

EVIDIAN

A Bull Group Company

7 rules for a successful SSO project

Based on 15 years of experience in single sign-on (SSO), this white paper describes the good practices for and the traps to avoid in order to achieve a successful deployment.

white
paper

Laurent de Jerphanion
April 2009

39 F2 33LV 00

Deploy SSO in your organization

Single sign-on (SSO) enhances user productivity, reinforces security, brings down helpdesk costs and helps an organization comply with legal constraints.

However, an SSO project cannot be implemented just like that. It must be well prepared to ensure speedy deployment, attainment of project objectives, and users' participation in the project.

For nearly 15 years, Evidian and its partners have implemented hundreds of SSO projects. The main lessons learnt from these projects are described in this document. As you will notice, most of these "golden rules" concern project organization, beyond the purely technical aspects:

1. **Clearly define** and share the project objectives.
2. **Demonstrate** that the project improves regulatory compliance.
3. **Involve** users actively in the project.
4. **Take account of** existing procedures and policies.
5. **Target** a simple architecture.
6. **Publish** figure indicators regularly.
7. **Assess** the attainment of objectives and plan extension to identity management.

What is single sign-on?

With single sign-on or SSO, you can access all your applications using only one authentication method; for example, a password, a USB token, or your finger if you have a biometric reader.

Typically, single sign-on uses on a PC a discreet software application which enters application passwords on your behalf.

If you are using web applications only, or if you are working in "thin client" mode, the SSO software is hosted by a server and enters the passwords remotely. In this case, you do not need any local software application.

(1) Clearly define and share the project objectives.

In summary

The objectives of a successful SSO project are always very concrete, for example:

- ▶ Reducing helpdesk costs
- ▶ Improving users' productivity: doctors, salespersons, traders, etc.
- ▶ Reinforcing security by controlling access to critical applications
- ▶ Complying with laws and regulations: medical secrets, PCI DSS, etc.

In general, each SSO project has one or two main objectives, with some precise sub-objectives. It is important to define in writing the expected concrete results.

This SSO target plan may be open to formal comments by project participants. It can even be subject to collegial decision-making, for instance, by external participants such as the systems integrator and internal participants: finance, internal control or operations departments.

Why is this important?

A well defined objective, with cost estimates, helps you to retain the support of your management in the course of the project, and will serve as reference for project participants.

External service-providers will be able to adapt their work to focus on the actual business priorities – or make proposals to ensure their attainment. Depending on the business objectives, some tools or methods are more suitable than others.

You will ensure the participation of an operations department or even other departments by working with them to evaluate the expected benefits. This will strongly facilitate project implementation and users' participation.

Practical case

A pharmaceutical company wished to introduce single sign-on. Its concrete objective: complying with US regulation 21 CFR Part 11 which requires that electronic documents submitted to *Food and Drug Administration* be validated and signed by the right persons.

Initially, the company planned to install a SSO solution for web applications only (this only required one secure SSO "portal"). But while reviewing the conformity objectives with the operations teams, the project participants noticed that many risks concerning document integrity came from "client-server" applications.

Evidian and the integration-service provider recommended that a complete enterprise SSO solution be deployed for the client-server applications. As this approach also takes web applications into account, the initial functional objectives were achieved – along with the actual business objectives.

(2) Demonstrate that the project improves regulatory compliance.

In summary

Even if the main objective of the SSO project is operational - productivity or cost reduction for example - it may be useful to contact the internal control unit. Indeed, a SSO solution can enable the company to achieve its regulatory compliance objectives, or to simplify existing control procedures.

Most laws and regulations aim to improve the integrity, confidentiality or availability of IT systems. It is easy to see why SSO can help the people in charge of compliance:

- ▶ **Integrity:** SSO limits access to critical resources (for instance, financial resources) to persons whose role requires such access.
- ▶ **Confidentiality:** the applications that manage personal data (medical information, payment cards) are protected by SSO. Access logs are stored at a central point.
- ▶ **Availability:** if a password is forgotten, the PCs and applications can remain available thanks to a system of security question and answer. Moreover, if the SSO solution uses existing directories, it is easily included in an emergency plan.

Why is this important?

If you include the internal control unit in the project, even for consultation reasons only, it can lend additional credibility to this effort. Regulatory compliance is a management-visible objective because non-compliance has a lot of consequences for the company.

Moreover, by expressing their opinion on the deployment project at a very early stage, the internal control unit may make some recommendations that will be useful later. The way you deploy SSO can help them perform their audit tasks better.

Practical case

A big Brazilian telecoms company wished to deploy SSO so its users can be more productive, and to comply with Sarbanes-Oxley. The purpose of this US law is to ensure the integrity of financial reporting.

While preparing this project, Evidian and its local partner consulted the client's internal control department, as well as external auditors. This consultation revealed other needs not identified initially.

For example, auditors verify control procedures by viewing consolidated access data. The auditors, therefore, asked that this SSO data remain unchanged, and that its origin be systematically documented.

Finally, the project team wrote procedures for verifying the information gathered. This made it possible to speed up by several days the annual audits of access procedures.

(3) Involve users actively in the project.

In summary

Employees are the main persons concerned by SSO. So, it is very important to seek their opinion and to take that opinion into consideration in the deployment process. It is not enough to seek the opinion of their managers!

Therefore, you have to identify the most influential employee categories. They may be wary of a novelty like SSO, but will become its driving force once convinced. All their observations will enable you to anticipate user reaction during deployment.

- ▶ Identify the profiles and persons who will benefit most from SSO.
- ▶ Hold regular meetings of 'pilot' users, with demonstrations.
- ▶ Propose to them to test the SSO solution prior to its release.
- ▶ Be aware that some of them may see SSO as a "spy" on their PC.
- ▶ Present to them the business - and not technical - advantages.

Why is this important?

Employees usually understand the advantages brought in by SSO quickly. You can, therefore, transform them into promoters of the project: SSO users are often the best advocates for it.

On the other hand, users' remarks help to detect and correct some hitches in advance. For example, you will identify a critical application to be taken into account, local requirements, or some overlooked needs.

Practical case

A French hospital wished to deploy single sign-on for its healthcare staff. In a hospital, the time lost entering passwords has an impact on the quality of healthcare services. Therefore, single sign-on based on the healthcare staff's smart card allows them to devote more time to patient care.

The project team made several demonstrations to healthcare staff representatives and performed a test in a department.

It noticed that some doctors, who regarded information systems as a constraint, wanted the system to be as discreet as possible. On the other hand, doctors appreciated the speedy launch of applications and the fact that accesses were logged. Moreover, nurses quickly adapted to SSO access on a PC on the inspection trolley.

However, doctors at the emergency department rejected the systematic use of a smart card for authentication. This impeded access speed.

The solution was to adopt a specific security policy at the emergency unit, based on a grace period and session mobility. As access to this unit is physically controlled by a smart card, it has been possible to combine speed with security.

(4) Take account of existing procedures and policies.

In summary

SSO is not just a "technical project": it may change the day-to-day life of an organization and its hierarchy. Most of these changes are positive.

However, some difficulties may emerge when managers discover that they must modify their procedures to take SSO into account. For instance, the manner in which they grant access rights to applications may change.

Therefore, you must ensure that these changes are reduced to a minimum, and anticipate them when they are unavoidable. Better still, allow each organization to plan some phases gradually according to their own needs.

Why is this important?

A well prepared deployment, with the participation of site or division managers, has excellent probability of success.

In general, reluctance on the part of managers is not a question of inertia: they do not all have the same priorities and calendar. For example, finance or sales departments avoid installing new tools near the end of a fiscal year.

Even if SSO simplifies the procedures – one can manage access to all the applications from just one screen – local administrators need to be trained. Moreover, if a procedure exists for legal reasons, it is certainly documented and audited; changing it is costly.

Practical case

An industrial company wished to deploy SSO on over 70,000 PCs. The division and site managers supported the SSO project. However, it soon became clear that each of them had different priorities and specific implementation requirements.

Only a few managers agreed to change their application access management methods right away. Some applications like mySAP had to be subjected to tests before being included in the SSO – in compliance with financial security laws.

The solution: defining, for each site and organization, 10 to 20 basic applications to be integrated immediately into SSO. Applications such as mySAP were initially excluded from that list, to respect the organizations' pace. The decision to "switch into SSO mode" was taken by each division.

In the same way, SSO does not necessarily change the way accesses are managed. It can just automate access to already existing accounts in a first step.

Therefore, SSO was deployed smoothly. Each organization remained free in its choice of calendar and options: which applications to integrate, when to integrate them, and how to manage access rights.

(5) Target a simple architecture.

In summary

A project stands a better chance to succeed if its cost is low, and if adapts well to the existing IT environment. Therefore, the architecture should be as simple as possible – but not more!

Note that the SSO solution itself is only a part of the equation. You also need to have a reliable – and up-to-date – list of users. And for each user to work unimpeded, the SSO information (encrypted passwords, list of authorized applications, etc.) must be available on each main site.

Still, these requirements do not necessarily make for a complex solution. By using already existing directories, servers and network resources, the project can make considerable savings during installation and use.

Why is this important?

Controlling the cost and complexity of a project contributes to its success. You will demonstrate a speedy return on investment more easily.

Your company already has a user identity repository: your LDAP directory. You might as well use this resource, and benefit from existing user update procedures.

In the same way, “appliances” can allow speedy deployment on some hundreds of users. But if your company is organized into several sites, you may have to multiply these devices and the associated support. By using existing local databases, you will take advantage of resident logistics and skills.

Practical case

A British hospital wished to deploy SSO for its 5000-strong healthcare and administrative staff. Its objectives: reducing helpdesk cost and securing access based on the healthcare staff card. Of course, high availability of clinical applications is essential in a hospital environment.

An appliance-based SSO solution was being deployed. However, in view of the volume and complexity of its organization, the hospital had noticed some performance and reliability issues. It realized that, when taking maintenance and replacement into account, operational cost would be higher than planned, and high availability was not guaranteed.

The hospital therefore chose to change the architecture and use the existing Active Directory. This directory can host SSO data itself: no new hardware was necessary.

The SSO data was thus available on each site, close to the users, making SSO faster. The high availability of the SSO solution is that of the directory. Moreover, emergency plans and backup procedures exist already: they are the ones used for the directory.

(6) Publish figure indicators regularly.

In summary

Like for any project, your SSO project is documented with progress reports. But the visibility of SSO goes beyond IT: therefore, these reports must be understandable for non-technicians, and contain indicators that make sense to them. For example:

- ▶ Number of PCs on which the SSO solution is installed, number of users concerned
- ▶ Volume of calls to the helpdesk, problems solved
- ▶ Size and range of collected audit data, activated security functions
- ▶ User satisfaction indices (surveys, etc.)
- ▶ Number of application accounts declared (total and per user)
- ▶ Number of applications covered by SSO
- ▶ Number of automated logins, with an estimate of saved time

More technical points are, of course, important. But reports are both communication and management tools. In a good number of cases, an automated audit tool collects the required indicators. This facilitates analysis and optimization work. Thus, it is generally easy to demonstrate the quick investment return of SSO.

Why is this important?

These reports give a view of the project status. As we have seen, you need to win the trust of operations and financial managers, auditors, etc. They expect objective results: provide them clearly.

Do not forget that deployments are easier when departments concerned participate actively. Once the solution is installed in the first sites and departments, the resulting facts and figures will convince the others. When SSO deployment is over, you will have gained enough credibility to speed up some future phases... or other projects.

Practical case

In the French subsidiary of an international bank, the security department had noticed that the multiplication of passwords was creating security loopholes and irritated the 1200 employees. So, it launched a SSO project, with biometric authentication. To get the green light, an important argument was the expected decrease in the helpdesk cost.

Deployment was accompanied by regular reports. Since the helpdesk is outsourced, it was easy to measure the evolution of calls. By regularly evaluating installations, the project team noticed that there were more diverse configurations than expected. They decided to devote more time to training users on biometrics, and correcting existing issues revealed by SSO, for instance shared passwords.

Thanks to this follow-up, the budget was not exceeded and SSO was very well received by the back office services. The practical lessons learned helped to convince the parent company to generalize the tool abroad.

(7) Assess the attainment of objectives and plan extension to identity management.

In summary

At the end of an SSO project, it is useful to assess whether objectives were met. Some pending points, such as strong authentication and integration of new applications, may result in future projects.

Evidian has noticed that SSO is an excellent first step for more ambitious identity management projects. For after a few months, you will have a useful SSO activity log database. This tells you which application accounts are actually used, and by whom.

Why is this important?

A successful SSO project is an opportunity to propose an extension to identity and access management. The reason for this is simple. Since you now know how applications are used, you can define a realistic security policy. Before enforcing it, you can predict its results.

In the same manner, you will be able to implement account “provisioning”, namely their automated update under the control of an approval workflow. Account passwords will be sent to the SSO solution.

Users will, thus, naturally comply with your security policy. Their accounts will be created and deleted automatically according to employee status in the company.

Practical case

A big European railway company wished to implement a security policy to manage more than 150,000 users of 80 applications, i.e. over one million application accounts.

It started taking an inventory of all accounts. But this turned out to be both utopian and costly. On one hand, getting these accounts was more difficult than expected. But above all, how do you know who is using account “sch002”: one employee, an entire team, nobody? The company quickly realized that working along this line would cost thousands of person hours.

Instead, the company decided to take an automatic inventory of accounts *that are actually used*. Evidian’s SSO client performed that task. For three months, it effortlessly gathered information on the actual usage of the information system. Each time a user accessed an account, this information was logged in a central database.

In a second phase, the company compared this database with the list of all accounts declared in the applications. This enabled it to eliminate obsolete accounts, and to build its security policy on a concrete foundation.

Implementing your SSO project

Each SSO project is different, but they all follow the same general pattern. Note that for deployment on over a few hundreds of PCs, you should use the services of system integrator.

1 – Model

Before choosing a supplier, ask him to install and test its product on some of your PCs with representative applications. Take notes: is the SSO tool easy to install, can it integrate applications easily, will it scale well when deployed on all your PCs?

2 - Planning

Define the functional objectives and inherent costs in writing. Establish a list of internal interlocutors with the system integrator and select some user representatives. Make an inventory of sites, applications to be integrated and specific requirements. This will help you to work out a projected schedule.

3 – Pilot phase

This phase is important; the pilot should be done in a representative department. For example, test the product on 100 users for 30 days. Use this phase as an opportunity to configure the SSO solution on the most common applications. Do not forget to make a detailed assessment and to learn some lessons from it for the general deployment.

4 - Deployment

First of all, check that you have a complete and reliable user directory. If this is not the case, there are tools that can create and keep this source of information up to date.

Secondly, the SSO client will be installed on PCs on a phase-by-phase basis, for example from one department to the other. Clearly notify the users in advance, or even propose some training sessions to some of them. Give the helpdesk some time to answer the unavoidable questions before moving to the next department.

During deployment, regularly provide managers with factual reports. They must notice the progress of the project and the results achieved.

5 - Assessment

Assess the deployment operation at the end of the project. The remaining points to be handled must be identified and described in action plans.

This will be an opportunity to plan the next phases, such as access policy management or application account provisioning.

For further information, please go to www.evidian.com

Email: info@evidian.com

© 2009 Evidian

The information contained in this document represents the view of Evidian on the issues discussed at the date of publication. Because Evidian must respond to changing market conditions, it should not be interpreted as a commitment on the part of Evidian, and Evidian cannot guarantee the accuracy of any information presented after the date of publication.

This is for informational purposes only. EVIDIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

We acknowledge the rights of the proprietors of trademarks mentioned in this book.

white
paper

EVIDIAN
A Bull Group Company