

**EVIDIAN**

A Groupe Bull Company

# Enterprise Single Sign-on

This white paper is an overview of the main functions of enterprise single sign-on products today. It also presents Evidian's Enterprise SSO solution.

white  
paper

Laurent de Jerphanion  
May 2008

39 A2 99LU 01

## What is single sign-on?

During the course of their day, users must enter multiple application passwords, and change them regularly. This can quickly turn into a drain on productivity and helpdesk resources.

With single sign-on (SSO), a user logs in once using a single authentication method, then just uses his or her applications - no need to enter other passwords. To log in, employees can use, for instance, a password, a USB key, or a finger if they have a biometric reader.

## How to use single sign-on

To use single sign-on, you typically install on your PC an unobtrusive software which enters application passwords on your behalf. Even this is not necessary if you are just running web applications or working in "thin-client" mode. In this case, the SSO software is hosted on a server and enters passwords remotely.

SSO makes life easier for users. Evidian has seen companies in which users needed to know about thirty different passwords: today, only one password is enough. SSO also reinforces security and reduces costs, especially helpdesk costs. This is why Gartner estimated in a recent report<sup>1</sup> that the growth of the enterprise SSO market is "robust", while ranking Evidian among the leaders in this field.

## Individual SSO and enterprise SSO

Many individual SSO tools do exist, for instance the auto-complete functions of web browsers. But providing SSO to hundreds – or even thousands – of employees in a company requires an entirely different approach. This is due to the functions that most large organizations require: administration, strong authentication, delegation, mobility and audit.

Therefore, you should choose an SSO tool that can perform these functions satisfactorily: this is an enterprise-level decision.

Evidian's *Enterprise SSO* solution is the fruit of over fifteen years experience in identity and access management. Close to 1.5 million users worldwide access their applications every day with Evidian's solution, and the largest customer is running the solution on 120,000 PCs. Based on this know-how, this white paper gives an overview of SSO functions in the state of the art.

---

<sup>1</sup> Magic Quadrant for Enterprise Single Sign-On, 2007

## What are the alternatives to SSO?

Other solutions reduce the number of passwords entered by users.

- **Password synchronization** allows you to use the same password for all your applications. If the password for your e-mail reader is "abcd", then the password for the financial application will also be "abcd". There is no client software on the PC, but a password-change module must be developed for each application.

This ease of use comes to the detriment of security. If password "abcd" is stolen on a poorly protected application, then all the applications will be compromised. And you cannot delegate your access to the financial application without revealing the content of your e-mails at the same time.

- With **access tokens** (such as Kerberos or SAML), applications delegate authentication to an external module. But in most cases, the application must be modified and it is not possible to delegate access among colleagues. Re-authentication functions, to access sensitive applications, are often not present either.

## Why do enterprises invest in SSO?

Evidian has noticed that there are three main factors that motivate companies in their decision to buy an SSO solution. The manner in which an SSO tool is deployed may vary according to these factors, even though this tool is the same in the three cases. Of course, some companies may decide to kill two birds with one stone and satisfy several needs at a time!

1. **Reinforce security** and satisfy regulatory constraints. By creating an obligatory passage point between a user and its applications, an organization can effectively control the accesses. Moreover, a log of these accesses and administration operations is kept centrally, which facilitates audit. This facilitates compliance with confidentiality, integrity and availability requirements.
2. **Reduce operating costs**. Multiplying passwords, often for excellent reasons, reduces users' productivity and the quality of work. But these "hidden costs" often have a visible side: up to 30% of helpdesk costs are due to lost passwords. This will be considerably alleviated through an SSO solution, with a return on investment that is easy to evaluate.
3. **Open up an information system without risk** to the outside world. This demand is getting increasingly frequent: access to the web has become easy, yet employees still have problems accessing intranet applications from outside. Doctors who must consult some medical records, engineers on a work site, sales reps in their hotel: SSO allows transparent and secure access to web applications, even from outside.

Depending on the type of need, some parts of a company are more demanding than others. Thus, the general management wants compliance with laws and regulations such as Sarbanes-Oxley in the USA or the Law on Financial Security in France. The IT

department seeks to reduce its operating costs. The operations department, on its own part, requires its mobile employees to be productive, even outside the company.

Security, cost reduction, scalability: Evidian *Enterprise SSO* meets these needs thanks to a modular architecture. The functional modules can be implemented gradually, providing useful and visible functions in each phase. Moreover, it is possible to first equip one department and then extend SSO to the rest of the company.

## The three architectures of single sign-on

The SSO software on a user's PC enters logins and passwords on behalf of the user. But where does the software find that information? The answer points to an important difference between individual SSO and enterprise SSO. In the latter case, data resides in a secure location outside the user's PC, basically for reasons of control (it should be possible to deny or grant access remotely) and user mobility.

On the market, you can find three basic architectures for making available SSO information such as logins, passwords and access rights.

- **SSO server:** the information is stored on a server, for instance a Windows or Unix server, that is generally dedicated to this task. The client on the PC queries the server whenever necessary. This server is often duplicated for high availability, although cache mechanisms on the PC can compensate for temporary unavailability. Therefore, start-up costs must be taken into account: servers (but you can dedicate an existing server) and software installation. In a distributed architecture, the number of these servers may be high.
- **SSO appliance:** it is just a variation of the SSO server solution: software and hardware are packaged together. Software-deployment costs are thus reduced. On the other hand, it is not possible to install the software on an existing server, which may increase the deployment costs. Finally, it is often impossible to add memory and disk on an appliance, unlike a server.
- **Enterprise directory:** SSO data is simply stored, in encrypted form, in the directory that already exists in most companies. For instance, the Active Directory base through which users access Windows. Therefore, you do not need to install any server or appliance. Your PCs are already configured to access the information, since they already access the directory. Deployment costs are reduced significantly.

In such an architecture, the directory is typically completed with some administration stations and a database in which the log of activities is stored (for audit). But these modules are not an obligatory and critical passage point for the entire system, unlike "server" and "appliance" architectures.

Evidian *Enterprise SSO* uses an enterprise-directory-based architecture. Experience has shown that this simpler solution is quicker to deploy, while maintaining the highest security level.

## Several enterprise directories

All companies have created a user directory - but some have several of them. The reasons may be historic (a recently acquired company, an independent subsidiary) or functional (partners are managed in a separate relational database). This may pose a problem if a user moves from one domain to the other.

In this case, Evidian proposes a directory synchronization solution: the most reliable information is obtained in the right place, and it is, thus, possible to create a central directory. This way, a user declared in the human resources databases will be rapidly operational in the entire company.

So, an architecture based on the existing enterprise directory is simple, easy to maintain and rapidly deployable.

### MY CRITERIA

Does the SSO solution require me to deploy new servers or appliances in my company?

Is it a problem if my users are listed in several databases, files and directories?

## SSO makes security becomes natural

With a well-designed enterprise SSO solution, your security policy is no longer a constraint for your users. They run the applications they are entitled to, without having to remember or manage their passwords. Your employees thus naturally comply with your security policy.

The SSO solution handles all password-related operations. It can even change them automatically, without the user's intervention. You can even prevent the user from knowing the password for a sensitive application: the user therefore can't reveal this password or to use it fraudulently outside the company.

From a central management console, you can decide who has access to which application. Of course, with thousands of employees and hundreds of applications, it is out of question to grant accesses one by one! The administrator simply decides which group of users has access to which group of applications, and if needed from which PCs. For example:

- "Back-office applications may never be used from a trading PC."
- "R&D PCs must always be accessed through biometrics."
- "The General Ledger application may be used by the finance department only."

### MY CRITERIA

Can access to an application be restricted according to a user's job, but also according to the location in which the application is run?

## Manage passwords naturally

With Evidian *Enterprise SSO*, you can enforce a strict password policy (for instance at least two digits, including one in front, more than ten characters, etc.), even if the application is more permissive. This is possible because all password operations take place under its control.

But what happens if an employee wishes to be replaced by a colleague while he or she is away? Previously, said user revealed his or her login and password, with all the inherent risks in terms of security and audit.

Evidian *Enterprise SSO*, on the contrary, allows an employee to temporarily delegate access to a colleague. Of course, he or she can only do so if your security policy authorizes it. Moreover, a record of accesses is kept, so you know which operations have been performed by which user.

### **MY CRITERIA**

Does the SSO solution allow an employee to personally delegate access temporarily to an application, for instance before going on leave?

## Reinforce security: strong authentication

Login/password is the most common access method. However, this universal “open sesame” is often not enough to protect sensitive resources. Does a password prove that the person connecting is actually the password owner?

This is why people sometimes choose to reinforce SSO with strong authentication methods. Although these methods are rarely deployed on all workstations, it a common practice to protect some workstations and sensitive applications: top management and traders’ PCs, doctors’ access to patient records, sensitive laptops etc.

Here are some common types of strong authentication methods:

Type	Examples of users	Examples of solutions
Smart card or USB token with certificates	Hospitals, industry, banks	Health professional cards - CPS (France) NHS Connecting for Health - CfH (UK) eID card (Belgium)
Biometrics	Industry, banks	Fingerprint reader
Card or USB token containing logins and passwords	Administrations	Company badge
One-time password	Banks	Calculator-based Printed sheet
'Defense' smart card	Defense	Multifunction secured card
Radio badge	Hospitals, retailing and distribution industry	RFID technology

Evidian *Enterprise SSO* is compatible with a large variety of strong authentication methods. As a software publisher, Evidian does not manufacture authentication hardware. But *Enterprise SSO* can manage these devices in an entire company: assignment of smart cards and USB tokens, lending operations, blacklisting, etc. Access security is thus reinforced without administration overload.

What to do if a user loses his or her strong authentication device, or if this device is faulty? An emergency access is necessary to prevent excessive helpdesk workload.

#### MY CRITERIA

Is the SSO solution compatible with the strong authentication method I have chosen?

Can I prevent an application from being run on a PC that is not protected through strong authentication?

Is it possible to support several authentication methods at the same time based on user or PC profiles?

Does the SSO solution provide continuity of user access if strong authentication fails?

## Your operating costs are reduced thanks to service continuity

A well-designed SSO tool reduces operating costs. Some of these costs are hard to evaluate since they affect user productivity. However, other savings are easier to measure: they concern helpdesk workload.

Evidian *Enterprise SSO* handles application password constraints so you do not have to worry about forgotten passwords or blocked accounts. Helpdesk calls fall by up to 30%, because users no longer need to remember application passwords.

However, you need to handle forgotten primary passwords or lost access cards. For example, what happens if a sales rep notices in a hotel that his or her smart card no longer works? Evidian *Enterprise SSO* will unlock their access offline and with or without helpdesk intervention. It is not necessary to be connected to the network for this.

If you activate this function, the user will choose three questions/answers the first time SSO is started on his or her PC. If the user forgets his or her access password or loses his or her access card, the user will answer the predefined questions and resets his or her password. This way, the user is not blocked by a lost access.

### MY CRITERIA

Will my users be able to reset their password without calling the helpdesk?

Is it possible to reset a password offline?

## How to integrate one of your applications into the SSO solution?

SSO replaces the user and enters logins and passwords on the user's behalf. For this, the SSO software must recognize the software's login window but also the password change window, or wrong password message window. This is done once for everyone in the company, then distributed to the employees' PCs through the enterprise directory.

This is generally easy for Windows applications that have been developed according to Microsoft recommendations. But less classical applications must also be taken into account:

- Internal applications developed many years ago
- Mainframe applications in terminal emulation mode
- Packages with special interface features such as SAP R/3 and Lotus Notes
- Java applications or applets
- Web sites and portals through Internet Explorer or Firefox.

How to ensure that the SSO software can integrate your applications, even the most 'exotic' ones? It is often wise to ask the vendor to test the solution on your site, and integrate the most critical applications.

Evidian *Enterprise SSO* allows you to integrate most applications with a few clicks. Start the application and point your mouse to the "login", "password" fields, etc. The application is now recognized everywhere in the company. Applications like Lotus Notes, SAP R/3, or browsers are supported natively. A graphical script tool handles the rare recalcitrant applications.

**MY CRITERIA**

Will the SSO solution allow me to integrate my applications simply, or does it require programming?

## Everyday SSO administration

The SSO solution allows you to make real savings. Yet, it should not generate heavy administration costs in return! When you have dozens of users, it is out of question to grant access rights individually. Instead, it must be extremely easy to manage the rights of a user arriving, changing function in or leaving the company.

Moreover, if some applications are 'discovered' in the company during deployment, you also have to quickly integrate them as well. And since the user may not know the passwords for his or her critical applications, how do you delegate the user's accesses during holidays without increasing the helpdesk's workload?

To appreciate the daily administrative workload of an SSO tool it is better to ask for an on-site evaluation. You can test administration scenarios for a few days. You will check whether the profiles of the persons who will manage it are adequate, and you will estimate their workload.

Evidian has incorporated many administration functions into *Enterprise SSO*. With over fifteen years experience, the ergonomics and functions have been refined to make administrators easily productive. For example:

- When a user is absent, he or she can delegate his or her accesses before leaving, without revealing his or her passwords.
- Local administrators incorporate their own applications and manage their teams' accesses.
- Specific administration roles cover applications, cards, passwords, audit, etc.
- When an administrator changes functions, his or her rights are easily transferred or delegated.

**MY CRITERIA**

What will be the daily management workload generated by the SSO solution?

## Your information system will open up to the world without risk

When your employees are away from your company's sites, must they use a specially configured PC to use the intranet applications? The better choice is to use SSO functions that allow them to securely access internal web applications from any browser (cybercafé or client site, for instance).

This can be extremely useful. Some Evidian customers use this function to make their mobile employees really independent: traveling salespersons, police officers on a mission, engineers on a site abroad, etc.

Some other SSO solutions consider web accesses as a weakly integrated add-on: therefore, the 'web' and 'intranet' parts do not exchange certain SSO information properly. Unlike these solutions, Evidian *Enterprise SSO* securely shares the same protected information, no matter the access mode.

### MY CRITERIA

If a PC's SSO changes the password for an application without the user knowing it, will the user still access it normally from outside?

## Scalability – extend SSO to the rest of the enterprise

You wish to equip your department or only one site of your company with an SSO solution. But it is wise to anticipate the time when SSO will be extended to the rest of your company, even if it is in the distant future. So, you need to choose a scalable SSO solution or risk changing your solution eventually, with the difficulties inherent in the necessary password migration.

Scalability is a real issue for certain SSO products that are designed for a few hundreds of users. How do you share data so that users can be mobile in several countries? Do you need to train an administrator per site or per department? Does the basic technology change as numbers grow? Are multi-domain directories supported? Do you have to install dedicated hardware in many places?

Evidian *Enterprise SSO* has been deployed in companies with over 100,000 users. The solution is easy to extend: the same simple technology, based on the enterprise directory, is used for clients of some hundreds or tens of thousands of users.

### MY CRITERIA

Has the SSO solution shown that it could be deployed for thousands of users?

## Integration with identity and access management

Evidian has noticed that SSO is often a prelude to a more ambitious identity and access management project. In a second step, an access policy can be defined rigorously, validated according to a strict process and audited regularly. Employees will naturally comply with it through the existing SSO mechanism.

But that is not all: since SSO provides information on the actual use of applications, it is possible to continuously audit compliance with the security policy. Finally, accounts can be created, updated and removed automatically in the applications themselves; the user is thus immediately operational.

Evidian *Enterprise SSO* is part of Evidian's *IAM Suite* identity and access management solution. It can be connected to Evidian *User Provisioning* to automate password management or send actual access data to Evidian *Policy Manager* in order to audit and refine the security policy.

Finally, you can stop distributing passwords to users: in coordination with your identity management processes, a provisioning module or workflow synchronizes application accounts with SSO.

<b>MY CRITERIA</b>	Can the SSO solution be extended later, by integrating role-based access management or provisioning?
--------------------	--

## Evidian Enterprise SSO: panorama of features

Evidian *Enterprise SSO* enables you to rapidly deploy an effective single sign-on solution. Users access their applications more easily and more securely. Building on the SSO features, you can add modules that provide strong authentication and additional administration functions.

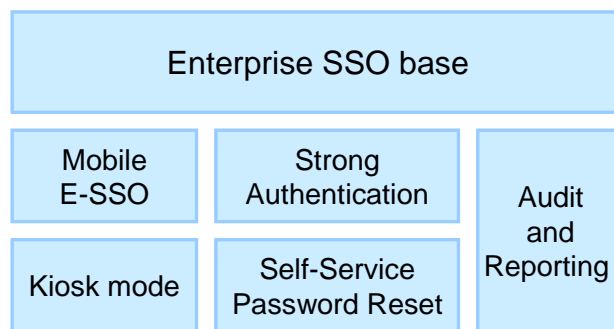


Figure 1 - A complete single sign-on solution

Evidian Enterprise SSO consists of several complementary modules:

- Quick access to single sign-on: **Enterprise SSO base** offers single sign-on functions such as access and password rules administration, delegation, re-authentication and audit collection.
- SSO access from the internet: **Mobile E-SSO** enables users to connect securely through SSO to their applications, from any web browser.
- Password management: with **Self-Service Password Reset**, users personally reset their unique password.
- The **Kiosk Mode** enables employees to share a PC without restarting the Windows session. Therefore, change of users takes place within a few seconds.
- **Strong Authentication** makes it possible to use authentication methods such as cryptographic cards, USB tokens, certificates, active RFID and biometrics
- **Audit and Reporting** generates reports about administration and authentication events, and about accesses to target applications. Application usage can be restricted to specific access points.

## Supported environments

- The SSO client is available for Windows 2000, 2003, XP, Vista, Citrix and Terminal Server.
- Most Windows, HTML or Java applications are configured through simple drag and drop. The features of specific applications are supported in standard (SAP, Lotus Notes, and mainframe emulators) or through graphical configuration.
- The directory containing users and the security policy may be Active Directory or ADAM, Sun Java System Directory Server, Fedora Directory Server, Novell eDirectory, IBM Directory Server or OpenLDAP.
- Audit events are stored in Microsoft SQL Server, MySQL, IBM DB2 or Oracle.

For more information, please visit our website: [www.evidian.com/](http://www.evidian.com/)

Email: [info@evidian.com](mailto:info@evidian.com)

© 2008 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 Groupe Bull Company