Single Sign-On Vendor Selection Evaluator's Guide

The right single sign-on (SSO) solution will allow your users to securely log on once to access all their applications. This:

- Protects information
- Reduces password-related helpdesk calls
- Improves employee satisfaction

But, not all SSO solutions are the same. As you start your evaluation process, it helps to know which questions to ask in order to have a thorough understanding of product features, implementation, and ongoing management. This list will guide you through your due diligence.

	Imprivata	Vendor 2	Vendor 3
Application Support			
Does the SSO solution support a variety of application types (web apps, legacy apps, and terminal apps)?			
Does the SSO solution require custom scripts, custom bridges between applications, or proprietary APIs? If so, what is the additional cost?			
Will the SSO solution have an impact on the run-time behavior or the performance of your applications?			
Does the SSO vendor have formal partnerships with your application vendors? If so, which ones?			
How will clients be updated when vendors release new versions of applications?			
What are the training costs associated with rolling out SSO solutions?			
Are there integrated tools available to help with testing and diagnosing SSO problems?			
Authentication Management			
Which strong authentication modalities (i.e., biometric, proximity, smartcards, or tokens) are supported by the SSO solution?			
Are there any additional server-side or client-side components that need to be installed in order to support a specific strong authentication mechanism?			
What type of support is available for embedded readers in your laptops and/or keyboards?			
Does the SSO solution support combinations of devices, PINs, and passwords for two-factor authentication workflows?			
Is the SSO solution flexible enough to allow for two-factor authentication at specific instances in an application, such as ordering of a controlled substance or credit card payment entry?			

	Imprivata	Vendor 2	Vendor 3
Integration with Existing Infrastructure			
What is the maximum number of users that the SSO solution is capable of managing?			
Will the SSO solution work with desktop and/or application virtualization technology that you've installed from VMware, Citrix or Microsoft?			
Can the SSO solution integrate with multiple directories and/or provisioning systems?			
Does the SSO solution support thin and zero clients?			
Will additional software and server components be required to provide self-service password reset and reporting/auditing capabilities?			
Does the SSO vendor have a mobile strategy?			
What out-of-the box reporting capabilities exist?			
Will the reporting capabilities provide real-time, consolidated data across all your sites and user groups?			
Is there event monitoring available out-of-the-box?			
What additional databases will be required?			
Ongoing Management Support			
Which IT resources are necessary to maintain the SSO solution?			
Which skill sets are required to handle administration of the SSO solution?			
Can administrative tasks be performed remotely?			
Does the SSO solution include tools to update users automatically?			
How will the SSO solution deal with security patches?			
What additional infrastructure is required for fault tolerance?			
What additional infrastructure is required for test environments?			
Does the SSO solution allow you to limit the number of concurrent user sessions?			
How and where are policies, credentials and log files of the SSO solution stored and made accessible for administrators?			
Does the SSO solution vendor need to be involved in creating or maintaining additional scripts, bridges, or upgrades?			
How difficult is it to train new staff should a team member leave?			
Security and Data Protection			
Does the system support off-line mode?			
Does the system support self-service password resets using common questions?			

	Imprivata	Vendor 2	Vendor 3
Is there a security model that describes how a user's credentials are secured on the server, in transit to/from the client, on the client machine and if applicable, in the offline cache?			
Which encryption technology is used to secure the credentials?			
How are the servers used in the solution locked down? For example, does the SSO solution automatically secure ports and configure firewalls and IDs?			
Do security patches to the SSO solution include updates to all the operating components? Or, are you required to patch individual components (operating system, directories, databases, etc.)?			
How will backups be created? If backups contain SSO credentials or audit records, will they encrypted to protect off-line information?			
Does the SSO solution have built-in redundancy, failover and backup for every component of the architecture?			
How does the SSO solution handle disaster recovery and failover?			
Will the SSO solution comply with industry requirements? And, if so, which ones is the SSO certified for?			
User Workflow			
Can the SSO solution easily adapt to existing security policies?			
Will the end user interact with the SSO system intuitively? Or, will they require extensive training?			
What is the log on/log off experience for the user? Is the SSO system designed to streamline access to the user's desktop?			
Does the SSO solution support saving and restoring the desktop state as the user roams? With Citrix? With VMware?			
If users walk away from their workstation will it be automatically secured? If so, what do users need to do for re-authentication?			
Is there support for fast user switching on shared workstations?			
Is there support for fast user switching in Citrix sessions?			

Enabling Healthcare. **Securely.®**

1 877 ONESIGN | 1 781 674 2700 | www.imprivata.com