Secure Your Systems From Within:
VASCO Strong Authentication for CAS

Integrate two-factor authentication security into your CAS-based applications and online portals

HOW IT WORKS
VASCO’s Two-Factor Authentication augments insecure personal passwords with constantly changing passwords that cannot be reused at the next login.

VASCO’S TWO-FACTOR AUTHENTICATION FOR CAS
Thanks to the interoperability of VASCO’s backend solution, two-factor authentication security can be integrated into your CAS* environment in three different ways, depending on the school’s individual setup.

Choose an authentication handler method: the handler makes a call to VASCO’s IDENTIKEY authentication server or utilizes an API-based authentication library, VACMAN Controller, to verify authentication requests.

END-USER EXPERIENCE IS UNAFFECTED
The end-user experience stays unaffected, not requiring any additional steps or login screens.

WHAT IS TWO-FACTOR AUTHENTICATION?
Two-Factor Authentication is a method of verifying a user’s identity that requires at least two elements: something they know (a PIN) and something they have (a DIGIPASS authenticator).

With thousands of students, faculty and staff affiliated with a college or a university, it is critical to secure their access to online resources at all times. Static passwords alone are not enough to ensure such protection. Two-Factor Authentication solutions have been helping thousands of organizations solve this issue for a number of years.

* CAS (Central Authentication System) is an open source Single Sign-On solution managed by Jasig**. It allows users to authenticate against a central authentication service without revealing their credentials to the system that they are attempting to access.

** Jasig, Inc., is a non-profit 501(c)(3), international consortium of educational institutions and commercial affiliates supporting open source software development and promoting open computing architectures for higher education. For more information, visit the Jasig website at http://www.jasig.org.
INTEGRATION SCENARIO 1
CAS authentication via IDENTIKEY Java-based plug-in:
A CAS authentication handler is coded to call upon VASCO’s central authentication server, IDENTIKEY, in order to perform authentication requests.
Suggested IT environments: hybrid environments requiring authentication for multiple clients such as VPN, Firewall, web site access, and others.
Advantages of this implementation include out-of-the-box authentication, data storage, web-based user management and administration, and protocol handlers (RADIUS, SOAP).

INTEGRATION SCENARIO 2
VACMAN Controller, an API-based authentication backend is directly integrated into CAS:
The integration allows for storage of authentication records within your existing database. One-Time Password validation is handled with a simple programming call to the VACMAN Controller shared library.
Suggested IT environments: colleges and universities with IT development staff.
Advantages of this implementation include seamless integration with existing applications while leveraging existing user and administrative interfaces, data repositories, backup and high availability strategies.

INTEGRATION SCENARIO 3
IDENTIKEY authentication server is integrated with CAS via a RADIUS protocol:
A RADIUS authentication handler within CAS is utilized to make a simple RADIUS request to VACMAN Middleware for authentication.
Suggested IT environments: smaller implementations or lack of dedicated IT resources.

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