2012 International Conference on Industrial and Intelligent Information (ICIII 2012)
IPCSIT vol.31 (2012) © (2012) IACSIT Press, Singapore

Identity Federation Management to make Operational and Business Efficiency through SSO

Karunanithi. D [1+], Kiruthika Balu [2]

[1, 2] Department of Information Technology, Hindustan University, Chennai, India

Abstract The Federated identity management (FIM) is an arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group. The use of such a system is sometimes called identity federation. The Identity Federation is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials Today , many of us have multiple accounts for email, chat services, banking, favourite websites, etc. Many different services that we sign up for need a user name and password, so, the problem we face is that they all require, or tell us we need unique identities and passwords for each service. This is a problem for anyone with a poor memory and many people fall into the trap of using the same passwords for many services .Wouldn't it be convenient then if we could just use one, unique single sign on service to log in securely to our accounts, without needing to remember all these passwords? So that no matter how many services or passwords we need to use, we can just sign in once and not have to worry about it. The answer lies in a system called single sign on.SSO, it's one main login in which we store all our other identities. We need this so that we can be safe, yet still have access to the information we need with real security. It's always important to choose a good, strong secure password to protect yourself and keep yourself safe online. The single sign on solution is a good system as long as the sign on is secure with a strong password This paper provides a way the SSO is used to achieved by Identity Federation.

Keywords: Identity, Identity Management, Single Sign-On, Identity Federation

1. Introduction

Identity is the fundamental concept of uniquely identifying an object (person, computer, etc.) within a context. Many identities exist for local, corporate, and national domains. Some globally unique identifiers exist for technical environments, often computer-generated. Unfortunately, many identities now in use are insufficient for the business requirements of most corporations. The most obvious of these is identity for people. As an example, the US Social Security Number is not complete in identifying all employees, nor does it assure uniqueness [1].

Identity Federation solution involves in defining the identity of an entity (a person, place, or thing), Storing relevant information about entities, such as names and credentials, in a secure, flexible, customizable store. Making that information accessible through a set of standard interfaces, Providing a resilient, distributed, and high-performance infrastructure for Identity Federation and helping to manage the relationships to resources and other entities in a defined context.

2. Identity Federation

In Let's show the classical example of identity federation.A web user is a client with an airline company and has logged in into their website to book tickets for his business trip. After selecting and paying for the proper tickets, the client wants to book a car at his destination airport too. He clicks on the link provided by the airline company for renting cars. At this time the user is redirected to the car rental company and is logged in automatically.The end user can book his car as well. He didn't need to login anymore, because he already had done that with the airline company.

[+] Corresponding author. Tel.: + 91-9445753975
E-mail address: karunanithid@gmail.com

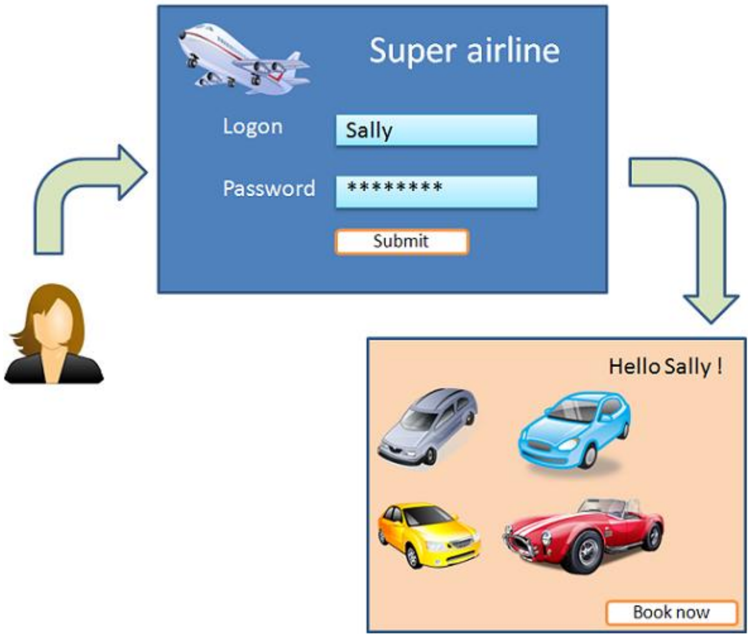

Fig1.Identity Federation

This automatic logging in by means of a trust relationship between the airline systems and the car rental company systems is called Identity Federation. So the car rental company is trusting the credentials of the user which were validated by the airline company.For the end user not having to login or register anymore is a major advantage and avoids loosing clients.From a technology perspective the protocols which are most commonly used for identity federation are SAML, Liberty Alliance, and WS-Federation.

3. Architecture of Single Sign-On

In the world of single sign on, many systems exist for users to assist them with managing their identities and passwords. Setting up and maintaining a single sign on system at the enterprise level could be costly. Fortunately there are open source SSO systems readily available. Specially designed for easy access and for those of user's tired of entering the same user and password tens of times daily on various applications, single sign on controls the access to related but still independent software systems. In simpler terms, user would only sign in once and be able to access any related systems without being nagged to enter your password and user id again and again.

The figure 1 shows when done browsing, just sign off and that's it, the user you have used is automatically signed out from the related systems user have used. By typing in any browser the main page of the SSO enabled software system user would like to use, type in user's, username and password and browse and shop away. Simple, easy and fast usage, plus a greatly reduced phishing success, due to the fact you wouldn't need to enter your password again and again without thinking.

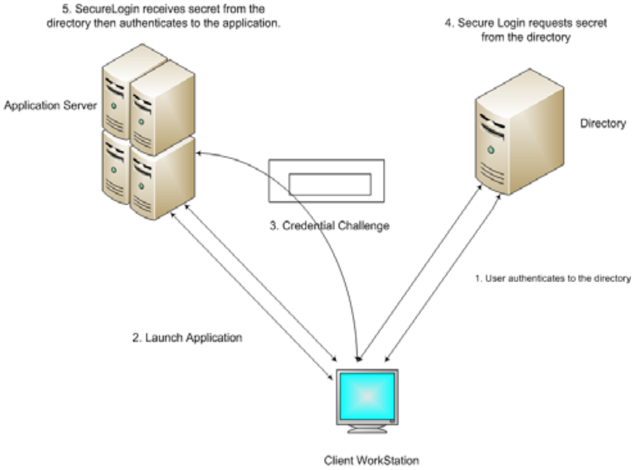
5. SecureLogin receives secret from the directory then authenticates to the application.
4. Secure Login requests secret from the directory
Application Server
Directory
3. Credential Challenge
1. User authenticates to the directory
2. Launch Application
Client WorkStation

Fig 2: Single Sign-On Process

4. Single Sign-On Components

Single Sign-On (SSO) is the means of passing users' credentials between applications without users having to authenticate each time they access another application--in essence a mechanism to seamlessly identify users across various identity domains. The following diagram explains the different components involved in achieving SSO.

The sign-on process involves:

1.The users (Internal/External) can access the application using normal HTTP request in the browser.
2.The browser sends the request for accessing the application/protected resources to the deployment container which holds the SSO component as well.
3.The Application logic intercepts all the request and checks whether a session token is embedded in a cookie. If yes, the logic component validates the token for SSO. Otherwise, the application directs the user to the login page to log in with the credentials, such as a user name and password, which the SSO component then verifies against the data in the identity repository

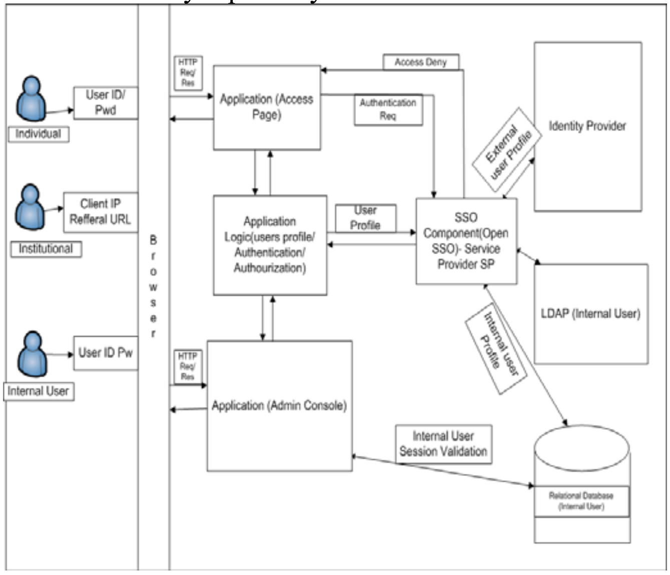

Fig 3: Single Sign-On Components

4.If authentication succeeds, the application establishes a session token and allows the access to the content requested, In addition, the application might create a cookie for the user's browser.
5. If authentication fails, the application denies the user access for the requested content.

5. Overcoming Issues and Challenges for Provision of Successful SSO

With the increasing number of logins faced by today’s IT system users, Single Sign-On has demonstrated that it can provide value added benefits to almost any environment. We can see that the technology as been evolving to a stage where it can now offer easy integration into existing and legacy systems as well as providing enhanced administration and security. Due to the many varied infrastructures that Single Sign-On may be applied to, it is almost impossible to generalize which solutions would be best suited for an average IT system. Integration of single sign-on should be considered carefully based on each individual environment. As a basic rule, a successful single sign on system should: 1.Meet the changing needs of large organizations. New software must be easily installed and configured for single sign-on. 2.Easily accommodate mobile users. Remote and roaming users must be able to access their Single Sign-On credentials and update them if necessary. 3.Provide ease of management, rapid deployment, and high availability. The single sign-on system must run efficiently, be easy for users to operate, and be easy for you to control and maintain.4.Employ industry standards and open architecture. The single sign-on system must be compatible with most existing software. 5.Be seamless to the user. The second time a user logs in to an application, the application should look the same as the first time. Subsequent attempts to open the application should involve no user interaction for authentication. 6.Be secure. The password storage and playback mechanism must not allow for stealing secrets. The usernames and passwords must be encrypted and stored in a secure database. 7. Be cost effective. The single sign-on system must save money and reduce the cost of ownership. 8. Extend to strong authentication. The single sign-on system should easily allow the addition of smart cards, authentication tokens, and biometrics.[2]

6. Process for Implementations

6.1. Using Federated Identity for Partner Site SSO

Federation establishes a standards-based method for sharing and managing identity data and establishing single sign-on across security domains, partner sites and organizations. By forming the trust of circle, it allows the 'Partner Site' to offer a variety of external services to the trusted business partners as well as corporate services to internal departments and divisions.

6.2. Federated services

A principal can have a defined local identity with more than one provider, and it has the option to federate the local identities. The principal might be an individual user, a group of individuals, a corporation, an institution or a user in the institution. A service provider is a commercial or not-for-profit organization that offers a web-based service such as a news portal, a financial repository, or retail outlet. Here Application can be considered as Service Provider.

An identity provider is a service provider that stores identity profiles and offers incentives to other service providers for the prerogative of federating their user identities. Identity providers might also offer services above and beyond those related to identity profile storage. For example, identity providers can be third party identity providers like Open ID, Athens, and Shibboleth etc.

To support identity federation, all service providers and identity providers must join together into a circle of trust. A circle of trust must contain at least one identity provider and at least one service provider.

Providers in a circle of trust must first write trust agreements to define their relationships. A trust agreement is a contract between organizations that defines how the circle will work. For example a protocol can be in place between all the subjects in the circle of trust like SAML 2.0 protocol.

6.3. Federation Management with OpenSSO Enterprise

Sun OpenSSO Enterprise provides a pluggable framework for implementing federated identity infrastructures. The Federation framework places no restrictions on the use of network technologies, computer hardware, operating systems, programming languages or other hardware or software entities. It is based on, and conforms to, open industry standards to achieve interoperability among different vendors on heterogeneous systems, and provides the facility to log identity interactions and erroneous conditions.

The following list describes some key features:

1.Exchange of credentials and security tokens across circle of trust partners for purposes of authentication and single sign-on.

2.Automatic federation of user accounts across multiple security domains.

3.Session management across authentication domains to determine when user interactions must be terminated.

4.Exchanges SAML security assertions among providers in a circle of trust.

5.Data management choices include an LDAPv3 directory (OpenDS, Sun Java System Directory Server or Microsoft Active Directory).

6.4. Virtual Federation

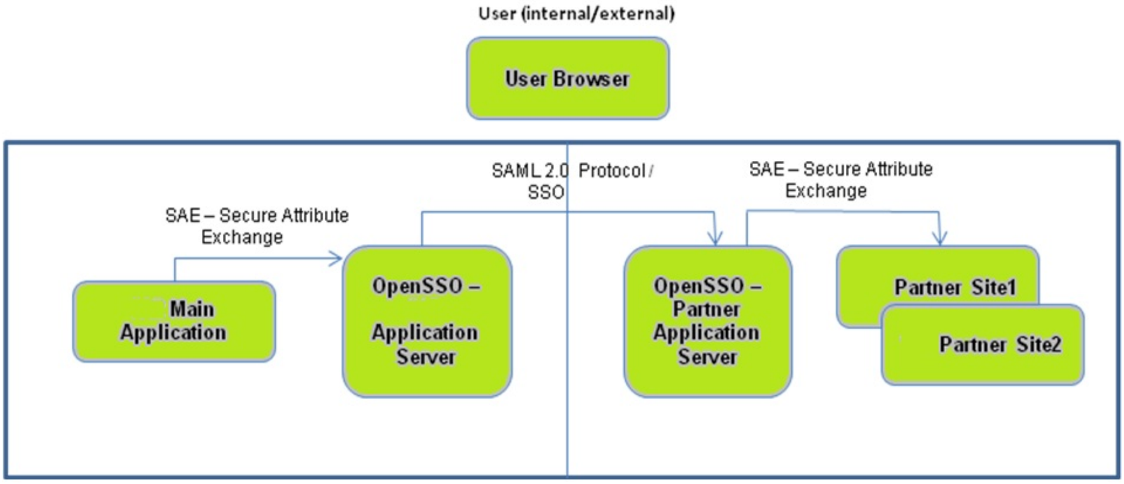
User (internal/external)
User Browser
SAML 2.0 Protocol / SSO
SAE – Secure Attribute Exchange
SAE – Secure Attribute Exchange
Main Application
OpenSSO – Application Server
OpenSSO – Partner Application Server
Partner Site1
Partner Site2

Fig4. Virtual Federation SSO Attribute Exchange Process

Sun OpenSSO Enterprise, tailored for identity federation and Web access management, tackles the issues with a new capability: virtual federation. Using this capability identity information (authentication, profile, and transactional attributes) can be pushed to the OpenSSO, which then transmits the data to external partners through standard federation protocols (SAML v2.0)

Currently, virtual federation only works with the following but will work with other federated protocols and profiles in the future:

1.SAML 2.0 browser-based transient federation and federated SSO

2.Browser-based HTTP GET and POST binding mechanisms of the SAML 2.0 protocol

Below is the Virtual Federation SSO Attribute Exchange Process.

6.5. Virtual Federation – Process

Transferring the user access from the main to any partner site can be achieved using OpenSSO with SAML v2.0 protocol. Below is the illustrative process flow of the user transition from main application to that of partner site.

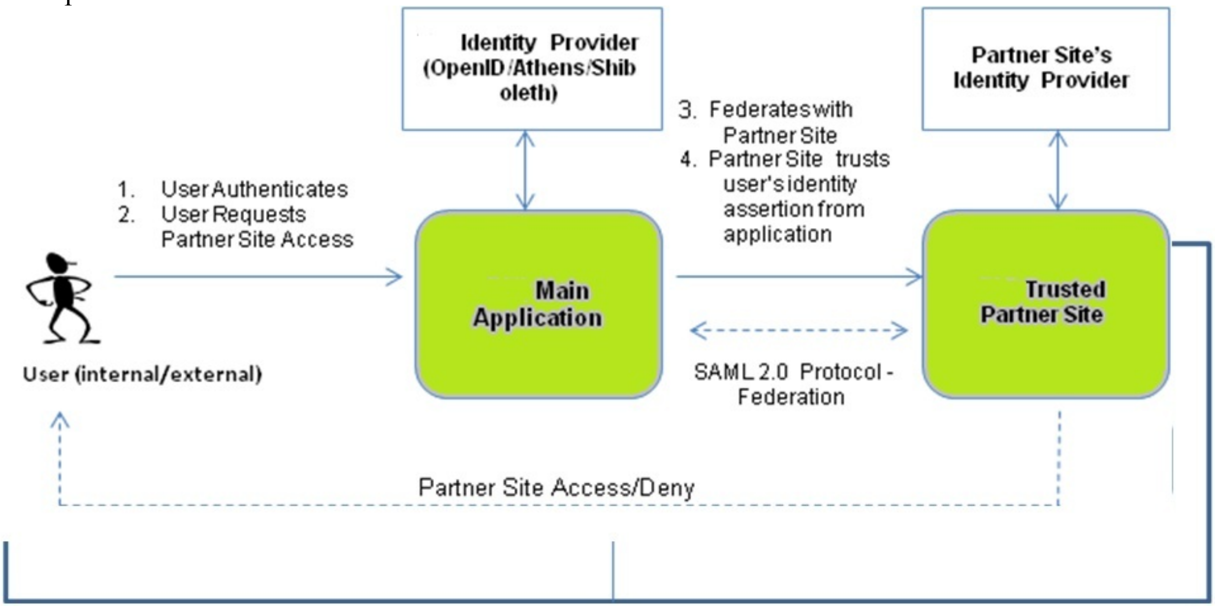
Identity Provider (OpenID/Athens/Shibboleth)
Partner Site's Identity Provider
3. Federates with Partner Site
4. Partner Site trusts user's identity assertion from application
1. User Authenticates
2. User Requests Partner Site Access
Main Application
Trusted Partner Site
User (internal/external)
SAML 2.0 Protocol - Federation
Partner Site Access/Deny

Fig5. Virtual Federation – Process

6.6. Virtual Federation – Process Flow

1.A transaction transmits authentication, identity, and transactional data to and from the main application (any organisation) and partner site through SAML 2.0 protocol.

2.When the user access the partner site link from the organisation's main application, to identify that user, the main application pushes the related user attribute and logical ID (transaction attribute) to the Partner Site using Secure Attribute Exchange (SAE) & SAML 2.0 protocol.

3.The Partner Site validates the user's authentication (single sign-on or SSO) credentials and receives the attribute payload, all from the same SAML assertion.

4.The user now can be accessed or denied the partner site information depending upon the authentication/authorization procedures.

6.7. Transferring From a Partner Site to another organisation

SSO is an access-control mechanism that enables users to log in and access multiple applications without having to log in again. SSO can be extended from the partner site to the organisation's main application. A user identity authenticated in the partner site can be extended to organisation 's application as well with out re-authenticating again in the organisation's main application. This type of SSO is called as Cross-Domain SSO (CDSSO).

6.8. Transferring From to a Partner Site

SSO can be transferred from to all other Partner sites. The user session created in the main application can be used to authenticate all other partner sites of , this can be achieved using OpenSSO configuration settings. All the trusted partner sites which are listed in the OpenSSO admin console can form a circle of trust and by pass the authentication process still user session lost

7. Conclusion

The Identity Federation solution consists of various software packages, often times coming from different vendors. Companies tend to select "best-of-breed" products that address five of the seven components of the identity federation infrastructure: directory, administration, directory integration, provisioning, and access control. The generalized application interfaces component is not included in the solution because it is custom developed after the software packages are selected. The generalized application interfaces component is not provided by any vendor, but is instead created by each company to address the specific identity management solution that is implemented. The ultimate goal of an identity management solution is to create federated identity systems so users can be effectively identified and provisioned across company boundaries. Using federated identities, information can be securely shared between companies, enabling employees to access another company's data without manually re-authenticating. This is made possible by leveraging Web Single Sign-On technology included in each company's identity federation solution.

8. Future Works

Federated identity systems "are the next logical evolution in authentication and entitlement system." however only after any company has the technology, infrastructure, and processes in place to effectively manage internal resources can your company begin to share and manage identity information with other companies [10]. Thus, the first step towards a federated identity system is to implement an identity management and federation solution in any company. The identity federation solution offers tangible results by increasing productivity and security while at the same time lowering the costs associated with trying to manage the identity chaos that has resulted from the influx of standalone applications. As the Internet continues to open new doors of business opportunity, it concurrently exposes the insecurities of corporate networks. Large enterprises are concluding that an identity federation solution, alongside an enterprise-wide security strategy, is necessary to ensure the confidentiality, integrity, and availability of critical resources.

9. Acknowledgements

My heartfelt thanks to my mother Yogamangalam. G for her divine blessings and to my father Dhandapani. A who is giving endless encouragement to go beyond boundaries of knowledge. My heartiest thanks to Dr. Paul Rodrigues who had sculptured me as I am now– Karunanithi.

I would like to convey my heartiest thank my unlces Dr.V.RAMADOSS and V.KALYANAM for their generosity and help have been a strong support and an inspiration to me from thousands of miles away for my education and also I thank my parent's G. Balumalliga who made my dreams come true for their everlasting support – Kiruthika.

10. References

[1] "Single Signon and single signout in Identity Management "by D.Karunanithi and Kiruthika Balu ,ICONSET2011.

[2] www.novell.com A White paper on *"Single Sign-on :Finding the best fit."*

[3] http://www.opengroup.org/dif/projects/im-scen /idmbs_1.pdf. " *An White paper by open group".*

[4] J. Kemp et al. Authentication Context for the OASIS Security Assertion Mark up Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-authncontext- http://docs.oasis-open.org/security/saml/v2.0/saml-authncontext-2.0-os.pdf.

[5] P.Mishra et al. *"Conformance Requirements for the OASIS Security Assertion Mark up Language (SAML) V2.0. OASIS SSTC*",March 2005. Document ID samlconformance- 2.0-os. http://docs.oasis-open.org/security/saml/v2.0/ samlconformance-2.0-os.pdf.

[6] S. Cantor et al." *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC"*, March 2005. Document ID saml-metadata-2.0-os http://docs.oasisopen.org/security/saml/v2.0/ saml-metadata-2.0-os.pdf.

[7] S.Carmody.Shibboleth *"Overview and Requirements. Shibboleth project of Internet2".* http://shibboleth.internet2.edu/docs/draft-internet2-shibbolethrequirements-01.html

[8] F. Hirsch et al. *"Security and Privacy Considerations for the OASIS Security AssertionMarkup Language (SAML) V2.0. OASIS SSTC*", March 2005. Document ID saml-secconsider-2.0-os.