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.

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 smart card or token-based authentication systems, the iKey 2032 offers onboard key generation and cryptographic processing to ensure that cryptographic keys and functions remain secure at all times.

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 smart cards 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 that relies 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/smart card 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 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.

SafeNet
The Foundation of Information Security

Technical Specifications

System Requirements
Operating Systems Supported:
- Microsoft Windows 95, Windows 98, Windows NT (SP4), Windows 2000, and Windows XP

Cryptographic APIs
- PKCS #11 v2.01
- 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 seconds 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
- 1.5Mbits per second transfer

Dimensions
15.875mm x 57.15mm x 7.9375mm

Regulatory Standards
FCC Part 15 - Class B CE

Custom brand graphics available

The iKey 2032 can be purchased as part of a complete solution with other SafeNet products:

SafeNet Axis, bundled with the iKey, provides strong authentication and Single Sign-On of usernames, passwords, and digital credentials stored on the iKey USB token. Easy to install and maintain, Axis fortifies security with two-factor authentication and automated enforcement of strong password policies. The user simply inserts the token, enters a PIN, and the Axis software assumes all login and password management functions.

SafeEnterprise™ SSL iGate is the leading SSL VPN appliance, providing secure remote access to sensitive data. The iKey 2032 enhances this security with two-factor authentication of the user's credentials. The iKey can store either the iGate password or a digital certificate—the user need only remember the PIN to unlock the iKey for simple and secure Single Sign-On to networks and 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	Japan +81 45 640 5733	U.S. (Minnesota)	U.S. (Torrance, California)
Brazil +55 11 4208 7700	Korea +82 31 705 8212	+1 952.890.6850	+1 310.533.8100
Canada +1 613.723.5077	Mexico +52 55 5575 1441	U.S. (New Jersey)	
China +86 10 885 19191	Netherlands +31 73 658 1900	+1 201.333.3400	Distributors and resellers
Finland +358 20 500 7800	Singapore +65 6297 6196	U.S. (Virginia) +1 703.279.4500	located worldwide.
France +33 1 41 43 29 00	Taiwan +886 2 27353736	U.S. (Irvine, California)	
Germany +49 18 03 72 46 26 9	UK +44 1276 608 000	+1 949.450.7300	
Hong Kong +852.3157.7111	U.S. (Massachusetts)	U.S. (San Jose, California)	
India +91 11 26917538	+1 978.539.4800	+1 408.452.7651	

SafeNet
The Foundation of Information Security