nShield™

HARDWARE SECURITY MODULE

產品功能

FEATURE	BENEFIT
FIPS 140-2 VALIDATION	Independently certified secure management and storage of private keys
OFFLOAD OF CRYPTOGRAPHIC PROCESSING	Removes bottlenecks and frees your server to respond to more requests
SECURE EXECUTION ENGINE SUPPORT	Allows developers to protect application code within a secure cryptographic boundary
FAILOVER CAPABILITY	Transparently passes all of the processing activities to the next nShield if a device becomes unavailable while in service
ON-BOARD REAL-TIME CLOCK	Enables access to a secure time source
ADMINISTRATION OF KEYS CONTROLLED THROUGH THE USE OF SMART CARDS	Smart cards authenticate administrators to provide a highly flexible means of sharing responsibilities between individuals within the organization
KEYSAFE KEY MANAGEMENT SOFTWARE	Securely create, store, import, back-up, restore or remove application keys
nCIPHER SECURITY WORLD FRAMEWORK	A unique and highly secure key management framework, allowing the definition and enforcement of specific security policies
DEVELOPER SOLUTIONS	A set of comprehensive development tools and samples to enable quick development of secure applications.
ROHS COMPLIANT	As of July 1, 2006 this product complies with the Restriction of Hazardous Substances (RoHS) directive (2002/95/EC) of the European Parliament

產品規格

PRODUCT	CONNECTIVITY	NUMBER OF 1024 BIT RSA SIGNATURES PER SECOND*	FIPS 140-2 VALIDATION	SEE READINESS	ECC SUPPORT
nShield F2 500	PCI	500	Level 2	No	Yes
nShield F2 2000	PCI	2000	Level 2	No	Yes
nShield F2 4000	PCI	4000	Level 2	No	Yes
nShield F3 500	PCI	500	Level 3	Yes	Yes
nShield F3 2000	PCI	2000	Level 3	Yes	Yes
nShield F3 4000	PCI	4000	Level 3	Yes	Yes

技術規格

作業系統
- AIX, HP-UX, Solaris
- Linux
- Windows

Form Factor and Dimensions
2000/4000 F2, 2000/4000 F3
- PCI MODULE
- PCI Full Height PCI and 174.6mm length
- 66 MHz, 64 bits
- PCI 2.3 compliant
- PCI 2.1,2.2,PCI-X, PCI-Express

Operating Specifications
- Maximum power consumption for PCI: 2 amps at 5 volts
- Temperature: 10-35 degrees Centigrade
- Relative Humidity: 10-85% non-condensing

500 F2, 500 F3
- PCI MODULE
- PCI Full Height PCI and 167.6mm length
- 33/66 MHz, 32 bits
- PCI 2.3 compliant
- PCI 2.1,2.2,PCI-X, PCI-Express

Operating Specifications
- Maximum power consumption for PCI: 1 amps at 5 volts
- Temperature: 10-35 degrees Centigrade
- Relative Humidity: 10-85% non-condensing

認證
- FIPS 140-2 Level 3
- RoHS Compliant

應用程式介面(APIs)
- PKCS#11
- CSP for Microsoft CryptoAPI
- Java JCA/JCE CSP
- OpenSSL
- BHAPI
- 'nCore' API 'C' or Java
- CHIL

支援演算法
- SYMMETRIC CIPHERS
  AES – Rijndael
  Arc Four (compatible with RC4)
  CAST
  DES
  Triple-DES
- PUBLIC KEY CIPHERS
  DSA
  El Gamal
  RSA (up 4096 bits)
- KEY EXCHANGE
  DH
  DES / DES3 XOR
- HASH AND HMAC
  MD2
  MD5
  RIPEMD 160
  SHA-2
  SHA-1

其它
- SEE (Secure Execution Engine)
- ISO Smartcard Support
- Elliptic Curve ['ECC'] Activation
- Remote Operator

**http://www.ncipher.com/cryptographic_hardware/hardware_security_modules/8/nshield

nCIPHER™