SafeNet iKey® 4000

Our Most Advanced USB Authentication and Encryption Token Technology

Industry-leading two-fac¬tor authentication security for verification, signing, and encryption through AES-256 and FIPS 140-2 Level 3 authentication support.

Benefits

High assurance security

Onboard cryptographic processing

Easy to deploy USB connectivity

Easy to configure for multi factor authentication

Reduces costs compared other identification structures

Compact and convenient

Reduces administrative overhead

Certifications:
FIPS 140-2 Level 3
RoHS
China RoHS
Common Criteria EAL 2 (Chip only)
FCC Part 15 - Class B
CE

High Assurance Security

The SafeNet iKey 4000 USB Token brings two-factor authentication to applications where security is critical. Unlike traditional password authentica¬tion that relies on weak, easily guessed pass¬words, 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 X.509 Digital Certificates. Because it is FIPS Level 3-validated the iKey 4000 can also be configured to add a higher level of security by providing a third factor (biometric) authentication requirement.

Onboard Cryptographic Processing

The iKey 4000 is capable of performing all private key, public and secret key cryptographic functions inside the token. Keys that are stored on a computer and protected only by software are vulnerable to accidental loss and malicious acts that could result in unfortunate economic consequences to the enterprise. Since the SafeNet iKey 4000 USB Token performs all cryptographic functions directly on the token, the private keys used for these functions are never exposed to a vulnerable host system.

Additionally on-chip cryptographic functions allow users to produce either RSA (PKCS #1) or DSS (FIPS 186) digital signatures with confidence because the signing key cannot be tampered with by any software that could be running on the host computer. Similarly, security ¬for the exchange of session encryption keys is supported by the onboard cryptographic functions such RSA key un¬wrapping and Diffie-Hellman key agreement and key exchange.

Easy to Integrate and Deploy

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. Its low-cost, compact design and standard USB interface make it easier to deploy than cumbersome smart cards or one-time PIN tokens. The iKey 4000 is designed to support a wide range of desktop applications and portable systems, Custom application integration

is facilitated by cryptographic API support that includes PKCS #11, AES-256 encryption algorithm, Microsoft CAPI, Microsoft and Apple PC/SC.

Third Party Validation

SafeNet works with software and hardware ven¬dors to ensure that the iKey 4000 USB Token offers the widest range of support for security solutions. iKey support is included in VPN authentication, e-mail en¬cryption, digital signatures, and many other PKI-enabled applications from leading vendors, such as Microsoft, Entrust, VeriSign, and others. SafeNet iKey 4000 USB Token is FIPS 140-1, Level 3 validated and compliant with the European Union's Restriction on Hazardous Substances (RoHS), assuring it is free of lead and cadmium.

Token Management Platform

The iKey 4000 uses the SafeNet token oper¬ating system and the client software, which includes a token/key management utility that can be used to initialize the token, change pass¬words and labels, and control the logging and tracking information. SafeNet's Borderless Security (BSec) Middleware, SafeNet's identity management platform for quick, efficient, and effortless lifecycle management of tokens is easy to install and maintain. The user simply inserts the token, enters a PIN, and the Borderless Security software assumes all login and password management functions. The middleware includes a comprehensive SDK with PKCS#11 and Microsoft CryptoAPI that allows easy integration with third party applications for authentication, encryption, digital signing and verification functions.

Multi Factor Authentication

Implementing multi-factor authentication has been growing in popularity as organizations look to increase security and meet the demands of industry and government regulations that require protection of sensitive consumer and employee information. The iKey 4000 easily makes three factor authentication possible by integrating with third party biometric reader that captures the biometric such as a fingerprint and matches it to the stored biometric in the token. The iKey 4000 is then used to authenticate the user to verify his or her identity, and then provide the user with the authorization level to access specific resources and data.

Enterprise Data Protection

iKey two-factor authentication tokens are a key component of SafeNet's comprehensive enterprise data protection (EDP) solution to ensure compliance, reduce complexity and cost, and protect critical data against potentially devastating data breaches. SafeNet Enterprise Data Protection is the only complete end-to-end enterprise data protection solution that secures data at rest, data in transit, and data in use from the core to the edge — across endpoint devices, applications, networks, and databases.

About SafeNet

SafeNet is a global leader in information security. Founded 25 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung , Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service and scores of other customers entrust their security needs to SafeNet. In 2007, SafeNet was taken private by Vector Capital. For more information, visit www.safenet-inc.com/IAM

Technical Specifications

System Requirements

Operating Systems Supported:

- *Microsoft Windows 2000*
- *Microsoft Windows 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, 192 256*

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

SafeNet
The Foundation of Information Security

www.safenet-inc.com

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

PB-IKEY4000-2.27.09