THE DATA PROTECTION COMPANY

SafeNet iKey® 4000

PRODUCT BRIEF

Benefits

Compact and Convenient

iKey 4000 is small and rugged, with a tamper-resistant construction for extra security, making it easy to carry so users can always have their unique digital identities with them.

Easy to Deploy USBConnectivity

iKey 4000 offers the security of a smart card without the need for a smart card reader. Plus, there is no need to deploy and maintain costly smart card readers or special biometric devices to enhance your security applications— iKey offers smart card security without the headache.

Onboard Cryptographic Processing

Unlike other smart card or token-based authentication systems, the iKey 4000 offers onboard key generation and cryptographic processing to ensure that cryptographic keys and functions remain secure at all times in hardware. In fact, there is 64k available EEPROM for the secure storage of keys, passwords, certificates, application programs, and data.

Certifications:

- FIPS 140-2 Level 3
- RoHS
- China RoHS
- FCC Part 15 - Class B
- CE

SafeNet's industry-leading iKey 4000 is a USB-based portable PKI, two-factor authentication token that provides security for verification, signing ,and encryption.

Built with the most powerful cryptographic token technology available today, SafeNet's iKey 4000 USB Tokens contain 64K EEPROM to securely generate and store passwords, private keys, public certificates, and other data on a device small enough to fit on a key chain. iKeys ensure that only authorized users can perform the cryptographic functions. An extension of smart card technology, the iKey 4000 simply plugs into any USB port of a user's computer to provide strong user authentication without the need for costly reader devices.

The iKey 4000 is RoHS compliant, and is designed to support a wide range of desktop applications and portable systems. Its low-cost, compact design, and standard USB interface make it easier to deploy than other token options. FIPS Level 3-validated (in progress) hardware and on-board key generation, key storage, encryption, and digital signing add a higher level of security assurance to client applications.

RSA/DSA Key Generation

The integrity of public/private key pairs is fundamental to the success of any crypto system. Keys that are stored on a computer and protected only by software are vulnerable to hacking techniques and illicit "key-stealing" that can go undetected. Since SafeNet iKey 4000 USB Token perform all sensitive cryptographic functions directly on the token, unauthorized users have no way of accessing a user's digital credentials without stealing the token and guessing the pass phrase.

RSA/DSS Digital Signature

On-chip cryptographic functions allow users to produce either RSA (PKCS #1) or DSS (FIPS 186) digital signatures with confidence in the long-term secrecy of their private keys. Only iKeys can provide this lasting assurance in digital signature key sets.

RSA and Diffie-Hellman Key Exchange

No system is complete without support for the exchange of session encryption keys. SafeNet iKey 4000 USB Token include both RSA key unwrapping and Diffie-Hellman key agreement and key exchange functions. The private keys used for these exchange functions are never exposed to a vulnerable host system.

Secure

SafeNet iKey 4000 USB Token brings two-factor authentication to applications where security is critical. Unlike traditional password authentication that relies on weak, easily guessed passwords, iKey 4000 requires both a physical token (the iKey itself) and the user's PIN to complete the authentication process. This two factor authentication token is designed for all Public Key Infrastructure(PKI) environments, including both X.509 Digital Certificates and PGP. Data storage is split into two areas, one where digital certificates and public keys can be stored and the other houses private keys and other secrets. The private area has authenticated secure access and is held in an encrypted form. The iKey 4000 is capable of performing all private key, public and secret key cryptographic functions inside the token.

Technical Specifications

System Requirements

Operating Systems Supported:

- Microsoft Windows 2000
- MicrosoftWindows 2003
- Microsoft Windows XP
- Microsoft Windows Vista
- Apple MacOS 10.4.6 and above

Cryptographic Performance

- 1024-bit and 2048-bit RSA key operations

Key generation with key verification:

- Less than 20 seconds for 1024-bit
- Less than 90 seconds for 2048-bit

Digital signing — Less than:

- .45 seconds for 1024-bit
- 1.23 seconds for 2048-bit

Cryptographic APIs

- PKCS #11
- Microsoft CryptoAPI
- Microsoft PC/SC
- Apple Native PC/SC

Cryptographic Algorithms

Asymmetric Key

- RSA 1024-2048-bit
- Diffie-Hellman
- Symmetric Key
- 3DES
- AES 128, 192 25

Digital Signing

- RSA 1024-bit, RSA 2048-bit

Hash Digest

- SHA-1
- Additional algorithm support available

EEPROM Memory

- Capacity: 64K
- Read cycles: Unlimited
- Write/erase cycles: 500,000
- Data retention time: 20 years minimum

Physical Characteristics

Hardware System

- 64K memory

Connectivity

- USB 1.1/2.0 compliant
- 1.5 Mbits per second transfer

Regulatory Standards

- FCC Part 15 - Class B
- CE
- Custom brand graphics available

The iKey 4000 uses the SafeNet token operating system and the client software, which includes a token/key management utility that can be used to initialize the token, change passwords and labels, and control the logging and tracking information.

iKey4000	RSA1024	RSA2048	3DES (2Key)	3DES (3Key)	AES128	AES192	AES256
Key Generation (in sec)							
Low	7.19	14.49	1.73	1.75	1.73	1.75	1.78
High	33.65	229.03	1.75	1.78	1.76	1.78	1.80
Average	14.41	65.69	1.74	1.76	1.75	1.76	1.78
Sign/Verify (in bytes/sec)							
Sign	114.94	49.42					
Verify	281,938.33	158,102.77					

iKey4000	3DES_CBC (2Key)	3DES_CBC (3Key)	3DES_ECB (2Key)	3DES_ECB (3Key)	AES_CBC (128)	AES_CBC (192)	AES_CBC (256)	AES_ECB (128)	AES_ECB (192)	AES_ECB (256)
Encrypted/Decrypted (in bytes/sec)										
Encrypt	333.45	333.43	334.34	334.31	327.48	327.47	328.31	328.35	328.30	328.31
Decrypt	333.45	333.47	334.33	334.32	327.49	327.49	328.32	328.32	328.33	328.32

Flexible

SafeNet works with software and hardware vendors to ensure that the iKey 4000 USB Token offers the widest range of support for security solutions. iKey support is included in Single Sign-On login, VPN authentication, e-mail encryption, digital signatures, and many other PKI-enabled applications from leading vendors, such as Microsoft, Entrust, Computer Associates, VeriSign, and more. iKey 4000 supports PKCS #11, Microsoft CryptoAPI, Microsoft PC/SC, and Apple Native PC/SC for easy integration into custom applications.

Convenient

SafeNet's iKey 4000 USB tokens small size and rugged, tamper-resistant construction make it easy to carry so users can always have their unique digital identities with them. The iKey 4000 is a compact, two-factor authentication token that provides client security for network authentication, e-mail encryption, and digital signing applications.

The SafeNet Family of Authentication Solutions

SafeNet's suite of authentication solutions includes certificate-based, OTP, hybrid and software authenticators. All authenticators, together with SafeNet's extensive management platforms and security applications, empower you to:

- **Conduct business securely and efficiently** and open new market opportunities with innovative products that enable secure remote access and advanced security applications such as certificate-based authentication, digital signing and pre-boot authentication.
- **Reduce risk with** strong authentication solutions that prevent fraud and data theft and enable compliance to industry regulations.

To learn more about SafeNet's complete portfolio of authentication solutions, please visit our website at www.SafeNet-inc.com

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected