

WHITE PAPER

Identity Management in a Virtual World

Sponsored by: Aladdin Knowledge Systems

Charles J. Kolodgy

June 2003

INTRODUCTION

Today's enterprises need new methods of developing trust in a virtual world. Wherever Internet access is available, business operations can occur. However, with expanded access to networks, enterprises are finding it increasingly difficult to authenticate who someone is. Doing business in the virtual world means that many business operations require some form of authentication to ensure that an authorized employee, customer, or partner is the one performing the operation. As well as being concerned about identifying authorized parties, enterprises are also becoming increasingly worried about ensuring and maintaining the security of proprietary information and privacy protection.

Ironically, complex and costly authentication and authorization systems have become an unexpected consequence of the technological advances that expand business efficiencies and market opportunities. Enterprises deploy dozens of applications which creates scores of fragmented user repositories with different authentication procedures. This is becoming a problem for the enterprise from a cost and manageability standpoint and users find it very difficult to keep up with the need to remember multiple user names and passwords. The bottom line is that numerous non-standard authentication and authorization mechanisms create inefficiencies, security problems, and cost concerns for many of today's businesses.

Successful enterprises are beginning to reject existing user ID and password systems and are turning to cohesive and stronger authentication solutions. Deployment of multi-factor authentication such as smartcards, one-time password tokens, biometrics, Public Key Infrastructure (PKI), and USB tokens is increasing. These methods dramatically increase the trust associated with identification by raising the level of security. Although all are better than diverse user name and password systems, they each differ in cost, ease-of-deployment, user satisfaction, and flexibility.

In this IDC White Paper commissioned by Aladdin Knowledge Systems, the requirements and issues associated with user authentication are explored and the reasons why many enterprises continue to struggle to implement cost-effective authentication mechanisms is addressed. The White Paper also looks at the inefficiencies associated with user names and passwords, multiple authentication methods, as well as the increasing requirements on user authentication. The solutions offered by Aladdin Knowledge Systems provide an infrastructure that allows organizations to address password authentication problems in a secure and cost-efficient manner. Their convenient USB-based two-factor authentication tokens, smartcards, and supporting software solutions are outlined in detail.

WHO ARE YOU? USER AUTHENTICATION DEFINED

Authentication is the means of verifying the identity of a person or entity. It can also be used to verify that information and data being transmitted is the same information that was originally sent and who sent it. Closely associated with authentication is authorization, which determines the level of rights and privileges available to the authenticated entity. Tying authentication and authorization together is identity management. Identity management encompasses a host of solutions and applications which provide varying levels of security and user management.

COMPROMISING SECURITY, COSTLY USER IDENTITY MANAGEMENT

The primary authentication method adopted for computer systems is standalone user name and password systems. This means that for each application or system that requires access, there is a specific user name and password created for the user. The application will maintain its own database of access credentials and they are not usually shared among multiple applications. This is fine when a user must access only a small handful of applications. However, as the number of applications and users expand, user name and passwords create security, scalability, and manageability problems.

What many enterprises are now seeing is password overload. Users have many more passwords than they can possibly remember. Just take a moment to consider how many passwords you are required to use on a standard day. The average user within an enterprise will have about a dozen. To add to the confusion, the password formats are different across applications and some passwords need to be changed periodically and others can last forever. Password overload is becoming a continual headache for IT and network security administrators.

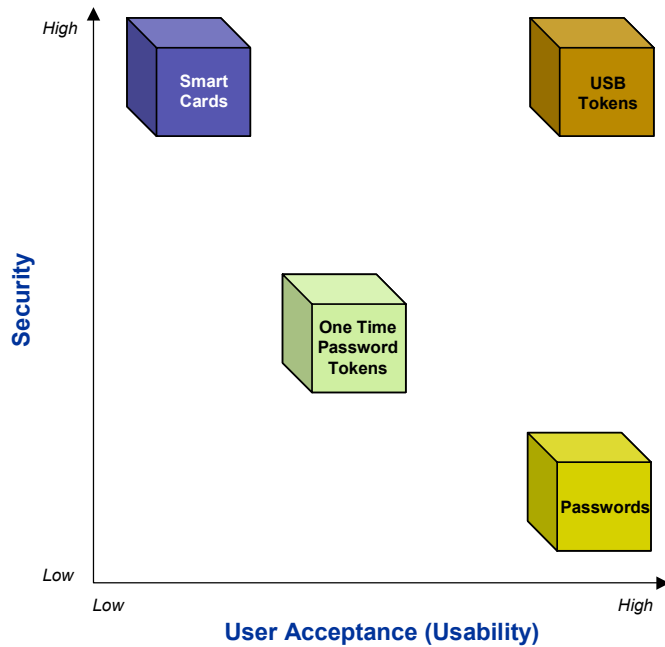
As well as the high ongoing maintenance of passwords, they provide the lowest level of authentication and offer little confidence of identification. The use of passwords compromises the overall security of an organization's network for the following reasons:

- They can be written down and are usually placed where they can be easily found (such as attached to the computer).
- They can be shared without any difficulty — even strong adherence to mandatory password change and rigid password rules do nothing to prevent password sharing or writing them down.
- Most passwords are selected because they are easy to remember (such as a birthday, a name, or a place) so they can be easily guessed. Machine-generated passwords or password selection criteria eliminate this, but in most cases, it just leads to the password being written down.
- Users generally select the same password for multiple applications so it will be easy to remember. However, once guessed, that password would be the first someone would try for another application.
- Most users need to get their passwords reset by the help desk because they forgot them. The resetting of passwords in itself can create vulnerabilities.

The many problems associated with passwords makes their use no longer acceptable for most enterprises. As an independent security consultant agrees, "On a recent project for a government department we discounted the use of passwords as a viable security solution immediately. Not only can passwords be used by someone else but they are a pain for people to remember and a huge hassle for administrators to change on a regular basis." Relying on passwords alone does not offer a secure, cost-effective, or even manageable solution. What enterprises need are additional authentication methods.

FIGURE 1

COMPARISON OF AUTHENTICATION MEANS BY SECURITY AND USER ACCEPTANCE



Source: IDC, 2003

ENHANCED SECURITY, IMPROVED USER IDENTITY MANAGEMENT

Better user identity management and security can be obtained from authentication methods that add a hardware component (something you have), to a password system (something you know), to a biometric (something you are). The hardware component can include smartcards, one-time password tokens, Public Key Infrastructure (PKI) certificates, and USB tokens. To be authenticated, a user must have the hardware and know a password, and all of these components must match with a software IT authentication system used by all entry points to a given system.

The use of a second or third factor greatly improves the assurance of the authentication system. Without this additional element, access to an application or network is not possible. Should the hardware component be missing, it can be identified quickly by the system administrator; however, if a password is stolen no one would be the wiser until after an unauthorized access to the system. With only one device that equates to an individual, it also eliminates the possibility that multiple users will use a single password, as an IT manager with a government healthcare organization states, *"our users like the idea of getting something that gives them that unique identifier to access the system."*

The specific authentication solution selected will depend on the needs of the organization and the deployment environment, as outlined by a security engineer for a defense contractor, *"Right now we use soft tokens, smartcards/smartcard readers, but we have to have the same equipment to make it work across the whole company. Many business units don't want to pay for the cards or readers. The USB token is more suitable as it can be used corporate wide because all the laptops and desktops have USB ports."*

An increasingly popular strong authentication method is Universal Serial Bus (USB) tokens which act like keys. A cryptographic algorithm is embedded in a plug that is inserted into the USB port. These tokens are popular because they are laptop compatible, but they do not have the same authentication strength as the traditional tokens that generate one-time passwords. USB tokens usually have digital certificates embedded within them and they can also be used as storage devices used to store MP3s or removable media.

Authentication methods deployed by enterprises must be able to perform their primary functions in a secure manner, but they must also be able to handle different environments and meet overall business objectives. The desire to cut costs, improve network efficiency, and offer an enjoyable user experience are also factors considered by businesses, as agreed by a user interviewed by IDC, *"Security was our number one driver and cost reduction was number two. From a security point of view, PKI certificates are taken off the desktop and from a cost point of view we have reduced the number of calls to the helpdesk asking for password resets."*

EXPANDING THE BOUNDARIES OF ACCESS

Previously, businesses only had to worry about controlling access to desktops or closed networks, but this is changing rapidly as highlighted by a security engineer, *"Contractors, suppliers, and partners have been granted access to our network so we need to know exactly who is on the network and we need to be able to watch what they access. Strong authentication is what we needed and tokens provide that extra level of protection."*

With the onset of virtual networks, a myriad of access points now require user authentication, including:

- Desktop access
- Network access
- VPN access
- Web access
- eMail access

In addition to the expansion of access to information systems, enterprises are also facing other internal and external pressures to implement stronger authentication, authorization, and identity management solutions.

INTERNAL DRIVERS

Enterprises are increasingly looking to ensure that the integrity of their information systems remain intact. Security is becoming the number one issue for many organizations, as highlighted by an IT security consultant, "*Many factors such as legislation and internal mandates are making security more popular, but the most obvious business driver is to reduce the maintenance and overhead cost involved in securing systems and to reduce risk by eliminating factors which are flawed by their very design and process.*" Internal issues are driving the need to improve security and to do so in a cost-effective manner. Key internal drivers include:

- Reduce the costs of maintaining present security systems
- The critical nature of information accessed by internal stakeholders
- Reduction of fraud
- Telecommuting requirements
- Expanding base of users as a result of advancements in technology
- Application needs (secure email, computer data protection, secure key storage, secure certificate storage, secure password storage, and secure key generation)

EXTERNAL INFLUENCES

Government legislation and other external pressures are increasing the awareness of security issues within the business community. Together with internal drivers, enterprises are beginning to realize the benefits of implementing stronger authentication methods.

GOVERNMENT REGULATIONS

One of the most important external factors impacting the need for stronger user identification is government regulation. These emerging regulations are raising the stakes associated with identification. The government regulations cover two different areas — privacy protection and electronic signatures.

Although there are many regulations looking at privacy protection, the regulation in the United States that has the most potential impact on the future development of privacy protection is the Health Insurance Portability and Accountability Act (HIPAA). This regulation, which went into effect in April 2003, requires healthcare organizations to protect the security and confidentiality of health information exchanged electronically. Unique authentication of users, refined access controls, and physical access controls are three focal areas of this regulation. Significant financial or criminal penalties will be levied for noncompliance.

The acceptance of electronic digital signatures for business transactions relies on the force of law. Worldwide, many governments have created regulations or passed laws that specify the minimum requirements required to conduct ebusiness with digital signatures. With government acceptance, the use of digital signatures will expand and by using strong authentication methods, the assurance associated with those transactions will increase.

BEST PRACTICE STANDARDS

In addition to government regulations, business best practices such as ISO 17799 are fostering the need for improved user identification and access controls. Continued acceptance of best practices by industry organizations and individual organizations will expand the use of strong multi-factor authentication.

BUSINESS PARTNERS AND CUSTOMERS

The transfer of sensitive information and transactions over virtual networks is driving the need for strong user authentication methods. As well as enterprises wanting to ensure who they do business with, suppliers, customers and other third parties also want to be assured that the information they are supplying is secure. As an IT manager with a government healthcare organization explains, *"We looked at standard user name and password encryption to access our Web site but we soon realized that the industry would not make proper reports through that system unless it was 100% secure. Our users understand security and they would not accept anything but a two-factor authentication system."*

BARRIERS TO STRONG AUTHENTICATION ADOPTION

User authentication enables organizations to control access to their systems and a USB token provides a cost-effective and user-friendly solution. However, some organizations are still reluctant to explore the feasibility of providing a cost-effective solution to added authentication. IDC's research has identified two main barriers to wider adoption of USB tokens: competitive issues, and concerns regarding the deployment of USB tokens.

COMPETITIVE BARRIERS

Typical barriers relating to the wider adoption of strong authentication methods identified by IDC's research include:

- Many people believe that passwords are free so unless they are forced to move to a more secure system they will hang on to the "free" passwords, or will move up to software tokens which would be the next step up from passwords.
- There is a large installed base of one-time password and challenge/response tokens. Many companies that have already invested in this technology may be less likely to swap out their installed product.
- As companies move to combine physical security identification cards and chip cards, they may discount the use of USB tokens.

While all of these concerns are valid for the people who have them, if they would look carefully, these barriers are ones of perception and not of reality. Passwords are not free when you consider the management and issuance of passwords and the costs of help desk calls when passwords are forgotten. Although very difficult to quantify, the yearly average cost associated with "free" passwords range from \$10 to \$35 per password. If a soft token is used, portability is lost and additional costs are added.

DEPLOYMENT FEARS

IDC's research also identified a number of fears and misunderstandings of the use of USB token systems, including:

- Some believe that USB tokens must require PKI to work.
- Fear that lost tokens will compromise the system.
- Concerns that the investment will be overtaken by another technology.

The deployment fears are also those of misunderstandings and the market can be educated to overcome them. USB tokens do not require a PKI, they work just as well storing user IDs and passwords. However, they do support many technologies, such as biometrics and PKI, thus they would still be useful if more advanced authentication methods are deployed. Lost tokens are not much different than a lost password and are much easier to manage because the user knows if they have lost their token but may never know if a password has been compromised.

DO YOU REQUIRE STRONG USER AUTHENTICATION?

User authentication is today's way of obtaining trust in the business world. It ensures that you control exactly who accesses your system and who you ultimately do business with. With a two-factor authentication system incorporating a USB device being a viable and cost-effective way of providing security, key decision-makers should be asking themselves the following questions:

- Am I currently using passwords to provide user access to systems?
- Does my system require users to remember at least 10 passwords?
- Do I have mandatory password updates or specific password creation rules?
- Do I need to control employee access to internal systems and applications?
- Am I able to track internal and external access to my information systems?
- Can I ensure secure access for my remote users?
- Are my customers and suppliers concerned about sending me sensitive information over virtual networks?
- Do I provide digital signatures and certificates to external users?
- Do I spend significant resources managing my existing authentication solutions?

If any of these questions apply to your organization then you should investigate the feasibility of implementing a strong, two-factor user authentication system.

Partnering with the right supplier will ensure that a secure, cost-effective, and manageable user authentication solution is provided. What should be considered when selecting a provider of a two-factor authentication system? Some key issues to consider are:

- Understanding of an organization's security needs and challenges
- Capability to provide suitable user authentication solutions
- A track record of supplying a cost-effective solution
- Ease of use of technology and implementation and user support services
- Providing a suite of solutions which exactly meet changing business needs
- Flexibility that allows for a staged deployment
- Ability to integrate their solution into existing infrastructure
- A history in the security field

HOW USB TOKENS ADDRESS THE BARRIERS TO AUTHENTICATION AND ADOPTION

IDC believes that the value of security lies in the following factors: convenience, loyalty, immediacy, privacy, transparency, and cost-effectiveness. All these elements will make security attractive to a broader audience. Making security a business enabler instead of an obstacle will result in deeper access, automated manual tasks, streamlined processes, increased revenue generation, and improved profitability.

Recent trends indicate that smartcards are migrating from their traditional credit card form into USB keys, thus removing the need for additional readers and decreasing the overall costs of production and deployment. IDC's research indicates that USB tokens are growing at a CAGR of 92.3% (see Table 1) and that the traditional challenge/response and one-time password token market will continue to lose share to USB token authentication because of decreasing costs and greater convenience afforded by USB tokens. IDC's Enterprise Technology Trends Survey, 2002, also highlights the increasing popularity for two-factor authentication, with over 40% of large enterprises evaluating or investigating the use of hardware or software tokens.

TABLE 1

WORLDWIDE USB TOKEN VENDOR REVENUE, 2001–2006 (\$M)

	2001	2002	2003	2004	2005	2006	2001–2006 CAGR (%)
USB tokens	7.6	12	23	60	120	200	92.3%
Growth rate	–	57.9%	91.7%	160.9%	100.0%	66.7%	–

Key Assumptions:

USB tokens will be widely adopted into the market due to the low price and greater convenience.

The adoption of USB tokens will also be driven by its ability to serve as a smart card in an alternative form factor, especially in environments requiring protected devices.

USB tokens will take market share from traditional tokens due to decreasing costs and greater convenience.

Source: IDC, 2003

The primary selling point for USB tokens are their low cost and ease of use, as explained by an IT manager, "Very little training is needed; you plug in your key, create the VPN tunnel, and enter your PIN, giving the same user experience as with a username and password. Even smartcards are more complex." USB tokens have a low cost per user and do not require an additional reader because virtually all personal computing devices already have USB ports. Key benefits of a USB token solution are:

- Single sign-on
- Security versus Convenience
- Support for multiple protocols and back-end systems (Network directories, SSL, IPSEC/VPN, SMIME)
- Cost
- Ease of use
- Portability
- Transparency
- Applications supported

The wider adoption of USB tokens will also be driven by their ability to serve as a smartcard in an alternative form, especially in environments requiring protected devices.

THE ALADDIN SOLUTION TO USER AUTHENTICATION AND IDENTITY MANAGEMENT

Aladdin Knowledge Systems is a leading provider of two-factor user authentication hardware and software. The flagship product is the eToken USB device which provides a secure and convenient method for securing networks and ebusiness applications. It offers a fully portable and cost-effective means of authenticating users and digitally signing sensitive business transactions. An eToken user sums up the Aladdin solution, "*Originally we bought the eToken just to store digital certificates securely. We allow employees to work from home, the office, or the road so with the token you don't need to have the certificate at multiple locations. Aladdin's solution provides additional software that allows you to store user IDs and passwords enabling the eToken to be used from other applications.*"

The eToken product range offers customers a robust solution for implementing strong two-factor user authentication designed to simplify login process and maximizes security. The product provides user flexibility in deployment through advanced smartcard technology. eToken can be packaged both in USB Token and a traditional smartcard form factor using the same software, which was a major consideration for the security engineer of a defense contractor, "*Aladdin was selected because they offer a smartcard too, so the drivers don't need to be changed, just the form factor.*"

eToken's versatile architecture enables organizations to use both existing authentication systems or introduce new ones based on advanced technology, while maintaining a similar end-user experience. All a user needs to do is insert the eToken into the USB port and type in the personal token PIN, regardless of the security system being accessed. As one user explains, *"We are using the eToken for two-factor authentication for remote access. We like that we could use our existing VPN client with eToken without needing to add any proprietary software. The Microsoft VPN client just recognizes it."*

Support for standard security interfaces, coupled with the ability to cache user passwords, enables the eToken solution to be operated with almost any authentication system. *"We are still using our existing log-in and user preferences. We selected the eToken because it was tied to standard log-in with Windows and Novell,"* explains an IT manager.

Aladdin's eToken product range includes the following:

DEVICE OPTIONS:

- eToken Pro** is a USB token authentication device that incorporates a high-security smartcard chip. Its smartcard includes an onboard cryptographic high-security processor capable of performing electronic signing, PKI key generation and operations.
- eToken Pro Smartcard** is an authentication card, the shape of a traditional credit card. Ideal for combining employee ID badges and physical access systems with logical access to networks. Its smartcard includes an onboard cryptographic processor capable of performing electronic signing, PKI key generation and operations.
- eToken R2** is a USB form factor token that offers secure and encrypted mobile storage.

SOLUTIONS:

- eToken Enterprise** is the framework for implementing eToken-based authentication with various types of enterprise security applications such as VPNs, network logon, and Web access. This framework also provides the ability to manage the tokens. The eToken Enterprise framework consists of the following:
 - eToken for PKI solution** enables interoperability with any standard PKI application. Any solution such as VPN, SSL Web access, Smartcard logon, secure email, and data encryption that relies on Microsoft CAPI or PKCS#11 interfaces will be operable with eToken.
 - eToken for Network Logon:** This solution enables secure login to any Microsoft or Novell domain servers using either PKI technology or by interfacing with the native Windows (GINA) logon mechanism directly or via Novell Netware.
 - eToken Web Sign-On (WSO)** stores all necessary Web logon information including passwords, PIN numbers, user accounts, credit card details, URLs etc. eToken WSO provides instant access to Web accounts by recognizing the saved page and automatically filling it with users' private credentials upon presentation of the eToken PIN; a single sign-on experience can be achieved without any changes to the back-end system.

- ☒ **eToken Simple Sign-On (SSO)** stores and submits logon information such as passwords and user names directly into the login screen of the security application. This solution is ideal for supporting non-PKI aware or legacy applications.
- ☒ **Token Management System (TMS)** is a management system that offers a bridge between the user, the organizational policies, the security system, and a personal token. The TMS enables the deployment, provisioning, and maintenance of security tokens, smartcard, and ID badges within an organization for use with a variety of security applications including network logon, VPN, Web access, secure email, data encryption, and other such applications.
- ☒ **eToken SDK** is the software development kit that allows for the smooth integration of eToken into authentication systems. With eToken's support for open, non-proprietary security standards such as Microsoft CAPI & PKCS#11, integration with security applications is quick and smooth. In addition to the robust Windows environment, the eToken SDK offers 16-bit real mode libraries to enable secure PC boot and full hard drive encryption, and support for various Unix flavors.

THE FUTURE

IDC predicts that USB tokens and smartcards will become interoperable because USB tokens also have PKI and digital-certificate capability. However, users must be able to distinguish between USB tokens and hardware authentication devices that are connected to the computer via the USB port. USB tokens, made by companies such as Aladdin, act like authentication keys with USB interfaces. As the technology develops, USB keys will be able to provide an integrated solution that could only previously have been provided through separate authentication devices.

Aladdin is already working to expand the functionality of the eToken by allowing it to store multiple credentials, such as digital certificates to simple passwords. These digital identity credentials can easily be retrieved from the token without user interaction, simplifying password management.

IDC feels that this unique decentralized form of single sign-on could resonate with customers, especially those that have multiple applications and force periodic password changes.

IDC believes a synergistic effect will drive the merger of information security with physical security. Authentication and authorization will become increasingly critical. Homeland defense will be based on tighter authentication of individuals as well as a more granular authorization for both IT infrastructure and physical access.

CONCLUSION

It has been demonstrated that stronger authentication methods are required by enterprises due to the expanding network boundary and increasing access points. However, security is only part of the equation. Ease of use, ease of integration, ability to support multiple applications, manageability, and cost considerations must all be taken into consideration.

Aladdin's eToken meets and exceeds all of these elements. Ease of use was a key factor cited by many respondents, as one user comments, *"When you access the system, it is identical to a password except you need to plug in a key."* Customers are also attracted to the ease of integration capabilities. *"We got the eToken to deliver a seamless network anywhere in the global community. Our solution had to be secure and everyone could use it,"* said one customer.

Many customers purchased eToken for one application but after seeing its potential are planning to extend its use. Improved security manageability has also been highlighted as a positive benefit of the eToken solution. The cost savings from the eToken solution was the most compelling benefit as one customer stated: *"One of the primary advantages of the eToken is its low unit cost and the low start-up cost — you can effectively get started for a few hundred dollars, whereas if we went for a system like the onetime passwords and challenge/response tokens there would have been a large investment in a back-end server which could cope with the constantly changing passwords."*

Ultimately, each organization will need to decide how to optimize their user authentication and identity management. Given the hidden costs associated with standard passwords (e.g., provisioning and help desk calls), all organizations should investigate how two-factor authentication, especially USB tokens such as Aladdin's eToken, can greatly improve user authentication security — while providing multiple access options and applications (such as digital signing and PKI portability), in a cost-effective way.

APPROACH

IDC developed this bulletin using a combination of existing market forecasts and direct, in-depth primary research. To understand the challenges enterprises face in dealing with user authentication and to learn more about how Aladdin's eToken helps address these challenges, IDC conducted interviews with IT executives at six organizations in the pharmaceutical, manufacturing, government, and security consulting industries to explore the particular issues and challenges they found most pressing. In addition, IDC reviewed its knowledge base from other primary research studies in the security arena. This White Paper reflects all of these research perspectives.

COPYRIGHT NOTICE

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

For further information regarding this document please contact:

Marketing Department

Tel: +44 (0) 20 8987 7100

Copyright 2003 IDC. Reproduction without written permission is completely forbidden.