

A Single Sign-On Approach

Ajay Lodha, Ram Sarma | March 2006



The complex issue of single sign-on

Single sign-on (SSO) is a mechanism whereby one action of authentication and authorization can give users access to appropriate computers and systems without entering passwords multiple times. SSO reduces human error, a major component of system failure, and is, therefore, highly desirable but difficult to implement.

As IT systems proliferate to support business processes, users and system administrators are faced with an increasingly complicated interface to accomplish their jobs. Users typically have to sign on to multiple systems, necessitating an equivalent number of sign-on dialogues, each of which may involve different user credentials and authentication information. System administrators are faced with managing user accounts within each of the

systems in a co-coordinated manner to maintain the integrity of security policy. These sign-ons are complex enough, but in addition, globalization, mergers and acquisitions are changing the organizational landscape at a fast pace. Assets, applications, and transactions now have

Digital identity:

A process in technology that authenticates or authorizes a user, application, or system to other users, applications, or systems. Digital identity can also mean the digital representation of a set of claims made by one digital subject about it or another digital subject.

Problem:

Multiple sign-on processes, such as passwords, user names, and authentication information, are costly in terms of user time wasted, potential security breaches, and system administration overhead.

Solution:

Through a coordinated plan, companies must determine the best single sign-on strategy.

Benefit:

With the right process in place, company data is more secure, employees don't waste time dealing with multiple authentication and authorization routines, and system administration costs go down.

to be accessed by a larger ecosystem of people, requiring merging employees, customers, partners, and vendors across these organizations. This process presents the following challenges:

- User credential consolidation
- Access to legacy applications
- Transactional security
- Centralized user enrollment
- Centralized provisioning
- Support multiple authentication mechanisms
- Fine grained authorization

This paper assesses the benefits and tradeoffs of implementing a SSO solution to tackle the following scenarios, and is written primarily for chief information officers, chief technology officers, enterprise architects, and division heads whose businesses require SSO.

Scenarios for SSO

The challenges identified above are solved by implementing a SSO solution with the use of tools like CA SiteMinder, IBM Tivoli Identity Manager, and Oblix (by Oracle).

Identity Management (IM):

An integrated system of business processes, policies, and technologies that enable organizations to facilitate and control their users' access to critical online applications and resources.

Security Assertion Markup Language (SAML):

An XML standard for exchanging authentication and authorization data between security domains, for example, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

WS-Security (Web Services Security):

A [communications protocol](#) providing a means for applying security to [Web Services](#). On April 19, 2004 the WS-Security 1.0 standard was released by [Oasis-Open](#).

Here are the main types of SSO solutions:

Enterprise Single Sign-On (E-SSO), after primary user authentication, intercepts login prompts presented by secondary applications, and automatically fills in fields such as a login ID or password. E-SSO systems allow for interoperability with applications that are unable to externalize user authentication, essentially through "screen scraping." This process is also called legacy SSO.

Web Single Sign-On (Web-SSO), also called web access management (Web-AM), works strictly with applications and resources accessed with a web browser. Access to web resources is intercepted, either by using a web proxy server or installing a component on each targeted web server. Unauthenticated users who attempt to access a resource are diverted to an authentication service, and returned only after a successful sign-on. Cookies are most often used to track user authentication state, and the Web-SSO infrastructure extracts user identification information from these cookies, passing it into each web resource.

Federation is a new approach, also for web applications, which uses standards-based protocols to enable one application to assert the identity of a user to another, thereby avoiding the need for redundant authentication. Standards to support

federation include [SAML](#) and [WS-Security](#).

Transactional Single Sign-On, also called transaction access management, works strictly with Web Services that need to be accessed either directly by end users or by an application.

SSO Components

SSO typically is composed of the following components:

- Authentication
- Authorization
- Portable user profile
- Trusted globally accessible user token
- Centralized User Store

An example of issues raised by implementing SSO

Let's take a hypothetical example of a financial services organization – ABC Financial Services – to outline the SSO requirements and dive deeper into the issues that can arise in implementing a SSO solution in such an organization. We'll also look at the considerations that can mitigate risks in such an undertaking.

Mergers and partner domains present additional issues

ABC Financial Services has just acquired an insurance company, which requires merging services and applications. Both organizations have a combination of:

- Legacy mainframe applications.
- Web Services.
- Common services that are provided by different applications in each organization, which will now need to be merged into one application.
- SAP applications.
- Portal implementations using IBM WebSphere Portal.

In addition to the above, employees of these organizations require access to services provided by some partners. These services are hosted externally in the partner's domain and require subscription and authorization prior to accessing them. An example is a benefits self-service site provided by a benefits partner. The above scenario within ABC Financials causes the following problems and business impacts:

Problems

- Too many credentials
- Mapping of credentials to applications
- Multiple sources of user information
- Provisioning new accounts for different applications
- Password management – mushrooming passwords
- Auditing user activity
- De-provisioning users
- Managing non-employee access
- Establishing and deploying enterprise-wide security policies

The business impact

- Increases risk of compromise
- Reduced productivity
- Increased help desk expenses
- People intensive
- Delayed access for new hires
- Risk of unauthorized access
- No single view of the user

Benefits of SSO for ABC Financial

A SSO solution alleviates the above problems for ABC Financials. It provides a number of business and end-user benefits derived from having a centralized authentication and authorization registry.

End-user benefits

- Only one authentication mechanism to remember. For password-based authentication, this means only one password to remember and update, and one set of password rules.
- Less likely to forget passwords.

System administrator benefits

- A single common registry of user profiles (possibly replicated).
- A single common way to manage user profiles.
- A single common security infrastructure.
- A common set of stronger policies enforced across all enterprise applications.
- Users less likely to use the “sticky note” method for remembering passwords.

Authentication:

A means of validating a user's identity.

Authorization:

A means of validating if the user, once authenticated, has access to an asset/resource that has been requested.

Authentication mechanisms:

- Passwords
- One time passwords
- Tokens and smart cards
- Public key infrastructure
- Digital / machine fingerprints
- Biometrics

Authentication protocols:

- Geo-location
- Kerberos
- SSH
- Encrypted key exchange (EKE)
- Secure remote password protocol (SRP)
- Closed-loop authentication
- RADIUS/CHAP/PAP/DES/EAP etc
- DIAMETER
- HMAC
- Two-factor / strong authentication
- Authentication OSID

Business benefits

- A common infrastructure leveraged enterprise-wide that can be centrally managed and secured.
- Secure delegation of credentials, enabling end-to-end security, across application and system boundaries.
- Enterprise-wide security policies.
- Reduced help desk costs by reduction in the volume of password requests.
- Transparent and discretionary role-based user access to resources.
- Self-enrollment and non intrusive architecture, requiring minimal if any application changes.

Issues in reaching an achievable and effective approach

SSO today is a buzzword and goal for many enterprises. It's extremely complex once you peel away the outer layer of strategic desire and look at the system and security implications. In order to decide on an approach that is achievable and effective, the following issues must be addressed:

1. What are the considerations for your SSO strategy?
 - a. Authentication methods
 - b. Identity management
 - c. Post authentication actions
 - d. Authorization methods
 - e. Post authorization actions
 - f. System integration
 - g. Directory strategies
 - h. Auditing
 - i. Overall risk
2. What is driving the need for SSO within the enterprise?
 - a. End users can't handle remembering different passwords to access the systems they deal with daily.
 - b. They don't want to carry in their wallets many separate forms of authentication devices such as loyalty cards, credit cards, smart cards, employee, and other forms of ID.



3. Does the organization have multiple **islands of trust**, which means many systems and applications with individual mechanisms of authentication and authorization or, alternatively, decentralized systems and applications that implement similar authentication and authorization mechanisms?
4. Should authentication and authorization mechanisms for each of the islands be bridged? This is the most important question the organization needs to answer in order to zero in on an approach.
5. Does the organization have a security guideline that outlines what information needs to be secured and the level at which it needs to be secured?
6. What are the scalability and availability requirements?
7. Has the overall load passing through the security platform been evaluated?
8. How many identities does a user have within the organization across the many applications?

SSO Approaches

Once a company has assessed its SSO issues, it needs to decide on one of the three following approaches to SSO:

Authentication hubs

This approach to SSO calls for a central location where all credentials are stored. The SSO server acts as an intermediary to distribute credentials when required and to authenticate/authorize users as needed. Characteristics of this approach include:

- Inline server – the SSO server falls between the user and the application.
- Central management and auditing.
- Usually requires application changes to integrate with the SSO server.

Password synchronization

This approach to SSO allows localized credential presentation and collection for each application through the use of client-based components. Characteristics of this approach are

- Client based – all credential presentation/collection components exist on the client machine.
- User maintains control over the client components, and profiles/passwords are synchronized to a central server.
- Non-intrusive – requires no changes to the application.

Centralized enterprise approach

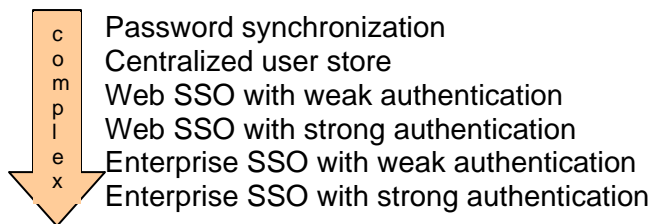
This approach provides centralized credential and authentication management services along with localized credential presentation and collection. Almost all of the current SSO products and architectures are based on this model. Characteristics of this approach include:

- Centralized credential and user store.
- Localized processing performed after the credentials have been obtained and validated by the centralized store.
- Changes required to an application to interact with the authentication tokens.

The centralized enterprise approach provides the strongest benefits of both the centralized and the de-centralized approach. Regardless of the approach taken, the SSO landscape presents the following scenarios:

- Commercial product -- Procure and customize a commercial product to serve the needs of the enterprise.
- Open-Source Option -- Use one of the open-source SSO products available in the market.
- Custom Build -- Build an SSO solution as an internal solution to the enterprise.

Whatever the approach towards an SSO solution may be, the complexity of the solution increases as risks and business needs are fulfilled. The main facets of an SSO solution, from the least complex to the most complex, are:

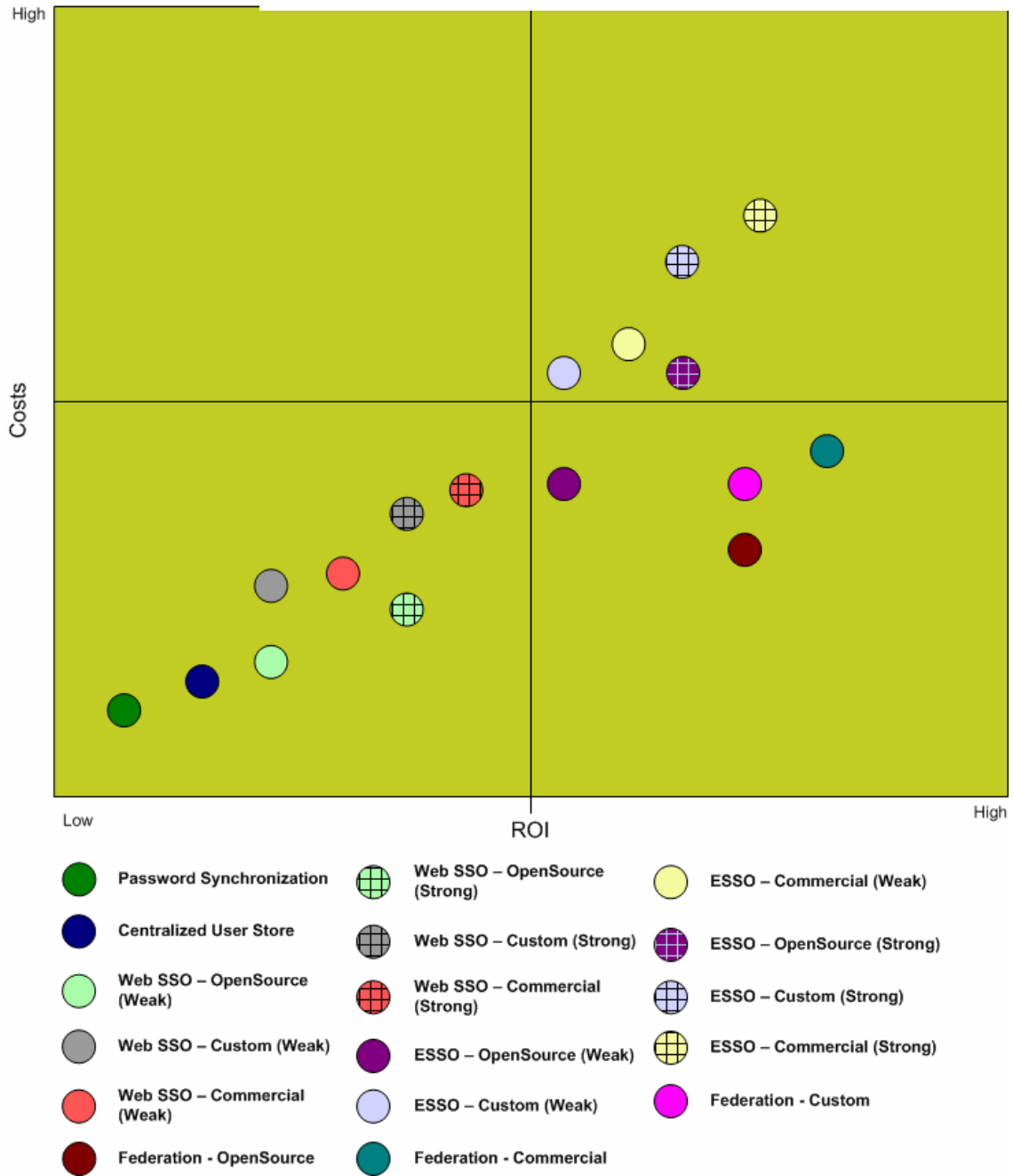


Another axis to complexity presents itself when an enterprise requires implementing a SSO solution with its partners and affiliates. This aspect of the solution involves:

- Web Services
- Federation services

This graph maps the potential costs incurred with the various facets of a SSO solution against the prospective benefits provided by the same.

Avenue A | Razorfish Cost-Benefit Analysis: SSO



Implementation

To implement a SSO solution, all systems that need to participate in an SSO must be evaluated for their readiness. The readiness of the enterprise systems and the enterprise as a whole for a SSO deployment can be evaluated by measuring each system based on several factors. Each factor is rated on a scale of 1 to 10; a low score indicates that the organization/system is not ready for SSO. The overall tally is then averaged out to obtain a total score, which can then determine the ease of move to an SSO solution. The factors to be considered are:

Avenue A | Razorfish Scorecard: SSO Readiness

Factor	Description	Score
Business Impact	What impact does the SSO solution have on the business? A score of 10 indicates that the solution has a huge positive business impact and the productivity gains far out weigh the costs for a SSO solution.	1-10
Security Processes	SSO requires that strict security processes be in place to govern existing and new applications coming into the environment. A score of 10 here implies that there are existing security processes in place that cater to the needs of a SSO environment and do not need to undergo changes. A score of 0 implies that new process must be set in place and old ones require a change.	1-10
Staff Skills	Are there resources for the enterprise (internal or external) who understand the technical aspects of an SSO solution? A score of 0 means that the required skill set to manage an SSO solution is currently unavailable and a score of 10 indicates that there is an abundance of such skills in the enterprise.	1-10
Application Readiness	Is the application in need of an SSO? If so, has the application been built/re-factored in such a way that an SSO solution can be easily plugged in? While making this decision, consider the various systems with which an application interacts. A score of 0 implies that the application has to undergo major updates to fit in an SSO solution. A score of 10 indicates that the applications' authentication/authorization processes can easily be replaced.	1-10
Audit/Compliance	Are there audit/compliance requirements which are driving the need for an SSO? A score of 10 implies that there are holes in the compliance to certain processes like, for example, Sarbanes–Oxley, which would be complete once an SSO solution is in place.	1-10

User Groups	How many users are going to reap the benefits of an SSO solution? A score of 0 indicates that the user base is limited, whereas a score of 10 implies that the entire organization is going to reap the benefits of a SSO environment	1-10
-------------	---	------

A sample scorecard for three applications/systems, Investments, MyBenefits and Privacy Portal in an enterprise may look as follows:

System/Factor	Business Impact	Security Processes	Staff Skills	Application Readiness	Audit/ Compliance	User Groups	System Score
Investments	8	7	8	6	8	8	7.5
MyBenefits	5	8	8	9	5	9	7.34
Privacy Portal	3	7	8	3	3	5	4.84
Factor Score	5.34	7.34	8	6	5.34	7.34	6.56

An analysis of the scorecard would inform an implementation path toward a full-fledged SSO implementation. Based on the scorecard and requirements of the enterprise, a prioritized approach can be composed to prepare the applications/systems to participate in an enterprise-wide SSO solution.

Getting started with implementation

Once an enterprise like ABC Financial is ready to implement a SSO solution, the organization can decide upon the approach that best fits its needs. For the purposes of this discussion, let's assume the centralized enterprise approach since it provides the most benefits from both an end-user and the business perspective. To achieve a full-fledged SSO implementation across all systems in the enterprise, the following phased approaches need to be considered:

- Phase 1: User identity aggregation and synchronization
- Phase 2: Single-sign-on (web/transactional)
- Phase 3: Enterprise single sign-on (ESSO)

SSO Challenges

There are a number of challenges in designing and implementing an enterprise-wide SSO architecture that is flexible enough to cater to the varying requirements of different enterprises. The salient ones are:

- Multiple application platforms and application models
- Multiple operating systems - Windows server, different flavors of UNIX, OS390, AS400
- Network gateways - VPN, wireless, Internet
- Different security protocols
- Different directory implementations and multiple directory accounts

- Complexities with business-to-business and business-to-customer connections
- Concerns about mixing partner and customer accounts with employee accounts
- Privacy (outbound) as well as security (inbound) concerns
- Getting external users and their entitlements up to date
- Day to day management issues (for example, password reset)

Despite these challenges, a SSO solution brings higher returns from both a business and end-user standpoint. Every enterprise needs to evaluate the need for such a solution in order to effectively manage sensitive information within and outside the organization.

Conclusion

As different systems are implemented in enterprises, integrating and sharing information across these systems becomes more and more a mainstream requirement. Security and personal information dissemination are becoming big issues that enterprises need to address. SSO implementations alleviate and ease such requirements and security concerns.

In summary, IT executives are well advised to:

- Ratify business requirements around security and access to systems.
- Identify the need and readiness for a SSO implementation.
- Investigate the current SSO technologies and vendors.
- Prepare for a phased implementation of a SSO solution.
- Get rid of the “sticky note” approach to remembering user profile information and passwords.

About the Authors



Ajay Lodha is a technology director in the Boston office of Avenue A | Razorfish. Ajay has over 15 years of experience building enterprise applications with an emphasis on security technologies, enterprise portals, content management technologies, defining the technical architecture and final implementation. Recent work for clients such as GE Silicones, MetLife, CitiBank, and Universal Underwriter's Group has involved infrastructure audit, data migration, SSO implementation, legacy platform integration and RIA implementation. Ajay has led large technical teams implementing mission-critical, custom-built J2EE applications with tight integrations to other systems.



Ram Sarma is a technical architect in the Boston office of Avenue A | Razorfish. Ram has over 10 years' experience building enterprise applications, with an emphasis on security technologies and learning management systems, performing architecture, technical design and implementation. Recent work for clients such as Metlife has involved building an effective strategy for SSO, security policies and diagnostics and helping lines of business align with the new requirements.

About Avenue A | Razorfish

Avenue A | Razorfish (avenuea-razorfish.com) is the largest interactive agency and an operating unit of Seattle-based aQuantive, Inc. (NASDAQ: AQNT), a digital marketing services and technology company. Avenue A | Razorfish solutions are entrenched in deep technology, rigorous analytics and a rich understanding of customer needs, including award-winning online advertising media & creative, search marketing services, email marketing, and world-class design and implementation of websites and intranets/extranets. Avenue A | Razorfish operates three regions – East, West and Central – with 11 offices located in major U.S. markets. Clients include AstraZeneca, Best Buy, Kraft, Microsoft/MSN, Ralph Lauren, and Wells Fargo.

Avenue A | Razorfish
821 2nd Avenue, Suite 1800
Seattle, WA 98104
Phone: 206.816.8800
Fax: 206.816.8808

For more information please visit: avenuea-razorfish.com.