

Benefits

On-Board Crypto

RSA sign/decrypt 1024-2048
3DES encryption
AES 128, 192, 256 encryption
Diffie-Hellman key exchange
SHA-1 Digest functions

Key generation in Hardware

Enhanced Crypto Co-processor for improved performance and speed

64k Available EEPROM for secure storage of:

Keys
Passwords
Certificates
Application programs
Data

User PIN unblocking

Hardware and Software protection against differential power and timing attacks

Certifications:

FIPS 140-2 Level 3 (in progress)
Common Criteria EAL 4+ (in progress)
RoHS
China RoHS
FCC Part 15 - Class B
CE

Cryptographic APIs

PKCS #11 v2.0
Microsoft CryptoAPI (CAPI) 2.0
Microsoft PC/SC

SafeNet Borderless Security iKey 4000

The most advanced technology — from the most trusted partner!

Built with the most powerful cryptographic token technology available today, SafeNet's Borderless Security 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. SafeNet 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 USB Token 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 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 iKeys 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 passphrase.



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

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 iKeys 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's Borderless Security iKey 4000 brings two-factor authentication to applications where security is critical. Unlike traditional password authentication that relies on weak, easily guessed passwords, the iKey 4000 USB Token requires both a physical token (the iKey itself) and the user's PIN to complete the authentication process.

The iKey 4000 is capable of performing all private, public, and secret key cryptographic functions inside the token. Data storage is split into two areas — one to store digital certificates, and the other to store private and secret keys. The private area has authenticated secure access, and the data is held in an encrypted form. This two-factor authentication token is designed for all Public Key Infrastructure (PKI) environments, including both X.509 Digital Certificates and PGP.

The iKey 4000 uses the SafeNet token operating system and the Borderless Security 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.

Flexible

SafeNet works with software and hardware vendors to ensure that the iKey 4000 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. SafeNet Borderless Security iKey 4000 USB Token supports PKCS #11 and Microsoft CryptoAPI for easy integration into custom applications.

Convenient

SafeNet's Borderless Security 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.

Technical Specifications

System Requirements

- Operating Systems Supported:
 - Microsoft
 - Windows 2000
 - Windows 2003
 - Windows XP

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

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

Custom brand graphics available



Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524, Email: info@safenet-inc.com

EMEA Headquarters: Tel.: + 44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters: Tel: + 852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

www.safenet-inc.com

