State of the art

PERSPECTIVES

Strong Authentication: Reducing hidden costs

This white paper details the strong authentication methods that are most commonly used in organizations.

It also details the problems that are most frequently encountered during deployment and day-to-day administration, and offers practical and commonly implemented solutions.

EVIDIAN
A Bull Group Company

Introduction

Strong authentication techniques are constantly changing. Organizations are using them more and more often to protect internal and external access to their systems.

In practice however, deploying strong authentication is often *more time-consuming and more expensive* than anticipated. The problem is rarely due to the technology itself, but rather due to how it is implemented and used on a day-to-day basis:

- Unforeseen use, such as a self-service kiosk, delegated accounts, mobility, conversational terminals, etc.
- Resolving lost card and supply issues
- Users (often influential) with very specific needs
- Managing equipment from many different suppliers

As a result, it is important to anticipate the *hidden costs* of deploying strong authentication, very early in the process. Otherwise, there might not be enough funds or available manpower after a few weeks. That said, making the right choices to begin with can greatly avoid disappointment at later stages.

This document is based on more than 10 years of experience in deploying authentication in organizations (500 to 110,000 users). It describes the authentication techniques and their limitations and offers practical advice for deploying and managing strong authentication.

Strong authentication: the basics

When used correctly, strong authentication helps to strengthen access control in the computer system. A user states who he is (*identification*) and then proves his ot her identity (*authentication*).
By reinforcing these two steps, your activity is made more secure:

Integrity: Prevent important information from being modified.	*Accounting data, financial data, analysis results, etc.*
Confidentiality: Only authorized individuals can access information.	*Medical record, credit card numbers, etc.*
Availability: The smooth running of the business is not affected.	*Administrator accounts, production management, etc.*
Audit: Avoid letting people deny actions they have carried out. Investigate incidents.	*Workstations used by traders in a bank, store sales, etc.*
Business: Increase the feeling of security among your customers.	*Online sales, outsourcing national defense, etc.*

Not all roles in a company are handled the same way. You may want to provide smart cards only to store vendors or to a hospital's clinicians, while the rest of the organization uses passwords. Another example is a pharmaceutical company that might use biometrics only for test-related activities.

It is therefore important to define the objectives clearly at the start of a project. These cbjectives should be expressed from a functional (or "business") standpoint, and not in technical terms. Once approved by the stakeholders, this "charter" will serve as a guideline over the course of the project:

- **Scope:** users, organizations, resources, etc.
- **Main objectives:** integrity, confidentiality, availability, audit, etc.
- **Constraints:** specific needs, critical profiles, deadlines, etc.

The seven most popular authentication methods

A user typically provides two pieces of information in order to access a protected resource:

- One element (name, directory number, etc.) used for **identification**
- One or more elements user for **authentication** itself.

Users can prove their identity by what they know (password), what they have (smart card), and who they are (biometrics). The following is a list of the seven authentication methods most commonly found by Evidian in organizations:

Authentication Type	Description
(1) Password	Simple, even rustic, its biggest flaw is that the security level depends directly on the complexity of the password. The result is that too many overly complex passwords make users take various measures to remember passwords, such as writing them down on Post-It™ notes or entering them in an Excel file or a smartphone. *A login and password combination is the most commonly used method of authentication. Single sign-on (SSO) solutions can reduce the increased number of passwords.*
(2) One-Time Password (OTP)	An OTP can prevent a password from being stolen and reused. An OTP system (usually a specialized calculator) provides a password upon request. This password is valid for a limited period of time and can only be used once. *OTP is generally used for initial authentication for external access via VPN. It does not require any configuration of the workstation or smartphone concerned.*
(3) PKI certificates on a smart card or USB key	X.509 certificates are often used to encrypt or sign messages without having to share a secret. The login ID is a public certificate that is signed and therefore guaranteed by a recognized certification authority. The user must provide a secret piece of information in order to use the cryptographic elements, such as the PIN code of its smart card or its USB key. In companies, smart cards are typically used more often than USB keys for authentication, even though the chip itself is often the same in both cases. *This solution is frequently used for initial authentication or for access to email or web applications. It requires a Public Key Infrastructure (PKI).*

Authentication Type	Description
(4) Login and password on a smart card or USB key	Storing the login and password on a smart card completely secures the authentication process. The password can be very complex, and it can be automatically and randomly changed very frequently. Without the card and its PIN code, there is no longer access to the password. *This solution is usually used for authentication on PCs without having to deploy a key infrastructure.*
(5) Cell phone	A cell phone can serve as an authentication object. There are two main methods used: * During authentication, a one-time password is sent by SMS to the user's cell phone. * A smartphone application calculates a one-time password itself. *The cell phone method is often used if the user forgets his password or smart card, particularly for access on the Internet.*
(6) Biometrics	Authentication using biometrics is based on verifying a part of the user's body. The most often type used is the digital fingerprint. The user's biometric data is stored on a central server (with major legal constraints), on the workstation, or on a smart card. *Biometrics is typically used for initial authentication or to protect access to highly sensitive applications.*
(7) Contactless card	A chip that is embedded into a contactless card contains a code that identifies a user. Therefore this is an identification method that, paired with a password, can be used in authentication procedures. There are two versions of this technology. With active RFID, the card has its own power unit. This enables detection over a longer range (e.g. when entering a room or office). *Active RFID can be used to detect absence for workstations in areas accessible to the general public.* With passive RFID (HID, MIFARE, etc.), the card does not have its own power unit. When it is read, it is powered by an electromagnetic field generated by the reader. *Passive RFID is often used to control physical access using a pass or for payment in a company cafeteria. This type of card can be detected from a few centimeters away.*

Variations in use

Other technologies exist, therefore it is possible to require authentication on only a limited number of machines. A workstation will then be identified by its network address or its unique hardware features.

In practice, there are many variations in use, as shown below:

- Some resources require multiple means of authentication, such as a digital fingerprint and a smart card. This is called multi-factor authentication.
- Conversely, an organization may feel that one simple identification is enough, such as presenting a contactless card to access a site.

Authentication Type	**PC + hardware**	**PC only**	**Smart-phone**	**Cost**	**Usability**
(1) Password	✓	✓	✓	●	●●
(2) One-Time Password	✓	✓	✓	●●	●
(3) PKI certificate on a card	✓			●●	●●
(4) Login/password on a card	✓			●●	●●
(5) Cell phone	✓	✓	✓	●●	●
(6) Biometrics	✓			●●	●●●
(7) Contactless card	✓			●●●	●●

Of course, security needs must be balanced with ease of use. A highly secure solution might be rejected by operations staff if it imposes too many constraints on them. It can be said that, "*Too much security kills security*."

Case Study	In hospitals, patient care is the top priority. Although there is a strong need for medical confidentiality, healthcare workers do not want to spend too much time being authenticated if it takes time away from looking after patients. For this reason, some hospital authentication projects are not very successful. For example, stations may be left open with a smart card permanently inserted in the slot, meaning that the identification is exactly the same for all categories of users. A solution that is often chosen is to use a *contactless card with limited authentication* in terms of time and space. The doctor uses a PIN code on arrival and can then access the PCs within his department for several hours, simply by presenting his card. This combines security and efficiency.

What do you want to protect?

This question is not as simple as it seems. Controlling access is only one way of protecting a company's true value, which may include its information, reputation, procedures, availability, and more. Therefore, if we can restrict the use of sensitive applications to certain PCs that are protected by smart card, it would be unnecessary to equip all of the company's PCs with card readers.

Knowing your objectives clarifies the goals of a project, which can then typically be broken down according to the technical targets:

1. **Physical** access to sites, buildings, or rooms
2. **Internet access**: logging onto the company portal in particular.
3. Access to **workstations**, such as for authentication on a PC, kiosk, etc.
4. Access to critical **applications**, including accounting, trading, production, etc.
5. Access to **functions** within an application, such as a signature page

Strong authentication methods often differ according to the target. A smartphone will not usually allow you to insert a smart card! Employees are therefore equipped with multiple authentication devices or multifunctional devices.

Controlling access to applications

In general, strong authentication solutions are not usually used for controlling access to **specific applications** and even less for resources within these applications. Indeed, a software company cannot physically account for every possible method of authentication.

However, it is crucial in some situations to protect individual applications. For example, if a doctor leaves his desk with his session still open, no one should be able to use the computer to write a prescription. For this reason, it is essential to be re-authenticated when confirming actions.

> *One solution involves software tokens, such as SAML or Kerberos. However, this requires applications to be designed (or modified) to interpret them. This is rarely the case, and usually you cannot modify a company's 'history' applications and software.*
> *Another solution is a single sign-on (SSO) tool that prompts for re-authentication each time an application is accessed. SSO usually does not require your applications to be modified, making it a more practical solution.*

If you want more 'refined' restricted access to specific resources, it would be unrealistic to assign individual permissions, considering that each user typically uses 3 to 10 protected applications. Administration consoles for strong authentication tools are not designed for that.

> *One solution is to combine strong authentication with an identity management tool. This can be used to control access based on employee profiles.*

Strong authentication: where are the hidden costs?

Beware of complexity

The costs of deploying and using strong authentication are usually much higher than the purchase cost of the equipment itself.

"1 mechanism, 1 user, 1 PC, 1 application." If your project involves equipping a few dozen employees with personal smart cards, each one being used to access a main application on one PC, are you sure there won't be problems?

In reality, it is rare for deployments to obey this "4x1" rule. Also, poorly prepared deployment can lead to unforeseen situations that will disrupt the installation and increase administration costs.

How can we ensure smooth and continued use?

Those who design critical systems know that failures are inevitable. We have to anticipate them so that they cause as few problems as possible. After all, your computer system is one of the most critical areas of your organization!

By adding new elements, strong authentication deployment increases the potential for blocking some crucial activity – and likewise increase the number of calls to the help desk. Therefore, you need to anticipate the most common or harmful problems for the organization upfront and plan quick, automated, and inexpensive responses.

In the beginning: use of tools

No matter how simple authentication tools may appear, you will find that many users will experience problems with them. To plan for this, have some non-technical users test the solution very early in the process, perhaps using a pilot site. Do not stick with seasoned IT specialists or operations staff who are highly competent computer users. This will allow you to provide training sessions during deployment, if necessary.

- Are there devices that rookie employees can use?
- Has the supplier provided any training materials?

In the beginning: security procedures

Deploying strong authentication can lead to security vulnerabilities. Since you are going to assign authentication devices to users, you have to be certain that their identity is correct. The best option is to use a procedure that involves a physical handover delivery so that you can properly identify users.

- How can you be sure of a user's identity when issuing a device?
- Are access rights verified once the device has been issued?

Over Time: Losses and Failures

The devices you will deploy have a known Mean Time Between Failures (MTBF), which manufacturers can provide you with. However, you must also take human factors into consideration, such as lost or stolen devices, forgotten PIN codes, automatic lockouts, or even sick leave. "Influential users," which we mentioned earlier, are highly sensitive to these issues. They want to be able to continue working, even in the event of a failure or forgotten information. It is therefore important to provide them with a clear and satisfactory answer.

- Can an employee who has forgotten his or her card be given a temporary password, even if the help desk is not available?
- According to the security policy, is an employee who is off sick able to delegate access to his or her workstation to another employee?
- Can a blacklist be updated and managed easily?

One common method is to list the problems that are likely to occur most frequently, such as a lost smart card or a failure involving the biometric device, and also acknowldege that these problems might occur when help the desk is not available.

Case Study	A large bank has decided to deploy a digital fingerprint biometric authentication system for its staff. The initial procedure requires the user to register three finger prints, to anticipate times when one of the fingers cannot be used, such as when it is covered by a bandage. In an office, three users tended to share their PCs. In order to continue working insecurely like this, they simply registered one finger from each person on each of the PCs. Once their trick was found out, the procedure was changed. Now, the fingerprint registration process requires a member of the deployment team to be present.

The law of large numbers

A successful pilot site is never a foolproof guarantee. What works well with a few workstations and employees may prove to be completely impractical for thousands of users spread across dozens of sites.

This is explained by two additional management costs resulting from (1) the large number of elements to be taken into account, and (2) the existence of several suppliers with their specific features and administrative tools that are often incompatible with one another.

Managing quantity

Introducing a large quantity of elements into the company can considerably increase management workload. Elements such as assignment channels, photographs, loss management, temporary passwords when a password is forgotten, card stock levels, and blacklists, often make setting up a card management system essential.

Problems also arise when a central administrator does not personally know each and every employee that he or she manages. How can their individual access rights be determined? The two traditional solutions are to delegate administration to a hierarchical level close to the employee and to assign permissions based on business activity rules. These two practices are often used together. Automatically determined rights are then confirmed with approval from the employee's manager.

Managing complexity

Within a project, it may be necessary for authentication hardware from multiple suppliers to work together. There may be cases which require hardware (ex. biometrics used internally and a one-time password used externally) different from the hardware that a single supplier may have in its catalog. Also, if existing hardware is already used at some sites, it may be very expensive to replace.

Heterogeneity costs are often high. For instance, equipment supply chains are duplicated, along with interfaces for day-to-day administration. Finally, changing suppliers becomes extremely expensive, which is detrimental to negotiations.

One answer is to find solutions that make the system as 'agnostic' as possible regarding the technologies used. Some authentication management software on PCs is compatible with equipment from several suppliers and can provide additional features, such as obtaining a temporary password using questions and answers, eliminating the need to call the help desk. Similarly, third-party card management tools can be used with cards from different suppliers.

Case Study	An automotive supplier wanted to allow more than 20,000 employees to use a single personal card to enter its sites, pay at the cafeteria, and access their PCs. The idea is clear: if employees always needed their card with them, they wouldn't then be able to keep them inserted in their PC. During the preparation stage, the company realized that most of its sites were already equipped with physical access control systems. The company quickly realized that there was no uniformity in this equipment. How in this case could they possibly deploy an international solution? The solution was to use a specialized integrator that adjusted the employee passes one by one so that their radio component could operate with a standard authentication chip. The project also included a pass management component.

Special use cases

In strong authentication deployments, discovering a special case for use that is not covered by the solution can cause users to reject the solution. This risk is even greater because users with special constraints are often highly influential users. Examples of these situations are described below, with items that should feature in your authentication solutions.

One user – multiple PCs used successively

The day-to-day tasks of some employees may require them to move around within a site, such as doctors in a hospital, production managers at an industrial site, store vendors, and others. In these cases, 'kiosk' PCs are often available. Employees must be able to authenticate themselves and quickly return to their work session, regardless of the access point used at the site.

- After authentication, does the employee return to his or her working environment within a few seconds, without having to wait to restart the session?
- Can we prohibit some categories of employees from using kiosk PCs in certain areas of the site?
- Does the solution work with contactless cards or with professional or governmental smart cards?

One user – accessing multiple geographical areas

A user may want to access his or her resources when travelling between the company's various sites. Also, it is becoming increasingly more common for employees to access their professional applications with their smartphone or personal PC. These means of access should be controlled without preventing these users from working.

- Can we assign permissions to a user for a company's multiple geographical sites?
- Are remote PCs configured to support the authentication solution?
- Can the user be authenticated on an offline laptop computer?
- How is a user authenticated if he or she wants to use a smartphone to access resources?

One user – using multiple PCs at once

Some of your employees need multiple PCs and monitors in order to work. These may include software engineers, trading room workers, and manufacturing operation controllers. It is unrealistic to ask these employees to log in (and log out) at each point of access.

- Can a single authentication unlock (and then lock) all of the user's workstations?
- How can the user delegate access to this 'cluster' of workstations to a co-worker or assistant?
- Can we keep some monitors in "surveillance" mode (active display without a keyboard or mouse) when the user is away?

As we have seen, it is important for the most critical cases to be covered. A frequently used solution is to describe **use scenarios** during the initial stages of the project. Gather the opinions of the stakeholders and have them approve these scenarios. You will then have buy-in from the users and test records for the pilots and the supplier selection stage.

Case Study	An international bank wanted to confirm the identity of the traders responsible for each and every transaction performed in the trading room. The goal was to prevent the person responsible for a transaction from being able to deny performing it. The problem here is that, in a trading room, workstation accessibility is extremely important. It is out of the question to miss an opportunity just because it took a few extra seconds to enter a password. In this situation, how could they get the traders to accept an access control system? The bank worked with Evidian to review all of the trading room's procedures in order to devise an authentication solution that would not disrupt operations for any of them. This made it possible to deploy an access control solution in all countries.

Technical Restrictions

Some authentication solutions have limitations in terms of use. A technical limitation may be intrinsic. Some solutions for virtual workstations do not natively support smart cards or biometrics. There must therefore be a separate solution in place for authentication management.

However, the limitations are not always so apparent. For example, a large oil company needed smart cards that were resistant to high temperatures for its employees working in Gulf states. Another example involves legal constraints that prevent the use of certain solutions, such as regulations on the export of encryption algorithms.

As you can see, some technical limitations might not be discovered by a pilot site. If they are discovered during deployment, alternative solutions may need to be prepared for some countries, departments, or user categories. It is therefore particularly useful to detail cases for use before deciding on solutions.

If the architecture of the overall solution does not depend on the strong authentication supplier, this is also an asset. It will then be easier to find workaround solutions with another supplier in the event of a problem.

Case Study	A major financial institution wanted to use digital fingerprint verification to protect all its customer managers' PCs. However, this solution is full of legal limitations. In France, it is illegal to store most *biometric signatures* centrally, i.e. information that is compared with the user's fingerprint during authentication. The solution was to provide smart cards to the employees, containing their biometric signatures. A simple procedure allows employees to record their fingerprints in order to link them up with the their Windows account. Once it is set up, only the card (and the employee's finger) are needed in order to log in.

Summary

An access control deployment will be successful, and less expensive over time, only if it is carefully planned around all of your major use cases. This makes it possible to avoid technical, organizational, and human obstacles during deployment.

By considering day-to-day management right from the start of the project, you will ensure that the strong authentication solution will be accepted by users and that there will be no unforeseen operational costs.

For further information, please go to www.evidian.com
Email: info@evidian.com

This white paper is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001).

39 A2 75LX 00