

DIGIPASS CertiID 3.1

A strong authentication solution that combines One-Time Passwords (OTP), digital signatures, PKI and data protection on a single device.

Banks, enterprises and government agencies can now benefit from PKI technology when signing transactions and confidential documents. Encryption functionality ensures privacy and eliminates the possibility of repudiation. DIGIPASS® CertiID 3.1 software suite is compatible with all common PKI industry standards and can easily be integrated into an existing OTP-based strong authentication infrastructure. Combining OTP technology with PKI technology is possible with the DIGIPASS CertiID and doesn't make a difference to the employees.

FINANCIAL REGULATIONS

You've worked hard to gain your customers' trust. Identity theft or unauthorized access to confidential data can destroy that trust and damage your reputation. Increased data security regulations such as Sarbanes-Oxley Act, Basel II, HIPAA, etc. necessitate stronger information security solutions throughout the business community. DIGIPASS CertiID can help financial institutions comply with these regulations and reduce the administrative costs of PKI credential management.

DIGIPASS CertiID used in conjunction with the DIGIPASS KEY 1 enables e-signature compliant with European regulations. The combination of these two products is ideal for anyone who needs to prove their identity to another party. For e-government, this feature is invaluable for completing and submitting an electronic tax bill to the appropriate government agency. Thanks to DIGIPASS CertiID financial institutions can choose between OTP and PKI functionality on one single platform.

FUNCTIONALITY

When the user initially requests a certificate, a private key is stored on the smart card and can never be exported. Multiple logins (Web, Windows and Citrix) are secured, and e-mails or documents can be signed or encrypted. A PIN code must be entered to activate the functionality of the device. Transactions and VPN access can also be secured with the DIGIPASS CertiID solution.

New security features can easily be added. For instance OTP functionality can be added to deployed smart cards in a later stage and remotely.

EASY MIGRATION AND EASE OF USE

DIGIPASS CertiID provides a smooth migration from weak static passwords to digital certificates or OTP to provide stronger security. Smart cards are the most secure data containers known in the world. The installation wizard ensures a higher security level capable of strengthening your security policies and corporate rules within minutes.

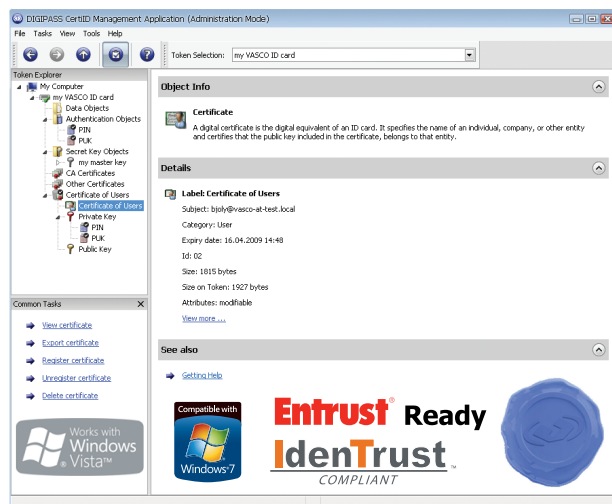
Developed for users unfamiliar with PKI technology, DIGIPASS CertiID enjoys a high user acceptance. The GUI is designed with the same look and feel of Windows Explorer and includes intuitive icons for each function. Users are up and running in no time, resulting in no loss of productivity.

AUTOMATIC UPDATES AND REDUCED HELP DESK CALLS

- Easy to maintain: DIGIPASS CertiID was developed with a built-in feature to ensure easy upgrades and support. An auto update function can be activated during installation. A troubleshooting and diagnostics tool is also included. These built-in tools will be valuable to your administrator for general maintenance during the life cycle of DIGIPASS CertiID.
- Reduced help-desk costs: DIGIPASS CertiID was specifically designed to simplify the complexity of PKI and the OTP initialization. This can be done remotely and the device can be distributed to end-users by post issuance. The distribution of smart cards, USB keys and their certificates as well as initialization and PIN/PUK management are facilitated by DIGIPASS CertiID 3.1.

LONG-TERM INVESTMENT

DIGIPASS CertiID belongs to a new PKI middleware generation. Microsoft CryptoAPI (CSP) or Crypto Next Generation (CNG) and PKCS #11 are supported. The flexibility of the software architecture simplifies adjustments to your specific environment, e.g. Vista with one click of a button. The product is suited for small and large deployments; it can be integrated into several environments or easily installed on a single PC.



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
- Assign and change a different PIN/PUK for each pair of credential keys
- Signing documents via digital signatures with Adobe, Microsoft office and Open Office
- Supports Microsoft Identity Lifecycle Manager (ILM /CLM)
- PKI Auto-Registration and Auto-Enrollment
- 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 supports to manage and deploy AAC policies
- Automatic setting for the user policies and Group Policy Objects
- Automatic software updates
- Troubleshooting and diagnostics with error reporting viewer

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

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

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 designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

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