The two-factor USB token 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 Identrust Compliant
- 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 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.*

The 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 makes 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. *The iKey 2032 also comes in a version that is certified by Identrust, marketed as the iKey 2032i.

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.

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

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.

The SafeNet Family of Authentication Solutions

SafeNet's suite of authentication solutions includes certificate-based, OTP, hybrid and software authenticators. All authenticators, together with SafeNet's extensive management platforms and security applications, empower you to:

- Conduct business securely and efficiently• and open new market opportunities with innovative products that enable secure remote access and advanced security applications such as certificate-based authentication, digital signing and pre-boot authentication.

- Reduce risk with strong authentication solutions that prevent fraud and data theft and enable compliance to industry regulations.

To learn more about SafeNet's complete portfolio of authentication solutions, please visit our website at www.SafeNet-inc.com

SafeNet®
The Foundation of Information Security

www.safenet-inc.com