DIGIPASS® KEY 860

One-time password (OTP), PKI-technology and secure USB storage all-in-one

DIGIPASS KEY 860 offers a solution to the growing authentication needs of banks, enterprises and governments. It combines OTP and PKI technology with secure mass USB storage. DIGIPASS KEY 860 is an easy-to-use end-user device which can be used for local and remote access, desktop and application log-on, disk encryption, data, e-mail and transaction signing and secure mobile data storage.

Increased identity and data theft, man-in-the-middle attacks, unauthorized access to confidential data… rising fraud statistics demonstrate the growing need for data security solutions. Security concerns aren't limited to network breaches alone. Bearing in mind that employees often carry sensitive corporate information on portable USB drives, additional security measures should be seriously considered as these data are freely accessible and the USB devices can easily be lost or stolen.

VASCO® Data Security has a solid reputation in helping financial institutions in securing transactions online through two-factor authentication. With DIGIPASS KEY 860, VASCO offers an innovative solution combining OTP and PKI-technology with secure USB mass storage.

DIGIPASS Key 860 is a hybrid end-user authentication device offering strong authentication. The use of OTP and PKI-technology are combined on a single device. DIGIPASS KEY 860 also offers secure mass USB storage for mobile data security. DIGIPASS KEY 860 is used in conjunction with DIGIPASS CertiID™, VASCO's PKI-based client software suite, and can be integrated within any application supporting PKCS#11, MS CAPI standards and CNG.

DIGIPASS KEY 860 is suited for use in corporate environments and for securing online banking applications:

- In enterprises it offers a solution for local and remote access to the network and business critical applications, locking of workstations, disk and file encryption, digitally signing e-mails and confidential documents, and mobile data security.
- In banking DIGIPASS KEY 860 helps to comply with more stringent financial regulations (Sarbanes-Oxley, Basel II, HIPAA) and enhanced security requirements. Both OTP and PKI technology can be used for digital signature of transactions and the possibility to store a secured browser on DIGIPASS Key 860 offers new opportunities to banks to effectively combat phishing and man-in-the-middle attacks.

BENEFITS

PKI functionality

DIGIPASS Key 860 combines the security of a smart card with the flexibility of a card reader. Digital certificates from any Certificate Authority (Entrust, Microsoft, VeriSign, IdenTrust,…) can be generated and stored on the device. The generation of private and public keys is managed on the device and the keys cannot be exported from the smart card.

OTP functionality

With one push on the button of DIGIPASS KEY 860, an OTP will be generated on the screen of the authenticator. The user will type the OTP into the log-on screen on the PC to access the application. When combining the use of PKI with OTP, customers will need to install VASCO's authentication server technology (VACMAN® Controller or IDENTIKEY®) to offer event and time-based OTP capability next to PKI-functionality.

Secure USB Storage and secure CD-ROM content update

DIGIPASS KEY 860 has three pre-defined memory partitions which cannot be altered by the user, making them highly secure:

- a partition with CD-ROM capability for software installation (e.g. secured browser installation)
- encrypted partition on the fly for secure data storage
- a non-secure hard disk partition to store accessory, non-confidential information

DIGIPASS KEY 860 comes with a secure CD-ROM update solution enabling customers to update the read-only content of the DIGIPASS KEY CD-ROM drive. Updates can be executed by VASCO or the customer himself through manually or automated downloads.

DIGIPASS CertiID embedded

The secure mass storage feature of DIGIPASS Key 860 allows for DIGIPASS CertiID™ capability to be embedded into the device. By embedding DIGIPASS CertiID, the deployment of DIGIPASS Key 860 requires no software installation on clients. DIGIPASS Key 860 becomes plug and play thus reducing administrative costs. Devices can be managed in user and administration mode: PIN and PUK are initialized on first use either by the end-user or the IT-administrator.

OPSEC CERTIFIED · IdenTrust COMPLIANT · Entrust Ready · CITRIX ready™

Mac · Linux · Works with Windows Vista™

VASCO
THE AUTHENTICATION COMPANY

DIGIPASS

FEATURES

- Strong password authentication
- OTP generation
- PKI functionality (signature, encryption, on board generation of RSA key pair)
- Hardware based 256 bit AES encryption, on the fly encryption
- Zero footprint capability
- File and disk encryption
- Ultra fast data transfer, high speed USB
- USB mass storage (available in 2, 4 and 8 Gbyte)
- CD-ROM upgrade content by VASCO or bank server

TECHNICAL SPECIFICATIONS

Size (LxWxT)	73.5 mm X 23.5 mm X 10.5 mm
Color	Black
Product Identification	10-digit serial number and bar code on the back side
Weight	24 g (including product cap)
Battery	5 years, 7 years life expectancy, Non replaceable
Logotype	With VASCO logo (unless specified otherwise)
LCD display	8-character
USB	2.0 (high speed, full speed, low speed) Connector type A
LED	Access activity indicated on both sides by orange LED

COMPLIANCE TO STANDARDS

Smart card	ISO 7816 3 - 4
Java card	Open Platform 2.1.1, java card 2.2, Oberthur Cosmo v5.4 or v7.0
Smart card reader architecture	PC/SC , CCID drivers
Public Key Mechanisms	1024-bit and 2048-bit RSA, X509 v3
Public Key Cryptography (PKI)	PKCS#11 v2.2, PKCS#1,7,8,10,12,15 Microsoft® CAPI 2.0, S/MIME. Crypto Next generation and key storage provider and minidriver architecture
USB Memory encryption	On the fly encryption by dedicated hardware processor, AES-CBC mode, 256 bits , FIPS -197
OTP	DES, DES3, AES
Certification	Smart card :Common criteria EAL4+ and compliant up Protection profile SSCD smart card: FIPS 140-2 Level 3 Entrust and Identrust ready: available with DIGIPASS CertiID 3.2 and under certification Vista smart card minidriver
Operating system supported	Microsoft® Windows® 7 / Vista /XP MacOS 10.6.4 Linux (Red Hat Enterprise Linux 5.5 Desktop, Ubuntu 10.04, SUSE Linux Enterprise Desktop 11) Citrix XenDesktop 5 Citrix XenApp 4.0X Citrix Presentation Server 4.5
Storage temperature	-10 °C to 50 °C; 90 %RH non condensing IEC 60068-2-78 (Damp heat) IEC 60068-2-1 (Cold)
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/s2 IEC 60068-2-6
Drop	1 meter IEC 60068-2-31
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

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

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com

DS-201206-v2