

Multi-Factor Authentication

*Protecting Applications and Critical Data
against Unauthorized Access*

CONTENTS

- What is Authentication?
- Implementing Multi-Factor Authentication
- Token and Smart Card Technologies
- SafeNet's Identity and Access Management Solutions



INTRODUCTION

Security. In today's business environment, it is the one word that continually poses challenges to organizations looking to protect their data assets. Everything from financial information, transactions, and intellectual property to customer and employee data—it all assumes an increased level of vulnerability as network access is broadened both within the organization and externally.

As networks become increasingly exposed through a wide range of access points, the traditional user name and password method of authentication is no longer sufficient for establishing and trusting user identity. Passwords are often so simple that they can be easily guessed, or so complex that the user needs to write them down, which is weakening security. And while changing passwords on a regular basis can somewhat minimize the risk of guessing or a brute force attack, the aforementioned vulnerabilities are still present. Yet many companies continue to rely on passwords as their only means of user authentication.

Password-based authentication is very expensive for organizations. The financial burden of resetting passwords represents a significant portion of an IT help desk workload. But there is a bigger picture to look at these days in terms of what it can cost a company should a data breach occur. The impact can be staggering on both finances and reputation.

Most methods of strong user authentication are based on two factors—something you know, such as a password or PIN, and something you have, such as a token or smart card. Once a secondary form of authentication is introduced, security is dramatically increased because both factors need to be present in order to successfully authenticate. Even stronger protection can be implemented with a third factor, something you are, which employs biometrics, such as a fingerprint.

Storing “digital identities” on a secured device, such as a token or smart card, is emerging as a preferred method for positive user identification. These devices can add security and convenience to widely used enterprise applications, such as Windows logon, VPN access, network authentication, digital signatures, file encryption/boot protection, password management, and biometric storage.

This paper will explore all of the key components of strong authentication, including the various form factors that can be implemented, the benefits of strong access control, and the solutions SafeNet has to offer.

Between January 2005 and June 2007 over 155 million individual records in the U.S. were reported compromised through unauthorized access to data systems, insider wrongdoing, administrative incompetence, or theft of computers and other storage media.

What is Authentication?

Authentication is the process of verifying that a person is who they claim to be. This can be done by using any of the following factors:

- something you know – password or PIN
- something you have – token or smart card (two-factor authentication)
- something you are – biometrics, such as a fingerprint (three-factor authentication)

Authentication ensures that the user is who he or she claims to be.

In this electronic age, where identity and data theft are on the verge of becoming commonplace, it is vital that a person's digital identity be trusted at all times. To achieve this, a level of challenge can be invoked in the authentication process, forcing the user to prove their authenticity beyond a simple password. The more factors used to determine a person's identity, the greater the trust of authenticity.

In terms of security, authentication is distinctly separate from authorization, which provides access to specific applications and data based on the user's identity. Authentication ensures that the user is who she claims to be, while authorization defines her role once they are granted access.


Password Authentication

Passwords are the most common form of authentication, but unfortunately, they are also the least secure. Although organizations can invest a great deal of effort in implementing password management systems that require varying levels of password complexity, it is still a fact that passwords can be fairly easy to "crack" by those wishing to gain unauthorized access to networks and data. In low risk/low data value environments, the use of password authentication may be sufficient. But for any computer or network that contains sensitive data, it is desirable, and in many cases required by law, that this data be more securely protected.

Two-Factor Authentication

The use of two-factor authentication provides a significant increase to the level of network security by forcing a user to provide two means of identification when attempting to log in. In most cases, this is a password (something you know) and a security token (for example, USB or smart card - something you have). These devices are small enough to carry and typically store cryptographic keys, digital certificates, and digital signatures. Since the user's digital credentials are saved on the USB token/smart card instead of the computer's hard drive, they are protected from compromise.

A USB token is a physical device that is typically small enough to be carried in a pocket or bag, or attached to a keychain. These devices are usually tamper-resistant, and their hard casing makes them quite durable. To log on to a computer or network, the token is inserted into a computer's USB port and prompts the user to enter a unique PIN number for authentication. The computer then communicates with an authentication server to verify the user.



A smart card is similar to a credit card in shape and size, but the difference is inside. A smart card, like a USB token, contains an embedded microprocessor that can be programmed with user credentials, including digital certificates, encryption keys, and digital signatures. To log on, the user inserts the smart card into a network-attached or embedded smart card reader and the reader communicates with an authentication server to verify the identity.

Three-Factor Authentication

The third factor of authentication is something you are, commonly referred to as biometrics. The most common type of biometric is a fingerprint, and this, combined with a password and token, provides exceptional security. Other types of biometrics include voice and facial recognition, and iris scanning. The use of biometric authentication has been slow to market due to the high cost of implementing readers that handle this type of identification. As the need for stringent security steadily increases, its use will become more prevalent.

Implementing Multi-Factor Authentication

The use of more than one authentication method is referred to as multi-factor or strong authentication, the most common of which is two-factor authentication. A familiar example of two-factor authentication is an ATM card, where, in order to access your account, you insert the card (something you have) into the ATM machine and enter your PIN (something you know).

Implementing multi-factor authentication has been growing in popularity as organizations look to increase security and meet the demands of industry and government regulations that require protection of sensitive consumer and employee information. Most organizations will typically already have a user name and password system in place for network authorization and access. Deploying a USB token or smart card solution is quickly becoming the method of choice for achieving increased security. Many factors contribute to the popularity of multi-factor authentication, including cost, convenience, and user acceptance.

Implementing multi-factor authentication has been growing in popularity as organizations look to increase security and meet the demands of industry and government regulations that require protection of sensitive consumer and employee information.

USB Token and Smart Card Technology

A USB token/smart card solution allows for the convenient storage of certificates for authentication, identification, and digital signing. Since an organization can issue and manage their own USB token/smart card strategy, they can also mandate the associated policies. USB tokens and smart cards are able to be easily deployed to large numbers of users in a short period of time with minimal system disruption, even if those users may be geographically dispersed. The USB token/smart card is used to authenticate each user to verify his or her identity, and then provide the user with the authorization level to access specific resources and data based on the user's job requirements.

USB token and smart card technology has opened up tremendous new opportunities for enhancing and simplifying security solutions. Because of their familiar and acceptable form factor, their processing power and storage capacity, and their certified mechanisms for securing digital credentials and other data.

Tokens and smart cards are becoming a preferred solution for securing access to online services and applications.



Typically, USB tokens and smart cards have only been deployed as vehicles to provide secure storage for private keys and certificates in PKI and VPN environments. Cryptographic USB tokens and smart cards have been the perfect complement to VPN solutions for enterprises that needed secure remote access to enterprise networks. However, multi-function USB tokens and smart cards have many additional capabilities that enable stronger, yet simpler security solutions while providing organizations with increased value and benefits. Some of these benefits include:

- **Security** — Cryptographic keys, certificates, and private information are securely stored in tamper-proof hardware.
- **Portability** — The small form factor allows digital credentials and private information to go wherever you go.
- **Flexibility** — A USB token/smart card can be used to store a variety of information and perform a variety of security functions, such as cryptography, credential storage, physical access control, and logical access control.
- **Simplicity & Ease of Use** — Simple insertion of a token into a USB port or a smart card into a reader, and the entry of a passphrase, unlocks a variety of automated security functions.
- **Upgradeability** — USB tokens and smart cards are easily upgraded to support biometrics, PKI, and other security functions, without needing to replace existing user devices.

Compliance

Corporations that handle sensitive financial and customer data must conform to certain government and industry mandates to protect this private information from compromise, unauthorized access, interception, or corruption.

For example, in the U.S., financial institutions offering online banking are required to comply with the Federal Financial Institutions Examination Council's (FFIEC) mandate to implement two-factor authentication.

The compliance maze may appear to be complex and expensive to navigate, but careful selection of comprehensive authentication and access control technologies can simplify the compliance process and substantially reduce financial, operational, and business risk.



SafeNet's Multi-Factor Authentication Solutions

SafeNet iKey™ USB tokens and SafeNet Smart Cards are secure authentication devices that can hold users' credentials, such as passwords, keys, certificates, or biometrics, in a highly secure fashion. The devices have an operating system (DKCCOS) that enables capabilities such as storing personal information or providing physical access credentials securely to the device. The cards/tokens can be used in both PKI and non-PKI environments. Whether smart card or USB token, both form factors have identical capabilities, and organizations can mix-and-match card/token types as requirements dictate.

SafeNet has earned a strong reputation in the industry for developing smart card and USB token technology that strictly adheres to industry standards, allowing for seamless integration with other leading information security products.

SafeNet iKey USB Token

The SafeNet iKey USB Token is a USB-based portable PKI authentication token—small enough to fit on a key chain—that generates and stores digital credentials, such as private keys, digital certificates, user names and passwords, and biometric templates. SafeNet USB tokens allow easy deployment of advanced authentication without the need to install additional smart card readers or expensive biometric devices. The iKey features tamper-proof hardware validated to FIPS 140-1, Level 2 as well as FIPS 140-2, Level 3, to provide high levels of security for your valuable digital assets.


SafeNet Smart Card

The SafeNet Smart Card is a multi-function card employing the highly secure DKCCOS operating system. Both devices are FIPS 140-2 Level 2 validated, and can be used to generate and store digital credentials, such as private keys, digital certificates, user names and passwords, and biometric templates, all on a familiar credit card-sized form factor. These smart cards can also be used as a physical access control card, employing magnetic stripe or RFID technologies. Several versions of the SafeNet Smart Card are available and designed with specific capabilities in order to meet a variety of needs. However, additional functionality can be easily added to any card as customer requirements dictate.

SafeNet MyID

SafeNet MyID enables corporate, financial, government, pharmaceutical, healthcare, and educational organizations to efficiently enroll, quickly issue, and effortlessly manage the lifecycle of smart cards, USB authentication devices, biometrics, and identity credentials. MyID is already integrated with most identity technologies and systems so that an organization can immediately start issuing smart cards and smart card-based devices to their employees. These devices can then be used to securely access both physical and logical resources.

SafeNet MyID provides enterprise customers with a powerful, interoperable, and secure system that reduces the cost of deploying and supporting smart cards and iKeys. Through innovative, policy-based enrollment features, SafeNet MyID significantly reduces the time an enterprise spends issuing and managing smart cards/tokens for geographically distributed users.



SafeNet MyID removes the complexities associated with deploying smart cards/tokens and digital identities, enabling enterprises to quickly leverage the benefits offered by these technologies.


Some of the benefits include:

- **Easy to Use and Quick to Deploy** — MyID is extremely easy to use. Users are automatically guided, step-by-step, through issuance and management tasks using unique and patented secure workflow technology.
- **Bureau Connector for High Volume ID Card Production Services** — The MyID Bureau Connector provides the capability to request and issue large volumes of ID cards. This connector enables the bureau request capability to be easily added to a MyID deployment without extensive systems integration or the use of additional products.
- **All of the Tools Required to Create Identities** — MyID is the ultimate identity convergence platform and is integrated out of the box with most smart cards and other identity devices plus their middleware with biometrics, public key infrastructure (PKI), physical access control software (PACS), authentication and single sign-on (SSO) systems, provisioning systems, plus directories and HR systems.
- **Tight Security Controls for Your Peace of Mind** — Access to MyID is controlled through the use of roles. MyID also employs a number of security mechanisms that help to significantly reduce the risk of fraudulent device issuance and use, while, at the same time, remaining resilient to attacks and misuse from unauthorized individuals and hackers.

Conclusion

Organizations, today more than ever, need to positively identify employees, contractors, and partners for both physical and logical access to sensitive information and facilities. Storing “digital identities” on a secured device, such as a smart card or token, is emerging as a preferred method for positive employee identification. These devices can add security and convenience to widely used enterprise applications, such as Windows logon, VPN access, network authentication, digital signatures, file encryption/boot protection, password management, and biometric storage.

SafeNet has earned a strong reputation in the industry for developing smart card and USB token technology that strictly adheres to industry standards, allowing for seamless integration with other leading information security products. For organizations looking to address the necessity of securing information assets and controlling user access to those assets, it starts with strong, reliable authentication. Whether smart card or USB token, both form factors have identical capabilities and organizations can mix and match card/token types as requirements dictate.



When introducing new technologies, end user acceptance is one of the top challenges. The implementation of a smart card or token-based authentication solution maximizes acceptance through ease of integration and simplicity of use. Users have quick access to their digital credentials at all times and can easily authenticate themselves for access to the information and services they need.

SafeNet Overview

SafeNet is a global leader in information security. Founded more than 25 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products, including hardware, software, and chips. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. SafeNet was taken private by Vector Capital in 2007. For more information, visit www.safenet-inc.com.

Corporate Headquarters

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524
Email: info@safenet-inc.com

EMEA Headquarters

Tel.: + 44 (0) 1276 608 000
Email: info.emea@safenet-inc.com

APAC Headquarters

Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.