

# DIGIPASS Pack for Remote Authentication

An 'Out-of-the-box' strong authentication solution that doesn't require an infrastructure overhaul and is ideally suited for SMBs. Allow access to sensitive information and internal applications from a remote location without compromising security or user convenience.

## INSECURE STATIC PASSWORDS

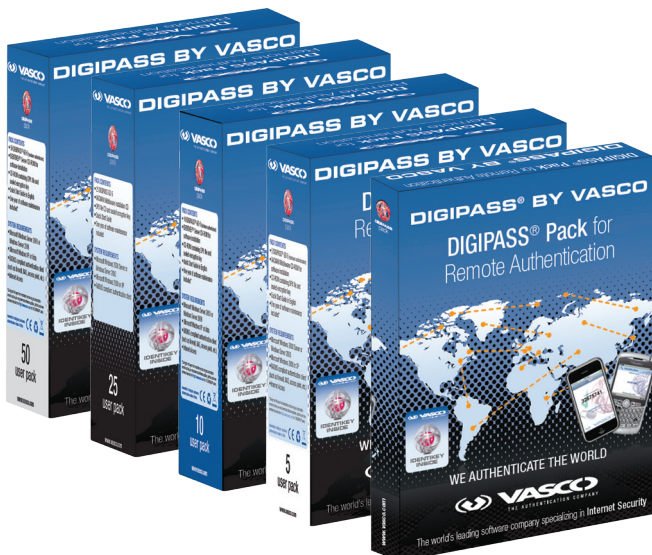
Static passwords are the weakest link in your network security, exposing your sensitive data and applications to online fraudsters. The growing need for a much stronger virtual proof of identity is evident across all industries whenever confidential data and resources are involved.

## STRONG AUTHENTICATION BASED ON ONE-TIME PASSWORD TECHNOLOGY

VASCO's two-factor authentication solution requires two elements to establish a user's identity: something they know (a PIN) and something they have (a VASCO® DIGIPASS®). Based on proven one-time password technology, VASCO DIGIPASS protects user login and insures only authenticated users gain access. Dynamic passwords generated by VASCO DIGIPASS cannot be reused at the next logon, therefore reducing the risk of fraudulent access.

## 'OUT-OF-THE-BOX' STRONG AUTHENTICATION

DIGIPASS Pack is specifically designed for small and medium size businesses to provide a high level of security to organizations with limited IT resources and budgets. It carries all functionalities of an a la carte authentication solution and includes all necessary hardware and software for a simple two-factor authentication rollout. You can be up and running in 1 day – it's that easy!



## THE ONLY STRONG AUTHENTICATION SOLUTION SUITED FOR SMBs:

### Fast and easy implementation

DIGIPASS Pack will interface with any RADIUS client with no additional programming requirements. This lightweight solution resides on your existing server and involves minimal setup and management. There is no client software required and companies can secure access to their VPN and SSL VPN without extensive system modification.

### Low Total Cost of Ownership

There is no need for new servers or appliances: you can realize additional cost savings from leveraging your existing infrastructure and reduce administrative and support costs.

### No Infrastructure Overhaul

DIGIPASS strong authentication does not change the underlying functionalities of your existing IT infrastructure and applications. It is compatible with most firewalls, access servers, and all RADIUS-based VPNs and supported by over 200 leading application providers.

### Suited for SMBs

DIGIPASS Pack is a user friendly and minimally invasive security solution that can be easily deployed and managed by one person. Its high flexibility allows adding more users and applications as required by growing companies.

## WHERE TO USE

- Remote access to internal networks via firewall or SSL/VPN
- For traveling staff, home workers, remote offices, business partners, consultants, etc.
- Intranets, extranets, and in-house web applications
- Expansion available for browser-based applications, such as Citrix CWI and SharePoint or Webmail access, such as OWA

## HOW VASCO'S TWO-FACTOR AUTHENTICATION WORKS

### Combat password theft with a cost-effective solution

#### SERVER SIDE

##### IDENTIKEY Server 3.x: Core Authentication Platform

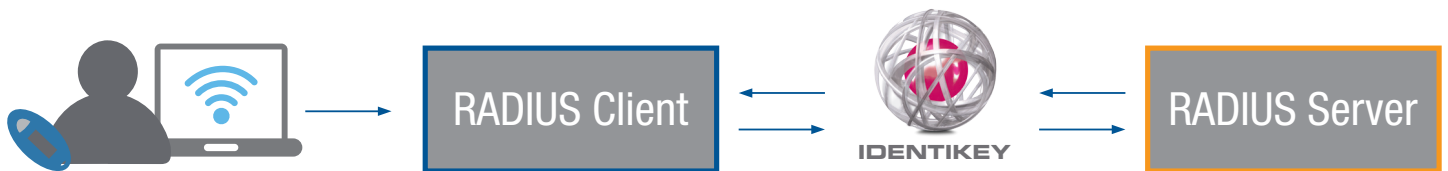
IDENTIKEY® Server 3.x is a lightweight software suite that enables DIGIPASS strong authentication on the back-end. It verifies authentication requests and centrally administers user authentication policies.

#### CLIENT SIDE

##### DIGIPASS: Client Login Devices

DIGIPASS GO 6 is a one-time password generator that is individually assigned to each user. With a simple push on the button, the user generates a dynamic password required for remote login to a network or application.

DIGIPASS for Mobile leverages the mobile phone for authentication purposes. It is available for Java phones, Windows mobile BlackBerry, iPhone,...



Standard Radius Setup with Authentication Server

#### HOW DOES IT WORK

1. The user presses the button of the DIGIPASS authenticator generating a one-time password (OTP)
2. The user then enters this OTP into a login screen on his/her computer along with a PIN
3. IDENTIKEY Server 3.x verifies the authentication request on the back-end
4. If the OTP generated by the user matches the OTP generated on the server side, IDENTIKEY Server 3.x grants access to the remote system or application
5. A new password will be generated at each login, therefore eliminating the risk of password theft and unauthorized access

#### FEATURES

- Supports RADIUS and web server environments
- Compatible with most firewalls and access servers
- ODBC compliant database support
- Active Directory integration
- Comprehensive audit and reporting system
- Microsoft Management Console Administration (MMC)
- Web-based centralized administration interface
- Policy-based authentication
- Bulk and auto management
- Flexible assign procedures for DIGIPASS
- Dynamic user registration
- Password auto learning

#### About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security and designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

#### www.VASCO.com

##### BRUSSELS (Europe)

phone: +32.2.609.97.00  
email: info-europe@VASCO.com

##### BOSTON (North America)

phone: +1.508.366.3400  
email: info-usa@VASCO.com

##### SYDNEY (Pacific)

phone: +61.2.8061.3700  
email: info-australia@VASCO.com

##### SINGAPORE (Asia)

phone: +65.6323.0906  
email: info-asia@VASCO.com