Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Considerations For Implementing Single Sign-On Within The Enterprise

The goal of this paper is to provide insight into many important areas that should be considered before implementing an enterprise SSO system. It begins with a general overview of an SSO system. Business management considerations are then discussed. Technical and customer service considerations follow. Vendors and their solutions are briefly covered. Some closing comments complete the paper.

Copyright SANS Institute
Author Retains Full Rights

AD

Considerations For Implementing Single Sign-On Within The Enterprise
Russell Hobbs
SANS GSEC Practical Assignment v.1.4b, Option 1
September 1, 2003

1 Abstract

The goal of this paper is to provide insight into many important areas that should be considered before implementing an enterprise SSO system. It begins with a general overview of an SSO system. Business management considerations are then discussed. Technical and customer service considerations follow. Vendors and their solutions are briefly covered. Some closing comments complete the paper.

2 Terms

API	Application Programmer Interface.
Application	A network based application accessed by a user.
Attribute	A database field.
ESSO	Enterprise implementation of Single Sign-On.
GUID	Global Unique IDentifier.
Host	A network attached server that hosts one or more applications.
JAAS	Java Authentication and Authorization Service.
J2EE	Java 2 platform, Enterprise Edition.
RDBMS	Relational DataBase Management System.
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SSL	Secure Socket Layer protocol [SSL]
SSO	A "user authentication process that permits a user to enter one name and password in order to access multiple applications." [TECHTARGET]
Target	A network based application accessed by a user
TLS	Transport Layer Security [RFC2246]
User	An end user of an application. This may be a human or another application.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3 A General Single Sign-On (SSO) System Description

An SSO system enables a company to enforce security policies and procedures upon a targeted application user community. The enforcement utilizes security information known about the user at that particular instance. The minimum functionality required in an SSO system is:

- Login authentication
- Application access control
- Application subscription method
- Monitoring

3.1 Basic Architecture

A basic SSO system architecture is comprised of three main components: access control, a centralized security engine, and the security databases. Each of the components provides critical real-time functionality necessary to effectively secure target applications accessible to users.

3.1.1 Access Control Component

The access control component is typically made up of many sub-components responsible for policing communications channels between the user and a target. It provides the centralized security engine with pertinent security information about the user and which target the user is attempting to access. Then, it enables or disables the communications based on commands from the centralized security engine. In some cases, the access control component may be commanded to redirect the user to another network target.

The functionality of the access control component can be embedded within the target or provided by a separate specialized SSO application. An embedded control is implemented using defined SSO Application Programmer Interfaces (APIs) that communicate directly with the centralized security engine. These APIs are located within a security framework specific to the target. This type control is generally used in custom built or legacy targets.

When access control is provide by a separate security application, it is inserted directly in the communication layer between the user and the target. It utilizes the same processes and APIs as the embedded access control. The target typically can function regardless of whether the security application is present. This type control is generally used to secure 3rd party targets or web sites that have little to no security framework themselves.

3.1.2 Centralized Security Engine

The centralized security engine accepts user information provided by the access control component. It then retrieves any available information about the user from the security database. Using this information, it then applies the appropriate security policies to determine if the user should be granted access to the target. Once a determination has

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

been made, it then sends the appropriate command to the access function. Any audit or status information is updated in the security log databases.

3.1.3 Security Databases

The security databases may be comprised of several different databases in different locations. One set is generally dedicated to maintaining all user pertinent data such as user login names, passwords, GUIDs, policies, user status information, and authorized target application lists. This set resides on the most secure database platform available. The second set is dedicated to log and status information. It generally contains log entries of user security events and system component metrics. These databases can exist on every host that is SSO enabled. A database engine of some type is required for all security databases.

3.2 Enhancements And Options

While a basic architecture and the functionality it provides will suffice in small implementations, an enterprise implementation will require more enhancements and options.

3.2.1 Architecture

Several of these enhancements are core to the architecture. The most important is a multi-tiered network architecture. This type architecture allows most, if not all, components to be located on separate hosts. This usually takes the form of having access control components reside on the web server layer. Then, the security engine is located in the applications layer, and the security databases are located in the highest secured data storage area. This type architecture allows the SSO system to be implemented within a layered defense security infrastructure where components communicate across security boundaries.

Currently, few security open standards have a large enough implementation base to be considered strongly accepted within the industry.

A fully featured set of embedded and separate application access control components will provide the flexibility needed to deal with legacy systems, 3rd party software packages, and transaction systems. The embedded components should be able to handle security down to the transaction level. The separate application access control components should be able to control URL access on a variety of popular web servers.

Access control components, that work with other security devices, should also be considered if the targets require higher security protection. Smart devices provided to the user, enable a higher level of authentication than passwords. Biometric devices can provide an even safer and user-friendly method of authentication. [GALLAGHER] Drawbacks to these type security devices are generally limited to cost and enablement of the device itself.

All SSO systems implement some level of standards support. The common ones are industry standards like LDAP for security databases, SAML for security information and X.509 for certificates. [SAML] Others are Java, C, and DCOM API implementations for

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the embedded access control component. Other vendor standards are not as commonly implemented and generally viewed as enhancements. These include connectivity support for web servers, proxy servers, J2EE application servers, and key management systems. The vendor that controls the standard should certify any of these enhancements.

The last architectural enhancement is the ability to integrate with an identity system. This will be discussed later in section 5.11.

3.2.2 Acceptance Of Terms And Conditions

Some companies are required to display legal agreements to the users and get their acceptance before a target application can be accessed. This may be due to contractual requirements by 3rd party content providers (News providers, financial information providers, NASDAQ, etc.). The best time for this to occur is immediately after the user has been authenticated. Linking this feature into the SSO system and associated auditing should enhance evidence presentation in any prosecution or defense action.

3.2.3 User Enabled Password Reset Feature

One of the best enhancements to implement is a automated user enabled password reset feature. External users interact with many security systems from many companies. Some percentage of these users will forget or misplace their password to your system. If the user must contact customer service, then the number of users will impact the number of customer service representatives necessary at the time of primary target access. Seasonal access times, such as the holidays, must also be accounted for. An automated password reset feature will help minimize human customer service demands.

Careful consideration must be applied to this area. There are many advantages to a friendly automated password reset process. But the difficulty of maintaining an adequate level of security increases significantly. Generally, the SSO system becomes less secure as the friendliness of the reset feature increases. The more secure it is, the less user friendly. This, in tern, equates to additional customer service staffing. Somewhere in this, a compromise will be made based on the number of users, the level of security required, and the funding available to staff a customer support group.

Some automated solutions may not help as much as expected. Take the case of a password reset based on a question and answer pair setup during target enrollment. If the users access the SSO system infrequently and they forget their password, they have probably forgotten the answers needed to complete the reset. Therefore, they have to call customer service, defeating the original purpose of the password reset.

3.2.4 Multiple Named Domains

Most enterprises have multiple registered Internet domain names. They are used to logically group related items such as divisions, product sets, or security levels. Some of the domains may be intranet only. There may be 3rd party domains that provide various functions for the enterprise. Examples are human resources, financial services, and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

hosting sites. The result is the need for the SSO system to authenticate, and possibly protect, multiple domains.

Most SSO systems have some type of functionality that will satisfy these needs. But care should be taken to fully understand any limitations or additional security risks introduced by this functionality.

3.2.5 Monitoring And Reporting

The importance of monitoring and reporting is usually overlooked and thus, sold as an add-on package. These needs generally do not become apparent until implementation begins. The implementation and support teams quickly realize the need for accurate metrics on component performance and errors. Security teams will focus on audit tracking to assist with security incident handling. And management will focus on metrics associated with response times, availability, total and concurrent users.

Determine which metrics the various groups will need and verify their collection within the system. Check accuracy and availability. There should be three different presentation formats available for viewing the data: 1) real-time for monitoring; 2) real-time with historical for troubleshooting; 3) and historical for trend analysis. All should be readily accessible by only authorized personnel.

3.2.6 Security Management Flexibility

Security management is the ability to implement restrictions and workflow on the user base. The better systems allow the implementation of policies, which are applied to user or application groups. The policies are sets of rules stored in the centralized security database. The rules usually dictate such requirements as password expiration, user id and password restrictions, etc. Consolidating these rules into a policy helps maintain consistency within the system.

Workflow deals with directing the user down pre-established paths based on knowledge of the user at the time. Some of the workflow systems are tied directly to identity systems. Care should be taken not to extend the workflow outside of the SSO system. The key to security management is obtaining the flexibility to perform the required security needs but not trying to solve non-security related needs.

3.3 Defining Enterprise Single Sign-On (ESSO)

The differences between a standard SSO system and an enterprise SSO system are mainly in requirements for scalability, availability, and legacy linkages. Because of the larger user base impact, enterprise implementations will have many more groups "assisting" with requirements. The more important groups are:

- Security
- Procurement
- System hardware and software support
- Management
- Financial

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Enterprise customer support

4 Leadership Details

Understanding, and educating, the enterprise leadership is one of the less obvious details that is extremely important to all phases of implementation. Some of the key areas follow and should be clearly understood by the leadership, and all other groups, associated with the effort.

4.1 Management Motivation For Implementing An SSO System

Establish the real reason for ESSO. It may be as simple as a more cohesive logon process across multiple target applications. More likely, it has to do with enhancing existing security. Regardless, explore the leadership's views on applying security consistently, risk reduction, multi-factor security, and legal or contractual requirements. Spend time validating that leadership understands Internet risks and issues not addressable by SSO. While this is a broad area, there are many good articles that can enlighten leadership. [CONCERNS]

4.2 Sponsorship And Ownership

The two most important ESSO leadership positions are the sponsor and the owner. The sponsor champions the ESSO to other high level leaders. They must be in a company's top-level authority position because of impacts to all user applications. They must have long-term commitment and financial resources. Ideally, this person is responsible for all enterprise security.

The owner is responsible for the actual implementation. They should be highly qualified in management as well as security technologies. They should work directly with the security owner and the applications owners. The more experience with enterprise utility implantations, the better.

4.3 Development And Support Leaders

A pro-active effort should be initiated to reach out to the applications development and the legacy support leaders. These leaders are going to be impacted most by an ESSO because they have pre-established goals, schedules, and funding commitments to their business partners. The impact is magnified in circumstances where a previous SSO system didn't exist. And this is where the ESSO vision plays an important part. The more the ESSO vision provides funding and packaged security solutions that require minimal application integration, the faster it will be adopted.

4.4 ESSO Vision

Both sponsor and owner must present a single clear vision for the ESSO from the start. The vision will mature over time but must remain consistent. The clearer this vision is, and the higher the authority backing it, the less impact of other group politics, priorities, and agendas.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The vision should address three primary areas: 1) benefits of ESSO; 2) application integration with ESSO; and 3) ESSO performance expectations. The benefits are directly related to the management motivation information. The application integration will be a compromise between two extreme positions: 1) Force all applications to implement ESSO on their own with little or no help, or 2) Provide supported packaged security solutions, funding and assistance with ESSO implementation. The development and support leaders will be increasingly difficult to work with when the compromise approaches the first extreme.

The performance expectations are addressed in ESSO service level agreements (SLAs). It is critical that leadership understand the risks and impacts of ESSO failure to downstream applications before determining SLAs. Many applications have application specific SLA agreements requiring a minimum of 98% availability to their user base. Most applications that are utilized by other companies will have some type of contractual penalty if the application SLA is not met. Once the application is protected by ESSO, it also inherits any outages that are experienced by the ESSO, thus decreasing the total availability to the user.

Additional customer satisfaction concerns occur when the user encounters multiple negative experiences with the ESSO itself. [Chen] The user will question the company's credibility after the first bad SSO experience. By the third bad experience, the customer may believe that the company has no credibility. This can have major impacts to "brand" based companies, especially in the financial industry.

The situation is compounded as the number of ESSO protected applications increase. The result is a need for 100% ESSO availability, or a maximum 2% ESSO outage that coincides with all application outages. The probability of either of these two situations occurring is remotely small regardless of how much funding is available or how lucky the corporation is. The end result is an ESSO SLA that drives fault tolerance and scalability.

Some companies have multiple types of outages such as scheduled, unscheduled, and degraded. These should be clearly defined within the ESSO SLA and accurately monitored. Monitoring should be internal, as well as external. Internal monitoring provides the ability to determine if outages are application specific, ESSO specific, or a combination of the two. External 7day by 24 hr monitoring by an independent 3rd party provides a realistic view as seen by the user. Both are absolutely essential in a high availability environment.

4.5 Funding

Several key funding issues should be resolved before the project begins and included in the ESSO vision. The first issue deals with how the funding actually occurs. A continuous budget based on phases is recommended over a yearly budget. This minimizes the need, or temptation, to play corporate "budget" games towards the end of the budget cycle. The results are almost all positive and range from the more realistic spending forecasts to adequate job level security felt by the support team.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The next most important funding issue addresses the ESSO support group. Be willing to attract, and maintain premium personnel. And fund continuous training. This group directly impacts SLAs and customer relations.

The next issue deals with vendors. Structure the contracts in a way that makes the vendor financially accountable, to some degree, for a successful implementation. But also exercise fairness with the vendors regarding accountability. Most corporations have problem groups, procedures, or politics that are internal to the corporation itself. Attempting to make a vendor accountable for these internal issues will ultimately result in blame pointing between the vendor and the corporation. This will have negative effects on a vendor relationship and future mutual efforts such as major upgrades.

Funding issues will occur with every legacy application that needs to be integrated with the ESSO. Proactively including this in the ESSO budget will pave the way for successful partnerships with the legacy teams.

Sufficient levels of funding for vendor package customization must also be addressed. The amount of customization applied to a vendor package will directly impact long-term maintenance and future upgrade costs. This can be justification for purchasing a more expensive vendor solution that requires significantly less customization to meet the requirements.

A separate hardware and software environment should be funded for ESSO testing and training. It should be configured like the other environments, including the security databases. This will allow the support group to repeated test installation and upgrading without impacting the other environments. It also allows isolated testing with applications.

And finally, plan on funding new hardware and OS environments for any significant future upgrade. This will save time and contribute to future scalability in the long run.

5 Important Technical Details

The technical details of implementing an ESSO are significantly easier to identify and address. The following sections cover areas that are important but rarely addressed.

5.1 Technical Staffing

The technical team will consist of members in four primary roles: 1) project managers directing the teams; 2) integration engineers responsible for application integration efforts; 3) system engineers responsible for ESSO infrastructure support and modifications; and 4) operations staff for ongoing monitoring and minor issue resolution. Because of the critical role of the ESSO, every effort should be made to staff these positions with experienced talented individuals that have excellent work ethics. Most of these individuals will command premium salaries. Caution should be exercised if there is an effort to introduce a significant number of inexperienced staff, especially in the beginning.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The team should also have sufficient resources and available time for testing and training. This applies especially to the system engineers. Most of their efforts will center on preparation for failure recovery. While this looks unproductive to management, it is essential to the successful ESSO. This group will be relied on to keep prime time outages limited to just a few minutes vs. several hours.

5.2 Begin With The Current Environment

Implementation of a new ESSO system should begin with a through examination of the current environment. Valuable information can be obtained from any legacy security system that may exist in the environment. The most important facts will deal with application integration efforts. If this information does not exist, a thorough survey of current and future application needs should be performed. Information on the following topics should be compiled and analyzed:

- Types and probable access components required
- Ownership contacts and support groups
- Available funding
- Estimate effort and cost to integrate with ESSO. Don't forget testing!
- SLA requirements for ALL environments

5.3 Change Management

Establishing a change management process is critical. It should be thorough, yet flexible. And it should be the same process for all environments to minimize confusion by integrating applications. A pre-development or test environment may be exempted for this process as long as it is isolated from all other environments.

5.4 Security Database

The security databases are the most critical components within the system. The most important decision with this component is the type of database engine in which it will be implemented. Vendors usually provide the choice between LDAP and a common RDBMS. LDAP is specifically designed for organizing object-oriented data in tree like structures. It is highly optimized for drill-down reading from the top of the tree. It is not designed for frequent updates, frequent inserts of new objects, or relational type searching. These drawbacks are the reason it is not commonly used. The RDBMSs are general database engines that are very flexible but not as optimized for reading.

Care should be exercised when deciding which database engine to use for hosting the security databases. The vendors will prefer an LDAP engine because of the reportedly faster response. And they will gladly assist with implementing a new one if desired. But the decision should depend on the supported database engines that all ready exist within the environments. The reason is due to available support resources.

Most enterprises have a support group dedicated to supporting their database systems. This is because of the skill required to design, assemble and maintain them. One small

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

mistake early in the design can cause massive negative performance impacts in production. Selecting a supported database engine minimizes implementation time and allows leveraging of an existing support infrastructure.

5.5 Tools

Support tools are very important and often overlooked. The most important aspect is that all tools are secure and reliable. Configuration tools should be as automated as possible. The process of migrating a configuration from one environment to the next should require minimal hand entry. The more hand entry that is required beyond the initial setup in the development environment, the more configuration or security issues will arise later. Configurations should also provide a "back-out" feature in case issues arise during a change.

Customer service will require a user interface to the security database information. It should work well within the established ESSO security processes and procedures followed by customer service. It should also allow integration of other legacy security system processes and procedures.

5.6 Component Communications Security

Security of communications between components is as important as the security of the databases. All communications should be encrypted and transmitted across an SSL connection. This includes the communications between the security engine and the security databases. The encryption method should rely on certificates, not passwords determined by the installer. This is because somewhere during the implementation there will become a set of "commonly" known passwords between the implementation and support group. The longer the components are in place, the more likely other support personnel will have access to these passwords. It is also a good practice to have the ESSO support group install and configure all components on all hosts.

5.7 Application Integration

The application integration significantly impacts the true security provided by the ESSO. And it is totally controllable. The impacts occur primarily due to the limited security experience of the application development group and the deadlines they must maintain. While they will make their best effort to implement all security requirements and linkages, they generally will not have time to truly understand the security ramifications involved. The best solution is to limit the amount of effort required by the applications developers. This is accomplished by assigning a dedicated ESSO integration engineer to every application before integration begins. The ESSO engineer should be responsible for learning about the application and recommending the best approach to integrating with the ESSO.

The engineer should have an available set of packaged and tested security solutions. These solutions will contain components that can plug directly into an application, or surround an application, and provide the required security linkages to the ESSO. Any new, or modified, solutions should be code audited and attack penetration tested to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

verify correct implementation. These solutions should function on encrypted communications links as well as non-encrypted links. This enables non-encrypted network traces to be effectively used in the development environment to quickly troubleshoot integration problems. The non-encrypted links should never be enabled in the production environment.

5.8 External Group Communications

The perception of security provided by the ESSO is crucial to application users, management, and others. The best way to control this perception is by establishing communication channels that provide accurate and timely information about the state of the ESSO system. Using web sites, standing meetings, and emailing newsletters can effectively accomplish this.

The public web site should present non-security sensitive information targeting the application user audience. The purpose is to provide information that addresses general user questions, builds customer confidence, and minimizes customer service calls. Some of the more important topics are:

- Customer service contacts
- Brief overview of the ESSO system, including flow diagrams
- Current and historical availability measurements
- Status of any current outage
- Enrollment process overview
- Password selection recommendations and requirements

The customer service group can assist with providing a list of most frequently ask questions, as well as the responses to those questions.

The private web site should present any information that could present, or increase, a security risk if made known to the public. Several topics will be briefly covered. The most important topic is current issue status information for every environment. The timeliness of the updates can depend on the criticality of the issue. The most critical issues should be updated every 15 minutes at a minimum. A related topic is information on the issue resolution process. This would include resolution methodology, root cause analysis, application owner notification procedures, and issue escalation procedures.

The next topic is current and historical metrics. Any metric that can address management questions or assist with issue resolution should be available. The metric presentation should be available in tabular and graphic form. The next topic is a daily calendar of events containing pending ESSO system changes and application integrations. Adding issue and outage information also provides management a high level view of events occurring within the environments.

Meetings will be necessary to effectively communicate with some groups. A monthly meeting should occur with application and customer support groups. The meetings should also support virtual attendees. Topics addressed should include recent issues and resolutions, review of the ESSO calendar, and a Q&A period. A monthly or bi-monthly education training session should be held that focuses on educating the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

application integration teams. Other meetings, such as integration or testing, may occur weekly or daily.

The monthly email newsletter is targeted at a broader audience that is interested in the ESSO system but does not have day-to-day interaction with it. This should contain summarization topics covered during meetings, metric evaluations, upcoming major changes, and a contact list. A method should be enabled for self-subscription to the email newsletter.

5.9 Customization Of Vendor Packages

Caution should be exercised regarding the type and amount of customization that is performed on a vendor package. The maintenance, support, and upgrade costs rise significantly as more customization is applied to the ESSO. Significant user confusion will occur if each application has its own customization. This is due to the inconsistent look and feel experienced by the user. The best approach to a new ESSO implementation would be to only customize branding and legal verbiage. Once the system is completely operational and an upgrade cycle has been completed, accurate impacts of requested customization could be determined before implementation.

5.10 Vendor Updates And Upgrades

Vendor updates are patches to fix issues experienced with their package. Create a process that allows for these updates to occur on a regular basis. And practice it regularly. This keeps the process integrated with all the other activities that must be performed. It is also less likely a major security breach or process issue arises unexpectedly.

The effort required to upgrade a system depends on the support provided by the vendor and the amount of customization previously made to the vendor's package. When negotiating the initial purchase of a vendors' product, require their partnering in implementation of upgrades to the pre-development and development environments. But don't expect them to support the customization because it is not effective to have them learn your company's non-security related polices and procedures.

5.11 A Need For An Identity System?

SSO systems only require a few attributes for each user. Such as GUID, current password, and application access list. This creates a dilemma when needs emerge to maintain information related to SSO security, but not required by the SSO. This usually occurs during requirements gathering. The information generally has something to do with user access control to application embedded functions. An example would be the need to maintain a link between a 3rd party's internal application security and the ESSO GUID. The link would be required to seamlessly log a user into the 3rd party application after the user successfully logged into the ESSO. The application group and the ESSO group generally have two different viewpoints on this topic.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The application group's view is that there are only a few attributes the ESSO system would have to maintain. There generally isn't a way for the application to link this information with the external access control components provided by the ESSO system. The ESSO group's view is quite different. Every application requires different attributes. Maintaining these attributes requires customization, which increases support and issue resolution costs. Additionally, applications with small user counts and large attribute requirements will have huge impacts on security databases that support large user counts for other applications.

Another need emerges from the ESSO customer service group to keep user information such as social security numbers, account numbers, or employee numbers. This information is used to authenticate users before performing security actions, such as password resets, on their behalf.

The industry promoted solution to this dilemma is the implementation of an Identity system. These type systems are designed to address inter-application identity linkage needs. They also generally contain workflow engines that are very useful in the customer service area. Regardless, they are well worth investigation as a support system for the ESSO system.

5.12 User Training

The last important technical topic is user training. Every effort should be made to minimize any training a user might need. This is achieved by maintaining a streamlined process for each SSO function. The same process and the look-and-feel should be used for every application. And the user should have a way to access customer service web or representative help at any point in the process. Be sure to follow-up regularly with the customer service group. They should be able to provide very accurate information on which areas the users are having difficulties with and possible solutions.

6 Who Provides Customer Service?

There are three viewpoints regarding who should provide ESSO customer service. The first is that existing application support groups should perform this function. There are significant advantages to this approach because these groups already exist. These groups are usually highly trainable in new processes and most staffing issues should be well under control. User discontent can also be minimized because a single customer service representative would be able to perform all functions without having to transfer the user to another representative. But this can place the representative in a precarious position.

Representatives are usually evaluated based on feedback by the users they have interacted with. If a situation occurs where a user cannot provide sufficient information for the representative to clearly authenticate the user, the representative should deny the user's request to reset or modify security information. The dissatisfied user could then provide negative feedback to management that would penalize the representative for taking the appropriate actions. If this occurs often, the representative may be motivated to take security risks in order to satisfy the user's request. One method to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

minimize this potential conflict is to implement a security exception process. The process should clearly document all actions by the representative and require a higher level of approval. It should also be completed quickly without the need to perform user callbacks or transfers.

The second viewpoint is that a dedicated ESSO customer support group should exist. This group could insure that consistently applied procedures were followed. They would not be as susceptible to pressure by the business partner to take security risks. They would also have better visibility of the ESSO system status enabling them to detect issues and initiate resolutions quicker. But staffing levels may be hard to efficiently maintain if application user counts change dramatically in short periods of time.

The third viewpoint is that of a dedicated ESSO customer service group within an existing application customer service group. This addresses the issues of the previous two viewpoints but is only feasible if a large consolidated applications customer support group all ready exist.

7 Vendor Selection

Before vendor selection begins, some basic questions about the effort need to be answered:

- Is the current staff competent enough?
- What are the funding limitations?
- What is the timeframe?

Once these are obtained, selection of a SSO vendor can proceed based on how effectively their solution meets the enterprise needs and requirements. Name recognition, or how much effort their sales representatives spent convincing top management that they were the best, should never impact the decision.

7.1 Research

Technical research services are very helpful in the initial research phase of vendor selection. Stick to the better fee based research services instead of the free ones. These services provide broad vendor comparisons that can be used to narrow the selection down to 3-5 vendors quite rapidly. Some well-known services are:

- Gartner Group (http://www.gartner.com)
- Giga Information Group (http://www.gigaweb.com)
- Meta Group (http://www.metagroup.com)

A good source list of SSO vendors is available from the editors of esecurityplanet.com titled “Authorization and Single Sign-on Products”. (URL: http://www.esecurityplanet.com/resources/article.php/964361) [VENDORS]

7.2 Major Vendors

Several major vendors have been providing SSO solutions for a number of years. Information provided below. Their web sites are great sources of information. Most will require registration to access the information but none charge fees.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7.2.1 Netegrity

URL: http://www.netegrity.com

Products: [NETEGRITY]

- SiteMinder – "access management solution for web-based and enterprise applications"
- TransactionMinder – "secured web access to Web services"
- IdentityMinder
  - Web edition– "a flexible, roles-based user administration and access management solution for Web-based applications"
  - Provisioning Edition – a "comprehensive provisioning solution for creating, modifying and terminating identity-based access to Web-based applications, enterprise systems, and physical resources."

7.2.2 Oblix

URL: http://www.oblix.com

Products: [OBLIX]

- NetPoint – An identity system with web access control and a work flow engine.
- IDLink - Identity management integration with CONTROL-SA™ from BMC Software

1.1.3 RSA

URL: http://www.rsasecurity.com

Products: [RSA]

- ClearTrust – "The RSA ClearTrust solution is an open, interoperable, Web-based architecture that is designed to provide a unified security management solution for integrating into existing, heterogeneous, multi-vendor environments. Supporting SAML, Java, C and DCOM APIs, the product can be further customized into your unique environment."

Misc.: An RFI/RFP Access management proposal template is available on this web site.

8 Closing Comments

Implementing an enterprise single sign-on solution is an intense and expense endeavor for any organization. Not only do the users have to be satisfied, but many other groups (security standards, management, customer service, application support) have to be satisfied as well. This ultimately leads to compromises between: 1) what security the users will accept; 2) the desired level of security; 3) what can be implemented technically; 4) the ability of the implementation and support teams; and 5) the budget size.

The potential impacts to the users are the most important considerations in this endeavor. The effort will be wasted unless the users can, and will, use the deployed solution.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[CHEN] Chen, Anne. "Single Sign-on? How About a Password That Works?" March 7, 2003. URL: http://www.eweek.com/article2/0,3959,921764,00.asp. (August 31, 2003)

[CONCERNS] Ellison, Gary; Hodges, Jeff; Landau, Susan. "Security and Privacy Concerns of Internet Single Sign-On." Sept 6, 2002. URL: http://research.sun.com/Liberty/SaPCISSO/sapcil.pdf. (August 31, 2003)

[GALLAGHER] Gallagher, Sean. "Getting a Handle on Biometrics." March 18, 2002. URL: http://www.baselinemag.com/article2/0,3959,818884,00.asp. (August 31, 2003)

[NETEGRITY] Netegrity, Inc. URL: http://www.netegrity.com

[OBLIX] Oblix, Inc. URL: http://www.oblix.com

[RFC2246] Dierks, T., Allen, C. "The TLS Protocol Version 1.0." RFC 2246. January 1999. URL: ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt. (August 31, 2003)

[RSA] RSA Security. URL: http://www.rsasecurity.com

[SAML] "An XML-based framework for exchanging system information". August 19, 2003. URL: http://www.oasis-open.org/cover/saml.html. (August 31, 2003)

[SSL] Freier, Alan., Karlton, Philip., Kocher, Paul. "The SSL Protocol Version 3.0." November 1996. URL: http://wp.netscape.com/eng/ssl3/draft302.txt. (August 31, 2003)

[TECHTARGET] URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci340859,00.html. (August 31, 2003)

[VENDORS] "Authorization and Single Sign-on Products." June 11, 2003. URL: http://www.esecurityplanet.com/resources/article.php/964361. (August 31, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced