

# iKey™ 2000 Series

Digital Signatures, PKI and Network Security



## Security Through PKI

### Security through Authentication

B2B, B2C, ASPs, online healthcare and other Internet-based technologies are enabling the electronic automation of business transactions and processes. However, many of these infrastructures are vulnerable—the security is based on traditional user name and passwords (weak security and expensive to maintain), or they store a digital identity on a computer's hard drive (non-portable and susceptible to viruses). Rainbow Technologies specifically designed the iKey 2000 series to be a secure, portable, two-factor authentication token. With two-factor authentication, the user requires two elements of identification – the iKey 2000 itself and the iKey's PIN.

For more information on how a Rainbow Technologies' iKey solution can benefit your business, visit our Web site at [www.rainbow.com/ikey/](http://www.rainbow.com/ikey/), or contact a Rainbow office nearest you.

The iKey™ 2000 series by Rainbow Technologies are powerful and portable two-factor authentication devices ideally suited for applications demanding high security. The iKey 2000 series specifically supports Public Key Infrastructure (PKI) needs by providing on-board cryptographic key generation, secure storage of X.509 digital certificates, PGP key pairs and performing digital signature signing operations on-board. The iKey 2000 series consists of USB smart keys and smart cards that are 100% compatible with each other.

### iKey 2000 Series Products

- iKey 2000; USB Smart Key, 8K memory
- iKey 2032; USB Smart Key, 32K memory
- Model 330 Smart Card, 32K memory
- iKey 2032 FIPS: USB Smart Key 32K memory (Black cover only)

### What is an iKey?

The iKey is a USB device utilizing a standardized interface included on all personal computers built since 1997.



# iKey 2000 Specifications

## Specifications

- iKey 2032 model is FIPS 140-1 Level 2 certified (Certificate No. 161)
- Model 330 Smart Card is FIPS 140-1 Level 2 certified (Certificate No. 94)
- 8-bit processor
- PKCS #11 middleware (v2.01)
- Microsoft CAPI middleware
- USB 1.1/2.0 compliant
- USB communication speed at 1.5 Mbits
- On-board 1024-bit RSA algorithm (Model 330 Smart Card also supports 1024-2048-bit RSA depending on reader environment)
- X.509 and PGP certificate storage
- On-board key signing – sub one second
- High quality on-board cryptographic key generation—under 90s
- Windows 95, 98, 2000, NT4 with Service Pack 4.0 or later
- ISO 7816-3 and 4 compliant
- FCC/CE certified
- Microsoft PC/SC compliant
- One year limited warranty

## 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 Systems and Applications

- Alcatel
- Baltimore
- Computer Associates
- Digital Signature Trust
- Entrust
- GlobalSign
- IDCertify
- Kyberpass
- iPlanet/Netscape RSA Keon CA and Xcert
- Secure Computing
- Thawte
- Verisign WISEkey

## Applications

- Netscape Navigator and Communicator, Microsoft Internet Explorer and Outlook
- Windows 2000 Smart Card Logon

## Cryptographic Algorithms

- RSA • DSA • DES • 3 DES • RC2 • SHA-1 • MD5
- Expandable to support additional algorithms



[www.rainbow.com](http://www.rainbow.com)

**Corporate:** 50 Technology Drive, Irvine, CA 92618 USA  
Tel: +1 949 450 7300 or +1 800 852 8569 eMail: [sales@rainbow.com](mailto:sales@rainbow.com)

**Australia**  
Tel: +61 3 9820 8900  
<http://www.rainbowaustralia.com.au>

**France**  
Tel: +33 1 41 43 29 00  
<http://www.fr.rainbow.com>

**India**  
Tel: +91 11 6917538  
<http://www.rainbowindia.co.in>

**Mexico**  
Tel: +52 55 5534 9600  
<http://www.rainbow.com/latinamerica>

**Brazil**  
Tel: +55 11 6121 6455  
<http://www.rainbow.com/brasill>

**Germany**  
Tel: +49 89 32 17 98 0  
<http://www.de.rainbow.com>

**Japan**  
Tel: +81 3 5642 7703  
<http://www.rainbowtech.co.jp>

**Taiwan**  
Tel: +886 2 2570 5522  
<http://www.rainbow.com/taiwan>

**China**  
Tel: +86 10 8266 3936  
<http://www.isecurity.com.cn>

**Hong Kong**  
Tel: +852 2333 6606  
<http://www.rainbow.com>

**Korea**  
Tel: +82 2 398 5879  
<http://www.rainbow.com/korea>

**UK**  
Tel: +44 1932 579200  
<http://www.uk.rainbow.com>