
# DIGIPASS ® 860 M

**Overview version 1.0**

This hardware key is in compliance with the following test specification:

CEI EN 61000-4-2; CEI EN 61000-4-3; CISPR22

as required by:

CEI EN 61000-6-1, CEI EN 61000-6-2, CEI EN 61000-6-3, CEI EN 61000-6-4

which are specified for the following test:

- "ESD Immunity test"
- "Radiated radio-frequency and electromagnetic field immunity test"
- "Radiated Emission Verification"

**In compliance with the "Essential Requisites" for the EMC Directives 89/336/EEC and 2004/108/EEC**

FCC ID: UZ4-AAB

VASCO DATA SECURITY NV/SA
Digipass 860 ([1])
Supply: 5V DC
Absorption: 250 mA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

*Caution: changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

IMPORTANT REMARKS
Due to the limited space on the product shell, all FCC certification references are on this technical manual.

[1] The models subjected to this mark are the following: ITSEC-I, ITSEC-P and FIPS.

# DIGIPASS® 860

**For banks and other organizations who need strong user authentication, digital signature functionality and hassle free remote user authentication, DIGIPASS 860 is an hybrid security device that supports both PKI and one-time password generation in one single product. DIGIPASS 860 is based upon 'state-of-the-art' technology and offers additional added value to the user.**

DIGIPASS 860 is a hybrid security device enabling strong two factor authentication based upon the knowledge of a password or PIN and the possession of secrets stored in the products. DIGIPASS 860 offers both DIGIPASS one-time passwords generation and PKI capabilities in one single device.
The DIGIPASS one-time password generation provides strong, hassle free, remote user authentication.
The PKI functionality provides document signing; strong authentication against PKI enable software systems (operating systems, virtual private networks, applications); as well as e-mail, file and disk encryption.

## FUNCTIONS

- Document authentication through the generation and validation of digital signatures
- Strong user authentication against PKI enabled software systems providing single sign-on functionality
- Strong remote user authentication through the generation of one-time passwords

## FEATURES

- Secure storage of certificates, credentials, encrypt-tion keys, strong static passwords and user data (memory stick)
- On-board generation of PKI key sets
- E-mail, file and disk encryption
- PKI functionality based upon highly secure smart card technology

## BENEFITS

- Support of both one-time password generation and PKI DIGIPASS in one single device
- 'State-of-the-art' technology and highly secure: leveraging VASCO DIGIPASS technology and Infineon smart card technology
- Added value for users: memory stick functionality, file & disk encryption
- Involves minimal IT effort and maintenance
- Fully customizable (logo, color)

**All DIGIPASS strong authentication products can be deployed concurrently to match your company's specific requirements.**

# DIGIPASS 860

## THE PRODUCT

DIGIPASS 860 comes with a protective cap; PKI middleware; device driver; installation software and documentation (manual and reference guide).


## INSTALLATION

DIGIPASS 860 can be easily installed and integrated on the user's PC, through an easy to use installation wizard.

## USAGE

Users simply plug the DIGIPASS 860 into a standard USB port on the PC and enter their password or PIN for workstation security and access to PKI enabled software systems, providing single sign-on functionality. Compliancy with various industry standards ensures interoperability within the Microsoft Windows domain as well as wide range of applications such as Microsoft Internet Explorer, Microsoft Outlook, Lotus Notes and Adobe Acrobat.

For hassle free remote user authentication to web-applications or telephone based services (telephone banking), the DIGIPASS 860 can be used in the unconnected mode. The user presses the button on the DIGIPASS 860 which generates a new one-time password which is shown on the display. This one-time password should be provided to the application for validation.

## TECHNICAL SPECIFICATIONS

### PHYSICAL CHARACTERISTICS

- Dimensions (lxwxh): 69,6 mm x 26,6 mm x 13,3 mm
- Weight: 22,3 grams (including protective cap)
- Logo area (lxw): 11,7 mm x 3,4 mm

### USER INTERFACE

- One button key-pad
- 8 Character numeric display

### PKI – SECTION

- Key generation: 1024 bit RSA key pair
- X.509 v3 certificates and secure key storage
- PIN based private key protection
- Crypto data transfer rate: 64Kbps
- RSA signature: 2048 bit
- Crypto processor: 32 KB or 64 KB
- ITSEC E4 High certified, FIPS 140-2 level 1 and 2
- Crypto processor available in 3 editions: 32KByte, 64KByte and 32KByte FIPS certified

### OTP – SECTION

- DIGIPASS algorithm support (time and/or event based)
- OATH algorithm support (option)

### MEMORY

- Memory stick: 128KB/256KB/512KB/1GB/2GB

### OS SUPPORT

- Microsoft Windows 98/ME/2000/XP and Linux (version?)

### POWER MANAGEMENT

- Connected mode: via USB bus
- OTP mode: via non replaceable batteries
- Avg. battery life time: 5 years

### STANDARDS AND COMPLIANCES

- X.509 v3
- PKCS#11 v2.11 Cryptographic Token Interface
- Secure / Multipurpose Internet Mail Extensions
- Microsoft Cryptography API

## About VASCO

VASCO designs, develops and supports patented "Strong User Authentication" products for the financial world, secure network access, e-business and e-commerce. VASCO's user authentication technology is carried by the end-user on its DIGIPASS products which exist in hard & software format.

At the server side, VASCO's VACMAN products guarantee that only the designated DIGIPASS user gets access to the application. VASCO's target markets are the applications and their several hundred million users using fixed password as security.

VASCO's time-based system generates e-signatures and a "one-time" password that changes with every use, and is virtually impossible to hack or break. With tens of million of DIGIPASS products sold, VASCO has established itself as a world leader in strong authentication for e-banking and for network access for blue-chip corporations and governments worldwide.

## www.vasco.com

**Belgium (Brussels)**
phone: +32.2.609.97.00
email: info_europe@vasco.com

**The Netherlands ('s-Hertogenbosch)**
phone: +31 73 691 88 88
email: info_europe@vasco.com

**USA (Boston)**
phone: +1 508.366.3400
email: info_usa@vasco.com

**Australia (Sydney)**
phone: +61 2 8920 9666
email: info_australia@vasco.com

**Singapore (Singapore)**
phone: +65 6323 0906
email: info_asia@vasco.com

**China (Shanghai)**
phone: +86 21 6443 2697
email: info_asia@vasco.com