

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.

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 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.

