

iKey 2000 Series – Smart Devices for Two-Factor Authentication

“Securing private keys and digital certificates”

For businesses seeking a highly secure way to authenticate users, Rainbow Technologies offers the iKey 2000 Series smart token and smart card solutions. Designed to support public key infrastructure (PKI) and digital signatures for legally binding electronic transactions, iKey 2000 Series products are portable devices that can effectively deter fraud and unauthorized access to confidential information.

iKey 2000 Series products are two-factor authentication solutions that help confirm a user's identity based on something the user *has* (an iKey) and something he or she *knows* (a PIN). The iKey 2000 Series is a PKI solution that provides secure storage for private keys and digital certificates. Digital signatures are processed within the iKey 2000 Series product, providing a very high level of security and control of private keys. Available in USB smart token and smart card configurations, the iKey 2000 Series supports international encryption and authentication standards for a wide range of global requirements. The iKey 2000 Series solution is ideal for secure authentication requirements such as e-mail, financial transactions and legal arrangements.

Unique product benefits:

- Securely generates and stores private keys within the iKey
- Digital signing process is performed inside the iKey, never compromising the private key
- Full PKI support including storage of key pairs and digital certificates
- Available in USB smart token or smart card form factor
- Highly robust and portable
- Protects private keys from virus infection
- Cannot be hacked
- Supports all major PKI cryptographic algorithms



Two-Factor Authentication: Creating Greater Assurance

Two-factor authentication is a security process that confirms user identities using two distinctive factors – something they *have* and something they *know*. By requiring two different forms of electronic identification, corporations reduce the risk of fraud and create greater assurance that the Internet is a safe place to do business.



The iKey 2000 smart token is a two-factor authentication product

iKey 2000 Series products are mobile two-factor authentication devices that provide the “something you have” portion of the two-factor process. A personal identification number (PIN) is required to use the iKey and satisfies the “something you know” factor. Only when a user has and knows both factors can an identity be confirmed and access granted.

Benefits of a two-factor system:

- Resistant to single-factor attacks including keystroke monitoring, social engineering, man-in-the-middle attacks, network monitoring, password cracking and IT staff abuse.
- Difficult for a user to deny involvement in a transaction because users are held accountable for all actions resulting from a successful user authentication.
- Less likely to lead to fraudulent or unauthorized access to corporate data.
- Easy for end-users to use.
- Durable and offers a long-term security solution.
- Easy to administer.

Smart Cards and Smart Tokens

Smart cards and smart tokens share similar underlying technology but rely on different form factors and equipment interfaces. The iKey 2000 Series includes a smart card and smart token authentication option. Both types of smart devices contain tiny computer chips that store information and can perform encryption tasks. Smart devices represent the most widely adopted form of two-factor authentication.

Smart Cards: First introduced in Europe in the 1970s, smart cards have found large international acceptance with more than one billion cards shipped annually. A smart card is a credit card-sized device with an embedded computer chip. A smart card must be inserted into a reader device for use. Smart cards are small, easy to transport and difficult to replicate. Smart card applications range from mobile phone identification to satellite television control. Internationally, banks have distributed smart cards to millions of customers to increase the security of credit and ATM cards. In Germany, 80 million people use smart cards to access Germany’s national health system.

Smart Tokens: Smart tokens are technologically identical to smart cards with the exception of their form factor and interface. Smart tokens are typically smaller than a house key and are designed to interface with the universal standard bus (USB) ports found on millions of computers and peripheral devices. USB-based smart tokens provide unique advantages in corporate IT environments. Smart card readers are not required because smart tokens simply plug into USB ports commonly found on most modern computer keyboards and on some monitors. Smart token drivers are installed on the client’s computer to interface with USB smart tokens – a much faster and less costly alternative to smart card readers. In addition, USB smart tokens are easy to use and designed to fit on a key chain. Studies have shown that when presented with a choice between a smart card or a smart token, 95% of users prefer the smart token.



Public Key Infrastructure: Protecting Electronic Transactions

Public key infrastructure brings the trust and security of the physical world to electronic transactions and communication. The flexibility of electronic messages brings both positive and negative consequences to the on-line world. The negative possibilities include the ease with which messages can be replicated and transmitted, leading to fraud. PKI enables positive consequences including the ability to easily encrypt, secure, track and decrypt messages, thereby counteracting fraud.



The iKey 2000 smart card securely stores private keys and digital certificates

Through strong encryption, asymmetric keys, digital signatures and trusted third-party verification, PKI meets the legal standards required to conduct verifiable and secure on-line transactions. Benefits include:

- Confidential communication: Only intended recipients can read files.
- Data integrity: Guarantees files are unaltered during transmission.
- Authentication: Ensures that parties involved are who they claim to be.
- Non-repudiation: Prevents individuals from denying involvement in a transaction.
- Authorization: When the above items are met, the user is authorized to carry out the transaction.

PKI creates a climate in which information piracy and fraud are absent and both parties accept legal standards. The iKey 2000 Series is under the users control at all times, is portable and requires a PIN number to activate or authorize a digital signature operation. PKI-based products such as the iKey 2000 Series are catalysts that will lead to greater acceptance of Internet-based products and services.

Public and Private Keys

PKI utilizes a key pair system of asymmetric keys that are mathematically related to each other and perform opposite functions. What one key locks, only its mate can unlock. The private key is created first. A one-way math function is applied to the private key to generate the public key. It is virtually impossible to determine a person's private key from his or her public key.

Private keys must be protected from compromise and are usually stored on physical devices such as smart cards or tokens. The iKey 2000 Series solution was designed as a secure storage device for private keys. Public keys, on the other hand, are made publicly available. Anyone wishing to send secure messages or transactions would use the recipient's public key as part of the encryption process. Encrypting something with someone else's public key ensures only that particular person's private key can decode the message.

Digital Signatures

When receiving an encrypted and/or signed message, it is important to verify that the sender of the message is who he or she claims to be. This is accomplished with a digital signature – a unique message-signing process that reveals the sender's identity and verifies the integrity of the message. Digital signatures are irrefutable, unique to each transaction and are virtually impossible to copy or transfer. Digital signatures are as legally acceptable as a handwritten signature on a contract.

Certificate Authorities

A certificate authority (CA) is a trusted third party – the electronic equivalent of a passport office. The primary purpose of a CA is to issue digital certificates that confirm the identity of the person associated with a certificate. CAs bring an added level of trust to PKI-based transactions.

Cryptology: Protecting Data via Encryption

Cryptology is the science of communicating and deciphering secret writings. Cryptology uses relies on ciphers to encrypt and decrypt data. The iKey 2000 Series allows cryptographic procedures to be performed on data, securing messages from eavesdropping and data theft.



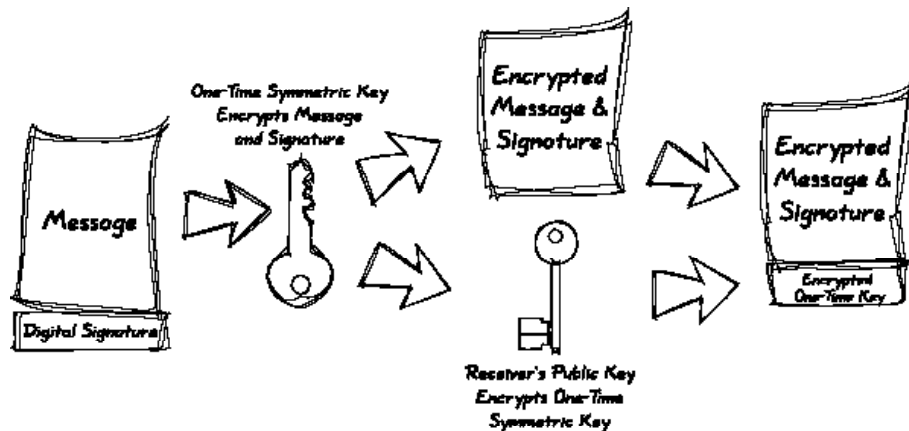
Ciphers

Ciphers are cryptographic algorithms that scramble data. The process used to secure a message depends on the cipher used. Clients and servers must use the same cipher for any given secure transaction. The cipher used in secure transmissions depends on a number of variables including the software used by both parties, corporate policy and government restrictions. For example, export laws limit the strength of a cipher that can be exported outside the United States. The iKey 2000 Series supports a large variety of ciphers including RSA, DSA, DES, Triple-DES, RC2, RC4, SHA-1 and MD5.

The iKey 2000 Series products encrypt messages, digital signatures and symmetric keys

The Encryption Process

When securely transmitting data, the iKey 2000 Series encrypts the message and its digital signature. The encryption involves a unique mathematical process that transforms data into a scrambled message that can only be unlocked with an encryption key.



The strength of the key depends on its number of bits. For example, a 20-bit encryption key has 1,048,576 possible variations. The advancement of computers has led to the need for higher-bit encryption. In the year 2001, the commercial standard for strong encryption is 128-bit which has 680,565,000,000,000,000,000,000,000,000 possible variations. Experts estimate that 2048-bit encryption will soon be the commercial standard, because existing supercomputers can break 1024-bit encryption in 20 years.

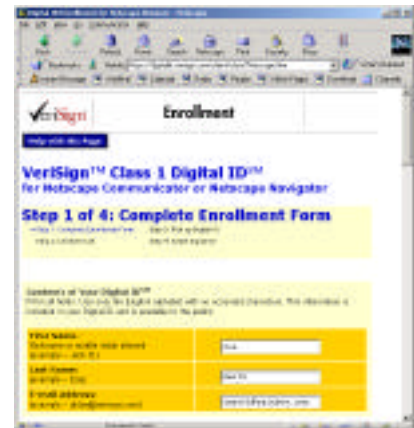
After the message and signature are encrypted, the decryption key must be securely transported. The key type used in message encryption is known as a *symmetric key*. The symmetric key is created for a one-time use and is able to lock or unlock a message. The sender and the receiver need the same symmetric key to encode or decode the message. If the symmetric key falls into the wrong hands, the message can easily be decrypted, compromising its privacy. PKI adds an extra layer of security by encrypting the one-time symmetric key with the receiver's public key so only the receiver can decode the symmetric key with his or her private key. The encrypted one-time symmetric key is appended to the encrypted message (see illustration above). The resulting encrypted message and key are transmitted to the recipient for decoding.

Digitally Sign and Encrypt Documents with the iKey 2000 Series

Initialization Process

The iKey 2000 Series initialization process creates the core components required to properly authenticate the user in future transactions. The user must first create a unique **PIN** to enable the iKey 2000. The next step is to register a **digital certificate**. Digital certificates can be provided by employers or issued through public certificate authorities (CA) such as VeriSign, Digital Signature Trust or WISeKey. The digital certificate will include data such as the user's name and address.

Once the initial certificate registration is complete, the CA will instruct the iKey 2000 product to generate a private and public key. The iKey 2000 releases the user's public key to the CA, which is used to generate the user's digital certificate. The digital certificate is downloaded and stored in the iKey 2000 Series product. Multiple digital certificates can be stored in a single iKey 2000 Series product.

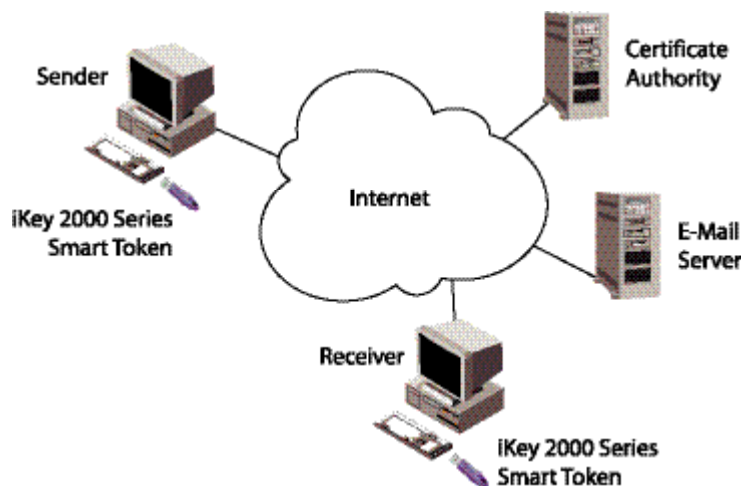


To enable third-party verification of users, a digital certificate must be created and posted at a CA

Signing and Encrypting a Message

An iKey 2000 Series user can easily sign and encrypt e-mails for private and secure transmission. The user simply plugs the iKey into his or her computer and opens the e-mail application. When the user finishes composing a message and attaching any files, he or she simply selects the "sign and encrypt" option in the e-mail application. The e-mail software will ask for the user's PIN to access the private key and digital certificate. Behind the scene, the e-mail program will create a message digest – an abstract representation of all the data contained within the message. The digest is transmitted to the iKey for digital signing and encrypting. The digital signature and the user's digital certificate are extracted from the iKey and appended to the message.

The e-mail software creates a one-time symmetric key and encrypts the message and the attached signature information. The one-time key is encrypted using the public key of the receiving party. This assures that only the receiver will be able to decrypt the key that will unlock the message. Once the receiving party decrypts the message, the sender's identity can be confirmed by verifying the sender's digital certificate with a trusted CA. The authentication process occurs behind the scenes.



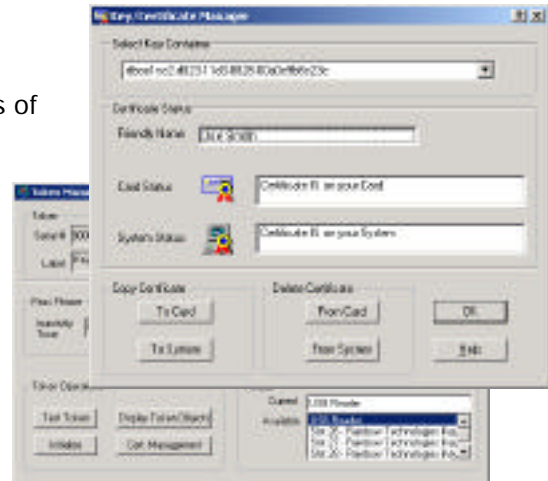
iKey 2000 Series Software

iKey Configuration Software

The iKey 2000 Series includes a certificate and token management application for managing important aspects of the iKey. The Certificate Manager application lists all certificates in the device. In addition, the certificate manager allows a user to name, copy or delete certificates.

The Token Manager performs a series of functions related to the operation of the smart card or smart token. Functions include:

- Setting the PIN
- Naming the token
- Setting the inactive timer and password
- Testing the token
- Formatting the token
- P12 import
- Certificate swapping



The Certificate Manager and the Token Manager allow a user to customize the iKey 2000 Series functionality

OS and Interface Support

The iKey 2000 Series solution is Windows 32-bit compatible and supports Windows 95, 98, NT, 2000 and Me¹. The smart device industry has standardized on specific interfaces to allow computer software to talk with smart cards and tokens. The interfaces provide standard methods for file management, creating key pairs and performing cryptographic operations.

The iKey 2000 Series supports the following interface standards:

- PKCS#11: The token interface used by most major PKI vendors including Netscape, VeriSign, Baltimore, Entrust and others.
- MS-CAPI: Microsoft's Cryptographic API, supported by Microsoft applications such as Internet Explorer, Outlook and Win2000 PKI services.
- PC/SC: The Personal Computer Smart Card interface is the standard smart card reader specification.



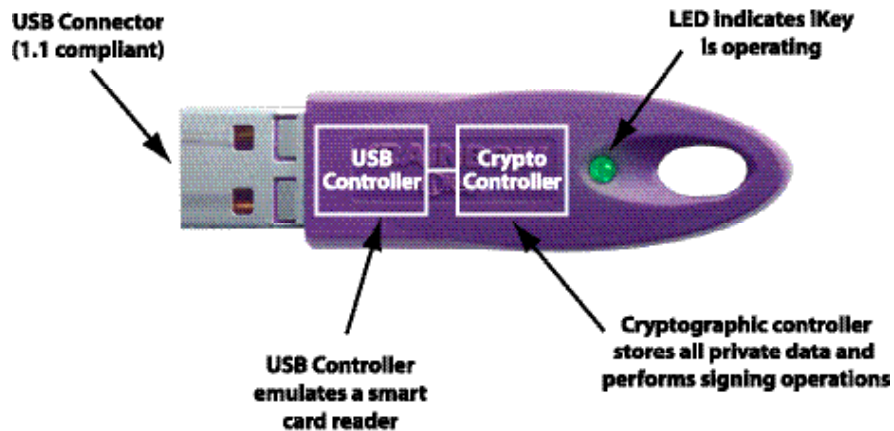
¹ Contact your sales representative for availability

iKey 2000 Series Family Overview

Rainbow Technologies iKey 2000 Series includes numerous models to meet a variety of security authentication needs for today and the future. Models vary based on storage, form factor and encryption strength capabilities. The iKey 2000 Series is based on two cryptographic controllers that offer highly reliable and internally secure storage capabilities from 8KB to 32KB and 1024-bit to 2048-bit encryption support for a wide range of requirements. Form factors include USB smart token and smart card.

iKey Product	Cryptographic Controller	Secured Storage	RSA Support
iKey 2000 USB Smart Token	Philips 858	8KB	1024-bit Encryption
iKey 2032 USB Smart Token	Philips 5032	32KB	1024-bit Encryption
Model 320 (iKey 2000 Smart Card)	Philips 858	8KB	1024-bit Encryption
Model 330 (iKey 2032 Smart Card)	Philips 5032	32KB	2048-bit Encryption

The USB smart token is USB 1.1-compliant device that supports transfer rates up to 1.5 MB per second. The on-board USB controller within the iKey 2000 Series smart token performs the same function as a smart card reader, converting data for use in the cryptographic controller



Cryptographic Controller

The iKey 2000 smart token and smart card have a dedicated cryptographic controller. The controller stores public keys, private keys, digital certificates, and performs all signing operations. Because all cryptographic functions are performed within the cryptographic controller, private keys are never exposed to the client computer, preventing hacking by malicious software. The cryptographic processor has a random number generator that creates cryptographic quality prime numbers for private key generation. In addition, the cryptographic controller can sense common attacks such as DPA, SPA, high/low voltage, high / low temperature and high/low frequency. The processor also checks itself during each operation to prevent spoofing and corrupt data. The iKey 2032 USB token and Model 330 smart card were designed for high security financial and government applications. Both models have received FIPS 140-1 Level 2 certification² and Model 330 has earned ITSec E4 High certified ASIC.

² Contact your sales representative for availability

iKey 2000 Series Specifications

Basic specifications:

- 8K or 32K secured storage, physical security at ASIC level
- iKey 2032 and 2032SC contains FIPS 140-1 level 2 certified ASIC and firmware, and an ITSec E4 high certified ASIC
- 8-bit processor
- PKCS #11 middleware (v2.01)
- Microsoft CAPI middleware
- Application controllable LED
- USB 1.1 compliant
- On-board 1024-bit RSA algorithm (iKey 2032SC also supports 2048-bit RSA)
- X.509 certificate storage
- On-board key signing – sub-one second
- High quality on-board cryptographic key generation – under 90s
- Windows 95/98/2000, NT4, Service Pack 4.0 or later
- ISO 7816-3 and -4 compliant
- FCC/CE certified
- Windows 2000 PC/SC compliant

Smart Card Reader Compatibility:

PCMCIA: Datakey DKR500 (SCM/SCR-201); Datakey DKR600 (Gemplus/GemPC400)

Serial: Datakey DKR510 (SCM/SCR-111); Datakey DKR610 (Gemplus/GemPC410)

USB: Datakey DKR630 (Gemplus/GemPC430)

PKI Solution Partners:

Alcatel
Ashley Laurant
Baltimore
Computer Associates
Cybertrust
Digital Signature Trust

Entrust
GlobalSign
IDCertify
Kyberpass
Netscape
PGP Security

RSA Keon CA
RSA SecurID
Secure Computing
Thawte
VeriSign
WiSeKey
Xcert

Applications:

Netscape Navigator and Communicator, Microsoft Internet Explorer and Outlook

Cryptographic Algorithms³:

RSA	DES	RC2	SHA-1
DSA	3DES	RC4	MD5



³ Expandable to support additional algorithms