

# Two-Factor Authentication Solution for the Entire Campus

Moving away from complex passwords while maintaining security throughout the user life cycle.



## THE PROBLEM: Static passwords do not provide security

Static passwords used by students, faculty, staff, and vendors are the weakest links in an educational institution's security infrastructure. These thousands of never changing passwords open up thousands of potential access points for online fraudsters.

## THE THREAT: Phishing, keyloggers, and viruses

Phishing, especially phishing targeted at specific groups (for example, university employees or students) can be very effective, tricking the recipients into disclosing their confidential information because they were made to believe it is being given to an authorized source. Keylogger viruses and simple password theft are also common, opening possibilities for confidential information misuse.

## THE CHALLENGE: A struggle with complex passwords

Never changing static passwords are too easy to compromise, while complex passwords, especially the ones required to be frequently changed, are difficult to remember and can be misused as easily.

## VASCO'S SOLUTION: Two-Factor Authentication at a fraction of the cost

VASCO's Two-Factor Authentication solution is based on proven One-Time Password technology that protects user login and ensures only authenticated users can gain access.

## HOW VASCO ADDRESSES THE CHALLENGES OF THE EDUCATIONAL COMMUNITY

**Your Challenge:** Often changing user population

**VASCO's Solution:** VASCO's fully-scalable solution can easily accommodate as few as ten and as many as tens of thousands of users.

**Your Challenge:** End-user groups with different risk profiles

**VASCO's Solution:** Customize the individual security level and authenticator type based on risk or application. Pick from hardware, software, and mobile authentication options.

**Your Challenge:** Budgetary concerns

**VASCO's Solution:** Recoup your investment year after year to ensure low total cost of ownership. VASCO's solution runs on single software backend platform and is capable of supporting thousands of authentication requests per second, with no need for additional servers.

**Your Challenge:** User acceptance

**VASCO's Solution:** DIGIPASS authenticators are easy to use and do not require additional training. Branding of hardware authenticators is another great way to increase user adoption and promote your school.





## SECURE ALL SYSTEMS FROM WITHIN

VASCO's solutions can be integrated in any language and on any platform:

- Single Sign-On solutions and authentication server technologies
- Open Source technologies, such as CAS, uPortal, CoSign
- Firewalls, access servers, and all RADIUS-based VPNs
- Assure initial authentication with federated solutions, such as Shibboleth
- Also supported by over 200 solution partners including Novell and Citrix

## SINGLE BACKEND PLATFORM

You can choose to secure your VPN access via RADIUS, your CAS login via a Java API call, and your web e-mail via our OWA filters – all on one backend platform, significantly reducing the complexity and cost of implementation. VASCO's backend platform is available in Middleware, Software Server, and API versions.

## BEST TOTAL COST OF OWNERSHIP

- No additional infrastructure required
- No need for separate authentication servers and replicas
- No need for separate authentication database

## SCALABILITY

- Easy to add more users and/or applications
- No need to rebuild the backend infrastructure

## PHASED ROLLOUT

VASCO's Two-Factor Authentication solution can be implemented in phases, since adding more users and applications is as simple as getting more licenses. No requirement to remove existing authentication solutions: simply phase them out as they expire.

## About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

## [www.vasco.com](http://www.vasco.com)

**BRUSSELS (Europe)**  
phone: +32.2.609.97.00  
email: [info-europe@vasco.com](mailto:info-europe@vasco.com)

**BOSTON (North America)**  
phone: +1.508.366.3400  
email: [info-usa@vasco.com](mailto:info-usa@vasco.com)

**SYDNEY (Pacific)**  
phone: +61.2.8061.3700  
email: [info-australia@vasco.com](mailto:info-australia@vasco.com)

**SINGAPORE (Asia)**  
phone: +65.6323.0906  
email: [info-asia@vasco.com](mailto:info-asia@vasco.com)

## WHERE TO USE

- Remote access via SSL-VPN
- Central Authentication Services
- Online portals and e-Learning systems
- Browser-based applications such as CWI
- ERP and CRM systems
- Online grading systems
- Enrollment management and student services
- Online billing, budgeting and planning

## MULTIPLE END-USER DEVICES

All form factors are supported in every installation.

- One-button hardware authenticators (tokens)
- Software-only authentication
- Mobile authentication
- SMS delivery
- USB authenticators
- Smart cards

## ADDITIONAL SERVICES

- **Branding** - Hardware authenticators can be customized with your school's colors and logo
- **Deployment** - Inventory management, packaging design and production, secure mailing to the end-users, and other services available on-demand

Ask your VASCO sales representative for a catalogue of customized branded products and packaging. Samples and industry references available upon request.