

*White Paper*



***Authentication Tokens:  
The Key to Secure PCs and Data***



# Table of Contents

|  |    |
|--|----|
| Abstract .....   | 3  |
| The Importance of PC and Data Security .....               | 4  |
| Composing a Solution.....                                  | 4  |
| Authentication Tokens to Enable a Secure Solution.....     | 5  |
| Presenting PC and Data Security Solutions.....             | 6  |
| The Truth about Authentication Tokens .....                | 8  |
| Guidelines for Optimizing the Benefits.....                | 9  |
| The eToken Offering.....                                   | 10 |
| eToken Support for Your PC and Data Security Solution..... | 11 |
| About Aladdin .....  | 12 |



# **Authentication Tokens: The Key to Secure PCs and Data**

## **Abstract**

It has already become well accepted that protecting data is critically needed for enabling digital business and activities. Consequently, a variety of PC and data security solutions are available in the market to answer this need, as well as to assist organizations in facing the growing threats of data theft and complying with the regulatory requirements for data protection. Together with authentication tokens, these solutions, ranging from computer pre-boot authentication and whole disk encryption to the encryption of specific files and email messages, can enable organizations to effectively protect their data. Authentication tokens are an essential component in PC and data security solutions for they provide strong user authentication, ensuring that individuals accessing data are who they claim to be. Furthermore, certain kinds of authentication tokens – such as USB smart-card-based tokens – can provide significant extended support for strong PC and data security by offering secure generation and storage of encryption keys.

The deployment of authentication tokens within an organization also intrinsically sets the foundation for additional security solutions including secure network access, physical access, and single sign-on. To make the most out of authentication tokens, it is important to select a token solution that can function as a platform for all the organization's access security needs, and that both administrators and users will find comfortable and easy to use. Since authentication tokens are a long term investment, organizations should opt to implement a scalable and flexible solution that can support not only their current but also their evolving security needs.

## The Importance of PC and Data Security

An organization's data assets, be they financial data, customer information, or transaction records, are one of its strongest and most valuable foundations. Providing the right people, whether they are staff, customers, or business partners, access to this data from multiple access points, is becoming increasingly important for enabling more business and creativity. Yet doing so, without compromising security, is becoming more and more challenging. When taking into consideration that data exposure can also mean a violation of confidentiality contracts or civil and government regulations and might lead to negative media coverage – security is a challenge no one wants to fail.

Laptops, in particular, make a fine example to demonstrate the challenge of enabling business without compromising security. Thanks to their mobility, expanding storage capacity, and available wireless network connections, laptops are considered to be a huge driver of the 'mobile business' dream. Yet these attributes are precisely what make laptops more easily stolen and misused, more accessible to unauthorized individuals, and consequently more important and challenging to protect.

Composing and implementing a security solution that meets this challenge enables organizations to offer enhanced business services, increase productivity, raise customer satisfaction, save password administration related costs, and comply with data protection and privacy regulations. It is important to note that all an organization's possible PC and data security needs cannot be answered by one out-of-the-box solution. The key is in selecting the components that together enable the organization to effectively achieve its security goals.

### Composing a Solution

The basis of practically every PC and data security solution is encryption. This is the process of encoding data in such a manner that it cannot be read or tampered with by any individual without the special key needed to decode the information. The significance of encryption may be easily understood when considering its use as placing data in a nearly impenetrable safe. The main advantage is that opening the safe is practically impossible without the right key; however, the shortcoming is that whoever gets hold of the key can open the safe and reach the data.

It is therefore obvious that when using encryption, the effectiveness of the PC and data security solution is widely dependent on the encryption key management strategy. A good strategy requires:

- *Strongly protecting the encryption keys* – Generating encryption keys and keeping them on the computer leaves the data vulnerable to physical and malicious software attacks. It is just like placing the safe's combination in the same room where the safe is located. To mitigate risks the keys should at the very least be generated and stored away from the computer.
- *Authenticating individuals before they can use the encryption keys* – Adding an authentication method to a solution based on encryption

**The 2005 CSI/FBI Computer Crime and Security Survey states the average loss per respondent from theft of proprietary information grew from \$169,000 in 2004 to \$356,000 in 2005. Further still, the average loss per respondent from unauthorized access to information increased from \$51,000 in 2004 to \$300,000 2005.**

can be thought of as placing a security guard at the entrance to the safe and instructing him to let only authorized people use the encryption key. With authentication it is possible to overcome the weakness of encryption and ensure that only authorized individuals can reach the data.

However, this is true as long as the authentication method used is strong and reliable; using a simple user name and password mechanism still exposes the PC and data to significant risk and cannot be regarded as an adequate security measure. It is therefore clear that one of the PC and data security solution components needs to be a reliable authentication method.

## Authentication Tokens to Enable a Secure Solution

A method increasingly adopted to ensure users' reliable authentication is *strong authentication*. This method is often used to enhance compliance to industry initiatives and government regulations such as the Sarbanes-Oxley (SOX) Act, the FFIEC Guidance of October 2005, Basel II, and the FDA 21 CFR Part 11.

With strong authentication, the security of the authentication process is augmented beyond passwords by requiring two or more of the following forms of authentication:

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

Strong authentication solutions commonly involve a physical token device used to prove the owner's identity. In today's market a wide variety of strong authentication token technologies and form factors are available.

### Which Device to Use?

For PC and data security solutions, it is most effective to use authentication devices that can support both user authentication and secure on-board generation and storage of encryption keys. The authentication device should therefore have:

- A physical connection to the computer to allow the use of encryption keys stored on the device, preferably through a USB port that can be found in almost every computer
- Highly secure microprocessor chips to enable the generation of encryption keys and cryptographic operations on-board the device

*USB smart-card-based tokens* have both a physical connection to the computer and highly secure microprocessor chips dedicated for cryptographic operations. They make data encryption solutions significantly more secure by never

**"Most data theft attacks would have failed if the stored information were encrypted and the encryption keys were sufficiently protected."**

– Gartner, "Data Protection is Less Costly Than Data Breaches",  
John Pescatore  
and Avivah Litan,  
September 2005

exposing the user's private key to the insecure computer environment. Smart cards offer the same functionality; however, unlike USB smart-card-based tokens, they require a unique separate reader for each machine in which they are to be used.

*One time password (OTP) tokens*, in contrast, do provide strong user authentication but cannot protect encryption keys on-board the tokens because they lack the physical connection to the computer and the secure storage capacity. Organizations wishing to use authentication tokens for PC and data security along with OTP access can use hybrid tokens, a combination of USB and OTP tokens that allow full USB-based strong authentication and security solutions, as well as OTP-based strong authentication in detached mode when needed.

For further information on strong authentication solutions and the different devices available in the market today, please see Aladdin's White Paper, "Strong Authentication: Protecting Identities and Enabling Business."

## Presenting PC and Data Security Solutions

A wide variety of available PC and data security solutions can be enhanced with authentication tokens. The various solutions can be generally summarized into two main categories: solutions that protect the entire PC, and solutions that protect specific files and ensure their confidentiality and authenticity.

### Protecting the PC

The first category includes solutions that aim to protect a PC, whether a laptop or a workstation, from the damage it may be exposed to if it is broken into, stolen or lost. The PCs' protection is achieved by combining disk encryption and pre-boot authentication solutions with authentication tokens.

#### *Disk Encryption Solutions*

Disk encryption solutions usually include:

- *Full Disk Encryption* – encrypting the entire content of the PC
- *Virtual Disk Encryption* – defining specific storage spaces within the disk in which all the stored data is automatically encrypted



Most disk encryption solutions are automatic and transparent to the user. As each user's encryption keys are securely stored on the authentication token, data cannot be decrypted until the user connects her token to the PC and authenticates herself.

## ***Pre-Boot Authentication Solutions***

To make it impossible to target the hard disk directly by manipulating the operating system and avoiding the regular boot procedure, disk encryption solutions are frequently further intensified with pre-boot authentication (PBA). PBA solutions carry out the user's authentication process before the operating system boots. Only after the user is strongly authenticated with her token is it possible to run the usual boot procedure and decrypt the hard disk.



## **Protecting Data's Confidentiality and Authenticity**

The second category includes solutions that aim to ensure files and emails can be read only by their intended recipients, verify the identity of the file's creator, and ensure the file was not tampered with to guarantee its integrity.

This category includes:

- *Encryption and decryption of files and emails* – users can encrypt and decrypt any document or email they desire using the encryption keys located on their token. Once the files are encrypted they can be safely stored or transferred wherever needed
- *Digital signatures* – users can sign any document or email they desire using their private key located on their token. The signature proves the integrity and authenticity of the signed document, and guarantees non-repudiation since the document could have been signed only by the token's owner

Beyond providing security, USB authentication tokens also offer portability – users can carry their credentials and keys with them and perform any of these operations from any computer with their token.

By deploying a token solution to secure PCs and data, organizations have already set the foundation for an additional scope of security solutions.

## The Truth about Authentication Tokens

Presenting USB authentication tokens only as a critical component of PC and data security solutions might provide a limited viewpoint. In fact, thanks to their security capabilities, USB authentication tokens enable organizations to establish a robust platform for a broad suite of security solutions with full scalability and flexibility for the solutions' implementation.



### Secure Network Access

USB authentication tokens can be used to safely allow users to access the organization's network. This could be either local access – authenticating users in the office to ensure authorized access to the company's servers, or remote access – authenticating users to provide secure communications between a laptop or workstation and a VPN or web server.

Providing users with widespread access to necessary business data and applications improves communication among employees, shortens the response time to customers, and increases productivity. Remote secure access enables organizations to create a secure digital community of trusted employees, customers, suppliers, and partners, and provides them with many tools and services that were otherwise risky or not practically possible.

### Certificate-based Operations (PKI)

Using tokens for PKI applications is a big step in maintaining full portability and ease of use while creating a secure digital environment. PKI based solutions enable secure authentication and communication as each user is allocated a cryptographic key pair – a public key and a private key with a unique mathematical relationship to one another. The public key is distributed openly, and the private key is kept secret. PKI can be used for secure network and web access, digital signing of records, and non-repudiation of transactions.

The implementation of PKI based solutions is traditionally considered costly and complex, but by automatically generating and storing the private keys inside the token, smart-card-based token solutions make a PKI implementation not only secure, but also operational.

### Single Sign-On

USB tokens can be used to securely store and manage all of their users' credentials and passwords. Users need not remember and handle their passwords;

they only need their token and token 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.

## Secure Physical Access

By incorporating elements such as ID badges and RFID coils on the authentication device itself, authentication solutions can provide the capability to integrate with physical access solutions. The combined physical and logical access provides more efficiency and unity, both in the solution's management and in its usage. Administrators can manage the entire secure access solution from one management system, and users need only use one device for all their security needs.

## Guidelines for Optimizing the Benefits

The success of PC and data security solutions depends on the qualities and abilities of each of the components it comprises. There are a few guidelines that can help in selecting an authentication token solution that will best support the PC and data security solution and optimize the benefits of the investment.

### Aim for Full Solution Coverage

For authentication tokens to provide full coverage for PC and data security solutions they should support:

- Strong authentication
- Secure on-board generation and storage of encryption keys and certificates
- Pre-boot authentication

These should be the minimum requirements, but not necessarily the only ones. Select authentication tokens that can support a wide range of solutions; for example, tokens that support single sign-on solutions can further improve security, save password administration costs, and increase the users' creativity and satisfaction by simplifying their day-to-day tasks.

### Ensure a High Level of Portability

Allowing users to securely carry their credentials, encryption keys and certificates, is only one facet of portability. Maximum portability can be achieved by using authentication tokens that do not require unique readers or servers and therefore do not confine the user to a specific location or computer. For example, it is possible to deploy smart-card-based USB tokens that can be used in almost any computer for encrypting and digitally signing data. Portability promises better solution acceptance, provides enhanced connectivity, and enables more business.

**Authentication tokens that support a wide range of solutions provide greater value to organizations, increasing security while reducing costs.**

**An open, standards-based authentication solution provides increased opportunities for extending solution support.**

### ☑ **Guarantee Manageability and Ease of Use**

A good rule of thumb is that the easier the solution is to use, the more willingly and effectively it will be adopted. Therefore, the solution should be as easy and intuitive as possible for both users and administrators, with user-friendly applications and simple self-service tools. Automated processes for day-to-day token management tasks such as handling lost or damaged tokens, or resetting the token's password, can reduce the load on the IT department and minimize errors. Management systems can assist in managing users' encryption keys and certificates, supporting tokens' deployment and life-cycle management, and handling the inventory of authentication devices.

### ☑ **Ensure Maximum Scalability and Flexibility**

A scalable solution lets organizations “future-proof” their investment by allowing them to gradually add security solutions while using the same platform. A flexible solution enables businesses to cost effectively select and modify the security solutions based on existing and evolving needs.

Look for vendors that not only offer a range of authentication tokens and a set of security solutions, but also offer products based on open architecture – such solutions can integrate with multiple third-party vendor products or customized applications. Offerings that include SDKs provide even increased opportunities for extending solution support. Authentication token vendors with many solution partners are likely to provide a more comprehensive offering and be more agile in responding to changing market needs.

## **The eToken Offering**

Recognizing the vital role of strong authentication and secure storage of user credentials in protecting organizations' digital assets, Aladdin has developed the eToken offering. Comprised of a wide range of smart-card-based devices, security applications and third-party integrated solutions with over 150 partners, the eToken offering gives organizations the ability to rapidly implement a full suite of security solutions. Alternatively, organizations can initially implement a portion of the offering while “future-proofing” their investment, and gradually adding other security features onto the same eToken platform at a later stage. With an open architecture and an SDK for integrating eToken into external applications, eToken gives organizations the flexibility to easily develop eToken support for PC and data security as well as additional solutions.



eToken enables organizations to deploy a mix of devices for users based on their specific security needs. Among the eToken line of devices are a USB-based token – eToken PRO, a hybrid USB and OTP token – eToken NG-OTP, and a token with flash memory – eToken NG-FLASH. These key-sized tokens are highly portable and easy to use, simply plugging into a USB port. By providing strong authentication and highly secure on-board cryptographic key generation and storage, eToken devices enhance PC and data security solutions with added security and portability.

To answer an organization's needs for enterprise-level deployment and 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 utilizing 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 TMS Connector SDK offered by Aladdin enables security solution providers to add management-level support to their integration with eToken by creating their own TMS connectors.

## **eToken Support for Your PC and Data Security Solution**

Aladdin has partnered with a number of leading PC and data security solution providers, offering organizations the possibility to quickly and easily deploy a PC and data security solution integrated with eToken security. With secure generation and storage of encryption keys, strong user authentication, and support for pre-boot authentication, eToken offers security capabilities that are critical for an effective PC and data security solution. Organizations can integrate eToken with their existing infrastructure and make use of the broad range of security solutions available with eToken, immediately or in the future. The ease-of-use, manageability, and portability provided by eToken make it possible for organizations to meet the PC and data security challenge and enable more business.

**Aladdin's Token Management System enables easy deployment and centralized life-cycle management of all authentication tokens and their associated security applications.**

## **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 information about Aladdin's solution partners, please visit [www.Aladdin.com/Partners](http://www.Aladdin.com/Partners)



For more contact information, visit: [www.Aladdin.com/contact](http://www.Aladdin.com/contact)

|                      |                                   |                            |                     |
|----------------------|-----------------------------------|----------------------------|---------------------|
| <b>North America</b> | T: 1-800-562-2543, 1-847-818-3800 | <b>Italy</b>               | T: +39(333)9356711  |
| <b>UK</b>            | T: +44-1753-622-266               | <b>Israel</b>              | T: +972-3-978-1111  |
| <b>Germany</b>       | T: +49-89-89-4221-0               | <b>China</b>               | T: +86(138)18184444 |
| <b>France</b>        | T: +33-1-41-37-70-30              | <b>Brazil</b>              | T: +55(11)5539-5688 |
| <b>Benelux</b>       | T: +31-30-688-0800                | <b>Japan</b>               | T: +81-426-607-191  |
| <b>Spain</b>         | T: +34-91-375-99-00               | <b>All other inquiries</b> | T: +972-3-978-1111  |

