



## IDENTITY AND PASSWORD MANAGEMENT

Enterprises and government organizations everywhere are grappling with the daunting challenges of managing secure access to their information. It can be a struggle to provide information access to a wide range of users without exposing sensitive data, except to those who need it. The situation becomes more complex with the introduction of multiple user identities. Indeed, information security is about protecting data well enough to thwart all unauthorized attempts to access that data.

One way to address access is to verify the established identities of those who are trying to gain access. There are a variety of ways to accomplish this. Identity management strives to authenticate<sup>1</sup> user identities and assign user rights and restrictions. To retain control of and safeguard an organization's resources, IT departments assign user rights. After all, the underlying purpose of identity management is to give information access to those who have authorization and to deny access to those who lack it.

The foundation for virtually all authentication techniques in use today is one or more tokens (either physical or virtual) or identifiers<sup>2</sup>.

Identity tokens tend to come in three flavors: (1) knowledge tokens (something you know), (2) physical tokens (something you have), and (3) biometric identifiers (something you are). All tokens and identifiers are surrogate identities for the individual or group that they represent.

A knowledge token is a PIN, password, or some obscure personal information that supposedly only that individual or a defined set of individuals know (e.g., the name of his childhood pet). Indeed, knowledge tokens are the oldest and still most widely used of all authentication techniques; from computer passwords to the challenge/response passwords uttered by a military sentry, humans have always used verbal information to authenticate one's claim to a given identity.

A physical token such as a key, badge, card, passport or license is almost as old and as widespread as knowledge tokens. The concept is clear: if an individual is carrying something that supports his professed identity, then he probably is who he says he is. Thus, an ID card / passport helps to verify the individual's identity claim.

A biometric identifier is an objective measurement of some physiological or behavioral characteristic that is used to authenticate identity. It might be the vein pattern in a given finger, one's iris, a thumbprint or a voice print. Biometrics are generally considered more credible than individually presented knowledge or physical tokens, as biometrics measure one's unique characteristics. But where a knowledge token (e.g., PIN) is correct or it isn't, and where someone possesses a physical token or he doesn't, a biometric token results in a match probability. Biometrics systems are based on probabilities and are not digital, yes/no validations.

---

<sup>1</sup> Authenticate or authentication mean exactly the same thing as verify / verification. They are interchangeable terms.

<sup>2</sup> A token is basically a representation of an individual; an identifier is a unique biometric characteristic.



The various token types have their merits and their limitations. Interestingly, in a given set of circumstances, each token or identifier might be the best solution for that situation. However, a token or an identifier offers only one security factor<sup>3</sup>. And so, authentication of an individual using only one security factor is generally not as strong as the solution that combines two or three security factors. Thus, strong authentication is the popularized term for employing two or three of these methods. So, the combination of a knowledge token (e.g., one's PIN) and a physical token (e.g., one's bank card) significantly improves the likelihood that an individual is legitimately who he says he is.

### The Reality of Passwords

For better or worse, the primary method employed for informational access is the lowly password which has become our key defense. But passwords are susceptible to a variety of attacks. Password length has become important because passwords less than 13 characters in size can be readily broken with today's computing power<sup>4</sup>. With the constant advancement in computing power, password length will probably continue to grow. Well meaning IT departments decree not only password length, but also the structure of the password (upper and lower case and special characters), insisting that we cannot reuse the password root (e.g., password\$01, password\$02, password\$03, etc.), and we must change them with accelerating periodicity<sup>5</sup>. Clever password variants such as pa\$\$w0rd, or pa55worD aren't really that clever, as they do little to thwart savvy attackers. Corporate password policies strive to ensure that passwords are too difficult to guess and too long to break; but unfortunately, they have become too hard for most humans to actually remember. And that is just in our office environments.

We often encounter situations where we use multiple user profiles, depending on our individual roles. We do so across a variety of networks and applications, each with varying password composition requirements, reuse rules, and differing expiry dates. Further, studies confirm that the average user has at least 15 password-protected accounts with which to deal. Is it any wonder that so many people are stressed with password frustration! Indeed, the trend to longer and more complicated passwords which must be continuously changed is actually fueling complacency among users. It is so difficult to remember one's credentials (IDs and passwords), that some people have given up trying. They simply write them down and keep an updated list in their billfold or other personal item. In fact, let us state without hint of ambiguity, most people write down at least some of their passwords or write hints to themselves regarding their passwords. Further, stringent password policies such as requiring a numeric or special character and citing the number of characters in a password actually provide fraudsters with a blueprint to help them break the password. This is not the security principle that IT departments wish to encourage; and yet by their well-meaning but

<sup>3</sup> Actually, in the biometric world multi-modal biometrics enables the use of multiple biometric modes (such as combining voice recognition with fingerprints and finger vein pattern recognition). Multi-modal biometrics is considered highly accurate, but can be expensive.

<sup>4</sup> The ability to break a password with computing power refers to a brute force attack, or its variant, a dictionary attack. While lengthy passwords can deter such attacks, they do little to thwart phishing, spyware such as keylogging, electronic eavesdropping, and other password compromise techniques.

<sup>5</sup> A password change based on time of use is called password aging. Frankly, while an annual change has some value, studies show that weekly and monthly changes are more self-defeating than useful security techniques. Indeed, frequent changes actually decrease security by frustrating users and compelling them to write the passwords down as a coping mechanism.



off-target insistence on rigid password rules, that is exactly what some IT departments have done. They inadvertently discourage good security practices and encourage the clandestine recording of user credentials among their staff.

So why not just stop using passwords and replace them with alternate technology solutions for information access such as public key infrastructure (PKI) and biometrics? In the right application PKI is an excellent solution to authenticate an individual; but a trusted certification authority must be established, and there must be a means to track private keys, revoke keys, etc. Moreover, PKI remains too pricey for many enterprise applications. Biometrics is relatively accurate, but has issues of interoperability among the numerous biometric modalities, a decided lack of universality among human populations, and it too carries a significant cost. In fact, no technology in existence today even approaches the relatively low cost of passwords; and that is the real reason we use them. However, it can be argued that the cost of forgotten passwords and the resulting loss of productivity render passwords quite expensive for most enterprises.

What does work and is gaining momentum is the trend to augment passwords with other authentication technologies to garner multiple factors of security. Used in concert with each other, two- and three-factor security provides better data protection, reduces vulnerabilities, and tends to better comply with privacy and security mandates such as SOX<sup>6</sup> and HIPAA<sup>7</sup>. And there are several technologies that can augment rather than replace passwords. The most economical and arguably the most versatile technology is an IC (integrated circuit) chip, better known as a smart card. There is a growing trend toward the storage of one's credentials in a smart chip (whose form factor might be a smart card, a smart chip-based USB token<sup>8</sup>, or even a SIM<sup>9</sup> chip in a mobile phone). A smart card is mobile, tamper resistant, and can store all data in an encrypted form.

### **The Reality of Password Management Systems (PMS)**

If we return to the initial business problem of managing passwords, there are two well-known solutions in use today – password synchronization and single sign-on (SSO) – and both have merit. Password synchronization coordinates passwords across multiple systems, synchronizing password resets such that a user has to remember only a single password, but he must input that password each time an application or target system requests it. A signature feature of password synchronization is its support for self-service password resets. Password synchronization systems reduce password management to one password; they are relatively easy to deploy across an enterprise; and they enable the enforcement of policy compliance. However, they cannot support third-party applications, such as Internet URLs; they only support those target systems on which they can control. Because of its initial set of fixed costs, password synchronization systems are considered expensive solutions for smaller enterprises.

<sup>6</sup>The Sarbanes-Oxley Act (SOX) came into force in July 2002 and introduced major changes to the regulation of corporate governance and financial practice.

<sup>7</sup>The Health Insurance Portability and Accountability Act (HIPAA) -- the HIPAA Security Rule identifies standards and implementation specifications that organizations must meet in order to become compliant.

<sup>8</sup>A smart USB token is essentially a USB physical device which houses a small computer chip that stores information and has embedded software to perform a given function. Smart USB tokens can provide strong authentication and secure access to corporate networks and Internet services, while stabilizing costs and increasing user convenience.

<sup>9</sup>SIM is a Subscriber Identity Module used in the majority of mobile phones today. The SIM chip can link the identity of the phone subscriber to a call, rather than link the phone itself.



Traditional enterprise single sign-on (E-SSO) solutions eliminate repetitive sign-on, don't require software deployment onto target systems, generally have less fixed cost than password synchronization systems, and can support both intranet and Internet applications as well as most desktop applications. On the other hand, traditional E-SSO solutions tend to have deployment challenges, single points of failure, and other limitations including no self-service password reset solution.

There is an array of password management systems (PMS) aimed at the consumer. These systems include software-based solutions which load to the user's PC; software-based solutions that can be stored on a flash drive for portability; and smart chip-based solutions, specific to a given PC. These systems work well enough for individuals, but depending on the solution may lack portability (e.g., software-based solutions) from PC to PC, and/or may lack security (e.g., many flash drive-based solutions).

### **The Movement to IT-Self Service**

Password reset calls generally account for 30-40% of a Help Desk's call volume. Deflecting these calls can generate tremendous cost savings for an organization. Self-service password reset used to be an enterprise wishlist item; now it is a requirement for many organizations who are doggedly determined to reduce their Service Desk staffing and costs.

Recognizing the value of self-service password resets, some companies invest heavily in the technology side to support their PMS solutions, building custom portals for content "how to's" and creating static solution sets with diverse application support. Unfortunately, many of these technology implementations lie dormant as users eschew their use. These enterprises seemed unaware that success in any self-service endeavor requires extensive planning, strong implementation with continual content refreshment, re-engineering of business processes, a focus on user adoption, and vigorously implemented managerial disciplines. A business cannot transform itself if its processes remain the same. Further, until significant user adoption is achieved, nothing will change.

The primary prerequisites to end user adoption are ease of use and a strong value proposition. Gaining user adoption is about changing human behavior. Organizations must keep the content and the processes fresh and accurate, enable end users to access that content quickly and without hassle, and support immediate password resets. Moreover, enterprises should reinforce adoption through a variety of support mechanisms such as end user forums, surveys and user training. In that way, they will provide the value to the end user who will adopt willingly.

To determine the success in implementing a new technology organizations logically want to quantify the results, and that usually implies the measurement of an adoption rate. Indeed, an adoption rate is not only a strong measurement for project success, but it often doubles as a reliable indicator of resistance to change. The organization should measure end user use as well as user satisfaction; and it should establish target objectives against which to evaluate the usage statistics.

So, an organization wishing to implement a password management strategy should not forget to provision for self-service password reset. Further, enterprises must realize that it is not a technology decision alone that will determine



success or failure of the program. It is the total solution which focuses on end user adoption of new, streamlined business processes that will transform ‘what is’ to ‘what could be.’

## The Solution Criteria

What the market truly needs is a highly secure, affordable PMS which is convenient, easy to use, and mobile. Every organization has to determine the solution that is right for them. However, we can suggest some basic evaluation criteria for use in selecting one’s optimal PMS.

- ▶ **Security** – Most PMS vendors will opine that their respective solutions are secure. However, security is relative. A software solution residing on one’s PC or in a standard flash drive may be adequate for limited personal use; but unless the credentials are encrypted and are themselves stored on a secure platform, then they are vulnerable to attack. Moreover, if a PMS is not easy to use, then bad security habits will surface; and that is not truly secure either.
- ▶ **Versatility** – A PMS that only supports some applications and not others may not be right for an organization. To what extent can the PMS be customized for functions unique to the enterprise? Can the PMS support intranet, Internet and desktop applications?
- ▶ **Convenience** – Some password management systems do nothing more than store a set of credentials on a token or in PC-based software, enabling the user to access the stored files for the credentials that he forgot, and then manually enter them into the application. That is marginally more secure than carrying a list of passwords in one’s billfold or purse; but it is not particularly convenient and the password must not be stored in the clear - ever! Encryption of one’s credentials when in storage is essential. What most organizations need is a system that automatically retrieves encrypted credentials, decrypts them and then automatically populates them to the application, upon request; and all a user should have to do is press the enter key.
- ▶ **Usability** – A PMS should be easy to install, easy to learn and offer intuitive navigation. It should enable the reset of a forgotten PIN or password, and it should be able to reconstitute a lost card or token with the original set of encrypted credentials. It should provide useful, accurate, self-help content to assist the user when he needs a quick answer to a question. Finally, users may just need access to a user group or favorite blog that has the same issues and may be able to share solutions with them.
- ▶ **Mobility** – The ability to use one’s PMS solution at any PC, at work or at home, knowing that one’s credentials are both safeguarded and immediately available for use, provides another dimension of value to many end users.
- ▶ **Scalability** – Some systems have strong fixed costs and are not really affordable unless an organization commits to a high level of usage. Other systems can address the needs of small organizations or consumers, but they cannot scale to support larger organizations, or they lack special functionality needed by larger enterprises. A PMS must be able to scale up and to scale down.



## Conclusion

Password usage permeates every aspect of our lives whether we are at work, college, playing computer games, performing a financial transaction, making a purchase over the Internet, accessing a membership site or social networking. For the foreseeable future we must co-exist with passwords. We must reduce the security exposure that our inappropriate procedures invoke (e.g., recording our passwords on paper and carrying them around); but we need not live with password frustration.

There are technology solutions available today that provide secure storage of our credentials and yet enable

us to use those credentials wherever and whenever we need to do so. These solutions combine security with convenience, functionality with affordability, and mobility with usability. Frankly speaking: unless a user has an automated secure device to manage his or her passwords, then he or she is probably at risk! Writing down passwords is just not appropriate; and the selected solution should not only automate password reset, but should include a device that securely safeguards the user's credentials, yet automatically logs them to whatever application he or she chooses!