

Benefits

Compact and Convenient

Although iKey 2032 is smaller than a stick of gum, it offers big security features. Its small size and rugged, tamper-resistant construction make it easy to carry so users can always have their unique digital identities with them.

Easy to Deploy USB Connectivity

iKey 2032 offers the security of a smart card without the need for a smart card reader. It features a built-in USB 1.1/2.0 port to easily connect to virtually any computer. 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 smartcard or token-based authentication systems, iKey 2032 offers onboard key generation and cryptographic processing to ensure that cryptographic keys and functions remain secure at all times.

iKey 2032

Personal USB Authentication and Encryption Token

iKey™ 2032 is a compact, two-factor authentication token that provides client security for network authentication, e-mail encryption, and digital signing applications.



The SafeNet iKey 2032 is a USB-based portable PKI authentication token that generates and stores a private key and digital certificate on a device small enough to fit on a key chain. An extension of smart card technology, the iKey 2032 simply plugs into any USB port and provides strong user authentication without the need for costly reader devices. The iKey 2032 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 cumbersome smartcards or one-time PIN tokens. Its FIPS Level 2 validated hardware and onboard key generation, key storage, encryption, and digital signing add high-assurance security to client applications.

Eliminates Weak Passwords with Two-factor Authentication

iKey 2032 brings two-factor authentication to applications where security is critical. Unlike traditional password authentication relying on weak, easily guessed passwords, iKey 2032 requires both a physical token (the iKey itself containing the user's unique PKI key) and the user's PIN to complete the authentication process.

Supported by Hundreds of Security Applications

SafeNet has worked with software and hardware vendors to ensure that iKey offers the widest range of support for

security solutions. iKey support is included in single sign-on/smartcard login, VPN authentication, e-mail encryption, digital signatures, and many other PKI-enabled applications from leading vendors like Microsoft, Entrust, Computer Associates, VeriSign, and more. iKey 2032 supports PKCS#11 and Microsoft CryptoAPI for easy integration into custom applications.

FIPS 140-1, Level 2 Validated Hardware Security

iKey 2032 is FIPS 140-1, Level 2 validated to offer high-assurance protection for applications that require high levels of physical and operational security. Compact and Convenient
Although iKey 2032 is smaller than a stick of gum, it offers big security features. Its small size and rugged, tamper-resistant construction make it easy to carry so users can always have their unique digital identities with them.

Technical Specifications

System Requirements

Operating Systems Supported
Microsoft Windows 95, Windows 98, Windows NT (SP4), Windows 2000, and Windows XP

Cryptographic APIs

- PKCS#11 v 2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC

Cryptographic Hardware Validation
FIPS 140-1 Level 2 validated —
Certificate No. 161

Cryptographic Functions

- Asymmetric key pair generation (RSA)
- Symmetric key generation (DES, 3DES, RC2)
- Hardware-secured key management and storage
- Onboard digital signing

Cryptographic Performance

- 1024-bit and 2048-bit RSA key operations
- Key generation: less than 90 second with key verification
- Digital signing: less than 1 second

Cryptographic Algorithms

Asymmetric Key Encryption

- RSA 1024-bit, RSA 2048-bit

Symmetric Key Algorithms

- DES, 3DES, RC2

Digital Signing

- RSA 1024-bit, RSA 2048-bit

Hash Digest Algorithms

- SHA-1, MD5

Additional algorithm support available

Physical Characteristics

Hardware System

- 8-bit processor
- 32K memory

Connectivity

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

Dimensions

15.875mm x 57.15mm x 7.9375mm

Regulatory Standards

FCC Part 15 - Class B CE

Custom brand graphics available.



Used by Many Security Applications Around the World

The iKey 2032 has been incorporated into many applications including single sign-on/smart card login, VPN authentication, email encryption, digital signatures, and many other PKI-enabled applications from leading vendors like Microsoft, Entrust, Computer Associates, VeriSign, and more. iKey 2032 supports PKCS#11 and Microsoft CryptoAPI for easy integration into custom applications.



Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 email: info@safenet-inc.com

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 3392 4600
Canada +1 613.723.5077
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538

Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (2) +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts)
+1 978.539.4800

U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)
+1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers
located worldwide.