

The 7 most used authentication methods

An Evidian white paper

Enforce your authentication policy with Single Sign-On.

EVIDIAN
A Groupe Bull Company

*By Stéphane Vinsot
Product manager*

Version 1.0

Summary

- The right authentication on the right workstation
- Strong authentication: from password to multi-factor and multi-device authentication
- The 7 most used authentication methods
- An example of authentication policy
- Enterprise SSO includes strong authentication in the security policy.

© 2007 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.

Table of contents

Warning	5
The right authentication on the right workstation	6
Authentication is the first step in the user-connection process.	6
Security level	6
Your security policy	6
Rules and regulations	7
Deployment and management costs	7
Strong authentication: from password to multi-factor and multi-device authentication	8
Authentication or identification?	8
Seven different authentication elements	8
Multi-factor authentication	10
Authentication token	11
Enterprise SSO enables you to apply strong authentication so as to control access to all applications.	11
SSO function and security policy: an example	11
An example of access security policy	13
Enterprise SSO enables you to include strong authentication in your security policy.	14
The 7 most used authentication methods	15
Windows authentication infrastructure	15
(1) Login and password	15
(2) Login and OTP (One-Time Password)	15
Architecture and principle	15
Deployment and administration	16
(3) USB key or PKI smart card	16
The different types of cards	17
PKI infrastructure	17
CMS functions	17
The authentication module	18
(4) "Confidential defense" key	19
(5) Smart card with login and password	20
(6) Biometric solutions	20
The three families of biometric solutions	20
(7) Active RFID	21
The components of an active RFID solution	22

An example of authentication policy 23

Enterprise SSO includes strong authentication in the security policy. 24

Warning

This document is an introduction to strong authentication and secure access to target applications.

It reviews the seven most frequently used authentication methods, and describes their main mechanisms. It associates with them the main functions of a Single Sign-On (SSO) engine.

It does not treat the domains of Web Services or identity federation.

For more information on a specific method, please refer to the more specialized documents.

The right authentication on the right workstation

Authentication is the first step in the user-connection process.

Any organization deploying an information system needs a reliable connection to its systems and applications.

Creating a single and reliable identity source, associated with rights management, is the basis for good identity and access management.

The user-connection process can then be implemented. Generally, it comprises four stages:

Initial process – common to all connections

1. Starting the workstation and authenticating a user
2. The workstation checks the user's rights and connects the user to his or her resources.

Connecting to the application itself

1. The user runs a secure application and authenticates to this application.
2. The application checks the user's rights and connects the user to his or her transactions and data.

User authentication is one of the main points of this process. It enables the information system to verify the user's identity and associate the user with his or her rights.

There are many authentication methods. Each of these methods has its specific characteristics.

Security level

Your security policy

Every organization has, or should have, a security policy for the protection of its workstations, applications, data, or information systems. This security policy can define minimum authentication levels based on the criticality of the resource used.

For example, it is possible to imagine, like in any good spy movie, that a critical workstation is placed inside a protected room, access to which is subject to a secret code, a smart card, and biometric identification of the right eye. In this case, protection is at its maximum, since you need to provide something **you know** (the code), something **you have** (the card) and something that is **part of you** (the eye).

This system protects a workstation effectively, but it is expensive to run (it requires one room per PC, as well as appropriate readers) and to manage (what happens if a user forgets his or her code, loses his or her card and right eye?).

Rules and regulations

New regulations, such as Sarbanes-Oxley, require the deployment of systems which allow an organization to implement a security policy and demonstrate that it is actually implemented.

User authentication is one of the major elements to take into account.

A user has to be actually authenticated when the workstation is started and/or when connecting to his or her application, by applying the security policy rules. There should also be proof of deployment of the right authentication method.

Deployment and management costs

The deployment of a strong authentication solution must also be analyzed by the yardstick of the efforts required to deploy and manage it:

For initial operations

- Creating and distributing physical devices (cards, keys, etc.) or logical elements (X.509 certificates, passwords, biometric data) to users
- Installing specific readers, if necessary, on workstations
- Deploying the right software infrastructure (PKI, Kerberos server, biometric authentication server, etc.)
- Integration with corporate applications or Enterprise SSO
- Training the users.

For management operations

- Managing new-comers, with assignment of their different elements
- Managing forgotten logical elements (password or login)
- Managing the loss of a physical device and its replacement (a card, for instance)
- Handling device invalidation (exposed PIN, invalid biometric data, etc.).

These efforts must be considered as investments which will enable the company to protect its most sensitive data and apply the corresponding security policy.

Strong authentication: from password to multi-factor and multi-device authentication

Authentication or identification?

There is a very simple difference between identification and authentication: the proof.

Identification is based on a simple declaration such as the reception or reading of an identification code (login, serial number, bar code, etc.). This identification code is not supposed to be secret. It is a public domain.

Authentication is based on a proof element such as a shared secret or an asymmetric secret. Authentication is used to verify a user's identity, with a reasonable level of trust.

Seven different authentication elements

To authenticate, a user generally provides at least two elements:

- His or her login, making it possible to identify him or her
- One or more elements for authentication itself.

These elements, thus, exist in different forms. Hereafter are the 7 most used ones:

Type	Description
<i>Login and password</i>	<p>Login and password are the most common authentication method.</p> <p>Simple, robust or even rustic, its greatest weak point is that the security level depends directly on the complexity of the password. Simple passwords are reliable while too complex passwords make users to adopt bypass password management strategies: Post-it, list in an Excel file or in a smartphone, etc.</p>
<i>Login and OTP (One-Time Password¹)</i>	<p>OTP enables you to secure the use of passwords on the network. In fact, with an OTP system, the user has a specialized calculator which provides him or her with a password on demand. This password is valid only for a limited period and for a single use.</p> <p><i>This solution is generally deployed during initial authentication for external access through IP/VPN.</i></p>
<i>PKI on a smart card or USB key</i>	<p>X.509 certificates use an advanced encryption technology that allows you to encrypt or sign messages without sharing any secret.</p> <p>The login is a public certificate signed and, thus, guaranteed by a recognized certification authority. The user must provide a secret so as to be able to use the different cryptographic elements: "his or her card or USB-key PIN".</p>

¹ OTP: One Time Password.

	<p><i>This solution is generally used for initial authentications or for connections to web or messaging applications.</i></p>
<p><i>Login and password on a smart card</i></p>	<p>You can complete the security of the authentication process by storing the login and password on a smart card. The password can thus be very complex and changed regularly, automatically and randomly. Without the card and the associated PIN, the password becomes impossible.</p> <p><i>This solution is generally used for initial authentication.</i></p>
<p><i>"Confidential defense" card</i></p>	<p>This is a special version of the previous method. It is generally a multi-function key: X.509 certificate storage, data storage, cryptographic resource etc.</p>
<p><i>Biometrics</i></p>	<p>Authentication through biometrics is based on the verification of a part of the user's body (most often, the fingerprint).</p> <p>A central server, the workstation or a smart card can be used to store the user's biometric data.</p> <p><i>This solution is generally used for initial authentications and/or to protect access to very sensitive applications.</i></p>
<p><i>Contactless identification</i></p>	<p>RFID is a technology deployed today in identification/authentication projects. An RFID smart card is built into a badge and bears an identification number. This number is then associated with a user in a computer system. Basically, it is an identification technology which, in association with a password provided by a user, for example, can be used in authentication processes.</p> <p>This technology exists in two forms:</p> <p>Passive RFID or HID, which assumes that the card does not have its own power unit. The card is powered up during the reading process by an electromagnetic field generated by the reader.</p> <p><i>This system is commonly used for badge-based physical access control, or for effecting payments in a staff canteen. A HID card is detected a few centimeters away.</i></p> <p>Active RFID is based on RFID communication protocols, but is associated with a card that has its own power unit. This power unit enables the card to be detected at a longer range (for example once the bearer enters a room or an office).</p> <p><i>The major advantage of active RFID is that it enables you to detect the absence of workstations in areas accessible to the general public.</i></p>

Multi-factor authentication

An authentication factor is **an element you know** (secret code), **an element you have** (physical device) or **a part of you** (biometrics).

Once several authentication factors come into play, we talk in terms of **multi-factor** authentication.

<i>Examples of a 1-factor authentication system:</i>	<ul style="list-style-type: none"> ▪ Login + password (an element you know) ▪ Contactless identification (an element you have) ▪ Biometrics or login + biometrics (a part of you).
<i>Examples of a 2-factor authentication system:</i>	<ul style="list-style-type: none"> ▪ Smart card + PIN (elements you have AND know) ▪ Smart card + biometrics (element you have AND a part of you) ▪ Biometrics + password (a part of you AND an element you know)
<i>Example of a 3-factor authentication system:</i>	<ul style="list-style-type: none"> ▪ Smart card + PIN + biometrics (elements you have AND know AND a part of you)

The more the number of authentication factors, the higher the level of security. But it poses the following problems:

- The lifecycle of each factor must be managed: password and PIN reset, smart card distribution, etc.
- The ergonomics may be too restrictive for users.
- The additional costs of peripherals (smart cards, readers, biometric sensors). Moreover, the helpdesk will have more workload managing all these methods (unlocking passwords and PINs, distributing cards, training users on biometrics, etc.).

Authentication token

After setting up the initial user authentication, you have to forward it to the target applications.

One of the techniques used is "authentication token". This "authentication token" is a set of data containing the elements that prove the identity of the user presenting it to the application.

The target application must be able to recover this authentication token on the workstation, then forward it to a specialized server which will confirm the validity of the authentication token and the associated identity.

The most widespread authentication tokens are Kerberos and SAML tokens.

Kerberos tokens

These tokens are used in Windows environments.

SAML tokens (also known as SAML assertion)

These tokens are used in SOA/J2EE/Web Services architectures.

Limits of the token approach

The token approach requires the target applications to be able to read the token and communicate with the authentication server. Unfortunately, the already existing applications (and even certain new applications) cannot always be integrated easily.

Thanks to Enterprise SSO, you can set up the link between initial user authentication and target applications in the most universal manner possible. Enterprise SSO interfaces directly with the login/password prompt window of the target application which no longer needs to be modified.

Enterprise SSO enables you to apply strong authentication so as to control access to all applications.

Enterprise SSO forwards automatically to the target applications the logins and passwords required at startup. Therefore, you can use Enterprise SSO to apply a policy to the management and use of these elements.

SSO function and security policy: an example

The definition of an access-related security policy depends on the available SSO features which can be applied to target applications and users according to their access types. These features are, for example:

Self-learning capacity

If the user starts an application integrated into the SSO system and the SSO system does not yet know the login and password to use for the said application, the SSO system prompts the user to provide his or her login and password for this application.

Multiple accounts

When the user starts an application integrated into the SSO system and for which the user has several application accounts, SSO allows the user to choose the account to which he or she wishes to connect.

Scheduled secondary password modifications

SSO changes passwords automatically according to the security policy, either in response to an application request or by generating actions that will display the password-modification window.

So, SSO enables you to create long passwords (for example with 32 characters) in a complex and random format. This password is then no longer managed by the user.

Access delegation

The user can delegate, from his or her workstation, his or her accesses to another user for a given period and for a given application. The delegated user does not need to know the login and password of the delegating user in order to connect to the target applications.

Integration of personal applications

The user can integrate him/herself his or her personal applications into the SSO system. In this case, he or she defines the attributes associated with his or her applications, as well as the logins and passwords.

Re-authentication for sensitive access

When a user starts an application integrated into the SSO system, the SSO system solution can prompt for so-called primary re-authentication (same as initial authentication) in order to check that the user is actually the right user.

Controlling access to an application according to workstation

The SSO system can limit access to the most critical applications from a given subset of workstations. For example, R&D applications may be accessible only from workstations on the R&D site.

Access via a web portal from any browser on the Internet

Certain applications must be accessible through the Internet from any workstation. SSO mechanisms must also be applicable in this case.

An example of access security policy

Here is a basic example of access security policy:

Classification of applications	Attributes associated with applications
<p>Standard</p> <p>These are applications used by everybody (e-mail, expense accounts, etc.). The passwords must remain visible to certain users who must access them from outside, via a secure web portal.</p>	<ul style="list-style-type: none"> ▪ Self-learning of logins and passwords is implemented. ▪ Delegation is allowed. ▪ No re-authentication when the application is started ▪ Web access through the Internet
<p>Critical</p> <p>These are applications the use of which is restricted to a user family. Passwords are hidden in order to control their access via the SSO solution.</p>	<ul style="list-style-type: none"> ▪ Passwords are hidden from the user. ▪ Password changes are automatically managed upon application prompts. ▪ Delegation is allowed. ▪ No re-authentication when the application is started ▪ No web access through the Internet
<p>More critical</p> <p>These are applications the use of which is restricted to a user family. Their access must be particularly protected.</p>	<ul style="list-style-type: none"> ▪ Passwords are hidden from the user. ▪ Password changes are planned and managed automatically. ▪ Delegation is forbidden for some users and allowed for others (for management teams). ▪ The user must re-authenticate when the application is started. ▪ Access is only from workstations in the departments concerned or from the area concerned (public, front-office, back-offices, etc.). ▪ No web access via the Internet
<p>Personal</p> <p>These are applications that users wish to include in their SSO.</p>	<ul style="list-style-type: none"> ▪ Applications and attributes are user-defined (no delegation). ▪ Logins and passwords are user-defined. ▪ No web access through the Internet

Enterprise SSO enables you to include strong authentication in your security policy.

With Enterprise SSO, it becomes possible to include different authentication modes and apply them according to type of workstation. For example, you can implement:

- Biometric authentication to protect your workstations and, thus, access to R&D applications
- Active RFID authentication used to manage self-service workstations
- Login/OTP-based authentication to protect external accesses via IP/VPN
- X.509 smart card-based authentication to protect web internet accesses on any browser
- Login/password-based authentication for “general-purpose” workstations.

Enterprise SSO can then manage accesses to target applications according to workstations and authentication type.

Re-authentication

When you start a sensitive application, the SSO engine may prompt you to re-authenticate. For workstations equipped with strong authentication, it is this re-authentication type that is then required.

This function enables you to apply strong authentication to an application running with login/password-based authentication, without changing the application concerned.

The 7 most used authentication methods

Windows authentication infrastructure

Implementing strong authentication in a Windows environment requires integrating your systems into a Windows authentication infrastructure. Sometimes, you have to replace or complete the existing Windows components. These components are, for example:

- The authentication module² of the PC in charge of initial authentication and managing exceptions initiated through "Ctrl+Alt+Delete". For the initial authentication part, it is in charge of supplying the security log with additional authentications to target applications.
- The user directory, which may be Active Directory
- The Microsoft PKI infrastructure used to issue X.509 certificates.

Moreover, when you install special readers (biometric, smart card readers, etc.), you have to install in Windows devices (drivers) which will enable you to manage communication with these items.

(1) Login and password

This method does not require any modification of the existing Windows authentication infrastructure. You only need to install the Enterprise SSO module on the workstation to apply the access security policy.

(2) Login and OTP (One-Time Password)

Architecture and principle

The user has a specific "calculator" which will enable him or her, during connection, to provide a password with a limited validity period.

To be able to use his or her calculator, he or she must first enter a password in it. The calculator then returns a one-time password, which the user will in turn supply to the PC's authentication module.

The authentication module then communicates with the OTP server to check the validity of the information provided, and to allow or refuse the connection.

² This module is also known as GINA.

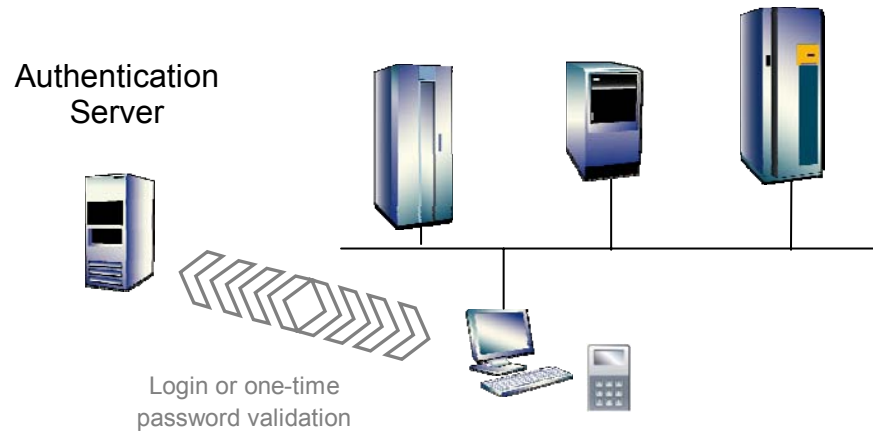


Figure 1: OTP mechanisms

Organizations use this system, among others, mainly to secure IP/VPN accesses from PCs located in their employees' homes.

Deployment and administration

Generally, this solution requires the use of one or more specific authentication servers, accessible 24/7.

Each user must have a specific calculator and the associated password.

Therefore, there must be procedures for managing requests from users who lose or forget their calculator or password.

(3) USB key or PKI smart card


PKI-based solutions are beginning to be deployed effectively for initial authentications.

The use of a smart card and certificate-based solution requires the aggregation of several components:

- The card with its reader, as well as the associated software code, which must be installed on the workstation
- The X.509 certificate infrastructure, which must provide the different components of a PKI infrastructure: the Certification Authority and Registration Authority
- The CMS (Card Management System), which will manage the assignment of cards (see below)
- The Windows authentication module
- The authentication server.

The different types of cards

There are basically two large families of cards:

- Cryptographic smart cards () , which require a reader. They allow the integration of other technologies for other uses, for example: a contactless antenna (physical access), or a magnetic track (canteen, time clock).
- USB keys (with chip), which do not need any reader and can be connected directly to the PC with the right drivers. These USB keys can bring in additional functions such as external disk.

PKI infrastructure

In general, a public key infrastructure comprises three distinct entities:

The **registration authority (RA)**: this entity is in charge of administrative operations like checking a user's identity or following up orders.

The **certification authority (CA)**: this entity is in charge of creating certificates or signing revocation lists.

The **depository authority (DA)**: this entity is in charge of certificate safekeeping for recovery purposes.

CMS functions

It must be possible to use a Card Management System to:

- Create a card for a new employee: associating a card with an employee and communicating with the PKI's AC in order to obtain the employee's certificate and integrate it into the card
- Lend a temporary card to an employee when he or she forgets his or her card
- Blacklist a lost card (or remove a lost card from the black list if found)
- Locally or remotely unlock a PIN "locked" by a user.

The helpdesk should be able to use it to manage the PIN unlocking functions and, through the reception structures of the different sites, to create and assign or lend a card.

The authentication module

A workstation's authentication module must allow user authentication:

1. It prompts the user for his or her login and card PIN.
2. It checks on the CMS that the card is not on the "black list" of cards.
3. It retrieves the public certificate in the card, checks the signature and also that it is not included in the "black list".
4. It prompts the card to sign a *challenge* and checks (or has a server check) that the signature actually corresponds to the public certificate.

If these elements are validated, this module allows access to the workstation with the required identity.

It must also manage other events:

- Loss or misplacement of PINs. The authentication module must enable a remote user, who cannot call his or her help desk, to recover a PIN by answering a few questions.
- Remote card PIN reset by the helpdesk
- Securing the workstation when the card is removed: closing the Windows session, or simple locking.
- Implementing the "fast user switching" function, which enables you to quickly change the Enterprise SSO context and open the target applications within the user's personal security context.

The authentication module is at the heart of PKI-based authentication.

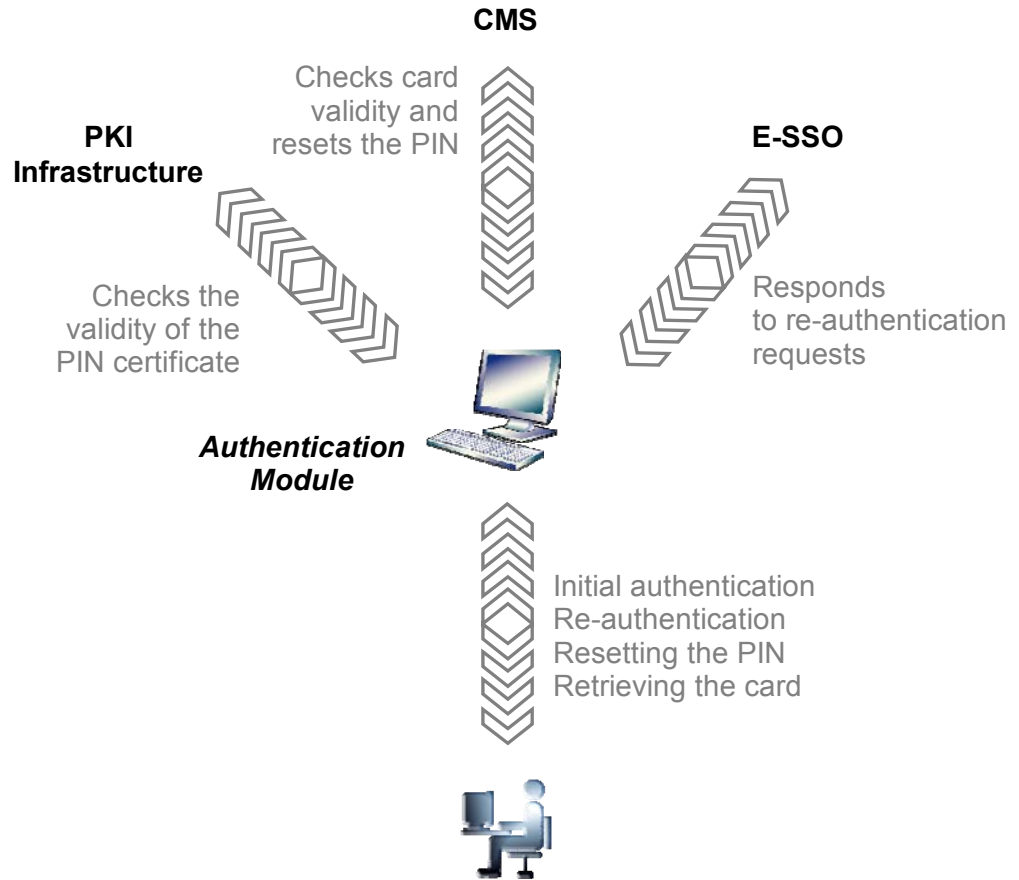


Figure 2: Workstation authentication module at the heart of strong authentication

(4) "Confidential defense" key

The "confidential defense" key is a special declination of the previous example. Generally, it is a multi-function key: X.509 certificate storage, data storage, cryptographic resource for encrypting the hard disk or any other component such as the VoIP or PC/server application flows.

To counter the activities of keyloggers³, the PIN of such a key is entered on the key itself to avoid using the keyboard.

This key can securely carry the different elements of Enterprise SSO which then becomes portable and can be used on any workstation.

³ A keylogger is a malicious program installed on a user's PC without the user knowing it, and which records the user's keystrokes to transmit them later to a server.

This type of key, a real electronic safe, is used to provide a portable, integrated and secure strong-authentication and Enterprise-SSO solution.

(5) Smart card with login and password

A thinner solution allows you to use the smart card to store a user's Windows login and password. During user authentication, the workstation authentication module will use these elements to authenticate the user in the LDAP directory.

The card will then be used to protect the security data, for example the SSO passwords.

The PKI infrastructure is no longer required; only the CMS and Enterprise SSO remain necessary.

(6) Biometric solutions

Biometric solutions use biometric readers to control physical accesses.

There are relatively few biometric reader suppliers. Some portable device manufacturers offer an option that allows you to integrate this type of reader into the portable device.

Biometric solutions are generally used inside a company to protect access to the most sensitive applications. There are currently no standards applied by commercially-available browsers, which would allow you to control access from any PC on the Internet.

The three families of biometric solutions

The storage and management of biometric data have come up against regulations on the protection of personal data. Some countries, for instance, do not allow the creation of central biometric databases.

Biometric solutions are used to deploy three different types of architectures.

	Biometric data storage	Authentication checks
Server-based solution	In the server	By the server
Workstation-based solution	On the user's workstation	By the workstation
Cryptographic card-based solution	In the cryptographic card	By the smart card or workstation

Server-based biometric solutions

They are based on the following components:

- A central server
- A biometric signature enrolment module
- A special authentication-management module.

Local solutions

These solutions are used to avoid centralized storage of biometric signatures by storing every sensitive data on the user's workstation.

Although from a legal viewpoint these solutions are more acceptable in many countries, it poses a problem of user mobility in companies.

Smart card-based biometric solutions

These solutions are used to bypass the use of a central server while enabling the user to move around within his or her company. In fact, the user's biometric signatures are stored on his or her smart card and follow him or her to all the workstations.

This solution is more secure and better accepted in many countries but it requires the use of a Card Management System for card deployment, and the availability of all the necessary peripherals on the different workstations.

(7) Active RFID

Active RFID-based solutions use the RFID protocol to identify a user without physical contact, a few meters away.

The user's badge has its own power unit which enables it to communicate with an antenna connected to the PC.

The PC can then detect a user's arrival or departure without the user having to take any particular action. It is possible to modify the different parameters which determine the PC's reactions:

1. The distances at which a user's arrival and departure are detected
2. The action to take when a user is leaving: close the Windows session, lock the session or leave the PC as it is
3. The action to take when a user arrives: prompt for the Windows password, unlock the screen saver...
4. The action to take when several users are detected at the same time.

These different parameters are used to describe different advanced operation scenarios, such as the "Quick user change" at the emergency department of a hospital or even the protection of a workstation in the public area of a bank's local branch.

The components of an active RFID solution

The main components of an active RFID solution are:

- Physical components such as user badges and the antenna for each PC
- The authentication module to install on the PC
- The Badge Management System which will manage badges and communicate with the workstation authentication module for badge identification, and administer the logins and passwords used to open sessions.

An example of authentication policy

Let us take the example of an organization, which for legal reasons and after a serious incident that led to theft of sensitive data, must implement an advanced authentication policy. It then decides to define the following rules for initial authentication:

1. Login and password are the standard authentication methods. A password must contain at least 10 characters; these characters must include at least 2 numerals and at least 2 alphabets. It must be changed every month.
2. Web applications, accessible from the Internet, must be protected with a cryptographic smart card with X.509 (PKI) certificate.
3. Biometric solutions are used internally to protect R&D applications.
4. Active RFID is used to protect PCs of branches, located in public open spaces. Only certain applications are accessible from these PCs.

It is Enterprise SSO that will enable the organization to effectively implement this policy.

Rule 1: password modification policy

A password policy thus defined is extremely restrictive. A user cannot apply it for all his or her applications. It is Enterprise SSO that will handle this.

On the other hand, the user **must and can** apply this policy effectively for his or her Windows authentication.

Rule 2: access to web applications via the Internet

The SSO engine's web access will make it possible to deploy X.509 card authentication without having to modify the target applications that will work with their login and password. The login and password are the same as the ones provided by the user from his or her PC inside the organization, or via the Internet.

Rule 3: protecting the most sensitive applications through biometrics

The SSO engine will allow the restriction of R&D-application access only to R&D workstations fitted with biometric readers for authentication. A user may use a normal PC to connect to his or her standard applications, or a PC with biometric reader when he or she wishes to connect to his or her R&D applications in addition to his or her applications.

Rule 4: access in a public area

Enterprise SSO will enable users to use active RFID badge-based identification to access only authorized applications in public areas.

Enterprise SSO includes strong authentication in the security policy.

There is no need to install an advanced authentication solution for initial authentication if you have not solved the problems of authentication for access to target applications.

Enterprise SSO will enable you to effectively deploy a global authentication policy on the information system:

- Managing and securing access to target applications
- Filtering applications according to the PC and the associated authentication mode
- Consolidating log information for all authentication types (initial authentication and authentication to target applications).

Evidian can help you design a user-authentication and application-access-control project.

For more information, you can contact us on: <http://www.evidian.com/evidian/contacts.php&c=lbstrauth>

Email: info@evidian.com