



DIGIPASS[®] 870

Secure connectable reader with 'what-you-see-what-you-sign' functionality.

DIGIPASS 870 is a USB connectable personal card reader which can be used in both connected and unconnected mode. DIGIPASS 870 has a sophisticated user interface, comprising a 16-key keypad and a full graphical screen that can display up to 6 lines. When connected to the PC, DIGIPASS 870 functions as a sophisticated secure PIN pad reader offering secure PIN entry features and "what you see is what you sign" functionality. All data to be signed is visually presented on the DIGIPASS 870 display for confirmation by the cardholder.

CONNECTED MODE

Protecting smart card pin

An alarming number of applications continue to use smart cards that are inadequately protected with static PINs. Applications such as PKI, e-wallet or e-banking applications are exposed to Trojans or key loggers if they rely simply on static PIN entry on the keyboard for smart card transactions. DIGIPASS 870 provides the secure advantage of entering the PIN directly on the reader and not on the computer keyboard. Therefore, the PIN is never available on the PC platform. Similarly, smart card PIN changes can be securely performed using the DIGIPASS 870 keyboard. Furthermore, a firewall mechanism protects the card from unauthorized access.

See it before you sign it

DIGIPASS 870 has a full dot matrix display allowing extended data field validation on the DIGIPASS screen. The large screen sets a new standard for e-signature offering high transaction security thanks to the "what you see is what you sign" (WYSIWYS) capability. With WYSIWYS, the user will validate the key data on his DIGIPASS 870 display before he signs the transaction.

Reader signature and multi secure channel

The bank which issues DIGIPASS 870 to its customers can verify that a transaction is approved and signed by his customer with a genuine card reader. When that same transaction is signed by an unauthorized reader it is fully detectable. The end-user can trust the data he digitally signed since they were displayed in the secure environment of a trusted reader. During the transaction, banks can even send messages to the user through a secure channel which can be easily implemented in any bank's security infrastructure.

Easy deployment, installation and use

DIGIPASS 870 uses a standard driver compliant with all popular operating systems such as Windows, Linux and MacOS. Leveraging the available CCID driver, DIGIPASS 870 does not require the installation of a separate driver on most of the popular PC platforms. The reader is not personalized and as a result can randomly be distributed to customers without compromising their security and benefitting deployment to large customer bases.

Firmware update optional

As an option, the DIGIPASS 870 supports secure firmware update. DIGIPASS 870 firmware and applications can be updated by the bank which issues the card reader at any time even when DIGIPASS 870 has already been issued to the end-user, making use of proven and standard cryptographic mechanisms.

UNCONNECTED MODE

When used in unconnected stand-alone mode, DIGIPASS 870 offers the same functionality as other DIGIPASS unconnected, including strong authentication and e-signatures. DIGIPASS 870 is perfectly suited for environments with high security requirements including digital signatures, secure PIN verification, corporate network access, strong authentication (internet banking), e-commerce transactions, etc.

DIGIPASS 870 can be delivered with a wide variety of applications including MasterCard CAP, Visa Dynamic Passcode Authentication (DPA) and various domestic and proprietary schemes. The reader leverages the inherent security of chip cards to store secrets with cryptographic calculations for maximum efficiency. For each function, DIGIPASS 870 uses a different cryptographic key to generate one-time passwords and e-signatures.




SPECIFICATIONS

| | |
|--------------------------------|--|
| VASCO Class 4 reader | |
| User interface | 102 * 46 full dot matrix display Up to 6 lines, 120 characters |
| Smart Card interface | ISO7816 Frequency up to 4 Mhz Supports ISO 7816 Class A and B smart cards (5V, 3V) Embossed smart card supported |
| Size | 97 x 61.7 x 13.5 mm |
| Weight | <80 g. |
| Keypad | Tactile keypad with silicon rubber key printed with an epoxy layer. Resistant to over 100,000 rubbings. 10 numeric keys and 6 function keys |
| Battery | 2 replaceable batteries |
| Power supply in connected mode | USB connection |
| Cable | 1m long USB cable with type A connector |
| Operating systems | Windows XP, Vista, Windows7, Windows 8, Windows server 2003, 2008 and 2010, Linux, Mac os x 10.6 and above |
| Standards | Mastercard CAP (2004, 2007) VISA dynamic passcode authentication version 1.1 Belgian eID card Connected EMV CAP ISO 7816 EMV2000 LEVEL 1 USB 2.0 Full speed PC/SC 2.01 CCID RSA, ECDSA, AES |
| Logo | Bank's logo can be printed on the reader. Color of the casing can also be customized |

COMPLIANCE

| | |
|--|--|
| Operating temperature | 0 °C to 45 °C; 85 %RH non-condensing IEC 60068-2-78 (Damp heat) IEC 60068-2-1 (Cold) |
| Vibration | 10 to 75 Hz; 10 m/s ² IEC 60068-2-6 |
| Drop | 1 meter IEC 60068-2-32 |
| Emission | EN 55022 |
| Immunity | 4 kV contact discharges 8 kV air discharges 3 V/m from 80 to 1000 MHz EN 61000-4-2 and EN 61000-4-3 |
| Compliance to European directives (CE marking) | 2004/108/EC (EMC directives) 2002/95/EC (RoHS directive) 2002/96/EC (WEEE directive) |

HOW TO SIGN TRANSACTIONS IN CONNECTED MODE

DIGIPASS 870 is directly linked to the bank system via a secure connection:

1. DIGIPASS 870 will display the transaction information (amount, account number, etc..)
2. The user confirms each data field separately or the full transaction as displayed on the screen of the device
3. Enter your PIN code and press the 'OK' button. The transaction is signed using the 'what-you-see-is what-you-sign' functionality

HOW TO LOG-ON TO YOUR ACCOUNT IN UNCONNECTED MODE

1. Insert your card into the slot of DIGIPASS 870 and press the login function button
2. Enter the challenge value provided to you on the bank's webpage
3. Enter your PIN code. The reader displays a response code (one-time-password)
4. Enter the response code in the application. The bank will validate the code and grant user access

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 DIGIPASS®, CertiID™, 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