federation project at the bank include facilitating core business models, increasing security and control, achieving efficiencies, simplifying the user experience and creating a scalable solution that allows the for future federated partners. It was also noted during interviews that federated identity allows addition of new applications. This assists in bank's future directions to position itself to generate revenue opportunities by helping businesses to acquire new customers and to enrich the value of client relationships. Security and control was stated as both one of the major expected benefits and one of chief concerns. We conducted separate interviews to understand the security dimensions. Most parties will accept some level of risk as part of the cost of doing business, but the benefits must be seen to outweigh it. Organizations must avoid complexity for the sake of complexity and start simple, creating a template for the next project using open standards wherever possible. Based on interviews, with 4 team members of the team, including 2 security analysts, 1 security manager and one technology support personnel, on security considerations for the project, we determined that their security related evaluations and concerns could be categorized into 5 broad dimensions as shown in the Figure 7. Each of the considerations as brought out during our discussions with the team is presented next.

4.1 Isolated Secure Infrastructure and Policies

As in the case of SAML implementation at the bank, the users log into an intranet application, *Compass,* by authenticating against corporate directory services. They gain access only to resources within the bank's firewall. They also need access to an application, *portfolio_architect* that is hosted over Internet and provided by a third-party service provider. Because the bank and the service provider did not (prior to the SAML project) federate their identity infrastructures, users have to log into the Internet site whenever they follow the link from Compass to Portfolio_architect. The problem aggravates when they also had to re-enter some of the information that is already available in compass, into portfolio_architect. Even if it were practical, the bank has no desire to put its proprietary information or user databases inside each of the partner they use applications of. The solution was to federate the identity systems. In that scenario, when users followed the link to the *portfolio_architect* application, the *compass* and *portfolio_architect* would automatically and securely exchange identity information. The user's identity would be matched with a record at the service provider, thereby providing direct access without a separate login. By implementing the SAML project, the distributed, heterogeneous architecture of the current IT environment was retained. The security policies could be enforced at the bank within it's own infrastructure, while the SSO mechanism suggested by *Liberty Alliance* is limited to supporting distributed authentication and not specifying and enforcing access control policies.

4.2 The Problem of Trust

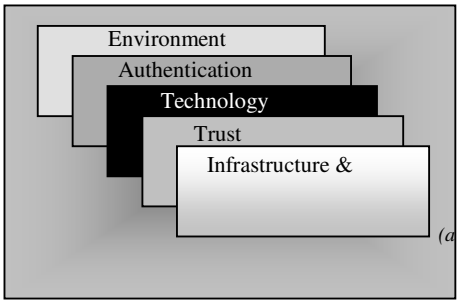

Figure 7. Security Considerations for the SAML Deployment

Federation defines processes and supporting technology to cooperatively link disparate identity stores together through higher-level mechanisms. For federated identity trust relations between parties need to be established. In an ad-hoc federation, trust is established one bilateral agreement at a time. Federated identity cannot establish trust—it can only communicate it. Bank's team realized that digital identities could be strongly authenticated and thus authorized for high-value online transactions across identity domain to the

Received September 19, 2008

Attack	Description	Impact	Probability
Replay Attack	The SAML Single Sign-on profile can be broken by hijacking the connection and replaying the encrypted redirect to the service provider. Details on this technique are described in [26]. This can happen when user's browser the service provider site can be observed and intercepted. This attack has low probability of being exploited, though if happened can result in severe impact.	*High*	*Very Low*
Man-in-the-Middle Attacks	This attack uses the well-known weakness that an attacker who modifies the Domain Name Service (DNS) can impersonate to the user's session. Here, in a man-in-the-middle attack the attacker acts as a proxy between browser and service provider site by breaking DNS. The attacker can impersonate the DNS entry of site of the service provider to the user's browser until it obtains unused SAML artifacts. The details of technique of man-in-the-middle attacks are described in [25] and [28]. The same attack can also be launched for any authenticated user of site of the service provider.	*High*	*Very Low*
HTTP Referrer Attack	This attack allows an attacker to provoke an information leakage of valid SAML artifacts. It uses the Referrer Tag of HTTP (see [27]) to obtain unused SAML artifacts. This attack can be carried out by tapping access channels and intercepting arbitrary connections from the user's browser to the service provider site. Again, it was determined that probability of this attack is very low, given the assumptions around the feasibility of the attack.	*Medium*	*Very Low*

Table 2: SAML related security threats

service provider by incorporating business, legal, and social processes to the software engineering issues that they were already dealing with. The federation of the project in the case study is an ad-hoc federation with one partner, where the trust relationship is created between the bank and the service provider. Going forward the bank anticipates to move to hob-and-spoke model where it will have more service providers connected through the same, though scaled, SAML infrastructure. The trust was established through agreements with the network and a common foundation that apportions liability. Bank has established process and procedures for evaluating and deciding what level of security precautions and privacy protections are sufficient, depending on the nature of the business and then to negotiate baseline operational agreements with partners. However, trend in the financial industry is to limit their identity interchanges to already-established federations, either through bilateral arrangements with existing business partners or through industry-specific clusters.

4.3 Risks: Need for stronger authentication

The primary concern as mentioned by the security team at the bank was that an attacker who obtains the primary password to *compass* application will also have access to all federated systems. The option to mitigate arising risks was to use of strong authentication technology changed the threat landscape. Some of countermeasures include:

Using strong passwords and limiting unsuccessful logon attempts for the primary logon.

Augmenting the application logon with strong authentication, such as a smart card or OTP token. This will reduce the risks of attacks against primary password data and keyboard logging of the primary password.

Risks can be further mitigated by requiring the target system, portfolio_architect, to use the strong authentication method when users log in the system directly.

4.4 Technology specific risks

The security team at the bank researched the SAML specifications and implementation specific technology risks. They concluded that these threats were present and while impact could be severe, the probability of exploit was low enough for the related risks to be accepted. The importance review of technology implementation is also echoed in the SAML specification document:

> *"Before deployment, each combination of authentication, message integrity, and confidentiality mechanisms should be analyzed for vulnerability in the context of the deployment environment."*

Their thorough analysis of the protocol specifications uncovered a few flaws that can lead to vulnerable implementations. Some of the attacks that were identified are *replay attack*, *HTTP referrer attack* and *man-in-the-middle attack* as presented in Table 2. The SAML SSO specification (version 1.1) does not prescribe how to use SAML assertions, except for the fact that an assertion must contain information, which allow the destination site to verify the identity of the user. The formats of the messages exchanged in the SAML Single Sign-On protocol are in form of XML elements; however, only a few of those are mandatory thereby leaving a lot of security decisions to the implementation.

4.5 Environment Security and Protection

The identity network (point-to-point) implemented by the bank provided an environment suited to protecting the privacy of personal information online. The identity is asserted through SAML assertion and there is limited access to personal information of users at the bank. As a result, the service provider does not have a complete view of any individual's identity information. The nature of the identity network ensured a secure operating environment for the bank's users. The policy-based privacy protections that are established and enforced by the identity network that shield the bank from the potential costs, including fines, legal

Received September 19, 2008

awards, and damaged reputation of failures to protect privacy. By creating a controlled environment, the bank's identity network mitigates the risk of fraud or security breaches and reduces the likely damages of any breaches that do occur. The bank also has designed and implemented monitoring, certification and tracking of its users, which is driven by corporate security policies.

5. Analyses, Discussions and Conclusions

Identity and access management is essentially a means of finding an efficient, manageable, auditable and secure way of connecting users or processes to enterprise resources. Federation fits into the overall identity management scheme by attempting to limit the management burden caused by external identities. The fewer times a specific identity must be ''managed," the more efficient the entire system will be. The federation technology creates or gathers the trust assertions that must be made when an internal user wishes to access an external resource or vice versa. Federation can, therefore, be viewed as an extension of identity management principles beyond the borders of the enterprise. Its goals extend well beyond merely increasing convenience for users of resources, to minimizing the costs of, and management requirements for, identity in the connected world. We believe that identity federation is crucial for advanced identity management and Web services. Implementing federated identity management can save costs and add user convenience. However, cost savings tend to be small and are more often indirect, rather than hard monetary savings.

Key Findings and analyses of cases: Evidence from the case study

Some of the key findings of the case study can be summarized as follows:

1) The biggest benefit for federation is user convenience in terms of reduced sign-on.
2) Most of the cost savings in the above federation is estimated to accrue to the identity consumer, the service provider, and not to the identity provider, the financial institution.
3) For the financial institution, the many investments involved in implementing federation offset any cost savings because it was the first federation project for the company. But future implementations will cost significantly less than the one in case study.
4) Executives and managers at the financial institutions rationale that the investments in federated identity and access management should be solidly rooted in business process improvements rather than cost savings.

The identity consumer can avoid the not-so-insignificant cost of provisioning external user identities and the cost of a directory to hold those identities. This savings is most common in federations that pass only roles between parties. However, other applications may require accounts to be linked across the federation. That means a user accessing the federated application may still need to be provisioned — for example, with account numbers and other account data — into the identity consumer's application repository. Therefore, there still may be identity consumer security administration costs for a new user at the application level. Gartner [27] estimates that identity consumers can save approximately 30 minutes in security administration labor per each user identity addition. This will translate to a savings of $120,000 for the financial institution if it were the SAML consumer.

1) Analysis: Case for improved accountability

The case for improved accountability was held from the financial services perspectives as the eTrust® product has robust accounting and auditing capabilities. With the service provider also using the same product, the auditing was holistic and all the transactions are logged with enhanced audit trail. We also learned that despite advancements in federation standards and technology, creating a federation still presents many of the same process, control and liability issues that were common with efforts to join disparate public-key infrastructures. Some of the key issues that were handled by the financial institution and the service provider was that each federation participant must trust the other participants to perform its identity management functions and protect issued-identity credentials. Based on opinions of the team members, it was clear that developing participation agreements and establishing the necessary trust can be a daunting challenge. Federated identity management technologies improve security by controlling access on an operation-by-operation basis and providing a detailed audit trail while enabling access for partners and customers.

2) Analysis: Case for Strong Authentication and Federated Single Sign On

From a technical standpoint, no significant risk is presented by providing single sign-on across domains, as long as the federation begins with authentication that is strong enough for the identified business needs and is built on the same protocols and the same security token format. For the project in the case study this was the case as initial authentication is based on complex password, which is more secure. However like in most standardized environments, most perceived risk lies in the trust relationship between the identity provider and the identity consumer. This was evident from the case study's project plan where major amount of time was assigned to understanding SAML consumer's environment and performing a SAS-70 audit. It is important to recognize that the financial institution provides identity information to the trusted partners (external service provider) and resource provider in "manual" form (for example, through lists of approved users). Both the enterprises in this arrangement had to consider trust agreements among themselves and the possible legal consequences of federation. However, based on our interviews we believe that people at financial institution also recognize that identity federation is merely an automated, perhaps real-time, version from the "manual federation"-based trust they have had all along.

Received September 19, 2008

Discussion Note: The introduction of a multi-protocol architecture — for example, one based on both SAML and WS-Federation — adds complexity and can reduce functionality. A serious concern related with identity management, whatever solution is chosen, is the risk of identity theft. Despite guidelines have been provided on how to protect against identity theft [10], not many identity theft protection solutions have been proposed so far. Security prevents theft and impersonation when the identity attributes are used and privacy protects against the disclosure of identity when the user has the right or expectation of anonymity [11]. Some of techniques that can be employed are zero knowledge proofs [5][19] and distributed hash tables [15]. Multiple weak identifiers may lead to a unique identification [28]. The three most important questions to be answered in a risk analysis, during initial establishment of trust agreements, are the following [25]:

How will each participating organization confirm the identities of individual internal users before issuing them credentials that can be used, internally and externally, as part of the federation?

How strong must the online authentication and technology be within each organization (for example, will a user ID and password be good enough to assuage risk concerns, or will a stronger form of authentication be required)?

Which organizations will be liable (and to what extent) if one participating organization's identity credential is used to commit fraud, or to improperly access the resources of another participating organization?

3) Analysis: Case for user convenience

User convenience is one of the major benefits of the federation for the financial institution. Besides, Increased user-friendliness (fewer clicks, easier account and password management, easier discovery of applications, automated service-oriented messaging, seamless integration) team members at the financial institution believe that Web SSO has helped them boost data transfer and content revenues. The biggest benefit for federation is user convenience in terms of reduced sign-on. The project team members mentioned that the users' experience, of the system in terms of convenience in automatically logging into or out of the system (Single Sign On and Single Log Out) and not having to remember another set of credentials, has improved. The users particularly liked the feature where transaction information and other details are also transferred from *Compass* to *portfolio_architect* behind the scenes as attributes in the SAML assertion. Also, initially there is one fewer step to register account with the federated application.

4) Analysis: Case for reduced costs and increased productivity

Most of the federated identity management (FIM) cost savings accrue to the identity consumer and are largely opportunity costs and not hard monetary savings. There are no cost savings for identity providers — they are still responsible for enrolling, administering and authenticating their own end users. This is also consistent with the case study of this paper, where similar opinions were expressed. But also was noted that there are huge economies of scale for the Identity provider – the financial institution in our case - where adding more trusted partners would cost significantly less than the first set-up. In a federation, for the provider of the application (the identity consumer), savings can accrue in two areas: reduced security administration costs and reduced help desk call volume associated with password-reset calls. Negligible savings are associated with users' reduced time to sign into multiple applications, and monetary savings are not typically calculated. However, any cost savings has been offset by a number of other investments in federation that include the software, hardware, integration and maintenance costs of the federation solution incurred by both sides of the federation partnership, the costs associated with the auditing of partner identity management practices and the fee for using a third-party identity provider, and the cost for switching if the business relationship with the first provider sours within the federation community, or if they go out of business.

Discussion Note: The ideal arrangement is what is sometimes called "federation in both directions," in which each partner manages some resources for the other's users, and both partners, therefore, realize some value from federating identities. There are no security administration savings for identity providers (sometimes a third-party service that charges a fee for the service) because they remain responsible for enrolling, administering and authenticating the user prior to them "federating" to the application. The cost of verifying an identity (the process known as identity proofing) can be quite high, especially when using third-party service providers; for example, credit rating organizations [27]. Because an identity consumer does not maintain user identities for its federation partners, federation reduces IT service desk costs for password-reset calls. To monetize the savings, the identity consumer must be able to reduce staff or reduce the number of calls to a customer service center or IT service desk if the agreement includes a cost per call taken. Otherwise, the cost savings are soft and associated with staff being able to do other work (referred to as opportunity costs).

5) Analysis: Case for IAM readiness for adoption of industry standards

Most cases of single-sign-on use are implemented using Web access management tools that, in turn, can be augmented with federated identity gateways provided by the Web access management (WAM) vendor or an independent vendor. The implementation of the case study was done using OASIS SAML specifications after deliberate considerations on industry trends and future inter-operability. While, most of the industry has converged on SAML as the identity federation protocol of choice Microsoft and IBM have developed a competing standard, WS-Federation, and Microsoft has implemented WS-Federation in Active Directory Federation Services (ADFS), which now included with Windows Server 2003 R2. This was one of the concerns of both the enterprises while they were getting into the federated relationship.

Received September 19, 2008

Discussion Note: While WS-Federation supports the SAML token format, it does not yet support the SAML protocols. We are seeing signs that this can create an interference pattern in organizations that have committed to using SAML but have lines of business or agencies that use Microsoft infrastructure for identity management and wish to participate in a federation. Two good examples of active and growing federation frameworks are the *shibboleth* and *United States E-Authentication Federation* [22]. Shibboleth is standards-based, open source middleware software that provides Web Single SignOn (SSO) across or within organizational boundaries [21]. Organizations that plan to adopt Liberty Alliance protocols based on the Security Assertion Markup Language (SAML) token format and protocols may have business partners with established commitments to Microsoft and WS-Federation protocols.

6) Analysis: Case for commercial products against open source solutions

The team at the financial institution believes that commercially supported products make for good candidates for enterprise grade deployments. However, the success of open-source software (OSS) such as the Linux, Apache, MySQL and PHP (LAMP) platform shows the real option that OSS offers. Identity and access management (IAM) solutions — which share many generic infrastructure characteristics with LAMP software — have proven their ability to attract sufficient skills to sustain a thriving development community. OSS IAM is now a real option for users that possess the integration resources. It is still very unclear on real benefits of open source in light of the fact that resources required to implement and support such products are much higher than commercial products. We believe that given the level of information that the team had, going with Computer Associate's product was a better decision. However there have been recent developments in space of OSS in IAM as discussed in the following note that puts OSS in better light.

Discussion Note: IAM solutions fall largely into the infrastructure category and include OpenLDAP, MIT's Kerberos and Yale's Central Authentication Service (CAS), among many others. More recently, we have seen specific community-backed OSS such as the identity federation solution Shibboleth. In this case, the community is higher education (the Internet2 Middleware Initiative) that funds and coordinates development efforts. Even vendors are backing the OSS trend in IAM, the most recent example being Sun's release of parts of its IAM suite into the OSS sphere. These efforts make a strong case that there is a critical mass of skills available to support OSS IAM solutions, making it a real option for IAM implementers. The necessary skills to support OSS IAM are becoming more available, making these solutions a real option for user shortlists. Nonetheless, a strong in-house development and integration team is a must for OSS IAM implementations.

7) Analysis: Case for opportunities for increased revenues

By functioning as an Identity Provider, the financial institution has created a re-usable and scalable business model around password and identity management. The technical implementation, with a blend of own and third party offerings, enables a business ecosystem of the financial institution, where, for instance, revenue-sharing models and co-marketing campaigns are methods that can help to increase revenues. Having set the infrastructure and competence for complex level identity federation initiatives, the financial institution has positioned itself to avail any opportunities to federate with other business partners with less work. Increasing federated partners will also translate to better and newer services to its customers for the Identity provider.

Discussion Note: The applications that federation partners wish to federate may not yet be Web-enabled, and it may be impossible, or too difficult or costly, to change these applications.

References

[1] B. B. Bhansali. Man-in-the-middle attack - a brief, February 2001.

[2] K. Bittner and I. Spence. Use Case Modelling, Addison Wesley, 0-201-70913-9.

[3] S. Cantor, F. Hirsch, J. Kemp, R. Philpott, E. Maler, J. Hughes, J. Hodges, P. Mishra, and J. Moreh. Security Assertion Markup Language (SAML) V2.0. Version 2.0. *OASIS Standards.* http://www.oasisopen.org/committees/tchome.php?wg abbrev=security

[4] P. Dave and N. Moussa. TCP connection hijacking, 2002.

[5] U. Fiege, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing*, pages 210–217, New York, NY, USA, 1987. ACM Press.

[6] R. T. Fielding, J. Gettys, J. C. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. RFC 2616: Hypertext transfer protocol – HTTP/1.1, June 1999. Status: Standards Track.

[7] J. Hodges and T. Watson. Liberty architecture overview v 1.2-03. *Technical report*, Available at www.sourceid.org, 2003.

[8] Identity-Management. Liberty alliance project. http://www.projectliberty.org.

[9] Internet2. Shibboleth. http://shibboleth.internet2.edu.

[10] I. T. Management. http://www.identitytheftmanagement.com/.

[11] K. Klingestein. Emergence of identity service providers, 2002.

[12] Liberty Project. http://www.projectliberty.org/

[13] P. Madsen, Y. Koga, K. Takahashi - Proceedings of the 2005 workshop on Digital identity, Federated identity management for protecting users from ID theft, Workshop On Digital Identity Management,

Received September 19, 2008

Proceedings of the 2005 workshop on Digital identity management, Fairfax, VA, USA, Pages: 77 – 83, 2005.

[14] E. Maler, P. Mishra, and R. Philpott. Assertion and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. Version 1.1. OASIS Standards. http://www.oasisopen.org/committees/tchome.php?wgabbrev=security

[15] G. S. Manku. *Dipsea: a modular distributed hash table*. PhD thesis, 2004. Adviser-Rajeev Motwani.

[16] C. Meadows. Analyzing the needham-schroeder publickey protocol: A comparison of two approaches. In *ESORICS: European Symposium on Research in Computer Security*. LNCS, Springer-Verlag, 1996.

[17] N. R. C. of the National Academies. *Who Goes There?Authentication Through the Lens of Privacy*. The National Academies Press, Washington, D.C., 2003.

[18] E. Norlin and A. Durand. Whitepaper on towards federated identity management. In *Ping Identity Corporation*, 2002.

[19] C. P. Schnorr. Efficient identification and signatures for smart cards. In *CRYPTO '89: Proceedings on Advances in cryptology*, pages 239–252, New York, NY, USA, 1989. Springer-Verlag New York, Inc.

[20] R. Semank. Internet single sign-on systems.

[21] Shibboleth, http://shibboleth.internet2.edu/

[22] *United States E-Authentication Federation*, http://cio.gov/eauthentication/

[23] W3C Note: Simple object access protocol v 1.1. *Technical report*, Available at www.w3.org, 2000.

[24] W3C note: Web services description language (WSDL) v 1.1. *Technical report*.

[25] R. Wagner and G. Kreizman, "Frequently Asked Questions About Federated Identity", *Gartner Research Report* (ID: G00139097) , 25 April 2006

[26] T. Watson. Liberty ID-FF implementation guidlines v 1.2.02. *Technical report,* Liberty Alliance Project, 2003.

[27] R. J. Witty, R. Wagner, G. Kreizman, Federated Id. Management Provides Limited Cost Savings, 6 October 2006, *Gartner Research Report* (ID: G00143328)

[28] D. Woodruff and J. Staddon. Private inference control. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 188–197, New York, NY, USA, 2004. ACM Press.

Author Biographies

Manish Gupta is a PhD candidate at State University of New York at Buffalo. He also works full-time as an information security professional in M&T Bank, Buffalo. He received an MBA from SUNY-Buffalo (USA) and a bachelors degree in mechanical engineering from I.E.T, Lucknow (India). He has more than a decade of industry experience in information systems, policies and technologies. He has published 3 books in the area of information security and assurance. He has published more than 30 research articles in leading journals, conference proceedings and books including DSS, ACM Transactions, IEEE and JOEUC. He serves in editorial boards of 7 International Journals and has served in program committees of several international conferences. He holds several professional designations including CISSP, CISA, CISM, ISSPCS and PMP. He is member of ACM, IEEE, INFORMS, APWG, ISACA and ISC2.

Dr. Raj Sharman is an assistant professor in the School of Management at State University of New York at Buffalo. He received his Bachelors degree in Engineering and Masters Degree in Management from the Indian Institute of Technology, Bombay, India. He also received a Masters in Industrial Engineering, and a Doctorate in Computer Science from Louisiana State University. His research interests are primarily in the field of Information Assurance, Conceptual Modeling and Ontology, Extreme Events Mitigation and Data Mining. He is a recipient of several grants, both internal and external. These include grants in the areas of Information Security from NSF and AFSOR in the field of computer Security. His publications appear in peer reviewed journals and international conferences in both the Information Systems and the Computer Science disciplines. Dr. Sharman serves as an associate editor for Journal of Information Systems Security. His past work experience includes developing and managing Hospital Information Systems.

Received September 19, 2008