

Technology White Paper



Secure Mobile Computing

*Using Two-Factor Authentication
With VPNs and Disk Encryption*



Executive Summary

Organizations of all types and sizes increasingly realize that mobile computing is critical to success. These organizations are giving their mobile users full access to the enterprise network, data, and applications through virtual private networks (VPNs.) Mobile users are also taking large amounts of sensitive corporate data on the road stored on their laptop hard drive, many of which hold up to 200 gigabytes. As a result, while mobile computing offers organizations many competitive advantages, it also entails significant security risks to corporate networks and sensitive corporate data. Indeed, the incidence of security breaches due to unauthorized access to the VPN and theft of laptop devices has skyrocketed, leading to high costs, lost competitive advantage, non-compliance with data privacy regulations, and tarnished reputations. And while organizations are attempting to secure access to their data through password authentication to the VPN and encrypting laptop hard drives, these measures leave significant security gaps. Passwords are insecure and encryption keys stored on the hard drive are insecure.

Strong authentication solutions successfully address these issues. Strong authentication goes beyond passwords to combine two or more types of authentication: something you know (e.g. a password) with something you have (e.g. a token or card) with something you are (e.g. a fingerprint). Unlike older authentication systems, today's strong authentication systems are paired with powerful management systems that make them easy to deploy, easy to use, and low cost. Today, there's no longer any excuse not to secure your mobile computers with strong authentication – and every reason to do so.

Table of Contents

| | |
|---|----------|
| More Mobility Means Greater Data Security Concerns..... | 1 |
| Growing Threats to Corporate Data | 1 |
| Greater Consequences for Break-ins and Data Theft..... | 1 |
| Existing Security Measures are Inadequate..... | 2 |
| Flaws in Securing Access to VPNs | 2 |
| Exposing Data on Laptop Hard Drives..... | 3 |
| The Solution: Two-Factor Authentication Using Tokens or Smartcards Supported by a Powerful Token Lifecycle Management System | 3 |
| Various Types of Two-Factor Authentication Hardware Devices are Available | 4 |
| How Two-Factor Authentication Devices work with VPNs and Disk Encryption..... | 5 |
| The Role of Token Management | 6 |
| The End of Excuses | 7 |
| The Aladdin Solution | 7 |

More Mobility Means Greater Data Security Concerns

From small-to-mid-sized businesses (SMBs) to the Fortune 500, organizations worldwide are realizing that mobility is critical to success. By year-end 2011, IDC expects that nearly 75% of the U.S. workforce will be mobile with mobile workers accounting for almost 80% of the workforce in Japan¹. Among the benefits, mobile computing allows companies to speed business response time, reduce corporate space and leasing requirements, and respond to worker demands for more flexibility by enabling telecommuting.

As high speed networks and public W-Fi hotspots proliferate, mobile employees are accessing corporate networks, data, and applications over virtual private networks (VPNs). And with many of today's laptops packing storage of 200 gigabytes or more, users are also taking more of sensitive data on the road with them.

Growing Threats to Corporate Data

Yet while mobile computing is key to an organization's success, it poses considerable threats to corporate data. A 2007 Ponemon Institute study found that 85% of midsized to large businesses spanning all industries have experienced a data security breach in the last 24 months – with nearly half of the incidents attributed to lost or stolen equipment such as laptops, PDAs, and memory cards². On any given mobile computing device, a data thief may find user identities complete with access information such as passwords and account numbers, personal directories of staff members and clients; data on how to access the VPN, intranets and server; financial information critical to corporate operations; email messages discussing sensitive projects or corporate operations; and even personal information and social security number numbers for customers, partners, and employees.

In just a two of hundreds of examples, in May of 2006 a laptop was stolen from the home of a Department of Veterans' Affairs analyst containing personal information and social security numbers for 26.5 million U.S. veterans and some of their wives. In September of 2007, a laptop containing personal information, including social security numbers, for 800,000 people who applied to the Gap, Inc. for jobs was stolen from the offices of a third-party vendor that manages job applicant data for Gap, Inc.

Greater Consequences for Break-ins and Data Theft

As highly publicized break-ins and data thefts have become more common, consequences have grown more serious. An expanding list of data protection laws and privacy legislation are holding organizations responsible for safeguarding personal data stored on their systems. These include the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) security standard, the European Union Data Protection

85% of midsized to large businesses spanning all industries have experienced a data security breach in the last 24 months – with nearly half of the incidents attributed to lost or stolen equipment such as laptops, PDAs, and memory cards.

¹ "IDC predicts the number of Worldwide mobile workers to reach 1 billion by 2011," emsnow, January 16, 2008

² "US Businesses Still Lack Adequate Security to Protect Client Information" Wall Street & Technology, By Melanie Rodier, June 18, 2007.

The risk of organizations damaging their reputations has heightened as many data privacy regulations require them to notify customers of any data privacy breaches and as third-party organizations report on these breaches publically.

Directive, Sarbanes Oxley, and more than 35 U.S. state data privacy laws. These regulations are levying increasingly stiff penalties; for example, PCI fines for serious data breaches reach as high as \$550,000, with additional sanctions that include increased auditing requirements and revocation of the right to process credit card transactions.

The risk of organizations damaging their reputations has heightened as many data privacy regulations require them to notify customers of any data privacy breaches and as third-party organizations report on these breaches publically. For example, the Privacy Rights Clearinghouse Web site publishes a complete list of all data privacy breaches that have occurred since 2005.

The costs associated with breaches have shot up as well. The Ponemon Institute³ found that the costs per breach grew to \$197 per compromised record in 2007, a 43% rise compared to 2005 as affected companies scramble to notify customers, bring in investigators, invest in new security technology and respond to lawsuits. The average total cost per reporting company was more than \$6.3 million per breach and ranged from \$225,000 to almost \$35 million. Potentially even greater are the costs to a company's long-term competitive advantage if a laptop containing sensitive intellectual property, such as product roadmaps, design plans, and financial information falls into the wrong hands.

Existing Security Measures are Inadequate

Given the elevated risk of data security breaches, the need for regulatory compliance, and the steep costs, it is imperative for enterprises to conduct all critical business workflows securely. Yet organizations using mobile devices continue to face gaps in data security. Of particular concern with mobile computing are the ease with which unauthorized users can access corporate resources via the VPN and the contents of a laptop's hard drive.

Flaws in Securing Access to VPNs

Corporations have long enabled mobile users to access the corporate network over a VPN secured through SSL or IPsec, secure Web access, or secure network login. But while the connections are secure, users continue to authenticate themselves to these connections using passwords. Passwords offer a weak means of ensuring that only authorized individuals reach the data for several reasons:

- **Passwords are difficult to use** – Studies reveal that users today have an average of 15 password-protected accounts. While one password may be easy to remember, handling many passwords is time-consuming task and a security risk.
- **Passwords are easy to share** – Companies need to ensure that the only authorized users access the network.
- **Passwords are expensive** – Complex password policies increase the likelihood that users will forget their password, requiring a call to the helpdesk to reset the password. Such calls drive up the cost of IT support and reduce productivity.
- **Passwords are not secure** – To handle multiple credentials, users often choose passwords that are easy to guess; use the same password for several accounts; or write down passwords and store them where they are easily found. Passwords

³ "Data breach costs soar" Information Security Magazine, By Bill Brenner, November 29, 2007

are subject to social engineering attacks where thieves use scams to convince people to disclose passwords. Adding to these risks, many tools are available that can “crack” a password using “brute force” attacks that attempt combinations of the accepted character set in order to find the one that provides access to the authorized area. These attacks are very efficient, accessing a seven character lower case password in as little as four hours.

Once someone steals a VPN password, the thief can access the corporate network and steal valuable corporate information. Organizations that leave authentication to alphanumeric passwords are thus increasingly seen as negligent. They need a stronger way to authenticate users.

Exposing Data on Laptop Hard Drives

As data and disk encryption solutions become easier to implement, faster, and more reliable, more companies are deploying this technology. Encryption is the process of encoding data in such a manner that it cannot be accessed without the special key needed to decode the information. The digital equivalent of locking a safe and providing access only to the person holding the key, encryption solutions are available in several types:

- Products that encrypt individual folders or subdirectories
- Full disk-encryption solutions that encrypt the entire contents of the hard drive
- Pre-boot authentication (PBA) solutions that carry out the user authentication process before the operating system boots, safeguarding the system from flaws in the operating system.

All of these encryption solutions have one major weakness. Anyone holding the key can open the encryption and reach the data, and in most cases, these solutions store the key together with the data. This makes the key easy to discover just as it is easy to find a real key placed under the front door mat.

The Solution: Two-Factor Authentication Using Tokens or Smartcards Supported by a Powerful Token Lifecycle Management System

The solution is strong token- or smartcard-based authentication supported by a powerful management system. Strong authentication increase the security of the authentication process beyond passwords by requiring two or more of the following forms of authentication:

- **Something you know** – something the user needs to remember, such as a password, personal identification number (PIN), or answer to a personal question.
- **Something you have** – something the user needs to physically carry such as a token or card.
- **Something you are** – a biometric feature, such as a fingerprint or facial characteristic.

The most effective forms of two-factor authentication for mobile computing combine a hardware token or smartcard with a personal identification number

The most effective forms of two-factor authentication for mobile computing combine a hardware token or smartcard with a personal identification number (PIN.)

(PIN.) Users authenticate themselves to their computer by plugging in the token into a USB port or the smartcard into a reader and entering the PIN. These devices remove the possibility that a thief will find the key by storing passwords and authentication keys on a device external to the laptop and they prohibit users from extracting or exporting passwords, certificates, keys or encryption keys. Tokens and smartcards also guard against brute force attacks by allowing the user a specified number of unsuccessful tries, determined by the organization's policy, before locking users out.

Hardware tokens and smartcards are also extremely convenient for users. A single device can store multiple passwords and credentials that users employ with their mobile devices, including credentials or passwords for an SSL or IPsec VPN, encryption keys, and passwords to multiple applications to which the user has access over the corporate network.

Tokens and smartcards can do even more for mobile users:

- Users can employ their token or smartcard to access their local network when they work in the office
- A specialized token or smartcard can implement digital certificates (PKI) by automatically generating and storing private keys. PKI can be used for secure network and web access, digital signing of records, and non-repudiation of transactions.
- Tokens and smartcards can provide single sign-on capabilities that enable users to access all devices, networks, applications and data to which they are authorized simply by plugging in the device and entering a single PIN.

With these capabilities, users need not remember and handle their passwords; they only need their token or smartcard and password to enter all of their accounts. Users can therefore choose more complex and secure passwords, or even randomly generate passwords to increase security. Meanwhile, the time spent on password administration and maintenance by both users and help desk personnel is significantly reduced, saving costs and increasing productivity.

Various Types of Two-Factor Authentication Hardware Devices are Available

A broad range of hardware devices are available that provide two-factor authentication in order to meet the needs of different organizations. These include:

Smart cards – Smart cards are credit card sized devices that contain highly secure microprocessor chips dedicated to cryptographic operations. To authenticate, users insert the smart card into a reader and enter a password. Smart cards provide highly secure storage of user credentials and keys. They also secure PKI implementations by generating keys and performing cryptographic operations on-board without exposing the user's private key to the computer environment. While smart cards are used to authenticate users to a VPN, they are not typically used on the road because they require a dedicated reader.

USB Tokens – USB Tokens are small hand-held universal serial bus (USB) devices, usually Flash devices, that users connect to their computer's USB ports to authenticate. Users are granted access upon plugging the token into the USB port and entering the token password. Tokens are often used to protect laptops.

Smart-card-based USB Tokens – Smart-card based USB tokens, which contain a smart-card chip, provide the greatest level of security, versatility, and mobility, leveraging the advantages of USB tokens and smart cards. They enable a broad range of security solutions and provide all the benefits of a traditional smart card and reader, without requiring a separate reader, allowing mobile users to take them on the road.

One Time Password (OTP) Tokens – OTP tokens are small handheld devices that generate a password meant for one-time use. A user wishing to authenticate enters the one-time password appearing on the token and this value is compared to the value generated by the authentication server. OTPs are best for users who wish to access their VPN from multiple points of entry, such as a public Kiosk, a laptop, a PDA, a cellphone and so on.

Hybrid Tokens – Hybrid tokens combine multiple types of authentication functionality on a single device. Hybrid USB and OTP tokens allow full USB-based strong authentication and security solutions, as well as OTP based strong authentication in detached mode (for example, for use on a laptop) when needed. Smart-card-based hybrid tokens that use the smart card chip for USB and OTP functionalities provide maximum security.

Software OTP Tokens – Software tokens enable strong authentication without a dedicated physical device. These tokens are software programs that can be stored on a user's laptop or on a mobile device, such as a cellular phone or PDA. Based on a secret key, the token generates a one-time password that is displayed on the computer or mobile device. Users can then use the generated OTP to access online services or authorize transactions. Though software tokens may add convenience to users, they are not as secure as physical tokens. The secret key can be more easily stolen or misused.

How Two-Factor Authentication Devices Work with VPNs and Disk Encryption

Two-factor authentication offers an easy and effective way to authenticate users for both VPNs and disk encryption solutions.

Working with VPNs

With a VPN, instead of specifying a password to connect to the enterprise environment, the user plugs a token into the USB port of a laptop and enters a PIN. The VPN application then authenticates the user through a challenge/response mechanism. When the token contains smart-card based PKI technology, the private key is never exposed.

Enhancing Disk Encryption Solutions

When used with a disk encryption system, the token stores the password or encryption key. Plugging the token into the USB port and entering the PIN unlocks the disk. Users can employ tokens for Pre Boot Authentication which requires them to authenticate themselves as they attempt to boot the laptop so that they access the machine in a secure manner. Because users carry the token with them, the system is more secure those that store the key on the disk. Users are also aware if they lose their token, which is not always the case with a stolen password.

When implementing two-factor authentication for mobile users, it is especially important for an organization to have an efficient and effective system for managing the token lifecycle.

The Role of Token Management

Many token management systems today make considerable demands on the help desk and administrators. When implementing two-factor authentication for mobile users, it is especially important for an organization to have an efficient and effective system for managing the token lifecycle. A token management system can dramatically improve IT efficiency by providing the following capabilities:

Token Lifecycle Management

As users go through their lifecycle in an organization, from joining to growing to eventually leaving, their tokens must be managed to support their changing needs and privileges. A powerful token management system simplifies the entire token lifecycle by making it easy to:

- Issue and deploy tokens by maintaining a physical inventory of tokens as they are issued.
- Enroll tokens by personalizing each one with the user's data, digital certificates and passwords.
- Maintain tokens by keeping a secure backup of existing credentials or cryptographic keys in a regulated archive and using automated logical processes to add or update credentials and applications on the tokens.
- Manage lost or damaged token by revoking the token immediately to ensure that no unauthorized person can use it; and then using the backup to quickly replace the token with a new temporary or virtual token that contains the user's credentials and cryptographic keys. This enables mobile workers to keep working, minimizing lost user productivity.
- Revoke credentials on user tokens to disable access for users who are no longer entitled to access the organization's networks and applications.

Self Service Tools

User self service capabilities improve IT productivity by enabling end users to manage their own tokens, for example by enrolling tokens or resetting passwords.

A Standards-Based Infrastructure

A token management system built on top of a directory service (e.g. the Microsoft Active Directory supporting directory standards such as LDAP and Open LDAP) provides a platform from which it is possible to view and manage tokens in association with the organization's user repository, rules and policies, and security applications.

A Flexible Solution

Older token management systems were monolithic. Today's systems are more flexible, allowing organizations to purchase only the hardware they choose (such as USB, OTP, or Smartcards) and the management modules necessary to support that hardware, with the ability to add new modules as their needs evolve. For organizations that chose to develop management applications themselves, a Software Developers' Kit (SDK) should be available.

The End of Excuses

In the past, two-factor authentication was expensive and required considerable effort to set up, deploy, and maintain. Now, there's no longer any excuse not to use two-factor authentication. Because of their comprehensive management capabilities, modern strong authentication solutions are now:

Easy to Deploy

Today's two-factor authentication solutions are far easier to deploy than their predecessors. Comprehensive and self-service token management systems offer automated, streamlined ways to manage the token lifecycle and handle lost tokens.

Easy to Use

End users are fed up with trying to remember multiple, complex passwords. To be effective, security must be transparent. Tokens offer users an intuitive, no hassle, and effective way to access an encrypted drive, VPN, and multiple applications.

Low Total Cost of Ownership

Not only have purchase prices for strong authentication solutions fallen to highly affordable levels, modern solutions also offer low lifetime costs. Because users only need to remember a single PIN, they are less likely to forget their password; minimizing the cost of password management. A strong token management system also makes it faster, easier, and less error prone to manage the token lifecycle and to replace lost tokens so mobile users remain productive.

The Aladdin Solution

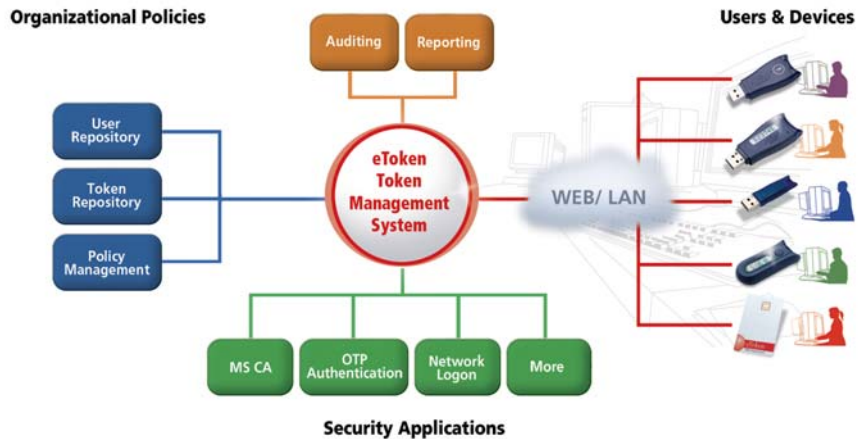
Aladdin has developed the eToken offering to meet all of an organization's authentication needs for its mobile workforce. Comprised of a wide range of smart-card-based devices, security applications and third-party integrated solutions with over 150 partners, the eToken offering enables organizations to rapidly implement a full suite of security solutions including secure VPN access, laptop protection, and much more. Alternatively, organizations can initially implement a portion of the offering while future-proofing their investment, gradually adding security features onto the same eToken platform.

eToken enables organizations to deploy a mix of devices for users based on their specific security needs. Highlighting the eToken line of devices are Aladdin's USB-based token, eToken PRO; a hybrid USB and OTP token, eToken NG-OTP; and a token with Flash memory, eToken NG-FLASH which offers encrypted flash memory. These key-sized tokens are highly portable and easy to use, simply plugging into a USB port. By providing strong authentication while seamlessly integrating into PKI architecture, eToken devices enable non-repudiation as well as on-board generation and secure storage of keys, passwords and certificates for digital signing and encryption.

eToken offers a full suite of strong user authentication and password management applications, all operable with the complete family of eToken devices. With an open architecture and an SDK for integrating eToken into external applications, eToken also gives organizations the flexibility to easily develop support for additional solutions. To answer the need for enterprise-level deployment and

eToken offers a full suite of strong user authentication and password management applications, all operable with the complete family of eToken devices.

Aladdin's Token Management System



life-cycle management capabilities, Aladdin offers the Token Management System (TMS), which manages all aspects of assignment, deployment and personalization of tokens and related security solutions. TMS is a robust system that offers full life-cycle management solutions, from automatic token and credential enrollment through token revocation to the handling of lost and damaged tokens. With TMS, token deployment is simple – users can easily enroll their devices online and immediately start using them. TMS integrates directly with an organization's existing user management system, providing a robust and flexible link between users, security applications, authentication tokens, and organizational rules.

TMS has an open, modular architecture that enables the management of token usage with third-party security solutions using TMS "connectors" – server-based, configurable plug-ins. In addition, the Aladdin TMS Connector SDK enables security solution providers to add management-level support to their integration with eToken by creating their own TMS connectors. With eToken, organizations can enable business and increase user productivity with secure access anytime, anywhere. Organizations can save password administration costs while empowering their users with additional benefits. With a robust and integrated product offering and an open, standards-based architecture, eToken provides the solution for organizations' current and evolving needs.

About Aladdin

Aladdin (NASDAQ: ALDN) is a leader in digital security, providing solutions for software digital rights management and Internet security since 1985. Serving more than 30,000 customers worldwide, Aladdin products include: eToken™, providing cost-effective strong user authentication and password management solutions; the eSafe® line of integrated content security solutions, protecting networks against malicious, inappropriate and non-productive Internet-borne content; and HASP®, a digital rights management (DRM) suite of protection and licensing solutions featuring the number one hardware-based system in the world.



For more contact information, visit: www.Aladdin.com/contact

North America: +1-800-562-2543, +1-847-818-3800 • UK: +44-1753-622-266 • Germany: +49-89-89-4221-0 • France: +33-1-41-37-70-30 • Benelux: +31-30-688-0800 • Spain: +34-91-375-99-00 • Italy: +39-022-4126712
Portugal: +351 21 412 36 60 • Israel: +972-3-978-1111 • China: +86-21-63847800 • India: +91-22-67255943 • Japan: +81-426-607-191 • Mexico: +52-1-55-4159-9733 • All other inquiries: +972-3-978-1111

1/16/2008 © Aladdin Knowledge Systems, Ltd. All rights reserved. Aladdin and HASP are registered trademarks and HASP SRM is a trademark of Aladdin Knowledge Systems, Ltd. All other names are trademarks or registered trademarks of their respective owners.