VASCO
THE AUTHENTICATION COMPANY

Battle Card

How To Sell The DIGIPASS Pack

MARKET BACKGROUND

The Challenge: Static Passwords Do Not Provide Adequate Security

- Static passwords do not prove the identity of the remote user, thus undermining security
- Growing risk of unauthorized access to corporate networks and confidential data via VPN or the Internet
- The rapid increase of cybercrime targeting private information

The Opportunity: Market Demand for Strong Authentication

- More and more sensitive data and applications are made available online
- Proliferation of remote access from anywhere, at any time via VPN or the Internet

The Solution: Two-Factor Authentication

- Secure user login with dynamic one-time passwords (OTPs)
- Dynamic passwords cannot be reused at the next logon
- Reduce the risk of fraudulent access

HOW TO IDENTIFY OPPORTUNITIES

What information should be protected?

Any non-public information that is accessible by static passwords over the Internet can and should be secured with two-factor authentication.

- Personally identifiable information
- Intellectual property
- Payment and credit card data
- Customer/patient/client/student records
- Sales data such as forecasts, customer lists
- Financial information / legal documents

What users should be protected?

- Remote workforce and telecommuters with access to sensitive data
- Mobile sales force
- Partners, vendors, contractors, suppliers with network or system access
- IT staff with administrator rights
- Contract workers in IT environment
- After-hours troubleshooting employees

Compliance drivers

- Multiple legal and government acts mandate two-factor authentication security to ensure data privacy. Examples include acts like PCI DSS, Sarbanes Oxley, CoCo (Code of Connection), BECTA, Basel II, and others.

Decision makers

- IT director / manager
- Compliance officer
- CSO, CIO
- Network administrator / LAN administrator
- VPN administrator
- Security consultant
- Business owner (SMBs)

KEY VENDOR PAIRINGS

Juniper Networks, aep Networks, Cisco, Microsoft, Fortinet (Real Time Network Protection), Citrix, SonicWall, NetASQ (Secure Internet Connectivity), Check Point Software Technologies Ltd., WatchGuard

Over 200 other compatible solution providers can be found at www.vasco.com/solutionpartners

KEY TERMS

- **Authentication** - the process of determining whether someone is, in fact, who they declared to be.
- **Static Password** - a constant, reusable, and guessable password used to authenticate a user.
- **One-Time Password (OTP)** - a time-based or event-based, dynamic password that is generated by a hardware or a software device to securely authenticate a user.
- **Two-Factor Authentication** - method of verifying a user's identity via electronic channels that includes at least two factors: something they know (a PIN) and something they have (a DIGIPASS).
- **DIGIPASS** - VASCO's client authentication devices, also referred to as "tokens" or "authenticators".

EXISTING CUSTOMER REFERENCES

Some of the existing customers include SITA (SUEZ), Volvo, ING, The Goethe Institut, PayPal, Rabobank, Leuven University Hospital, The Royal Belgian Football Association, Saint-Gobain Isover, BEBAT, Promedico.

MORE INFORMATION

www.vasco.com

www.digipasspack.com

For product details and specifications, pricing information, and special requests, contact your VASCO Authorized Distributor.

VASCO AUTHORIZED DISTRIBUTOR

Battle Card

How To Sell The DIGIPASS Pack

VASCO
THE AUTHENTICATION COMPANY

WHAT VASCO OFFERS TO THE END-USER

DIGIPASS Pack - Prepackaged 'Out-of-the Box' Solution Designed for the SMB Market

The DIGIPASS Pack is a complete, prepackaged two-factor authentication solution that includes IDENTIKEY server software (Standard Edition) and a DIGIPASS authenticator for each user. The DIGIPASS Pack is an ideal fit for small and medium-sized businesses with limited IT resources and budgets. It also makes a good choice for pilot projects as it can be easily expanded without an infrastructure overhaul.

Fast
- Speedy set-up and deployment
- Out-of-the-box software-based backend
- Seamless integration into existing infrastructure
- No programming required
- No installation on client PC

Easy
- Easy to install
- No infrastructure overhaul
- Can be deployed and managed by one person
- Appropriate for small deployments (5+ users)

Affordable
- Lowest total cost of ownership in the industry
- No need for dedicated servers or appliances
- No client hardware to repurchase
- DIGIPASS authenticators do not expire and will last for the lifetime of the battery (7+ years with average use)

Scalable
- Adding users and/or applications is simple without the need to revamp existing infrastructure

FREE PRODUCT TRIALS AND DEMOS

Server software free trial, 45 days: www.vasco.com/dppacktrial

DIGIPASS authenticator demos can be requested at your VASCO Authorized Distributor.

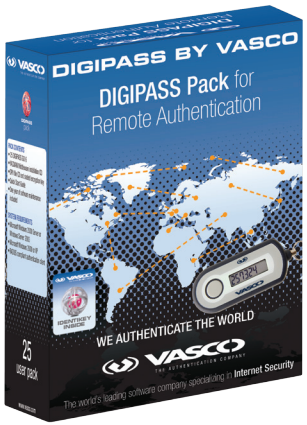
WHAT VASCO OFFERS TO THE VARs

The DIGIPASS Pack was designed specifically for channel sales to maximize VAR profitability, shorten sales cycles, and increase growth opportunities.

Faster Sale
- Shorter sales cycle
- No special hardware/server setup is required
- Hassle-free setup and administration

Easier Sale
- Ideal tool to round out any remote access or VPN sales
- Affordable price
- No special training is needed for customers
- Appropriate for small deployments (5+ users)

Sales Opportunities
- Ideal for pilot projects, intro ductory sales, or "try-and-buy" campaigns
- Easy expansion for existing customers due to flexibility and scalability
- Additional leverage in negotiations with larger prospects



Growth Opportunities
- Increase your customer footprint and grow market share
- Generate new revenue from your installed base

WHAT'S IN A BOX

Everything you need for a fast two-factor authentication rollout.
- DIGIPASS GO6 hardware authenticators
- Software server Installation CD ROM
- CD ROM containing DPX file and sealed encryption key
- Quick Start Guide and supporting documentation
- License Key
- End-user License Agreement
- One Year of software maintenance & support

DEMONSTRATED CAPABILITIES

Centralized user management
- Web-based admin GUI
- Microsoft Management Console Administration (MMC)

Automated deployment function
- Bulk and auto management
- Dynamic user registration
- Flexible assign procedures for DIGIPASS authenticators
- Policy-based authentication
- Password auto learning

Comprehensive audit and reporting system
- Extensive XML or HTML-formatted reporting
- Security audit function

Multi- database support
- ODBC-compliant database support
- Active Directory integration
- LDAP lookup and authentication on AD, ADAM, and eDirectory

SUPPORTED ENVIRONMENTS

Supported IT environments include:
- Windows Server 2003 (32- & 64-bit) with SP1 and above, or R2
- Windows Server 2008 (32- & 64-bit)
- Windows XP SP1
- Windows Vista
- Novell Suse Linux Enterprise Server 10
- Ubuntu 8.04 Server Edition
- Redhat Enterprise Linux 5
- RADIUS-compliant authentication client

TECHNOLOGY PAIRINGS

- VPN and SSL-VPN
- Firewall
- NAS
- SSO
- Any RADIUS software or hardware
- Web applications, Intranets, Extranets
- Web mail