

# DIGIPASS®

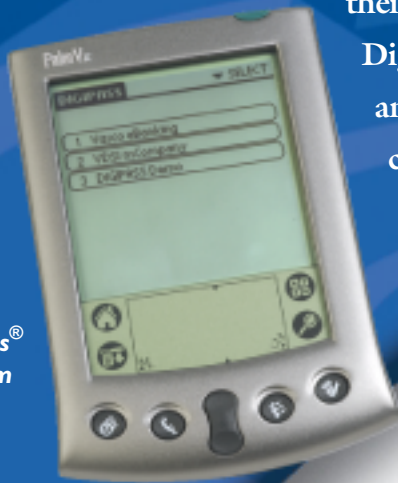
for Palm

## **Strong Authentication and Digital Signature for Mobile Security with the PDA!**

Digipass for Palm protects access to corporate networks, e-business and e-commerce applications by eliminating the weakest link in the security infrastructure: the use of static passwords.

Unlike human-created passwords that are easily stolen, guessed, reused, or shared, Digipass for Palm generates single-use passwords that change every 36 seconds. Protect the network from the inside-out, for internal employees on their desktop machines to the outside remote users on their laptops.

Digipass for Palm offers secure remote access and extended digital signature capabilities on PDAs and smart phones.



Digipass®  
for Palm

data exchange, between the end-user and the m-commerce store or bank. It does not rely on the underlying wireless connectivity infrastructure. Digipass works equally well over GSM, CDMA, GPRS or future 3G networks.

### **Another step towards Digital Convergence**

PDAs are merging with mobile phones, digital cameras, digital music players, GPS receivers and are becoming all-in-one universal digital assistants. Digipass for Palm adds yet another functionality: it turns the PDA into a personal hardware security device.

### **Strong authentication for m-Commerce**

Many PDA devices have wireless connectivity, relying on WAP, GPRS or similar technologies. As a result, PDA's enabled with Digipass for Palm provide strong user authentication and digital signatures for wireless mobile commerce transactions.

Digipass for Palm provides end-to-end secure

### **Work off-Line or over Legacy Networks: Anytime, Anywhere**

Digipass for Palm can work on-line, off-line or wirelessly. Digipass one-time passwords and digital signatures can be communicated over any available medium. Telephone lines, Internet, VPN, corporate LAN, Kiosks or even fax – everything will do. Digipass can also be used for traditional touch-tone phone banking. One-time passwords can even be used with a live operator by voice: truly anytime, anywhere connectivity.

### **One device to Access Multiple Networks and Web Sites**

Digipass for Palm allows more than one virtual token in one PDA, each with its own secret key for access to different servers, networks and web sites.



THE AUTHENTICATION COMPANY

## Easy to Deploy

Digipass for Palm can be easily installed by individual end-users or centrally deployed throughout the organizations. It is installed in a straightforward, wizard-assisted process with a customary use of the cradle and the specific Sync technology.

Two types of activation are supported: (i) offline, whereby each client receives a personalization file and activation code and (ii) online / interactive, allowing initialization via e-mail or telephone.

## Supported Platforms

- Palm OS 3.0 and higher

## Key Features

- Remote user authentication with one-time passwords or challenge / response
- Digital signatures (message authentication codes)
- Multiple applications:
  - Mobile commerce, mobile banking
  - Traditional phone / fax banking
  - Network security, remote office, telecommuting
- Wireless protocol agnostic: works over TDMA, CDMA, GSM, GPRS or future 3G networks
- Works off-line or over legacy networks: LAN, dial-up modems, Internet, fax, voice. Operational when no wireless connection available

- Compatible with all Digipass family members and server tools
- Multiple profile support: one PDA to access all networks and web sites

## Password Management

- User-chosen and changeable password
- The system operator defines usage and length of the password
- Server based lock mechanism after a number of invalid password entries.

## Cryptographic Functions

- Data Encryption standard (DES) and triple DES
- Challenge input up to 16 digits long.
- Responses are shown in decimal or hexadecimal format
- Different functions can be assigned to each application:
  - Time independent response with external challenge (X9.9)
  - Time-based response with external challenge
  - Event-based response with external challenge
  - Time-based one-time password generation
  - Event-based one-time password generation
  - Time- and event-based one-time password generation
- A single check digit (per ISO 7064-6) can be applied on the challenge and / or response

**For regional offices or to learn more about us, visit our web site at [www.vasco.com](http://www.vasco.com)**



THE AUTHENTICATION COMPANY

### EMEA

VASCO Data Security nv/sa  
Koningin Astridlaan 164  
B-1780 Wemmel, Belgium  
phone: +32.2.456.98.10  
fax: +32.2.456.98.20  
email: [info\\_europe@vasco.com](mailto:info_europe@vasco.com)

### APAC

VASCO Data Security Asia-Pacific Pte Ltd.  
#14-01 Prudential Tower, 30 Cecil Street  
049712 Singapore  
phone: +65.6.232.2727  
fax: +65.6.232.2888  
email: [info\\_asia@vasco.com](mailto:info_asia@vasco.com)

### AMERICA

VASCO Data Security, Inc.  
1901 South Meyers Road, Suite 210  
Oakbrook Terrace, Illinois 60181, USA  
phone: +1.630.932.8844  
fax: +1.630.932.8852  
email: [info\\_usa@vasco.com](mailto:info_usa@vasco.com)

All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for any infringement of patents or other rights of third parties resulting from its use.