

## White Paper



### Linux Single Sign-on: Maximum Security, Minimum Cost

---

Abdul Najam Safarulla and Kavitha D

*Linux-based Single Sign-on (SSO) solutions offer benefits that enhance security, reduce costs, offer a better user experience and increase productivity, especially for Banking and Financial Services organizations with global operations, complex application portfolios and multiple data centers.*

#### SSO – A critical part of security strategies

SSO is a critical part of the IT security strategy of most BFS organizations, which are perhaps more exposed to the risk of unauthorized access to sensitive financial and customer information than others.

For many BFS organizations, mergers and acquisitions and expanded service offerings have resulted in increasingly complex IT environments. As the number of application-specific user IDs and passwords grow in these organizations, so also does the amount of helpdesk support required for password management.

What's really important for any BFS organization doing business with third-party vendors today is the ability to protect information in its indirect control from improper usage and distribution. By tightly integrating complementary technologies such as provisioning and user authentication, an enterprise SSO solution can help BFS organizations improve information security, minimize associated help desk costs, increase customer satisfaction, and realize immediate workforce productivity gains.

The key benefits associated with implementing an enterprise-wide SSO solution are:

- a. **Minimizing security risks:** Studies by research firms like the Gartner Group and IDC have shown that users resort to either writing down their passwords or choosing very common ones, which results in significant security risks to organizations.<sup>1</sup> SSO minimizes this by invoking secondary domain applications on an authenticated primary domain password. This accelerates access and makes it easier for users, who now have to authenticate only once for every session.
- b. **Ability to audit user transactions:** When combined with tracking and reporting by the SSO solution, a BFS organization can confidently tie every access to customer information to a specific access event. The result is simple-to-use security combined with verified privacy and confidentiality. Audit trails facilitate accountability for customer information usage. SSO, therefore, appeals not only to the end-user but also to organizations as it significantly reduces security risks arising from the use of multiple passwords.
- c. **Minimizing account management costs:** Managing multiple passwords is expensive and, at the same time, poses security threats. Reports from the Gartner Group indicate that anywhere from 15-45% of all helpdesk calls are related to forgotten or expired passwords. According to the Securities Industries Association, a Wall Street trade group, users spend an average of 44 hours every year logging into an average of four applications every day, resulting in an overall loss of productivity.
- d. **Simplify regulatory compliance process:** Introduction of the Graham Leach Bliley Act of 1999 (GLBA) is another reason for the growing popularity of SSO among the banking and finance community. The Act, which talks about safeguarding customer information and privacy, makes it mandatory for BFS firms to implement technology that will aid regulatory compliance. Authentication as part of a written, comprehensive security program is critical since it allows for tracking of all attempts to access specific information. An enterprise SSO solution allows BFS organizations to produce the audit trail of every record accessed to the governing authorities during an examination of the institution's security standards, which is a requirement under GLBA.

Almost all large multinational BFS organizations today are in some stage or the other of SSO implementation. SOAR, a consortium of the management of 33 Italian banks, has deployed an SSO solution for more than 50 internal and external banking services, which includes authentication, access control, SSO and audit.

Dresdner Bank, a leading European bank, and Barmenia and RheinLand Versicherungen, two of Germany's prominent insurance companies, are amongst those organizations which have implemented SSO to facilitate management, authentication, access control, and audit SSO for user applications.

From a systems management perspective, a major goal of these implementations is to provide a single user account management interface through which all the component authentication systems may be managed in a coordinated and synchronized manner.

The other common goals include:

- Meeting regulatory laws designed to protect customer data
- Ensuring network security while keeping budget expenditure at a minimum
- Enhancing staff productivity and maximizing return on investment on security expenditure

## Do all SSO solutions meet organizational needs?

The fact that SSO enables a user access to multiple applications using one-time authentication has led to a very common misunderstanding among users and organizations – that SSO uses the same password for all applications. While some have mistaken it for password synchronization, a method that distributes a single password to multiple systems, others have mistaken it for a solution that retrieves the password from a database where all passwords are stored.

However, a true SSO solution invokes secondary domain applications on an authenticated primary domain password to provide authorization and authentication to all the applications that a user is authorized to access.

A variety of true SSO solutions exist in the market today offered by leading vendors like Novell, Microsoft, IBM, Computer Associates, and so on. Most commercially available solutions provide both authorization and authentication. However, in terms of initial implementation as well as ongoing running and scalability costs, they can prove to be expensive.

<sup>1</sup> Gartner Group: Enterprise Single Sign-on tool are comprehensive but costly, Ant Allan, October 21, 2004

The cost of configuring a complete enterprise SSO solution for a large organization with global operations and complex portfolio (and numerous existing systems) is staggering. A summary of the costs of SSO implementation is presented below:

### a) Initial costs

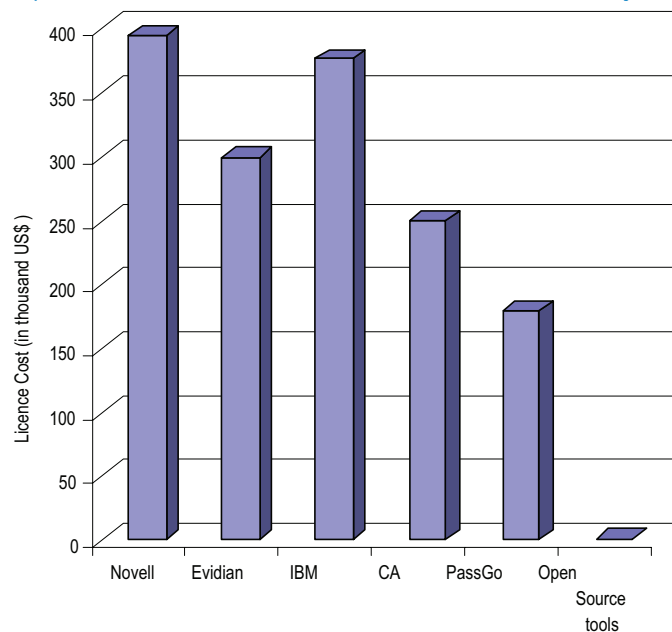
- Product purchase
- Customization of product for existing systems – this work effort usually involves creating custom scripts to drive legacy systems
- Loading existing user information into the proxy-SSO solution and deploying to users

### b) Ongoing costs

- The recurring software upgrade cost
- Another registry to maintain – this system must be highly available
- Password management by users – when passwords expire in various legacy systems, users must update the legacy and the SSO system. The user may no longer be familiar with the login procedure for the legacy system and may, or may not, remember the passwords. This will make it impossible for users to change their own passwords without assistance
- Script maintenance – as the legacy system user interfaces change, the scripts have to be changed, which involves a significant effort

A quick comparative study (refer chart and table below) of some of the commercially available SSO solutions in the market today indicates that organizations can find respite in open-source tools like Java Open Single Sign-On (JOSSO), as they outweigh other commercially available solutions in terms of both costs as well as features.

### License fee comparison: Open Source (OS) tools vs. other commercially available SSO tools



Note: Cost presented for 5000 users; Solutions covered for the comparison include Novell – SecureLogin, Evidian - Access Master, IBM - Tivoli Global SSO, Computer Associates - eTrust SSO, PassGo Technologies – PassGo, and JOSSO - Open Source Tool

Table: Open Source SSO tools

Criteria	JOSSO (Java Open Single Sign On)	Yale CAS (Central Authentication Server)	PubCookie	JAAS (Java Authentication and Authorization Service)
Supported Server Platforms	Windows, Linux, Unix	Windows, Linux, Unix	Windows, Linux, Unix	Windows, Linux, Unix
Supported Client Platforms	Windows, Linux, Unix	Windows, Linux, Unix	Windows, Linux, Unix	Windows, Linux, Unix
Scalability	Provides JAAS-based Transparent Single Sign-On across multiple applications and hosts	Scales well, mainly used in Universities	Scales well, mainly used for intra-institutional web-based authentication	Used across multiple applications and hosts
Smart Card Support	Yes	Yes	Yes	Yes
Pricing	Commercial friendly. Released under the BSD License	Freely available from Yale (with source code)	Released under the BSD License	Freely available. Introduced as an optional package in J2SE 1.3
Source	<a href="http://www.josso.org">www.josso.org</a>	<a href="http://www.yale.edu.tp/cas">www.yale.edu.tp/cas</a>	<a href="http://www.pubcookie.org">www.pubcookie.org</a>	<a href="http://Java.sun.com/products/jaas">Java.sun.com/products/jaas</a>

## Linux SSO enhances productivity, curtails costs

Linux SSO solutions offer the best of both worlds to organizations looking at implementing this technology. Besides curtailing many of the above-mentioned costs, organizations can also reap rich benefits in terms of heightened security and increased user productivity by carefully designing underlying applications to work with a Linux-based SSO solution.

Linux SSO also helps administrators recognize and monitor different types of screens. The application program generator and workflow help the system administrator SSO-enable most applications. This makes the whole SSO system transparent to end-users, whether they use Windows, the command line, or plug values into a mainframe application.

Vendors today offer combination hardware/software solutions on Linux, which is attractive for small-to medium-sized enterprises as IT managers can keep their password management under control with minimum architecture, complexity and effort. Linux-based SSO solutions also help with regulation compliance as they allow administrators to cross-check for correlation of similar user names on applications.

The key benefits of a Linux SSO solution are:

- a. **Better administration and control:** One of the key features of a Linux SSO solution is that it can consolidate the authentication database, administrator interface web server and fail-over logic into a tightly controlled and integrated Linux machine. This while minimizing the security risks also cuts down on problems associated with off-the-shelf software only solutions. Besides, Linux SSO solutions come with an application profile generator that allows IT administrators to use a point and click-based tool to understand all types of applications – be it a Win32 program, a web application in any browser, a host mainframe application, or even user interfaces such as the command line and Java/JVM applications.

- b. **Minimizes security risks:** The Linux operating system's strict security system prevents viruses, worms and unauthorized users from modifying system files without root access, so it is far less of a target than platforms such as Windows. If security issues exist, the open source design philosophy makes them easier to troubleshoot and repair than with a Windows system. The key benefits of coordination and integration of authentication into a Linux-based SSO include the following:
- Improved security through the reduced need for a user to handle and remember multiple sets of authentication information
  - Reduction in the time taken, and improved response, by system administrators in adding and removing users to the system or modifying their access rights
  - Improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration, including the ability to inhibit or remove any individual user's access to all system resources in a coordinated and consistent manner
- c. **Minimizes account management costs:** One of the most compelling benefits of a Linux SSO solution is the drastic reduction in account management costs. For an organization with as few as 100 employees who sign-on to only three different registries per day, a Linux SSO solution can save up to \$25,000 per year by reducing both the number of password reset help desk calls and the time end-users spend signing-on to different registries. This translates into a productivity gain of nearly one day per employee over the course of a year.
- d. **Helps achieve regulatory compliance with ease:** The GLBA regulation is designed to protect a financial services user's privacy. System access control and user transaction audit trail are key factors in meeting this requirement. Linux SSO solutions allow systems administrators to achieve compliance to the GLBA regulation with ease by cross checking for correlation of similar user names on applications and, accordingly, restrict or allow access to applications. Built-in audit trail functionalities of a Linux SSO solution enable IT administrators to easily track usage and culpability.

Considering these benefits, an effective enterprise Linux-based SSO product can be easily implemented at reasonable rates to quickly meet an organization's strategic security needs. Budget considerations often factor into security decisions – biometrics, smart cards and public key infrastructure are more expensive and time-intensive security technologies to implement. Enterprise SSO does not preclude applying these technologies in the future. It is important to note at this juncture that the complete benefits of SSO will not be realized unless an organization endeavors to have full coverage of its IT assets.

## Linux SSO implementation best practices

A chain is as strong as its weakest link. All the components of the Linux SSO server should therefore be reliable, durable and secure. The key security aspects of a Linux-based SSO model are presented below:

- a) An application service must trust a third-party system to:
- Correctly assert the identity and authentication credentials of the end-user
  - Protect the authentication credentials used to verify end-user identity to the secondary domain from unauthorized use
- b) The authentication credentials have to be protected when transferred between the primary and secondary domains against threats arising from interception or eavesdropping, leading to possible masquerade attacks

To ensure this:

- Use Security Enhanced Linux kernel (SELINUX) from any distribution
- Adhere to best practices for Linux server hardening
- Subject the Linux SSO server and network resources to periodic preventive vulnerability assessments
- Patch the Linux SSO server according to latest security advisories and patches issued from time to time – this activity may be automated for immediate patch application
- Periodically audit log messages from kernel and network traffic
- Install an intrusion detection mechanism
- Use URL-based resource access policy agents

- Confirm that whenever a user logs out, the SSO token instantiated earlier is invalidated and confirmed again
- All applications should receive notification of the SSO token termination and the sessions need to be cleaned up appropriately.

## Conclusion

Identity and access management are not new concerns for the BFS industry. This and other regulatory constraints are dealt with every day. Post 9/11, the rules for identity management have become stricter and government involvement has increased. Governing bodies such as the U.S. Office of the Comptroller of the Currency, for example, are showing a particular interest in how banks authenticate employees.

The ability to conclusively authenticate users quickly and easily across a growing number of networked business applications is a challenge. The strategy adopted herein needs to not only improve customer service but also mitigate identity thefts and fraud risks. A scalable solution that focuses on these issues and follows sound user identity management practices will be the cornerstone for both security and continued business growth.

Linux-based SSO solutions can help organizations achieve this goal faster and in a cheaper way. They fortify security, facilitate quick deployment, work virtually everywhere, require minimal integration, and support other authenticators. In effect, Linux-based SSO solutions offer a secure and cost-effective way to authorize access to personal information while, at the same time, holding users accountable for their activities. If properly implemented, a Linux-based SSO solution will maintain the security of countless applications, track and log access of customer information, and speed up access to crucial information.

## About the Authors

Abdul Najam Safarulla and Kavitha D are software engineers working for the Linux COE in Infosys Limited. This team involves work on Linux and Open Source migration Solutions.



For more information, contact [askus@infosys.com](mailto:askus@infosys.com)

## About Infosys

Many of the world's most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow's enterprise.

For more information about Infosys (NASDAQ:INFY), visit [www.infosys.com](http://www.infosys.com).