

White Paper



***Strong Authentication:
Critical Enabler for Security and
Identity Management in Higher
Education Institutions***



Table of Contents

Introduction	3
Authentication: A Key Component of Identity Management.....	4
Passwords are No Longer Sufficient for User Authentication	5
Strong Authentication Options	5
Key Drivers of Strong Authentication in Higher Education	7
Strong Authentication Trends in Higher Education.....	8
What to Look for in a Strong Authentication Solution	10
The eToken Solution.....	12
Case Study #1: Dartmouth College a Leader in PKI and Strong Authentication	14
Case Study # 2: eToken Goes the Distance for FernUniversität Hagen in Germany.....	15
Case Study # 3: University of Wisconsin Gets Mac Support.....	15
Case Study # 4: Rice University Secures IT Administration	16
Case Study #5: University of Texas Health Science Center Manages Mandates	17
Conclusion	17
References	18
About Aladdin	18

Strong Authentication: Critical Enabler for Security and Identity Management in Higher Education Institutions

Introduction

A recent study conducted by the EDUCAUSE Center for Applied Research (ECAR) surveyed higher education institutions to determine their top IT issues related to their strategic success. Among all sizes and all types of higher education institutions, security and identity management (IdM) were consistently named in the top two or three most important issues. In fact, ECAR's Current Issues Survey of 2005 named security and identity management (IdM) as the issue most likely to become "much more significant" in the future. (1)

Given the need for greater access to online resources, the expanded number of government and policy mandates, increases in the sophistication of threats, and the demands of diverse audiences and stakeholders, it's not surprising that institutions of higher education are seeing strong user authentication and password management solutions as a critical enabler of their identity management strategies. They are seeking solutions to help their institutions:

Comply with expanded mandates and regulations – Much of the emphasis on identity management stems from specific mandates such as the Family Educational Rights and Privacy Act (FERPA), a U.S. federal law designed to protect the privacy and accuracy of student records. Also in the U.S., the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and transfer of health information, including universities and health research facilities. In Europe, several European Commission (EC) Directives, such as Directive 95/46/EC provide rules for protecting data and privacy.

Enhance the productivity of faculty, students and staff – Providing users with widespread and mobile access to necessary data and applications in the classroom, at home, or on the road, is rapidly becoming a necessity among colleges and universities worldwide. Not only does identity management with strong authentication facilitate and improve secure communication among individuals, institutions and research partners, it can also significantly reduce the time spent on password administration and maintenance by both users and IT help desk personnel.

"Our ongoing commitment to protect students' personal information, now reinforced by FERPA requirements, compels us and other schools to protect our online systems as much as possible while still simplifying access for students and staff. Two-factor authentication is proving to be a cost-effective way to accomplish this and strikes a healthy balance between enhanced security and ease-of-use."

– Mark Franklin, PKI Lab Project Manager, Dartmouth College

Protect users from increasing threats to personal data – The number of security incidents, whereby personal data on students, faculty and staff has been compromised has increased dramatically in the past few years. A 2005 Gartner/Chronicle of Higher Education Global Survey, for example, indicated that stolen laptop computers represented a growing data security risk for higher education. In the first nine weeks of 2006, 13 universities in the U.S. reported data losses, and five of the 13 cases involved mobile computers or laptops. (2)

Meet the growing demands of diverse stakeholders – Relationships with business, pharmaceutical and medical research, and government agencies, indicates that higher education institutions must increasingly provide security and privacy assurances when users interact with these organizations online. In many cases, universities that expect to conduct research and “do business” with outside organizations have to meet minimum authentication standards in order to gain access to digital resources.

Experts generally acknowledge that for higher education institutions to protect users and deliver services with adequate security and privacy, they must develop more sophisticated means of identity management – including stronger authentication methods.

Authentication: A Key Component of Identity Management

The process of identity management in higher education typically involves four key functions:

Establishing Identity – the process of associating a physical person with verified identity information prior to the issuance of digital identifiers and the creation of a user account. This would be your name or network/system identifier. Traditionally, U.S. higher education institutions have used social security numbers for identification, but for the obvious reasons of identity theft and security, most are moving away from this approach.

Authentication – the process of gaining confidence that the person using a digital identity is the person who is qualified to use it. This provides proof that you are who you say you are. In most cases, higher education institutions still rely on passwords alone, or what is known as “single-factor” authentication.

Authorization – the process of determining a specific person’s eligibility to gain access to an application or function or to use a resource. This tells what resources you have permission to access.

Enterprise Directory – a central institution lookup repository that holds data regarding the institution’s people and services, informing authentication and authorization processes. This provides information about you and what you are allowed to do.

While the ability to authenticate, authorize and provision user access rights in a unified and consistent manner may be logically understood, the actual implementation in a higher education setting (or in any industry) is far more complex and difficult to achieve. (3)

Passwords are No Longer Sufficient for User Authentication

Passwords have long been regarded as inexpensive, easy to use and secure. Through many decades of use and technological developments, passwords are still the most popular form of authentication in higher education institutions. However, there are several reasons why educational institutions – especially those leading in the implementation of identity management systems – are recognizing that passwords alone are insufficient for proper authentication of users.

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 risk.

Passwords are costly – Every forgotten or lost password results in significant costs. A recent Burton Group report estimates that each call to the IT help desk costs between \$25 and \$50, and typically 35% to 50% of help desk calls in an organization are password related. (4) The cost is even greater when taking into consideration lost faculty, staff and even student productivity.

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. Adding to these security risks the abundance of available password cracking tools, it is easy to see that passwords are no longer a sufficient security measure.

In many cases, relying solely on passwords for authentication is not acceptable by government agencies or those organizations in private industry that have working relationships with universities. As it becomes more evident that passwords are not a sufficient method for authenticating users, higher education institutions are turning to stronger authentication solutions.

Strong Authentication Options

Strong authentication solutions enable higher education institutions 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: (5)

- 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 USB token or a smart card.
- Something you are – a biometric feature of the individual such as a fingerprint or facial characteristic.

Strong authentication methods typically involve a physical device, or token, used together with a password to prove the owner's identity – hence the “two-factor” label often applied in conjunction with strong authentication. A wide variety of strong authentication token technologies and form factors are available on the market, generally falling into the following categories:

“The typical user ID and password combination have never really been sufficient for authenticating access to IT assets. Only strong two-factor authentication gives the high level of assurance we need for our IT operations.”

**Barry Ribbeck, Director
of Systems Architecture
& Services, Rice
University, Houston,
Texas.**

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 card into a “reader” and enter a password. Smart cards provide highly secure storage of user credentials and keys and help secure PKI (Public Key Infrastructure) implementation by generating keys and performing cryptographic operations on-board, without exposing the user's private key to the computer environment.

While providing extensive functionality and high security, smart cards often lack the mobility of a USB token because the smart card requires a separate reader for every machine in which the smart card is to be used. Unlike the ubiquitous USB port, most computers do not have a built in smart card reader, so that organizations implementing a smart card must add the extra expense of installation and maintenance of readers.

Smart-card-based USB Tokens – Smart-card-based USB tokens, which contain a smart card chip inside, provide the greatest level of security, versatility, and mobility, leveraging the advantages of both USB tokens and smart cards. 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 USB and OTP tokens have recently been introduced, providing increased flexibility. These 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. Though software tokens may

add convenience to users, they are less secure than physical tokens. The secret key can easily be stolen or misused.

Key Drivers of Strong Authentication in Higher Education

For institutions that need to reduce security vulnerabilities, assure secure access to digital resources, comply with regulations mandating data privacy and protection, and provide multiple levels of authorized user access, a strong and robust authentication system provides several benefits.

Comply with Policies and Regulations and Improve Security

A growing number of rules and regulations across the globe hold higher education institutions responsible for the integrity of their data and for the protection of personal information that has been entrusted to them by students, faculty and staff. To comply, institutions at the forefront of implementing identity management solutions have recognized that strong authentication constitutes a basis for compliance with many of these regulations.

The U.S. Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Federal Drug and Alcohol Patient Records Confidentiality Law (42 CFR), mandate higher education institutions in the U.S. protect their data and meet IT security standards. In addition, HIPAA regulations in the U.S. require educational institutions with health care research and provisioning facilities to securely authenticate individuals before granting them access to sensitive patient data. Strong authentication enhances compliance by enabling secure user access and providing a proven and demonstrative method for protecting internal data and networks.

Increase Faculty, Staff and Student Access and Productivity

Providing users with widespread access to necessary data and applications in the classroom, at home, or on the road, improves communication among faculty, staff and students, and increases productivity overall. Strong authentication enables educational institutions to offer online access to services, such as library resources, personal student records, networks and portals, online forums and communities, that would incur substantial risk or not be practical at all without reliable user authentication.

Thus strong authentication provides access to network resources anytime and from almost anywhere, without sacrificing security. Strong authentication solutions also increase productivity by significantly reducing the time spent on password administration and maintenance by both users and IT help desk personnel.

Improve Efficiency and Reduce Costs

Strong authentication enables higher education institutions to provide increased services online that enhance efficiency and thereby save significant costs in their ongoing education and research activities. Strong authentication solutions provide the needed security, for example, to enable university

“Two-factor authentication for key administrative applications and single sign-on authentication for just about everything is becoming the norm. Federating authentication and PKI are just around the corner.”

– Doug Gale, “Security: Trend Report: Identity Management,” Campus Technology Magazine

professors to allow their students to securely submit examinations and view their grades electronically. They also provide the needed security to protect access via open, wireless networks on campuses by providing different levels of credentialing to distinguish the casual visitor from the dedicated researcher.

When implementing strong authentication with single sign-on capabilities, higher education institutions can also reduce the ongoing costs associated with password administration, as users no longer need to manage and remember multiple passwords. For example, USB 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.

Enable Secure Collaboration and Email Communications

By implementing strong authentication solutions, higher education institutions enable their students, faculty and staff to gain access to data from a variety of sources that require more rigorous levels of assurance and credentials. For example, the U.S. federal government's E-Authentication initiative now requires multi-factor authentication for defined levels of assurance when accessing information from government agencies. University centers of medical and health education working with pharmaceutical companies on research projects must also meet two-factor authentication standards based on U.S. Federal Drug Administration 21 CFR Part 11 regulations.

In addition, strong authentication via a USB token enables PKI-based digital signing of emails to ensure the integrity of any content from a sender, and to verify for the recipient that the sender of the email is who he or she claims to be. Strong authentication through a USB token also allows the sender to encrypt email and assures only the specific recipient will be able to decrypt and read the message.

Prevent Security Breaches, Preserve Reputation

Strengthening security through strong authentication saves significant costs and preserves the reputation of the institution by preventing potential security breaches. This includes misuse of data and networks by insiders, lost data from stolen laptops, and other security attacks from student hackers. With strong authentication it is possible to block unauthorized usage and to hold authorized individuals accountable for their usage of the institution's digital resources, thereby providing a powerful incentive, especially among students, to reduce accidental breaches or deliberate harmful behavior.

Strong Authentication Trends in Higher Education

As experience with strong authentication increases among higher education institutions, two-factor authentication solutions are evolving to become more practical and cost-effective. Higher education institutions are showing a preference for open solutions that enable them to incorporate many capabilities and support varied environments using a single system. At the same time, they are implementing two-factor authentication solutions that are easy to use, ensur-

ing acceptance by a diverse set of users, and maximizing the return on their investment. Following are some of the recent trends in strong authentication among higher education institutions.

Cross-Platform, Integrated Solutions

To make a strong authentication solution more efficient and effective, leading universities and other institutions of higher education are looking for a complete solution that encompasses many platforms in a heterogeneous IT environment, rather than implementing and combining multiple separate systems. They seek integrated solutions that provide a mix of authentication devices, applications, and management tools to meet their current and perceived future needs, and that fit into their existing, complex IT infrastructures.

In many cases, these institutions have instituted a PKI, or Public Key Infrastructure. PKI is a framework that allows secure data access and digital communications through the use of public and private cryptographic key pairs, obtained from a trusted authority and unique to each user or system. Various entities, including the Higher Education Bridge Certification Authority (HEBCA) in the U.S. and the German Research Network in Germany, facilitate and promote the use of PKI-based security in higher education facilities. Institutions adopting PKI are increasingly implementing authentication token solutions, namely smart-card-based USB tokens, which provide security, simplicity, and usability to PKI solutions by generating users' keys and storing them on-board the token.

Maximum Value from a Single Authentication Device

To gain maximum benefit from their investment and increase user acceptance, higher education institutions are increasingly seeking authentication solutions that offer multiple combined capabilities in a single device. In response, more sophisticated authentication devices are being introduced, providing combined capabilities in one unit. For example, hybrid USB tokens now provide the flexibility to use different authentication methods based on user needs, while providing all of the functionality benefits of USB tokens. Tokens with combined flash memory enhance the token's functionality by providing mobile data storage together with strong authentication, and have the additional ability to store the device drivers and other value-added applications on the token – potentially obviating the need for laptops.

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.

Federated Identity Capability

Federated identity enables users to be identified between institutions without the need for individual credentials being issued from each institution. New assertion based technology standards such as SAML are being used in federating applications like Internet 2 Shibboleth that can leverage any type of authentication, including PKI to provide strong authentication across insti-

“The focus on Identity Management and authentication has a long history among certain institutions in higher education as opposed to the private sector for a very good reason – no private company is faced with the massive turnover in users that every university must manage at least once a year.”

– Barry Ribbeck, Director of Systems Architecture & Services, Rice University, Houston, Texas.

“We are seeing a significant change in the mindset of higher education administrators and IT managers. It is a focus on developing reliable credentials for individuals rather than simply relying on a password.”

**Dr. William Weems,
Assistant Vice President
for Academic Technology,
and Associate Dean for
IT at the Medical School,
University of Texas
Health Science Center.**

tutional boundaries to Web based resources as well as providing Web initial sign on (Web ISO) capabilities.

In the U.S., the Higher Education Bridge Certification Authority (HEBCA) has been formed to facilitate trusted electronic communications within and between higher education institutions as well as with federal and state government agencies, and commercial enterprises. By working with the Federal Public Key Infrastructure (PKI) Steering Committee and the National Institutes of Health (NIH), EDUCAUSE and the HEBCA Board of Instantiation and Development (BID) began design for a PKI bridge for US higher education, modeled on the Federal Bridge Certification Authority (FBCA) to prove the model of bridge-to-bridge interoperations. After proving the technology, EDUCAUSE funded the creation of a production HEBCA at Dartmouth College's PKI Lab facility. This bridge will allow users at higher education institutions to share trusted electronic credentials necessary for a broad range of applications in education, research, and administration.

USB tokens can facilitate federated access by serving as a platform for federated identity solutions and providing 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.

What to Look for in a Strong Authentication Solution

With the plethora of strong authentication offerings available today, it is important for higher education institutions to carefully evaluate the available solutions before making a decision on which solution to implement. The following list reviews the most important features that should be considered when adopting a strong authentication solution.

☑ *Solution Coverage*

When investing in a strong authentication solution, educational institutions should carefully examine their access security needs, and select the solution that best answers those needs. Following are some of the questions that should be considered:

- *Who are your target users?*
Undergraduate students, lab assistants, IT administrators, distance learning instructors, and tenured professors each engage in different academic activities and therefore need access to different digital resources. Consider strong authentication solutions that support your users' varied needs.
- *Which operating systems do your users use?*
Strong authentication solutions that work with various computer operating systems, including Windows, Linux, and Macintosh, provide greater capabilities for enhanced security in diverse user environments.
- *Do your users need to connect from remote locations?*
If so, consider portable solutions that enable secure VPN and web access for remote users.

- *Are you implementing a PKI for certificate-based authentication, digital signing of data and online transactions, data encryption, or other uses?*
If so, consider smart-card-based solutions that provide secure on-board PKI key generation and cryptographic operations, as well as mobility for users.
- *Do your users need to access many password-protected resources, such as software applications and library databases licensed to your institution?*
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.
- *Would you like to firmly protect data that sits on your users' PCs and laptops?*
If so, consider token solutions that integrate with PC security products such as boot protection and disk encryption applications, requiring the use of a token to boot a computer or decrypt protected data.
- *Have you or do you want to implement a secure physical access solution?*
If so, consider token solutions that enable integration with physical access systems.

Beyond supporting diverse current needs, strong authentication offerings that provide broad solution coverage also allow colleges, universities, and other education facilities the flexibility to expand their implementations to meet future needs using the same platform.

Usability

A strong authentication solution that is simple to use will more willingly and effectively be adopted. Installation, updates, and similar processes should be made easy and intuitive for both users and administrators. Easy-to-learn and user-friendly applications will more likely be adopted and used on a day-to-day basis. 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 educational institutions 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 solution support.

Flexibility

A flexible strong authentication solution provides many benefits, enabling every institution to modify the solution based on its existing and evolving needs. Strong authentication vendors that offer a range of devices which operate with the same set of security applications, provide a great deal of cost

savings and flexibility. Higher education institutions can deploy any mix of devices for their users and change that mix over time as desired.

☑ **Manageability**

A comprehensive management system can significantly reduce the challenge of implementing a strong authentication solution by enabling institution-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 IT departments, 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 offering. It is important to choose a solution that provides the needed capabilities and falls within budget. Educational institutions 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 higher education institutions to establish strong authentication and password management solutions in varied user environments, offers the eToken product suite to satisfy institutions' authentication needs. Comprised of a wide range of smart-card-based devices, security applications and third-party integrated solutions with over 150 partners, eToken offers colleges and universities the ability to rapidly implement a full suite of security solutions including secure network and web access, laptop and PC protection, e-mail encryption, single sign-on, and much more. Alternatively, higher education institutions 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 Provides High Security with Mobility and Convenience

eToken offers a range of smart-card-based authentication devices to meet varying user requirements. 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. These key-sized tokens are highly portable and easy to use, simply plugging into a USB port. eToken devices enable on-board generation and secure storage of keys, passwords and certificates for digital signing and encryption, seamlessly integrating with PKI architectures.

"In eToken, we found a solution that could easily be integrated into our PKI. While providing the same level of performance, use of eToken on several systems was more practical, flexible, and cost-effective than a conventional smart card in which the reader had to be moved from system to system or several card readers had to be purchased."

**– Henning Mohren,
Project Manager,
FernUniversität Hagen**

eToken offers a full suite of strong user authentication and password management applications, all operable with the complete family of eToken devices. eToken supports Windows, Linux and Macintosh and enables secure certificate-based network access in those platforms, allowing for broad usage in diverse academic environments. With an open architecture and an SDK for integrating eToken into external applications, eToken also gives institutions the flexibility to easily develop support for additional solutions.

Because eToken offers a variety of authentication devices that all operate with the full range of eToken security applications, higher education institutions have the flexibility to deploy any mix of devices for users based on their specific security needs, providing both enhanced functionality and significant cost savings.

For example, users who generally need secure access to academic resources only on campus can use eToken PRO, while users who also need remote network access – such as professors who travel frequently – can use eToken NG-OTP for one-time password authentication from any computer. For users who can benefit from mass data storage capabilities on-board the token, eToken NG-FLASH is available in multiple memory sizes. eToken NG-FLASH can be initialized with a read-only partition for storing device drivers and applications, while the standard flash partition can be used for storing academic work. Educational institutions may choose to provide their students with eToken NG-FLASH instead of laptops, significantly reducing costs.

eToken Delivers Comprehensive Token Life-cycle Management Capabilities

To answer the higher education institutions' needs for campus-wide 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, or alternatively administrators can enroll devices for users using TMS tools. TMS integrates directly with an institution'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, educational institutions of all types and sizes can enable enhanced user connectivity and increase productivity with secure access anytime, anywhere. Higher education facilities 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,

“We’re trying to evolve beyond usernames and passwords for enhanced security and usability. eToken is a robust solution that provides us with a secure way of storing our PKI credentials. It also minimizes the hassle of managing multiple passwords by storing many passwords directly on the key itself and only requiring the one eToken password.”

– Mark Franklin, PKI Lab Project Manager, Dartmouth College

eToken provides the solution for educational institutions’ current and evolving needs.

Case Study #1: Dartmouth College a Leader in PKI and Strong Authentication

Dartmouth College, an American Ivy League institution in Hanover, New Hampshire, has been one of the “early adopters” of PKI technology among higher education institutions – including two-factor authentication using eToken. eToken stores the digital certificates for the PKI system of credentialing students, faculty and staff, enabling the user to access online resources with only a single eToken password.

The college has issued eTokens for the past two years to all incoming freshman, and is planning to issue tokens for all undergraduates and graduate students within the next two years, as well as to all faculty, staff and even alumni. With complete rollout, Dartmouth will have more than 10,000 eTokens in use by 2008, according to Scott Rea, senior PKI architect for Dartmouth College and Director of the HEBCA Operating Authority.

“Much of the impetus for strong authentication has been driven by legislative mandates such as FERPA and HIPAA,” Rea said, “but we also have a very open (in terms of access), wireless network on campus, which means we have to be sure that we can still protect information assets. Passwords alone are simply not secure enough for assuring proper access.”

eToken Mobility, Convenience a Prime Advantage

“We have multiple levels of credentials for access,” Rea explained, “and the convenience and mobility that eTokens give us made them a logical choice for us. We need to have an infrastructure we can trust,” he said, “and eToken has become a key enabler for the two-factor authentication our PKI system requires. eToken now works with Macs as well as PCs – a big advantage when a third of our student body uses Apple computers.”

Rea recalled that Dartmouth had also considered smart cards as a strong authentication and password management device but selected eToken USB devices instead for their flexibility and ease of use. Because smart cards require readers, there would have been additional cost and maintenance compared to the ubiquitous USB ports available on nearly all computers.

As a pioneer in the implementation of PKI and strong authentication, Dartmouth’s PKI Lab Outreach program promotes the benefits of PKI to other institutions of higher education, and the HEBCA (also based at Dartmouth) provides the infrastructure for an inter-institutional trust fabric. “PKI can seem very intimidating to colleges and universities,” Rea said, “but the technology is getting less complex and more affordable, and the benefits of PKI are beginning to be realized on campuses. The real question is: What is the risk of not properly securing our network assets?”

Case Study # 2: eToken Goes the Distance for FernUniversität Hagen in Germany

Offering online studies through the Distance Learning section of FernUniversität Hagen helped to spur innovative leadership in PKI solutions at the German university through a project that began nearly ten years ago. The PKI project has evolved since then to provide web-supported certification services that are simple to use, an automated certification routine that issues digital certificates to students and employees for authentication, and the option of more secure access enabled through a strong authentication token device.

By choosing eToken from Aladdin to deliver its strong authentication, FernUniversität Hagen gained two important advantages in terms of security, ease of use, and cost according to Henning Mohren, who is in charge of the Certification Authority at the university. With user certificates safely stored on eToken, they provide secure access to online resources and cannot be misused once the eToken is removed from the USB port. Just as important, Mohren noted, is that eToken is easy to use, works with any computer regardless of student location, and enables student self-service eToken password reset if necessary. The eToken is also less costly than a smart card alternative.

“In eToken, we found a solution that could easily be integrated into our PKI system,” Mohren explained. “While providing the same level of performance, use of eToken on several systems was more practical, flexible, and cost-effective than a conventional smart card in which the reader had to be moved from system to system or several card readers had to be purchased.”

Given its extensive experience in PKI as an exclusively “distance learning” institution, FernUniversität Hagen now provides an identity management model that traditional German and European universities can take advantage of when offering online access to their own students and staff. Mohren estimates that more than ten universities now use some form of PKI implementation based on FernUniversität Hagen’s certificate management system, as well as using eToken for strong authentication. In fact, he noted, the University of Applied Science in Bochum, Germany is currently starting to issue eTokens as part of its identity management for all 5,000 of its students.

Mohren emphasized that eToken’s delivery of strong two-factor authentication has recently provided added assurance to auditors at the university seeking to verify compliance with the European Union’s strict data protection regulations. He also cited the extra advantage that eToken provides in securing email communications through email sender verification, encryption, and digital signatures.

Case Study # 3: University of Wisconsin Gets Mac Support

Nearly six years ago, the University of Wisconsin-Madison got a six-figure grant to explore the use of PKI in higher education. The main drivers behind the initiative were the growing availability of applications online via the Internet, and an increase in regulatory mandates that required privacy and data protection, according to Nick Davis, PKI Project Manager at the university.

“With regulations such as FERPA and HIPAA,” Davis pointed out, “sensitive

“We have been using the eToken system at FernUniversität Hagen for several years now and are totally convinced of the quality and practicability of this authentication solution.”

**– Henning Mohren,
Project Manager,
FernUniversität Hagen**

“We chose eToken from Aladdin because it had already proven itself in places such as Dartmouth College, and because it’s the only hardware token that provides Macintosh support.”

– Nick Davis, PKI Project Manager, University of Wisconsin

information has to be protected with more than just a password. We’ve been implementing strong authentication on a volunteer basis for more than two years, and have made strong authentication using eToken a key part of our digital certificate strategy.”

“Everyone has a USB port on their computer or access to one,” he explained, “and everyone is used to having a set of keys so a token is easy to use and carry around.”

“We chose eToken from Aladdin,” Davis continued, “because it had already proven itself in places such as Dartmouth College, and because it’s the only hardware token that provides Macintosh support.” With more than 20 percent of students and staff at the university relying on Macintosh computers, he said, Aladdin has been “more than responsive” to requests that eToken become fully compliant with the platform.

Davis said one of the ultimate goals of the PKI project is to consolidate authentication methods for students, faculty and staff through a convenient, mobile solution such as the form factor of a USB token. In addition to strong authentication to a variety of applications, Davis sees email encryption, sender verification and digital signatures as key benefits to be gained from a USB token.

“The need for strong authentication in the higher education environment will only get greater as more and more applications become available online,” he concluded.

Case Study # 4: Rice University Secures IT Administration

As one of the leading U.S. teaching and research institutions, Rice University in Houston, Texas recognized early on the need for strong authentication to help protect its IT systems according to Barry Ribbeck, Director of Systems Architecture & Services.

“We realized that in an Active Directory environment,” Ribbeck said, “it was essential that we protect access by IT administrators with more than an ID and a password. That means implementing strong authentication for administrator access to AD domains.”

Rice University’s IT department had been relying on older technology to authenticate users but Ribbeck cited the high costs, single use and a limited life to the authentication device as important reasons for switching to eToken.

“Your security is only as good as the ability to identify who is accessing your systems,” Ribbeck noted, “and eToken provides the technology and flexibility we need from a token for strong authentication plus added benefits of S/MIME and document signing.”

Ribbeck explained that users gain added security from using digital certificates with eToken to assure the privacy of email communications (only the intended recipient can read the message) and authentication (the recipient can be assured of the identity of the sender). Certificates can also be used for verifying digital signatures to documents.

“We agree with our IT security staff that recommends the use of strong authentication with eToken to as many users as they think appropriate,” Ribbeck said. “It makes sense to use strong authentication as a means to protect the reputation and prestige of our institution.”

Case Study #5: University of Texas Health Science Center Manages Mandates

Like many of its fellow pioneering institutions of higher education, the University of Texas has been evaluating and exploring identity management and PKI solutions for nearly a decade. In 1998, for example, the university signed a master service agreement with a commercial digital certificate authority and has been developing its PKI infrastructure ever since.

Within the past two years, the Health Science Center based in Houston has been evaluating strong authentication in the form of smart cards and USB tokens, according to Dr. William Weems, Assistant Vice President for Academic Technology, and Associate Dean for IT at the Medical School.

The main drivers of digital certificates and strong authentication for a health-care institution, Weems explained, are mandates and regulations such as FERPA, HIPAA and collaborative research projects with private industry and the federal government. He noted that the U.S. federal government e-Authentication initiative defines two-factor authentication as one its highest levels of assurance. “In some cases,” Weems said, “strong authentication that goes beyond the user name and password helps in grant applications for federal funding of medical research as well as research conducted with pharmaceutical companies. The risk reduction offered by strong authentication can make a difference.”

eToken from Aladdin was chosen as the delivery format of choice by the Health Science Center because of its convenience, cost and compatibility with multiple systems according to Weems. Evaluating both smart cards and USB token form factors, Weems found that the USB token costs less when considering the additional expense of smart card readers. eToken provides complete mobility and ease of use for strong authentication, along with added benefits such as email encryption and digital signature integrity.

Weems looks forward to the day when a single identifier can be linked to an individual through a credentialing authority. With emerging standards in PKI and Identity Management, he expects a system of federating agreements will enable a simpler and more secure method for accessing multiple applications and resources. “While PKI technology has been around for quite a while,” Weems said, “the policies and procedures necessary to conduct federated identity management based on strong authentication are gradually falling into place.”

Conclusion

The ECAR study of higher education key findings noted in its survey conclusion: “Though the agendas of our respondents were crowded with [IdM] activity, it would be more accurate to say that we found most of them standing at the threshold of identity management rather than practicing it.” (1)

But as one expert in *Campus Technology* magazine noted in a trend report focusing on Identity Management, “The general trend is from weak to strong authentication. Two-factor authentication for key administrative applications and single sign-on authentication for just about everything is becoming the norm. Federating authentication and PKI are just around the corner.” (3)

As institutions of higher education throughout the world continue to extend online services to their faculty, students and staff, strong authentication will increase in importance as a key enabler of secure yet mobile access. By delivering a cost-effective, flexible solution for strong authentication and password management, Aladdin’s eToken continues to expand its value in providing secure network access (including VPN access) and data security including secure e-mail, PC and laptop security, and digital signatures. With eToken, institutions of higher education can utilize strong authentication to help increase user productivity, comply with policies and regulations, and reduce administrative costs through a product offering that answers their current and evolving needs.

References

- (1) “Identity Management in Higher Education: A Baseline Study, Key Findings,” Ronald Yanosky with Gail Salaway, EDUCAUSE Center for Applied Research, April 2006.
- (2) 2005 Gartner/Chronicle of Higher Education global survey on security
- (3) “Security: Trend Report: Identity Management,” Doug Gale, www.campus-technology.com
- (4) “Enterprise Single Sign-On: Access Gateway to Applications,” Phil Schacter, Burton Group Report, 22 September 2005.
- (5) “Security: It’s Not All About Hackers,” Doug Gale, *Campus Technology* magazines, September 2005.

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	T: 1-800-562-2543, 1-847-818-3800	F: 1-847-818-3810
International	T: +972-3-636-2222	F: +972-3-537-5796
UK	T: +44-1753-622-266	F: +44-1753-622-262
Germany	T: +49-89-89-4221-0	F: +49-89-89-4221-40
Benelux	T: +31-30-688-0800	F: +31-30-688-0700
France	T: +33-1-41-37-70-30	F: +33-1-41-37-70-39
Spain	T: +34-91-375-99-00	F: +34-91-754-26-71
Israel	T: +972-3-636-2222	F: +972-3-537-5796
Asia Pacific	T: +852-2166-8605	F: +852-2166-8999
Japan	T: +81-426-607-191	F: +81-426-607-194



0 7 3 9 5