

DEP PCI

Hardware Security Module (HSM) Combines security and speed in an all-in product



DEP/PLATFORM INTEGRATING DEP/PCI

DEP SECURITY FOR A RANGE OF APPLICATIONS

The encryption processes performed by the DEP can be applied to a wide range of applications including:

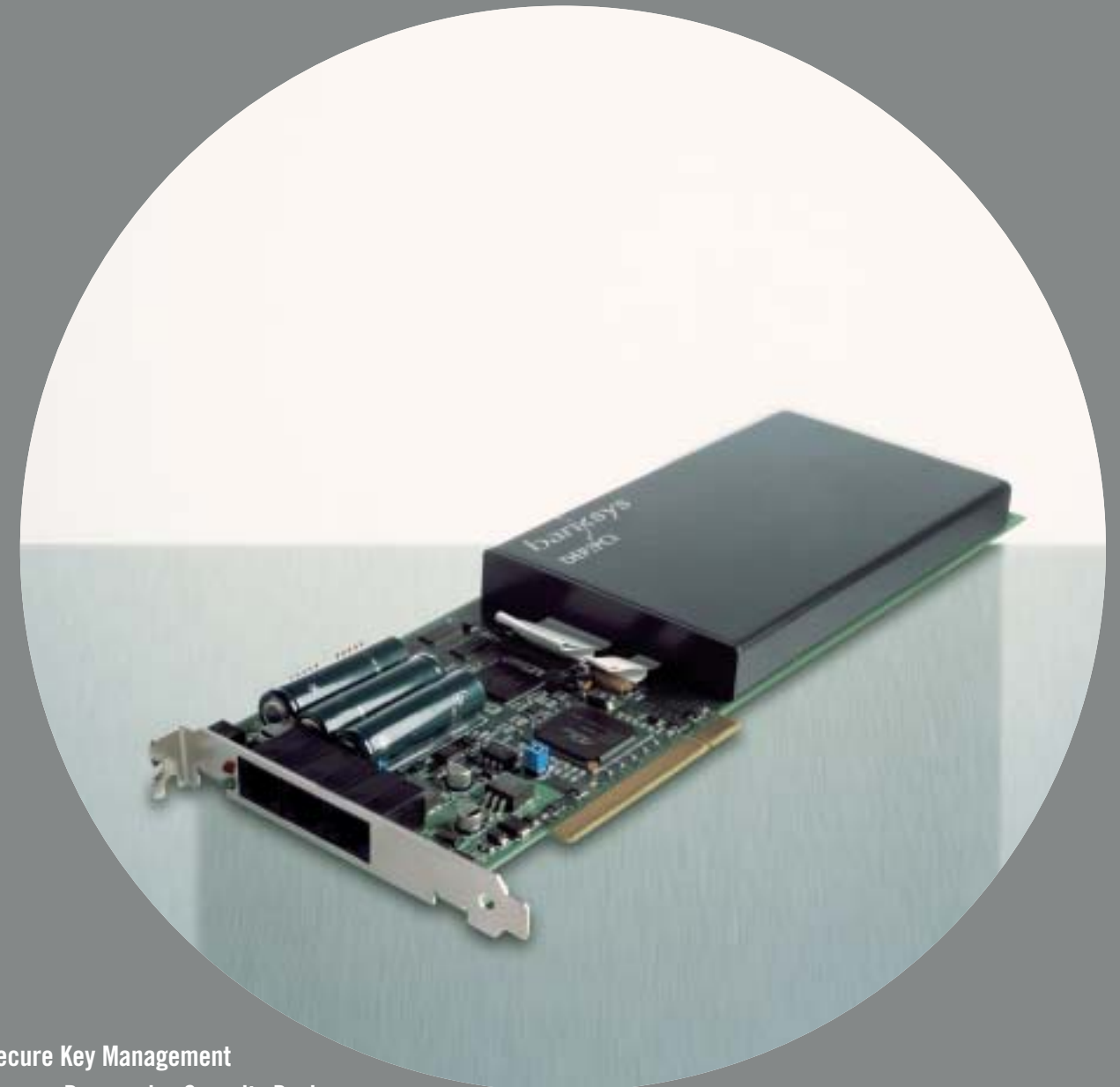
- EFT
- Electronic purse
- Secure card production
- PIN mailing
- Pay TV systems
- EMV
- Visa 3-D secure
- PKI (X509)

TECHNICAL SPECIFICATIONS DATA ENCRYPTION PERIPHERAL HOUSING

- Desktop or rack (standard 19 inches)
- Up to four DEP/PCI

INTERFACES

- Asynchronous on RS232
- TCP/IP over Ethernet (double)
- Multi-session



Haachtsesteenweg 1442 Banksys™ Chaussée de Haecht, 1442 - B-1130 Brussels, Belgium
Tel +32 (0)2 727 66 44 - Fax +32 (0)2 727 72 83 - sales.marketing@banksys.be - www.banksys.com



- Secure Key Management
- Tamper Responsive Security Device
- Common Criteria Certified
- Suitable for a large range of applications

banksys
end-to-end transactions

DEP/PCI

Banksys Data Encryption Peripheral (DEP) already provides 24/7 total network security for many of the world's leading financial institutions. Now Banksys engineers have taken this cutting-edge technology, condensed its functionality, and produced a single PCI board which can be installed in any server or PC running a Windows O.S. or Linux.



DEP/PCI is a cryptographic accelerator board providing functionality to load data (an application, application keys, application data) and to execute cryptographic operations. The confidentiality and integrity of all data in the DEP/PCI is physically protected by tamper resistant and tamper responsive hardware. Those data are also logically protected by only allowing well defined interfaces via access control mechanisms. Physically the DEP/PCI can be plugged into any platform that supports PCI cards. Application areas for DEP/PCI are endless: EMV, Visa, 3-D secure, e/m-commerce, Payment Systems, CA Solutions, Key Management Applications, PayTV access control systems and more. Custom solutions can be made available on request or developed by the customer using the DEP/PCI Development Kit. DEP/PCI offers high levels of physical security. The components handling the cryptographic processing are located in the tamper-resistant area of the board. Any drilling, electrical probing or chemical attacks will cause a critical alarm and instant erasure of all the data present in the protected area (application, cryptographic keys and application data). No plain text keys are exposed outside the tamper-resistant country.

THE DEP/PCI

A wide range of cryptographic algorithms are supported and others are available on demand. Besides the Banksys proprietary interface, PKCS#11 will be supported. Most popular EFT security protocols for PIN management are supported.

KEY MANAGEMENT TOOLS

All accesses to the device are subject to control and audit with only authorized users permitted access to the crypto module.

SECURE REMOTE MANAGEMENT

Efficient management and securing communications is a prime consideration to allow an enterprise wide security management.



DEP/PCI TECHNICAL SPECIFICATIONS

FEATURES

- Hardware accelerators for (3)DES & RSA
- Tamper-responding design
- On-board secure key generation and storage functions
- True random generator
- Secure code loading
- Suitable for high-security operations
- Key management via the C-ZAM/DEP and chip cards (DCC, DEP Control Card)
- Only authorized administrators can manage the card
- Secure life-cycle management from the factory to the operational environment
- Card can be configured in different operation modes (development, test or live)
- DEP/PCI development kit available
- Secure remote management

PHYSICAL CHARACTERISTICS

- Dimensions: Long format PCI card
- Operating temperature: 10° <-> 40°
- MTBF (estimated): 8 years

PHYSICAL SECURITY

The DEP/PCI detects tamper events like:

- Physical penetration
- Chemical penetration
- Removal of the protected area cover
- Unusual temperatures
- Unusual voltage
- Removal of the card from its PCI slot
- Unusual physical acceleration

The DEP/PCI logs all alarms and the alarm data are available either via the alarm interface (back plate), either via the standard command interface.

SUPPORTED HARDWARE PLATFORMS

- The DEP/PCI operates under multiple platforms where a PCI 32/64 bits bus slot is available. Drivers are available for Windows O.S. and Linux. Others on request.

SUPPORTED APIS

- Banksys API Suite
- PKCS#11 (planned)

SUPPORTED CRYPTOGRAPHIC ALGORITHMS

- DES (56 bit) / 3DES (112 & 168 bit) - ECB, CBC, CFB modes (ANSI X9.9, X9.32, X9.52)
- AES (128, 192 & 256 bit) - ECB, CBC, CFB modes
- SHA-1, SHA-256, MD5
- RSA up to 2048-bit key length (ISO/IEC 9796-1&2, PKCS#1)
- Elliptic curves
- Random number generation (meet the requirements listed in FIPS 140-2 Level 4 and the DIEHARD statistical tests)
- Key generation (symmetric & asymmetric)
- X509 certificate handling
- Ready to integrate customer specific cryptographic algorithms and protocols (by banksys or by yourself)

PERFORMANCE

- DES (single): 1,8 Mbits/sec
- AES (128 bit): 300 Kbits/sec
- RSA key generation (exponent: x'10001'):
 - 1024-bit key: 3" (average)
 - 2048-bit key: 10" (average)

CERTIFICATION

The card is evaluated according to the Common Criteria Evaluation Assurance Level EAL3+ (EAL4+ in progress).