



## Server Authentication

### Enhance remote access security with a two-factor authentication solution

#### ARE STATIC PASSWORDS ENOUGH?

The proliferation of telecommuting, mobile sales forces, portals, and remote access requirements have made the use of and importance of strong passwords even more important. With critical company data available to anyone over a VPN or firewall that has the right username/password combination, many companies have begun to require stronger passwords, and force users to reset passwords at set time intervals. These users have responded by putting their passwords on post-its and affixing them to their monitors, sharing passwords with other employees, or hiding them under their keyboards, which serves to undo the strong data security that was the aim of the stricter password policies in the first place.

#### MULTI-FACTOR AUTHENTICATION

A recent trend to help protect sensitive data that can be accessed over the internet is the use of MFA (multi-factor authentication) instead of relying on static passwords. A popular method of MFA, or strong authentication, is two-factor authentication. This authentication method requires the user to verify their identity through two electronic channels: their PIN (something they know), and their token (something they have). This token generates a one-time password (OTP) on-demand, which is verified by the authentication server and grants access if the OTP provided matches the one on the server side. This OTP cannot be reused at the next login, reducing the risk of fraudulent access.



#### WHO NEEDS IT?

If your company is providing access to the following data over the internet, protected by only a static password, you should be considering an MFA solution:

- » personally identifiable information
- » intellectual property
- » credit card data
- » customer/patient/student records
- » financial or sales data
- » legal documents and HR files

If your company needs to meet any of the following compliance mandates, you should be considering MFA:

- » PCI
- » HIPAA
- » Gramm-Leach-Bliley
- » FACTA
- » FFIEC
- » CJIS



## EXISTING MFA VENDORS

There are a number of vendors currently providing MFA, including RSA, Entrust, and Active Identity. These vendors position their products to the upper-end of the market, targeting companies that have large IT departments that can afford the complexity involved with their solutions, in addition to a dedicated authentication appliance. Some vendors set their tokens to turn off after three years, so they can renegotiate prices with the customer, forcing them to repurchase client hardware and tokens, and redeploy them to telecommuters and remote sales forces.

## THE VASCO DIGIPASS PACK ADVANTAGE

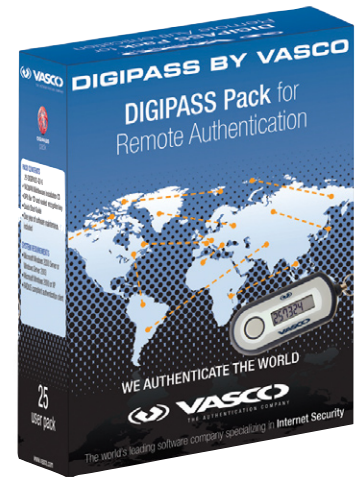
VASCO is another major player in the MFA server authentication market, and has developed a specific product called the DIGIPASS Pack, for small- and medium-sized businesses with limited IT resources and budgets. Ideal for 5 - 500 users, this technology is the same MFA two-factor authentication technology used by VASCO's larger customers including PayPal, Shell, HSBC, and Citibank.



## PLUG-AND-PLAY

The DIGIPASS Pack solution is designed to use existing infrastructure to prevent IT departments from having to make additional investments and adjustments to deploy MFA in their organization. The VACMAN server middleware doesn't require dedicated hardware or even a dedicated operating system. In addition, no additional software needs to be installed on the client PC.

The DIGIPASS Pack includes everything you need to rollout two-factor authentication, including the tokens, the middleware, the encryption and license keys. The software is designed to be so easy to install, that one person should be able to implement it in less than a day. Investment protection is provided by having tokens last the time of the battery, which can be up to 7 years.



## OTHER FEATURES

- » easy to scale, adding users is as simple as buying another pack of tokens
- » family concept enables use with multiple end-user devices and authentication methods
- » integrates with any RADIUS-based SSL-VPN, and compatible with most firewalls and access servers
- » policy-based authentication with bulk and auto management
- » comprehensive audit console and reporting program
- » ODBC compliant database support
- » Active Directory integration
- » dynamic user registration
- » password auto-learning
- » supported by over 200 leading application providers
- » Microsoft Management Console Administration

## TRY IT FREE

North American Systems is fully qualified to help you price and configure a DIGIPASS Pack product that will fit your needs, depending on your API and application infrastructure requirements and number of users. We offer installation services of this solution, as well as technical support for our customers. To find out more about this solution, contact us today, and we can set you up with a online demo of the product and how to install it. If you like what you see, we can let you demo the software and a small number of tokens for evaluation.