

Important Considerations for Single Sign-On Solution

¹Khalid Bashir and ²Saman Asif

^{1,2}School of Agriculture and Resource Economics,
University of Western Australia

Abstract - Single Sign-On is a central component of the centralized architecture of an organization. In IT, there is a slight misconception that it is expensive to deploy an enterprise single sign-on solution that is secure, scalable and importantly well-suited to meet variety of applications in place. Conversely, there is ongoing awareness rising in IT management about the fruitfulness of its implementation. Over the years, many successful implementations of intranet single sign-on have been achieved. Scaling them to internet level is still an issue. This paper is related to similar domain; provide a single sign on that is equally secured and compatible to match the environment versatility at enterprise and internet level. The paper begins with a comprehensive high level summary of the single sign on. We then swim through the knowledge of some issues that are often unintentionally overlooked when designing and making choice of SSO products. And finally the reader will take a ride through the solutions of ensuring a complete product. This paper aims to provide guidance to professionals struggling to supply their organization a secured single sign on solution making them easy to understand what is actually required in a beneficial SSO. The target audience is the solution designers and developers, and decision makers who need to know what factors to consider when evaluating a single sign on solution. The Single Sign On considerations shared on are based on strong security actions other than typical user and password authentication mechanism. The lessons learnt from research, are made public, as well as further reading recommendations are included at the end.

Keywords- Single Sign-On, Centralized Architecture, Intranet Single Sign-On and Decision Makers

1. INTRODUCTION

Enterprises in industries are progressively realizing the fact that guarding applications by user id and password is no longer a practical way of authenticating their users and preventing unauthorized access to sensitive data.

To ensure demanding security for data and application protection, organizations are digging down for implementation of strong authentication systems that are more sophisticated in identifying users. At the same time, organizations are also aware of the fact that in today's IT era, security and business efficiency are often found at odds with one another, Demanding more security for their business applications, can lead to higher user input thereby decreasing productivity. With time, Enterprise Single Sign-On (ESSO) solutions have filled in this crust gap and hold the exclusive place of benefiting both the business efficiency and system security to their highest limit. These

products though automate access to all applications and systems through a single logon requiring one time input from user (Figure 1a and 1b). The deployment of an ESSO undoubtedly provides improvements in user productivity and contentment reflecting remarkable growth rates in business. However in past few years, there has been seen reduction in adoption of ESSO at organization level due to some security issues and concerns [2]. The story not limits to this; SSO at intranet level are not practical enough to provide protected work environment over the internet. This paper begins with facts why user id and password combination is no more inviolable for security.

Later we discusses some of the important security considerations that are often overlooked when developing SSO solutions and that finally some considerations that must be incorporated in to ensure safety to customer and success to product.

Pain of Passwords Management and Security Lack:

Passwords have been associated with computers and applications since 1961 and even today are a required component of any computing environment [3]. Their role in frequent tasks of daily work is such vital that they needn't be painful. With the time IT takes charge of securing weak and vital information. This places much pressure on part of choosing difficult, leak proof and un-hack able passwords. The safety of an organization's data requires vigilant security. Ensuring passwords are current and properly created is critical to the assurance of security and for that strongest user and password combinations can be selected which includes alphanumeric characters, rotating passwords on monthly basis and few others.

These approaches still forced the user to remember passwords more accurately and change it uniquely every time. Later tools were developed that dealt with the problems of password selection and management. Tools that manage password management are primarily responsible with taking much of this pain away from the user. These tools assisted in the administration of a user's password, primarily by creating a strong for the user and managing the profiles. Such tools took much of the pain away from the user but the tools needed further management. When none remedy worked and help desks costs increased beyond limit, single sign on took over the charge. Other than the user, organizations were sure to have their security fool proof by automating the authenticating process. But this was not the end of the story and research world. As industry adopted this solution by leaps and bounds, there arose a wave of fear that even this solution was not the final one. User was relaxed of the pain taking

password remembering task but the organization was exposed to hacking threats. The security was put to lose. In an era where risks to corporate data and processes abound, organizations understood that they can no longer afford to rely on passwords alone, that could be either manual authentication or automated sign on, for identity verification as it is not only difficult to manage but also has many security loop holes in them.

Organizations that were early adopters of enterprise SSO face some additional risks: threat of security breach over internet and exposure to third part interfaces and incompatibility factors. From a security perspective to functionality view, SSO projects are subject to numerous pitfalls. Some of such concerns are of high importance that are over shadowed during the product development and selection. We will discuss them briefly one by one in order of importance. Some are problematic in local SSO while others relate to internet SSO.

Password Cracking: Single sign on technology has enthused forward in leaps and bounds in recent past. In ideal experience, user can access all company networks, servers, emails and applications with one logon using one password. This means employees are free of multiple hard-to-remember passwords; they only need to remember one. This makes the employees more agreeable to remember a single difficult password as opposed to recall dozens of easy passwords and related hints like their pet's name, favorite star or place etc. This has a serious disadvantage of password being guessed out by hackers. Not only this sort of guessing works accurately at times, but also if user writes down password some place, it's all over.

Third Party Access with Web Agents: Enterprise organizations are looking to establish single sign on over internet after its in-house success to reuse their existing proprietary SSO. To grant their employees access to external web sites, services and platforms and allow inbound access for external partners, organizations provide provided a web agent that establishes communication link for inbound and outbound access for external partners and employees respectively. This is at ease for the organization since the proprietary SSO application is not thrown to garbage. But since an organization can have multiple partners, the situation is not better as projected.

Each time access is needed for a new partner, a new web agent is to be implemented, and hence organization needs to support different software for each of its business partners. Over a short span of time, the growing number of different web agents will ultimately be troublesome to manage due to their lack of reusability and scalability to support multiple partner connections. As one IT staffer at a fortune 50 company stated, "*we need to do single sign-on with fifty external partners and we have fifty different ways of doing it*" [5]. With each associate link taking at least two months to put into operation, organizations need a healthier way to implement SSO over the internet; if not, it would take years to hook up all their partners.

Lack of Ability to Review Cryptographic Mechanisms of External Security Points: When the enterprise network is communicating and information flow between the native and foreign end point is allowed, the entire network is exposed to all sorts of virus and intruder attacks. The foreign network might have implemented some cryptography to transform usable information preventing it to be readable by an interrupting user. Since the communication between the two parties is via SSO, it is the duty of SSO to verify the information before it lands in enterprise domain. Encrypted information is decrypted to its original usable form at the user end. By the time user decrypts it, it's too late in case that information was a viral attack. This ability is missing. Cryptography secures information but due to SSO inability to track the encrypted information it has turned a huge risk for the organization domain. Solutions need to be implemented in SSO products that can decrypt information and detect malwares.

Platform and Architecture Interoperability: Organizations who maintain mixture of windows and non-windows based environments including Linux and UNIX face the unique challenge of providing directory access across multiple platforms. To come across this challenge, they sustain multiple directories or use tools to enable file sharing across platforms [10]. Integrating active directory in mixed environments would provide a way to share files and would let Linux and UNIX users take advantage of the power of directory-based applications. But curtail comes when extending this AD infrastructure to further platforms like Solaris, Mac and so on. The concern in single sign-on can be difficult because disparate systems in enterprises typically do not use a uniform authentication methodology. In short, a lack of standards often derails single sign-on.





2. LITERATURE SURVEY

User operating environments evolved from traditional desktops to terminal services to cloud computing and finally to centralized processing popularly achieved with single sign on solutions. Over the years, each has remarkably reflected its strength and weaknesses. Table 1 taken from a research conducted by Dell Inc. reveals a comparison of benefits of some of the user operating environments.

From information provided in table 1, single sign on products provide apparent benefits to end users like ease of password remembrance, elimination of dependencies on help desk to reset passwords and many more; on other end if you notice, security factor is missing ins benefits which indicates that SSO do present security risks to the organization. For example, chances are likely there that security will breach if username and password are standardized across all servers and applications. An intruder's attack to penetrate into servers can turn successful to take away information if the attacked servers have in common the same authentication credentials.

Table 1: Comparison of User Environment Benefits [8]

Benefits	Traditional Desktop	Best Practice Traditional Desktop	Terminal Services	Managed Single Sign On
Centralized Data	—	◐	◐	●
Remote Access	○	◐	◐	●
Session Mobility	—	—	○	●
Performance	○	◐	◐	●
End User Satisfaction	○	◐	◐	●
End User Productivity	○	◐	◐	●
Secure Stable Environment	○	◐	◐	●

-  No Features Offered
-  Minimal Features Offered
-  Moderate Features Offered
-  Full Features Offered

Not only internal to organization, users now demand interoperability outside of the enterprise’s own domain with outsourced services, including business process outsourcing (BPO), software as a service (SaaS) providers and with affiliates and subsidiaries. Employees today need to access different applications over the internet in execution of their daily jobs often with different usernames and passwords for each one. Such a situation is not only unwieldy; it is intrinsically insecure, being especially susceptible to phishing, Trojans and other malware that can quickly spread and spoil the organization domain. When the business demands that employees are able to traverse the internet outside the secured domain with highly-sensitive data, the connection has to be secure to protect the user, enterprise and the service provider; a call for secure SSO.

Not only one, all ESSO products that include IBM Maximo, Oracle SSO, Schlumberger Dexa Badge, IBM Tivoli and many others offer trivial user and password combination for verifying users. Because of such security concerns, IT organizations round the globe have taken the alternative approach – the reduced sign-on. With a reduced sign-on approach, organizations settle on a point that which servers and applications can afford sharing of common

Table 2: Comparison of Security Strategies [2]

Authentication	Adoption	Security Level	Management
Passwords	Very High	Very Low	High
Biometric	Low	Variable	Medium
Smart Card	High	Very High	Medium High
Grid Card	Low	High	Low
Knowledge Based	Medium	Low	Low

credentials and which servers and applications are critical to have a separate sign-on. With this solution, a user signs on to a desktop can access one set of applications and server resources without having to sign on again. To access other server he requires additional sign-ons’ with the same or different username and password, and still for another set of applications, he requires more sign-ons’. Reduced sign-on approach is a less perfect solution from the user’s perspective. It may be more secured and pain relieving for business security management but the user is exposed to stress and frustration.

The sign on is in place but of no use to user. Reduced sign on approach not only hurts the user, rather the meaning of SSO itself dies away. Reduced sign on approach is a byproduct of security lack in single sign on solutions. Reducing user’s complexity problems and rectifying the decrease in adoption trend requires a balance between user satisfaction and security. If the scale swings too far toward security when trying to prevent a breach, user satisfaction decreases. Similarly, if the scale swings toward user satisfaction, you have to compromise IT security. In view of decrease in single sign on adoption, Gartner offered some blunt advice in February 2007 that all organizations should look to use stronger authentication in high-risk situations such as remote access [1]. What meant by choosing stronger authentication not only confined the scope to setting difficult passwords but something beyond this trivial approach. According to a survey based research, user and password combination is the least secure form of authenticating authorized access as explained in Table 2.

Other than the password limitation even in SSO, the SSO migration over internet is also a mystery so far. Many such existing products work only with the newest releases of the product suite, forcing massive and timely upgrades just to add keep internet SSO on the air [5].

3. PROPOSED SOLUTIONS

Once ESSO solutions are deployed, they become a significant part of an organization’s IT infrastructure and play a vital role in employees’ routine tasks. Realizing the importance of an ESSO, it should not be the one that limits the ability to reap the full benefits of single sign on or one that cannot scale as the organization evolves. In view of some features, discussed in previous section, that current

solutions lack, following are the proposed elements to be kept in mind while designing ESSO solutions.

Strong Multi-Factor Authentication: Strong authentication means replacing standard way of logging that is user ID and password credentials with a more safe form of validation such like biometrics, digital certificates, smart cards, grid cards or tokens. The use of strong authentication much secures the SSO single point of application entry. Of all, biometric systems are normally well secure because these features are unique to each individual. Also they do not require the user to memorize anything and are considered fairly difficult to spoof. This is to be kept in mind that the strong authentication strategy must be integral with the organization legacy applications and third party services. Strong authentication methods should also support a multiple-factor authentication scheme. Example of a multiple factor authenticated system is such where username (first factor) is entered while the user's fingerprint is accepted as a password (second factor). Such systems allow quick access to applications while improving to unique authentication of each user. For multi-level, any two strategies can be used. The SSO Solution must support strong authentication out-of-the-box as much as possible. Such authentication systems offer a highly reliable security infrastructure appropriate for extensive deployments in practically any type of environment.

Federated Identity: Business is becoming increasingly decentralized while relations with employees, suppliers, contractors, partners and customers are becoming ever more critical. Even in a single corporation, applications reside on different platforms and servers and not to be forgotten on third party domains. To facilitate this third party access and ease the implementation of web agents, federated identity becomes a paramount concern. All that is required is a single identity provider and rest is its job to do. No more multiple web agents required; no more scalability issues and no more hassle to maintain the proprietary SSO. By this mechanism companies can share identity information over secure networks [6]. As a result, companies can trade and communicate with each other easily without any need to implement further web agents that fulfill the needs to establish link. This will offer several compelling benefits to organizations such as local identities and associated data stays in place, yet they are linked together via higher-level mechanisms. This will benefit and protect many connections of the enterprise including (Figure 1) [7]:

- i) Outbound SSO over the internet for employees who need to access SaaS, BPO and managed services.
- ii) Inbound SSO for trading partners like suppliers and dealers into a supply chain portal.
- iii) Internal SSO for access to systems operated by acquisitions, affiliates, subsidiaries and joint ventures.
- iv) SSO with third-party hosted hubs for information and application sharing by users.

v) SSO with customers.

Example of an SSO system with federated identity implemented would be one that has browser based federation and users visit the business partner's domains with browsers. This will provide identity federation both within the company and with external business partners.

Cut-Across Encryption: The highest challenge for an SSO employed to facilitate the users over the internet is to cut through the encryption of the inbound communication and detect for virus and malicious information. Vendors explain it as being easy to implement but reality is opposite.

The SSO must be intelligent enough to decrypt the information at its own end before allowing the receiving end to obtain it. When we talk of intelligence, the user might misinterpret that the SSO must automatically decrypt the input data stream. It is intelligent but not that much. The solution has to have the decryption algorithm implemented. This can be costly for an enterprise to make SSO a decrypting tool for all. This can be cut down at customer or vendor level. The organization need to know how the customer, vendor or third party server will share data with its domain server. Having the encryption strategy of the other end, its decryption algorithm can be generated and embedded into system. When the domain SSO listens for information, it converts it to original form and checks for nasty information. In the case that SSO receives information that it is unable to decrypt, it will block it enter

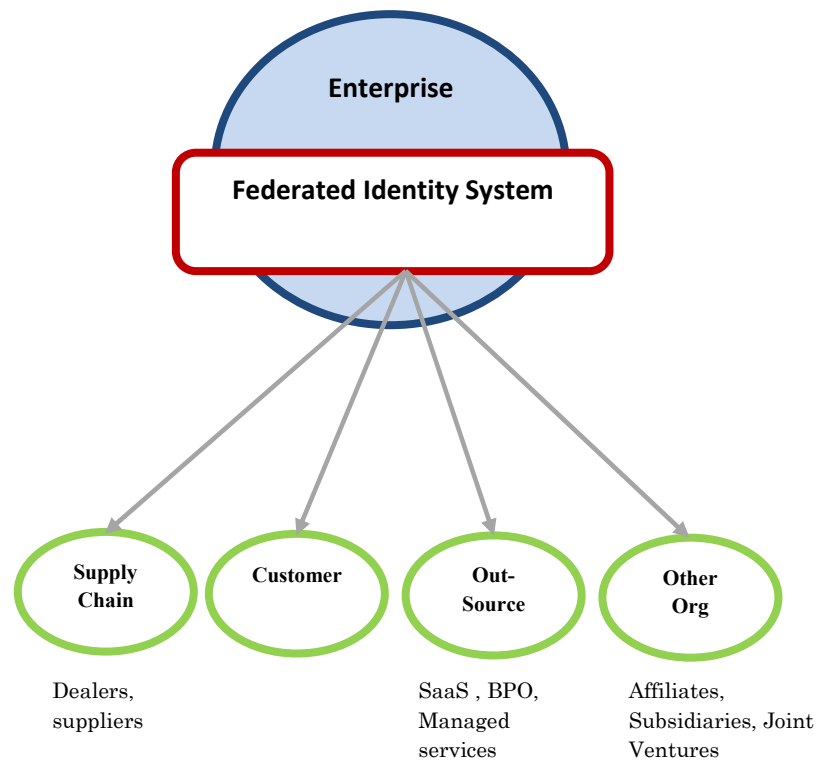


Fig. 1: Federated Identity System within an Enterprise

the enterprise domain. This decision will be based on assumption that the SSO has all the strength to decrypt information from sharing partners and vendors and the one

not able to decrypt is from an intruder. The need to have such a SSO server is where the organization has business links with partners implementing encryption and ciphering at their ends. For example, a company ABC has partners American Express, Citibank, BancOne and etc.

All the marker leaders have different encoding strategies working at respective ends like RC2, RC4, RC14, LDAP and etc. The SSO server will have decryption algorithm working at its own end. Accordingly it will decrypt all the receiving information verifying it safe and malware free and encoding it into local code words for use within the organization system.

Cross Platform Interoperable Services: The ideal state for an organization with heterogeneous networks is to consolidate around a single, secure, and robust directory for all platforms. This requires services that extend the active directory beyond Linux and UNIX operating systems. Such services provide a number of powerful capabilities that help quickly achieve the goal. In a mixed environment, integration is not an issue; authentication however is. To keep the single sign on the track, solution must provide a single sign-on platform for disparate systems. Since most organizations make use of active directory services, the solution need to on active directory with some other additional standards including support for:

- i) Kerberos
- ii) Lightweight Directory Access Protocol applications
- iii) Pluggable Authentication Module (PAM)
- iv) Name Service Switch (NSS)
- v) Security Support Provider Interface (SSPI)

These features rationalize the procedure of joining Unix/Linux systems and users to the AD field and assist relocation from multiple authentication mechanisms, directories and identities to a single infrastructure for all systems and users. Not only this, the organization is flexible enough to implement the solution at their own pace and specific to their own requirements. And finally, the implemented SSO would be compatible over multiple operating systems and interoperable between them majorly include Red Hat, CentOS, Fedora, Mac OS, Linux, Ubuntu, Oracle VM, IBM AIX etc (as shown in Figure 2) [9][11].

With the platform dependent SSO in place, centralized authentication is achievable even in the most complex environments including Cross Forest authentication [12].

From all the considerations and issues discussed in the paper, we can summarize it in key facts of decision making as:

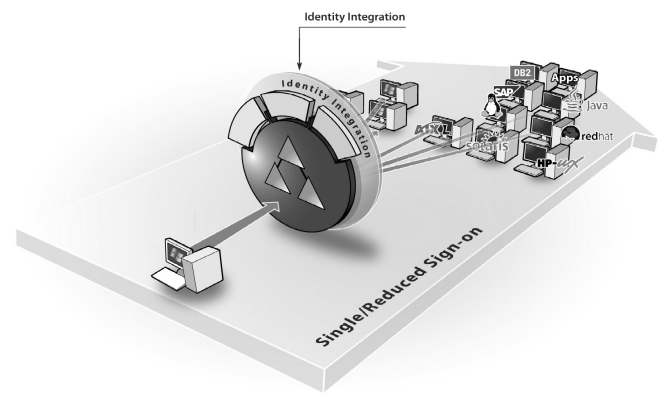


Fig. 2: Simplified Identity Management Across Platform [9]

- i) The first step is methodically evaluating the organization by evaluating which applications drive most of their password-related trouble tickets.
- ii) Once the list of applications is in hand, examine the login processes of each of the application and match the login of applications with the facility provided by SSO. This need is to select a solution based on the ability to support robust and flexible login parameters.
- iii) Look at the language and standards of existing applications and check if all the standards are supported by SSO solution.
- iv) Look for changes required in making SSO meet organization requirements and statistics.
- v) Security factors that SSO takes care of and that which are not catered by company has implemented them as part of infrastructure.
- vi) Infrastructure, security implementation, login process of external partners and third party vendors.
- vii) And finally, is the product scalable to meet future necessities of up to two decades.

4. CONCLUSIONS

Customers who deploy SSO are showing a lot of fast, positive results. It is also becoming a strategic component in the scheme of large system deployments. Given all this, it is critical for an organization to start by examining its needs and selecting a solution that meets those needs.

A number of Enterprise SSO solutions are available but choosing the one out of numerous is an intelligent and worthy to be analyzed task since not only costly it is, the future of scalability also depends on it. Companies need to investigate how matching characteristics of their organization onto single sign on functionality will lead to an improved user experience, because, at deployment, it will pay off in immediate and long-term success with SSO.

The one single sign on that can be successful for customers of all sizes and industries must meet the standards defined in this paper.

REFERENCES

- [1] The Twilight of Passwords: A Timetable for Migrating to Stronger Authentication, Ant Allan, Gartner, Inc., Feb. 28, 2007.
- [2] Single Sign On Products, John Enck, Windows & .NET Magazine November 2006
- [3] <http://en.wikipedia.org/wiki/Password>
- [4] Managing string Authentication: A Guide to creating effective Management System CA transforming IT Management, www.ca.com
- [5] Secure Internet Single Sign-On 101, Ping Identity
- [6] <http://www.technewsworld.com/story/33197.html?wlc=1276710785>
- [7] Five Steps to Internet SSO, Ping Identity
- [8] Virtual Desktop Solutions: A Comparison of Costs and Benefits Dell Inc. 2010
- [9] Vintela Authentication Services Quest Software, Inc 2006
- [10] Vintela Authentication Services Windows IT Pro 2010
- [11] <http://www.quest.com/authentication-services/supported-platforms.aspx>
- [12] <http://www.quest.com/authentication-services/features-active-directory-for-unix.aspx>