

SafeNet

iKey 1000 USB TOKEN

Workstation Security and Secure Remote Access

With the proliferation of remote access communication capabilities, incidents of unauthorized system access and theft of digital data are on the rise. Mobile workers accessing corporate resources, business partners accessing an extranet, or a home user shopping on-line have all become vulnerable. But unauthorized access isn't just a remote access problem; it is also prevalent at the desktop.

Benefits

Compact and Convenient

Although the SafeNet iKey 1000 USB Token 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

The SafeNet iKey 1000 USB Token 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 plug-and-play security without the headache.

Onboard Cryptographic Processing

Unlike other smart card or token-based authentication systems, SafeNet iKey 1000 USB Token offers onboard key generation and cryptographic processing to ensure that cryptographic keys remain secure at all times.

Security through Authentication

Most computers and networks use simple user names and passwords to protect themselves. But passwords alone do not provide adequate protection—they are easily shared or guessed. The SafeNet iKey™ 1000 USB Token was designed specifically as a portable and secure authentication token addressing the password replacement needs of both users and system administrators. For users, the SafeNet iKey 1000 USB Token is convenient and easy-to-use; simply plug it into an open USB port and enter the iKey's PIN. For system administrators, the SafeNet iKey 1000 USB Token is a powerful authentication device incorporating random challenges and real-time calculated responses, while shielding the user from the underlying process. The SafeNet iKey 1000 USB Token is a powerful, portable two-factor authentication device ideally suited for e-mail security, file encryption, Windows 2000/XP/2003 logon security, and iKey partner solutions.

The iKey

The SafeNet iKey 1000 USB Token was originally designed with the developer in mind. As a result, the SafeNet iKey 1000 USB Token has a robust and well-documented Software Developer's Kit appropriate for integrating the iKey into client/server and browser-enabled applications.

The SafeNet iKey 1000 USB Token's drivers and support software are modular in design allowing for no-hassle post-sales support.

What is an iKey?

An iKey is a USB device that provides cryptographic processing and secure storage for user credentials that enables strong authentication of users to desktops, networks and applications. Included are client middleware software and drivers that allow the iKey to be used on a large range of workstation models.



Solutions:

- Workstation
- File and disk encryption
- Web Access
- VPN
- PKI
- Network
- E-mail

For more information on how a SafeNet iKey 1000 solution can benefit your business, visit our Web site at www.safenet-inc.com, or contact a SafeNet office near you.

System Requirements

Operating Systems Supported

Windows 95 (OSR 2.5 or later) with MSCAPI and USB patches

Windows 98 or 98SE

Windows ME

Windows NT 4 Desktop (SP6a or later)

Windows 2000 Pro and Server (SP2 or later)

Windows XP Home and Pro

Windows 2003 Server





PKI Systems and Applications

iKey is supported by a wide range of security applications from many vendors, including:

Alcatel	BeTrusted
Computer Associates	Digital Signature Trust
Entrust	GlobalSign
IDCertify	iPlanet
Microsoft	Netscape
RSA Keon and Xcert	Secure Computing
Thawte	VeriSign



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

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
PB-IKEY1000-09.04.08

Technical Specifications

- iKey 1000 8K memory
- iKey 1032 32K memory
- PKCS #11 middleware (v2.01)
- Microsoft CAPI/CSP middleware
- Browser-based access to the iKey via ActiveX and Java components
- 1024-bit RSA (software)
- X.509 digital certificate storage
- MD5 hashing algorithm (hardware)
- Three security levels of file access
- Two-level file directory
- 64-bit unique serial number
- Application controllable LED
- USB 1.1/2.0 compliant
- USB communication speed at 1.5 Mbits
- Maximum power consumption at 28mA
- 3 second write time for a 4Kb file
- ISO 7816-4 compliant
- FCC/CE certified
- Microsoft PC/SC compliant
- Approved for Windows
- One year limited warranty

Applications

- Workstation security through Windows 2000, XP, and 2003 smart card support
- Integrated with Check Point™ VPN-1 Logon, partner solutions SecuRemote Software (iKey VPN solution series)
- email signing and encryption through Netscape Messenger and Microsoft Outlook Express
- PKI compatibility with MS Windows 2000/XP/2003, Netscape Navigator, and MS Internet Explorer

Software Interfaces

- Windows 95, 98, NT 4 SP4, 2000, XP, and 2003
- Delivered as Win32 DLL and ActiveX components for easy integration and post sales support
- Supports Visual Basic, C++, Java
- Component installer included
- API: PKCS #11, MS-CAPI/CSP, Microsoft PC/SC and iKey
- Royalty-free distribution license

SafeNet iKey 2032

Enterprise Grade USB Authentication and Encryption Token

The two-factor authentication token that provides client security for network and application authentication, e-mail encryption, and digital signing applications without the need for a smart card reader.

Benefits

Protects access to data and sensitive applications

Most advanced two-factor authentication

Portable and compact storage of digital credentials

Proven compliance with mandates requiring secure access

Reduces costs through single management platform and easy to integrate software developer kit

Onboard Cryptographic Processing

*Certifications
FIPS 140-1 Level 2
RoHS
China RoHS
FCC Part 15 - Class B
CE*

The SafeNet iKey 2032 USB Token is a portable USB-based PKI authentication token that generates and stores private keys and digital certificates on a 32KB storage crypto device small enough to fit on a key chain. iKey 2032's compact and rugged, tamper-resistant construction make it easy for the user to carry his digital IDs.

High-Assurance Security

SafeNet iKey 2032 USB Token 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 private PKI key) and the user's PIN to complete the authentication process. The iKey is FIPS 140-1 Level 2 validated hardware and offers onboard key generation, key storage, authentication, encryption, and digital signing functions which add high-assurance security to client applications such as Windows logon, VPN access, network authentication, digital signatures, file encryption/boot protection, and password management to name a few. These onboard cryptographic functions eliminate the risks associated with software based authentication such as accidental loss and malicious acts that could result in unfortunate economic consequences to the enterprise. Effective key management only goes as far as how well the cryptographic keys are protected. Protecting the keys within the secure confines of the hardware make it easy for only authorized administrators to securely generate, use and change keys, as well as archive them. Archived keys can be used for key recovery purposes and long-term data access—for example, if a user leaves an organization unexpectedly and administrators need to access the user's archived and encrypted information.



Easy to Integrate and Deploy

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. 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 2032 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, Microsoft CAPI, Microsoft and Apple PC/SC.

Third Party Validation

Extensive third-party validation for the iKey 2032 comes from customers, partners and recognized regulatory bodies, to ensure that the iKey 2032 offers the widest range of support for physical and operational security. Certification is important in the encryption world in order to provide assurance of security claims and help meet compliance requirements.

SafeNet iKey 2032 USB Token is FIPS 140-1, Level 2 validated and compliant with the European Union's Restriction on Hazardous Substances (RoHS), assuring it is free of lead and cadmium. iKey 2032 supports PKI enabled applications from leading vendors such as Microsoft, Entrust, Identrust and VeriSign.





Token Management Platform

The iKey 2032 requires installation of SafeNet's Borderless Security (BSec) Middleware, SafeNet's identity management platform for quick, efficient, and effortless lifecycle management of tokens. Easy to install and maintain, SafeNet Borderless Security fortifies security with two-factor authentication and automated enforcement of strong password policies. 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.

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:
- MS Windows 2000, 2003, 2008, XP and Vista
 - Apple Mac OS 10.4.6 (Tiger) and above

Cryptographic APIs

- PKCS #11 v2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC
- Apple Native 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)
- 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
- RSA 1024-bit, RSA 2048-bit
- Symmetric Key
- DES, 3DES
- Digital Signing
- RSA 1024-bit, RSA 2048-bit
- Hash Digest
- SHA-1

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
 - ISO 7816-3 compliant brand graphics available



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

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
PB-IKEY2032-10.16.08

SafeNet iKey® 4000

The Most Advanced USB Authentication and Encryption Token Technology

Industry-leading two-factor 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 to 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 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. 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. In addition, the embedded iKey 4000 chip is also common criteria certified.

Onboard Cryptographic Processing

The iKey 4000 is capable of performing all private and public key cryptographic functions inside the token. Cryptographic 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 as RSA key unwrapping 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 vendors 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 encryption, 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 140-2, 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 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. 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 readers 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



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

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
PB-IKEY4000-11.12.08

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
- Writet/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