

Technology White Paper



Strong Authentication:
Securing Identities and Enabling Business



Table of Contents

Abstract	3
Introduction	4
Passwords Are Not Enough!	4
It's All about Strong Authentication.....	5
Strong Authentication Token Solutions – What is Available?	7
Strong Authentication Solutions Are Evolving	10
Practical Considerations for Selecting a Strong Authentication Solution.....	12
The eToken Solution	14
About Aladdin	16

Strong Authentication: Securing Identities and Enabling Business

Abstract

In today's world, digital data and communications have become an inseparable part of people's day-to-day lives, holding enormous value for organizations. Thus, the need for data protection has taken the spotlight. Organizations are turning to identity and access management solutions – which increasingly include strong authentication as a vital element – to establish secure and trusted digital environments. Numerous forces are driving organizations to implement strong authentication solutions:

- Enablement of secure high-value transactions and provision of secure access to important information, to increase productivity and business
- Compliance with regulations such as SOX, HIPAA, FFIEC, and more
- Defence against attackers who exploit weak authentication for identity theft and fraudulent transactions
- Reduction of costs derived from poor password management
- Attraction of an increasing number of security-conscious consumers

Organizations are increasingly looking for holistic strong authentication solutions, rather than combining multiple systems. Holistic solutions can offer a mix of authentication devices for flexibility and cost savings; a broad range of supported security solutions to meet current and future needs, management tools for cost-effective deployment and life-cycle management of the full solution, and the capability to integrate with existing IT infrastructures and security policies. Together with this growing demand for advanced strong authentication solutions, more comprehensive and integrated product offerings are offered that support present and emerging requirements, improve ease-of-use for both users and administrators, and provide significant ROI.

The growing need for enhanced online services and network connectivity is bringing attention to the importance of securing user access.

Introduction

In today's environment, the need for organizations to increase connectivity to their networks, enhance their online services, and open new opportunities for electronic business is bringing ever-growing attention to the importance of securing user access. In addition, the recent barrage of identity theft and corporate fraud cases has brought corporate responsibility and the protection of sensitive data to the spotlight. Consumer demands and compliance pressures bring organizations and institutions to search for new ways to strengthen their internal controls, authentication methods, and identity management practices. The message is clear – action is needed to stay ahead in the fast-changing, security-conscious market.

The weakness of passwords can no longer be tolerated, and organizations are increasingly moving from password-centric to strong authentication solutions. This enables organizations to securely authenticate identified users and gain one of the most crucial elements of any business relationship – trust.

Organizations are realizing that security is vital for enabling business, cutting costs, complying with regulations, establishing a productive work environment, and attracting customers. Meanwhile, strong authentication solutions are developing to answer the organizations' needs by providing easy-to-use solutions with numerous benefits to both users and organizations.

Passwords Are Not Enough!

When first introduced in the early sixties passwords were regarded as cheap, easy to use, and secure. Forty years and many technological developments later, is there any reason to believe these facts still hold?

Passwords are difficult to use – Studies reveal that users today have on average approximately 15 password-protected accounts. One password may be easy to remember, but handling many passwords is a time-consuming task and a security hazard.

Passwords are expensive – Every forgotten or lost password results in significant costs. The expense is even greater when lost employee productivity is taken into consideration.

Passwords are not secure – To handle their multiple credentials, many users choose easy-to-guess passwords, use the same passwords for several accounts, or even write down passwords where they can be easily found. Add to these security risks the abundance of available password cracking tools and it is easy to see that passwords are no longer a sufficient security measure.

It has become evident and widely accepted that passwords are not a reliable method for authenticating users. To achieve the benefits of information security and overcome the inherent weakness of passwords, organizations are turning to stronger authentication solutions.

It's All About Strong Authentication

For organizations wishing to enable more business, reduce security vulnerabilities, comply with regulations mandating data privacy and protection, save costs, and attract security-conscious customers, a strong and robust authentication system can lead the way to achieving their goals.

Enable Business

By implementing strong authentication solutions, organizations can allow legitimate users to access sensitive data anytime, anywhere. With the enhanced security, organizations can provide their users with tools and abilities that are otherwise risky or not practical. For example, hospitals can enable their patients to securely access personal medical records online, businesses can enable their executives to access confidential business data from the corporate network while traveling; and university professors can allow their students to securely submit examinations and view their grades electronically.

Strong authentication enables organizations to offer services that are otherwise risky or impractical.

Comply with Regulations

A growing number of rules and regulations hold organizations responsible for the integrity of their business data and for the protection of personal information that has been entrusted to them. To comply, organizations need to ensure that individuals who access their network, applications, and portable devices are indeed who they claim to be. Therefore, strong authentication constitutes a basis for compliance with many of these regulations.

As an example, the Federal Financial Institutions Examination Council's (FFIEC) Authentication Guidance considers "single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties...Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation." Another instance is the Health Insurance Portability and Accountability Act (HIPAA), which requires healthcare related organizations to securely authenticate individuals before granting them access to sensitive patient data.

These are only two examples from an ever growing list of regulations, including Sarbanes-Oxley (SOX) Act, Electronic Signatures in Global and National Commerce (E-SIGN) Act, Basel II, Food and Drug Administration (FDA) 21 CFR Part 11, and more, that mandate organizations to protect their data and meet IT security standards. Strong authentication enhances compliance by enabling secure user access and providing a proven and attestable method for protecting internal data and networks.

Strong authentication increases regulatory compliance by enabling secure user access and providing a certifiable method for protecting internal data and networks.

¹ "The Twilight of Passwords: A Timetable for Migrating to Stronger Authentication," by Ant Allan, Gartner, Inc., February 28, 2007.

Strong authentication enables users to spend more time engaging in value-added activities.

Strong authentication saves costs by enabling more efficient business, significantly reducing password administration expenses, and preventing costly security breaches.

Increase Productivity

Providing users with widespread access to necessary business data and applications in the office, at home, or on the road, improves communication among employees, shortens the response times to clients and customers, and in short – increases productivity. Strong authentication solutions provide the needed security for organizations to give their users such access.

Strong authentication solutions also increase productivity by significantly reducing the time spent on password administration and maintenance by both users and help desk personnel.

Save Cost, Increase ROI

Strong authentication enables organizations to provide increased connectivity and secure access to digital data and applications. By offering additional services online, organizations can enhance efficiency and thereby save significant costs in their ongoing business activities.

When implementing strong authentication with single sign-on capabilities, organizations can reduce the ongoing costs associated with password administration, as users need not handle multiple passwords. For example, smart-card-based authentication tokens can securely store all user credentials on-board, and users need only remember their single token password to access their credentials. Strong authentication solutions that offer user self-service token and credential management tools enable organizations to reduce costs even further.

Strengthening security also saves organizations significant costs by preventing potential security breaches. These include misuse of data and networks by insiders, lost data from stolen laptops, and other security attacks that affect many organizations today^{2,3}. With strong authentication, it is possible to block unauthorized access and to hold authorized individuals accountable for their usage of the organization's digital resources, thereby reducing errors or deliberate harmful behavior.

In general, different strong authentication offerings provide various levels of solution support. The broader the range of security solutions enabled – such as secure network access, single sign-on (SSO), PC security, and secure data transactions – the greater the return on investment (ROI).

² According to the 2007 CSI Computer Crime and Security Survey, close to 46% of respondents suffered a security incident; 59% reported insider abuse of network access and 52% reported insider abuse of email. The average loss reported in the 2007 survey skyrocketed to \$350,424 from \$168,000 the previous year.

³ A 2007 Ponemon Institute study found that 85% of midsized to large businesses spanning all industries experienced a data security breach in the previous 24 months - with nearly half of the incidents attributed to lost or stolen equipment such as laptops, PDAs and memory cards. "US Business Still Lack Adequate Security to Protect Client Information," Wall Street & Technology, Melanie Rodier, June 18, 2007.

Attract Customers

The dramatic increase in fraud and online identity theft has led consumers to demand better online security. Organizations are now viewing security not only as a need for compliance, but also as a marketing differentiator, attracting customers, increasing sales, increasing brand loyalty, and improving their reputation by positioning themselves as security-minded. Consumers are dictating to the market that the better product is also the safer product. Strong authentication provides an effective solution users can easily understand and adopt.

Strong authentication helps organizations to attract security-conscious customers.

Strong Authentication Token Solutions – What is Available?

Strong authentication solutions enable organizations to ensure that a user is indeed who he or she claims to be. They 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, a PIN, or an answer to a personal question
- Something you have – something the user needs to physically carry, such as 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 device, (e.g. token), used together with a password to prove the owner's identity. A wide variety of strong authentication token technologies and form factors are available in the market. The following are descriptions of the key form factors available today:

USB Tokens

USB tokens are small handheld devices that users connect to their computers' USB ports to authenticate. Users are granted access upon plugging the token into the USB port and entering the token password. The physical connection between the token and the computer enables these tokens to be used for multiple security applications such as secure local and remote network access, web access, laptop and PC protection, file encryption, user credential management, and secure transactions.

Smart Cards

Smart cards are credit card sized devices that contain highly secure microprocessor chips dedicated for cryptographic operations. To authenticate, users must insert their smart cards into their readers and enter a password. Smart cards provide highly secure storage of user credentials and keys. They also secure PKI implementation by generating keys and performing cryptographic operations on-board, without ever exposing the user's private key to the computer environment.

While providing extensive functionality and high security, smart cards lack mobility. Using a smart card requires a separate reader for every machine in which the smart card will be used.

Smart-card-based USB Tokens

Smart-card-based USB tokens, which contain a smart card chip leverage the advantages of both USB tokens and smart cards to provide the greatest level of security, versatility, and they enable a broad range of security solutions and provide all of the benefits of a traditional smart card and reader – without requiring the separate reader.

One-time Password (OTP) Tokens

OTP tokens are small handheld devices that allow authentication using one-time passwords generated by the device, based on a secret key shared by the device and an authentication server. 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.

While OTP tokens are highly portable, they do not provide the same level of support for multiple security applications that USB tokens and smart cards offer. Also, because the tokens are operated on batteries, they have limited lifetimes.

Hybrid Tokens

Hybrid tokens provide multiple types of functionality, which increases flexibility. Hybrid USB and OTP tokens allow full USB-based strong authentication and security solutions, as well as OTP-based strong authentication in detached mode when needed.

Smart-card-based hybrid tokens that use the smart card chip for both USB and OTP functionalities provide maximum security.

Software Tokens

Software tokens enable strong authentication without a dedicated physical device. These tokens are software programs that can be stored on a user's computer, or on mobile devices 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. Software OTP tokens are also available for use with mobile devices.

While software tokens are convenient for users, they are less secure than physical tokens because the secret key can be stolen or misused relatively easily.

The table below summarizes the key advantages and disadvantages of the presented technologies:

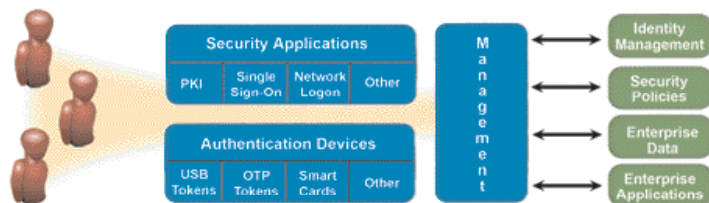
Product	Key Advantages	Key Disadvantages
USB tokens	<ul style="list-style-type: none"> • Mobile – can be used in any computer with a USB port • Support multiple security applications • Evident personal benefit to users 	<ul style="list-style-type: none"> • User software installation required
Smart cards	<ul style="list-style-type: none"> • Highly secure • Easy to carry – fit in a wallet • Support multiple security applications 	<ul style="list-style-type: none"> • User software installation required • Low mobility – reader required
Smart-card-based USB tokens	<ul style="list-style-type: none"> • Highly secure • Mobile • Support multiple security applications • Evident personal benefit to users 	<ul style="list-style-type: none"> • User software installation required
One-time password tokens	<ul style="list-style-type: none"> • Mobile • Easy to understand • No user software installation required 	<ul style="list-style-type: none"> • Limited solutions supported • Authentication server required • Limited lifetime – battery operated
Hybrid tokens	<ul style="list-style-type: none"> • Mobile • Support multiple security applications • No user software installation required for OTP functionality • Evident personal benefit to users 	<ul style="list-style-type: none"> • Limited lifetime (unless battery replacement option is available)
Software tokens	<ul style="list-style-type: none"> • No separate hardware device required 	<ul style="list-style-type: none"> • Token key is not secure • Limited solutions supported • Authentication server required

Strong Authentication Solutions Are Evolving

As market sophistication and experience with strong authentication increases, authentication solutions are evolving to meet market demands. Organizations are looking for broad, open solutions that enable them to incorporate many capabilities using a single system. At the same time, they are looking for solutions that are easy to implement and use, to ensure user acceptance and maximize return on their investment. The following are some recent trends in strong authentication:

Comprehensive Integrated Solutions

To make the authentication solution more efficient and effective, organizations are looking for a full solution in one system, rather than implementing and combining multiple systems. They seek integrated solutions that provide a mix of authentication devices, applications, and management tools to meet their current and perceived future needs that fit well into their existing IT infrastructures.



Full, integrated strong authentication solutions are increasingly offered, providing enhanced security solution support and linkage with external systems.

In response, managed service providers and authentication solution vendors are increasingly offering full integrated solutions that they offer their customers: A range of devices – enabling them to implement a mix based on the needs and requirements for different users; A breadth of security applications – enabling extensive solution support in one system; Comprehensive smart card and token management systems – enabling enhanced management capabilities and linkage with multiple security applications as well as, identity and access management systems.

More Value from a Single Device

To gain maximum benefit from their investment and increase user acceptance, organizations are increasingly seeking solutions that offer multiple capabilities combined in a single device.

In response, vendors are introducing more sophisticated authentication devices that are being combine capabilities in one unit. For example, hybrid USB and OTP tokens provide the flexibility to use different authentication methods based on user needs, while furnishing all of the benefits of USB tokens. Tokens with combined encrypted Flash memory enhance the token's functionality by providing mobile data storage together with authentication, and have the additional ability to store the device drivers on-board.

In addition, security vendors are increasingly creating applications that integrate with strong authentication. For instance, many of the leading PC security vendors now provide the option to increase the security of their products by requiring users to connect tokens to their machines to gain access.

Combined Physical and Logical Access

Organizations in all segments and secure access solution providers are realizing the great functionality and cost benefits of combining physical and logical access security. Consequently, authentication solutions increasingly integrate with physical access solutions by incorporating elements such as ID badges and RFID coils on the authentication device itself - with management systems that support the integrated solution.

With combined physical and logical access systems, administrators can become more efficient, managing their organization's entire secure access solution from one place. At the same time, users no longer need to carry multiple devices – their one token enables them to enter their office building, go into their office, log on to the network, and access their business data and applications.

Authentication devices are increasingly integrated with physical access elements, enabling users to enter the building and log on to the network with a single device.

Emerging Solutions

Two authentication solutions that are expected to gain significant ground in the next few years are biometrics and federated identity. These can be combined with existing authentication token solutions to offer enhanced security, functionality, and usability.

Biometrics

Biometric authentication is based on examining a biological characteristic of the human body to determine identity. This rising technology offers significant appeal because it is user-friendly and measures an intrinsic feature of the person being authenticated – the user always carries his access identifier with him and cannot lose or forget it. Though widespread acceptance of biometrics is still hindered by technology development, reliability, and cost issues, this market is expected to grow rapidly in the next few years as these issues are overcome and new innovative, reliable, and practical technologies emerge.

Developments in biometrics such as match-on-card technology, which enables users to carry their biometric templates and perform biometric authentication on-board a smart card, USB token, or other secure portable storage device, provide an appealing combination of security and mobility while alleviating user privacy concerns.

Federated Identity

Federated identity enables users to authenticate once and gain access to a number of entities within an established trusted environment. Federated identity systems go beyond the single sign-on concept – enabling users to authenticate once and access all applications within one organization – to allow access to a network of trusted entities. This enables, for example, a patient to obtain medical records from multiple health care providers with a single logon.

Federated identity solutions open opportunities for more automated and convenient e-business transactions. As standards for communication between federated identities, such as the Security Assertion Markup Language (SAML), are increasingly developed and accepted, organizations will increasingly build more alliances with their business counterparts and adopt federated identity.

Authentication tokens can act as a platform for federated identity solutions and provide added value by securely storing authentication credentials for multiple trusted entities in a single device. Users need only authenticate once to gain access to all federated organizations, while the organizations involved benefit from the added security of strong authentication.

Practical Considerations for Selecting a Strong Authentication Solution

With the plethora of strong authentication offerings available today, it is important for organizations to carefully evaluate the available solutions before making a decision on which solution to implement. When choosing a strong authentication solution, organizations should take a number of factors into account. The following are some of the key elements to consider:

Solution Coverage

When investing in a strong authentication solution, organizations should carefully examine their current and future needs, and select the solution that best answers those needs. The following are some questions to consider:

- *Do I want to protect my internal network from unauthorized access?*
If so, consider strong authentication solutions that enable flexible and comprehensive secure network access, both in the office and remotely if needed.
- *Do my users need to connect from remote locations? Do my employees travel frequently?*
If so, consider portable solutions that enable secure VPN and web access for remote users, and that enable employees to secure their laptops and data while on the road.

- *Do my users need to access many password-protected applications?*
If so, consider solutions that provide single sign-on functionality, either by storing user credentials on the token or by integrating with external single sign-on systems.
- *Do I want my users to digitally sign and encrypt sensitive data or transactions?*
If so, consider smart-card-based solutions that provide secure on-board PKI key generation and cryptographic operations, as well as mobility for users.
- *How sensitive is my business data?*
The more sensitive the data, the higher the priority on the robustness and security of the solution.
- *Do I want to firmly protect data that sits on my users' PCs and laptops?*
If so, consider token solutions that integrate with PC security products such as boot protection and disk encryption applications that require the use of a token to boot a computer or decrypt protected data.
- *Have I or do I want to implement a secure physical access solution?*
If so, consider token solutions that enable integration with physical access systems.

Usability

Users will be willing to adopt a strong authentication solution that is easy to learn and user friendly. Installation, updates, and similar processes should be easy and intuitive for both users and administrators. In addition, solutions that offer automated processes for resetting token passwords, handling lost or damaged tokens, and other token management tasks are likely to have increased acceptance.

Openness

A strong authentication solution based on an open architecture gives organizations the flexibility to integrate the solution with multiple third-party vendor products or customized applications. Offerings that include (SDKs), and a large set of solution partners that integrate the strong authentication offering into their products, provide increased opportunities for extending support for the solution.

Flexibility

A flexible strong authentication solution provides many benefits, enabling every organization to modify the solution based on its existing and evolving needs. Strong authentication vendors that offer a range of devices that operate with the same set of security application, provide considerable cost savings and flexibility. Organizations can deploy any mix of devices for their users and change that mix over time as desired.

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

☑ **Manageability**

A comprehensive management system can significantly reduce the challenge of implementing a strong authentication solution by enabling enterprise-wide deployment and life-cycle management of the entire solution, including the full inventory of authentication devices and their associated security applications. Token and card management systems provide automated tools and procedures that not only significantly reduce the load on the IT department, but also minimize errors. User self-service management tools further simplify the management of the solution and reduce the workload on the administrators. Therefore, when evaluating a strong authentication solution, the availability and extent of management capabilities offered as part of the solution should be seriously considered.

☑ **Cost**

Strong authentication solutions vary in cost and offerings. It is important to choose a solution that provides the needed capabilities and falls within budget. Organizations should take into account the overall long-term cost of the solution, including initial investment costs, recurring fees, token replacement costs, and the costs involved in extending the solution as needed in the future.

The eToken Solution

Aladdin, recognizing the need for organizations to establish enterprise-wide strong authentication and password management solutions, has developed the eToken offering to meet all of an organization's authentication needs.

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 that include secure network and web access, laptop and PC protection, e-mail encryption, single sign-on, and much more. 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.

eToken enables organizations to deploy a mix of devices for users based on their specific security needs. Highlighting the Aladdin eToken line of devices are eToken PRO, a hybrid USB and OTP token, eToken NG-OTP, and a token with encrypted 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 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 wide, integrated range of authentication devices and applications, providing organizations with the flexibility to meet their evolving needs.



The Aladdin eToken devices run on the Java card operating system, which enables multiple applications to be deployed on a single smart card, and new ones to be added even after the token has been issued to the end user. Java card technology also makes it easy to integrate security tokens into a complete Java software solution.

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 institutions' 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 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 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.

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.

Aladdin's Token Management System enables full deployment and life-cycle management of 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 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