

DIGIPASS CertiID 3.2

A strong authentication solution that combines PKI technology with One-Time Passwords (OTP) on a single device

DIGIPASS CertiID offers a solution to the growing authentication needs of banks, enterprises and governments. It combines PKI and OTP technology, allowing OTP to be used for remote access, desktop and application log-on, while PKI is used for disc encryption, data, e-mail and transaction signing. With DIGIPASS CertiID proven identity, privacy and non-repudiation issues are tackled.

Increased identity and data theft, man-in-the-middle attacks, 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.

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

DIGIPASS CertiID is a client-based software suite combining PKI-technology with OTP technology. In corporate environments DIGIPASS CertiID can be used to secure VPN access, lock computers, encrypt files and discs and sign e-mails or transactions. In banks, DIGIPASS CertiID can be used for the digital signature of high value transactions.

HOW DOES IT WORK?

DIGIPASS CertiID has been designed for users unfamiliar with PKI technology. DIGIPASS CertiID is installed on the PC of the end-user and is used in conjunction with a DIGIPASS KEY solution, the end-user authentication device. The DIGIPASS KEY product range is VASCO's offering of authentication devices which support PKI-technology.

When the end-user initially requests a certificate, a private key is stored on the smart card of the authentication device and can never be exported. A PIN code must be entered to activate the functionality of the device.

PRODUCT BENEFITS

Combines PKI and OTP technology

DIGIPASS CertiID allows a smooth migration from insecure static passwords to OTP and PKI. Financial institutions and corporations can choose between OTP and PKI functionality or migrate from one to the other. The combination of PKI and OTP on one platform allows companies to use OTP for specific applications (remote access, log-on to applications) whereas at the same time PKI can be used for other applications (document signing, file encryption, transaction signing).

Simple to deploy and maintain

The DIGIPASS CertiID Setup Builder allows customized set up: the user can install only those options he needs. An auto update function can be activated during installation. Support is provided through a troubleshooting and diagnostics tool. These features help IT-administrators with general maintenance.

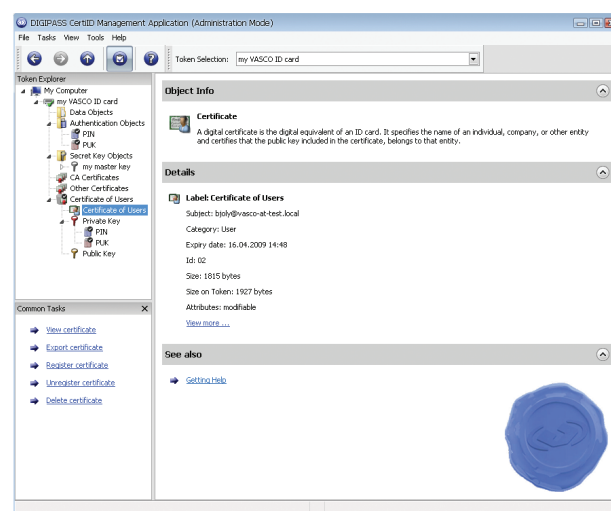
Furthermore, deployment can be done remotely and new security features can easily be added in a later stage, even after physical roll-out of devices to the end-users

Ease of use

Developed for users unfamiliar with PKI technology, DIGIPASS CertiID enjoys a high user acceptance. The GUI is designed with Windows Explorer look and feel and includes intuitive icons. Users are up and running in no time, resulting in no loss of productivity.

Offers compliance with financial regulations

DIGIPASS CertiID helps financial institutions to comply with data security regulations such as Sarbanes-Oxley Act, Basel II, HIPAA, and European e-signature regulations or guidelines.



FEATURES & BENEFITS

- One product supports multiple types of PKI and OTP and can be used with a multitude of Certificate Authorities, multiple card manufacturers and card operating systems
- Support of DIGIPASS KEY 860 and DIGIPASS KEY 200, encrypted mass USB storage capability
- Signing documents via digital signatures with Adobe, Microsoft office and Open Office
- Supports Microsoft Identity Lifecycle Manager (ILM /CLM)
- DIGIPASS CertiID management console for user and administrator to manage the smart card and their credentials
- DIGIPASS CertiID setup builder is available and allows automatic integration with third party product
- Online OTP time + event based are supported for all smart cards and USB devices
- Online and offline OTP activation, compliant with IDENTIKEY® Server 3.1 or VACMAN® Controller
- Active directory templates support the management and deployment of AAC policies
- Automatic setting for the user policies and Group Policy Objects
- Automatic software updates
- Troubleshooting and diagnostics with error reporting viewer

COMPLIANCE TO STANDARDS

Smart card	ISO 7816 3 –4
Smart card operating system	Card os 4.0 to 4.3b 32k-64k Startcos 3.1 72k
Java card	openPlatform 2.1.1 , java card 2.1 & 2.2 Oberthur platform 5.4 and 7.0
Smart card reader architecture	PC/SC, Pinpad Reader, contactless reader
Public Key Mechanisms	512-, 768-, 1024-bit and 2048-bit RSA, X509 v3 certificates EC-DSA (dependent on the card used)

Public Key Cryptography (PKI)	Microsoft® CAPI 2.0, SSL, S/MIME, IPsec/IKE. Microsoft® Crypto Next Generation and Key Storage Provider (KSP) and minidriver architecture. PKCS#11 v2.2, PKCS#1,7,8,10 and 12 PKCS#15
Hashing algorithm	SHA1, SHA256
One-Time Password	3DES, ANSI X9.9
Certification	Smart card: Common criteria EAL4+ and EAL5+, compliant up to Protection Profile SSCD smart card: FIPS 140-2 Level 3 Entrust ready Identrust compliant Vista smart card minidriver certified Windows 7.0 certified

SYSTEM REQUIREMENTS

Operating System 32-bit and 64 bit editions	Microsoft Windows 2000/XP/Vista, Windows 7.0 Windows 2003/2008 Server, Microsoft 2003/2008 Terminal Server, Citrix Presentation Server
Deployment System	Microsoft Systems Management Server, Microsoft Active Directory
Hardware	PC with 400 MHz or higher processor clock speed 256 MB of RAM minimum 100 MB of free disk space

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