DIGIPASS® 300

Secure Your Network Users' Identity with Strong Authentication and Digital Signatures.

The hand-held Digipass® 300 personal authentication device eliminates the weakest link in any security structure, the use of static passwords. Digipass generates a one-time password that enables you to identify customers and employees who are accessing your computer systems or networks. Digital signatures can also be generated to sign financial transactions. Most importantly, it provides secure access from any location.

Digipass® 300

Strong Two-Factor Authentication

The Digipass 300 solution is based on strong two-factor authentication. To gain access to applications and services you must have a Personal Identification Number (PIN), and a hand-held Digipass 300. The PIN code is entered into the Digipass 300 which then calculates a dynamic password. This one-time password enables authorized access into the network.

Intuitive User Interface and Advanced Design

Tough, shock-resistant materials and an expected battery-life of 7 to 10 years make the Digipass 300 a reliable part of any total enterprise security solution. Its ergonomic keypad and simple graphic interface are so easy to use, no technical training or User's Guide is needed. Universally recognizable display icons walk you through simple steps that always provide an option for going back or restarting from the beginning.

Maximum Flexibility

The Digipass 300 can be customized to your specific applications. Security parameters such as PIN length, number of PIN trials, type of cryptographic algorithm, lengths of challenge and response, are all programmable. Result: you get an optimum balance of user-friendliness, cost-efficiency and security.

Banking with Digipass

VASCO's Digipass 300 technology is used successfully in a wide array of application environments. For example, VASCO helps more than 170 financial customers around the world cost-effectively face the challenge of online banking and trading—without compromising existing infrastructures. Easy-to-use Digipass 300 solutions provide highly secure and totally reliable e-banking services via phone, fax, and PC / Internet. In the process, these institutions have increased their existing customers' loyalty while offering potential new customers the benefit of heightened security.

VASCO

SECURITY BEYOND e-MAGINATION

DIGIPASS® 300

Low Cost puts it at the Top of its Class

In the academic world, e-transactions usually concern an exchange of information, not money. Nevertheless, the importance of security must not be diminished. VASCO's Digipass 300 can provide educational institutions with highly secure solutions for guarding against breaches of confidentiality and unauthorized access to data. Further, VASCO's technology wins high marks for offering high functionality and flexibility at a low total cost.

Making Internet Transactions More Safe

Digipass 300 technology enhances the security of your Web-based services. Whether it is using Digipass 300 dynamic passwords to log-on to a restricted web site or create digital signatures to sign a financial transaction, you have greater control over who is trying to perform what activity.

Key Features

- Internal real-time clock
- Expected battery life of 7 to 10 years
- Intelligent battery management conserves battery life
- After programmed number of invalid PIN attempts, device locks automatically
- Remote de-blocking
- Limitation settings can be time-based or based on a maximum number of operations
- Dual function on-off / erase button
- Electronic signatures guarantee integrity of transmitted data
- Code-based optical programming / reprogramming is unique to every Digipass 300
- PIN is user-changeable
- Usage and length of PIN (up to 8 digits) is defined by System Operator

Digipass 300 Cryptographic Functions

- Conforms to the Data Encryption Standard (DES or triple DES)
- Supports programmable number (maximum 3) of applications (each application has different DES keys and parameters)
- Up to 16 digits of challenge input can be keyed in or optically read from any computer screen
- Responses are shown on the display in decimal or hexadecimal format (maximum length, 16 digits)
- A single check digit (according to ISO 7064-6) can be applied on the challenge and / or response
- Different functions can be assigned to each application:
  - Time-independent response calculation with external challenge (X9.9)
  - Time-based response calculation with external challenge
  - Event-based response calculation with external challenge
  - Time-based one-time password generation
  - Event-based one-time password generation
  - Time- and event-based one-time password generation

For regional offices or to learn more about us, visit our web site at www.vasco.com

VASCO

SECURITY BEYOND e-MAGINATION

AMERICAS HQ
VASCO Data Security, Inc.
1901 Meyers Road, Suite 210
Oakbrook Terrace, Illinois 60181, USA
phone: +1.630.932.8844
fax: +1.630.932.8852
e-mail: info_usa@vasco.com

EMEA HQ
VASCO Data Security nv/sa
Koningin Astridlaan 164
B-1780 Wemmel, Belgium
phone: +32.2.456.98.10
fax: +32.2.456.98.20
e-mail: info_europe@vasco.com

APAC HQ
VASCO Data Security Asia-Pacific Pte Ltd.
#15–03 Prudential Tower, 30 Cecil Street
049712 Singapore
phone: +65.232.2727
fax: +65.232.2888
email: info_asia@vasco.com