



DIGIPASS[®] KEY 202

PKI authentication based on SIM card technology and secure USB storage

DIGIPASS KEY 202 offers a solution to the growing authentication needs of banks, enterprises and governments. It combines PKI technology with secure mass USB storage. DIGIPASS KEY 202 is an easy-to-use end-user device suited for secure local and remote access, desktop and application log-on, disk encryption, e-mail and data transaction signing and secure mobile data storage.

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 considered as these data are freely accessible and the USB devices can easily be lost or stolen.

With DIGIPASS KEY 202, VASCO[®] offers an innovative solution combining SIM card-based PKI-technology with secure USB mass storage. By using a SIM card, VASCO has facilitated the personalization process of the end-user devices. Instead of personalizing every device prior to customer distribution, end-users receive a personalized SIM card. This severely reduces the cost for organizations for the renewal of smart cards and mass deployment of the USB devices. When certificates expire after two years, organizations only need to redistribute a new SIM card to their customer base instead of replacing every authentication device.

DIGIPASS KEY 202 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 and data, the locking of workstations, disk and file encryption, digital signature of e-mails and confidential documents... In banking, DIGIPASS KEY 202 helps to comply with more stringent financial regulations (Sarbanes-Oxley, Basel II, HIPAA) and enhanced security requirements. PKI technology is used for digital signature of transactions and the possibility to store a secured browser on DIGIPASS KEY 202, offers new opportunities to banks to effectively combat phishing and man-in-the-middle attacks.

DIGIPASS KEY 202 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. The CertiID software can be embedded in the device, turning it into a zero footprint solution and ensuring a cost-efficient installation. Additionally, a hardened browser or PDF signature software suite can also be stored in the memory disk partition.

BENEFITS

PKI functionality

Digital certificates from any Certificate Authority (Microsoft, VeriSign, IdenTrust, Entrust...) can be generated and stored on the device. DIGIPASS KEY 202 with its replaceable SIM smart card can address different security requirements in just about any market by inserting the appropriate SIM card.

Cost reduction for the total solution

Thanks to the SIM card form factor, the cost for organizations for the renewal of smart cards and mass deployment of the USB devices is severely reduced.

Secure USB Storage and secure CD-ROM content update

DIGIPASS KEY 202 has three pre-defined memory partitions which cannot be altered by the user, making them highly secure:

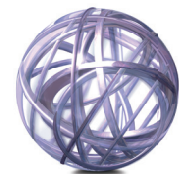
- a partition with CD-ROM capability for software installation (e.g. secured browser installation)
- encrypted partition on the fly for secure data storage
- a non-secure hard disk partition to store accessory, non-confidential information

DIGIPASS KEY 202 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.

Smart card-based OTP generation

DIGIPASS KEY 202 also provides the possibility to generate one-time passwords (OTPs). Users can select this option via the DIGIPASS CertiID software program. DIGIPASS CertiID software will access the secret on the smart card of DIGIPASS KEY 202 and an OTP will be generated and displayed on the PC screen.




FEATURES

- Strong password authentication
- PKI functionality (signature, encryption, on board generation of RSA key pair)
- Hardware based 256 bit AES encryption CBC mode
- Zero foot print capability (driver less)
- CD-ROM upgrade content by VASCO or bank server
- E-mail, file and disk encryption
- Ultra fast data transfer, high speed USB
- USB mass storage (available in 2, 4, 8 and 16 Gb)
- Smart card based OTP generation
- SIM card reader

TECHNICAL SPECIFICATIONS

Size (LxWxT)	71 mm X 21 mm X 10.7 mm
Color	Black transparent housing with black non-transparent USB lens with VASCO logo (unless otherwise specified)
Product Identification	10-digit serial number and bar code on the back side
Weight	14 g (including product cap)
Logotype	Printable on lens and/or transparent for picture support
Led	Orange for activity access
USB	2.0 (high speed, full speed, low speed) Connector type A

COMPLIANCE TO STANDARDS

Smart card	SIM compliant ISO 7816 3 - 4 class B Oberthur cosmo v V7.0.x; IAS ECC applet
Java card	Open Platform 2.1.1, java card 2.2
Smart card reader architecture	PC/SC, CCID Drivers
Public Key Mechanisms	1024-bit and 2048-bit RSA, X509 v3

Cryptographic supports ¹	AES 128 to 256 bits, EC-DSA up to 512bits, SHA up to 512
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
One-time password	DES3
Certification	SIM Smart card: Common criteria EAL4+/EAL5+ and compliant up Protection profile SSCD SIM mart card: FIPS 140-2 level3 Entrust ready. IdenTrust compliant. Vista smart card minidriver
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 50 °C; 90 %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 60068-2-31
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
Compliance to European directives (CE marking)	2004/108/EC (EMC directives) 2002/95/EC (RoHS directive) 2002/96/EC (WEEE directive)

¹ Depending on the chip used.

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