

# DIGIPASS KEY 200

## PKI-technology and secure USB storage all-in-one

DIGIPASS KEY 200 offers a solution to the growing authentication needs of banks, enterprises and governments. It combines PKI technology with secure mass USB storage and physical access capability. DIGIPASS KEY 200 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 and unauthorized access to confidential data demonstrate the growing need for data security solutions. Next to that, more stringent regulation has been put in place ensuring data security for companies and financial institutions. Furthermore employees often carry sensitive corporate information on portable USB drives. 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 200, VASCO offers an innovative solution combining PKI-technology with secure USB mass storage.

DIGIPASS KEY 200 is a USB end-user authentication device offering PKI-based strong authentication and secure mass USB storage for mobile data security with physical access capability. DIGIPASS KEY 200 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 200 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 200 helps to comply with more stringent financial regulations (Sarbanes-Oxley, Basel II, HIPAA) and enhanced security requirements. PKI technology is used to digitally sign transactions. The possibility to store a secured browser on DIGIPASS KEY 200, offers new opportunities to banks to effectively combat phishing and man-in-the-middle attacks.



### BENEFITS

#### PKI functionality

DIGIPASS KEY 200 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.

#### Secure USB Storage

DIGIPASS KEY 200 has three predefined 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

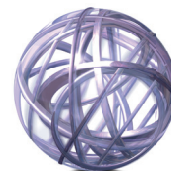
#### Support RFID technology

DIGIPASS KEY 200 supports RFID technology. DIGIPASS KEY 200 combines physical access with logical access in one device. When using the contactless functionality of DIGIPASS KEY 200 a contactless transaction can be executed in a single step, multiple environments and applications are federated in a single end-user device.

#### DIGIPASS CertiID embedded

The secure mass storage feature of DIGIPASS Key 200 allows for DIGIPASS CertiID capability to be embedded into the device. By embedding DIGIPASS CertiID, the deployment of DIGIPASS Key 200 requires no software installation on clients. DIGIPASS Key 200 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.




**FEATURES**

- Strong password authentication
- PKI functionality (signature, encryption, on board generation of RSA key pair)
- Hardware based 256 bit AES encryption CBC mode, on fly encryption
- Zero footprint capability and driverless
- E-mail, file and disk encryption
- Ultra fast data transfer, high speed USB
- USB mass storage (available in 2, 4 and 8 Gbyte)
- Smart card based OTP generation

**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	14 g (including product cap)
Logotype	VASCO logo (unless specified otherwise)
Led	Access activity indicated on both sides by orange led
USB	2.0 (high speed, full speed, low speed) Connector type A

**COMPLIANCE TO STANDARDS**

Smart card	ISO 7816 3 –4. Oberthur cosmo v 5.4 or V7.0D
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 <sup>1</sup>	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
Wireless interface <sup>2</sup>	Iso 14443 Type A, T=CL & 1k Mifare emulation
OTP	DES3
Certification	Smart card: Common criteria EAL4+ and compliant up Protection profile SSCD Smart card: Common criteria EAL5+ Smart card: FIPS 140-2 Level 3 Entrust and Identrust ready: available with DIGIPASS CertiID 3.2 and under certification 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 system supported	Microsoft® Windows® XP/Vista/ Windows 7 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.OX Citrix Presentation Server 4.5
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 <sup>2</sup> 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)

<sup>1</sup> Depend on the chip used.

<sup>2</sup> Interface available only on option.

**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 patented DIGIPASS®, DIGIPASS PLUS®, 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