

iKey™ 3000 Series

Enhancing Security



Enhancing the Security of Public Key Infrastructure

Security through User Authentication

Internet based technologies are enabling the electronic automation of business transactions and processes. However, many of these infrastructures are vulnerable if they rely on traditional user name and passwords for authentication/logon. Not only are user names and passwords weak security, but they are also expensive to maintain and are unlikely to support accurate auditing information required for electronic transactions. PKI creates a further set of challenges; where to securely generate and store private keys and digital certificates and how to carry your identity from one system to another. To satisfy these requirements, Rainbow Technologies specifically designed the iKey 3000 series to be a secure, portable, two-factor authentication Smart Key that helps to confirm a user's identity based on: "**something the user has**" (an iKey) and "**something the user knows**" (a PIN).

Enhancing the security of PKI

The iKey 3000 easily integrates with all the major PKI systems adding two-factor authentication devices for storage of digital identities. iKey 3000 enhances the security of Public Key Infrastructure (PKI) systems and applications by providing on-board cryptographic key generation and secure storage for X.509 digital certificates. With iKey 3000, all the digital authentication and signing operations can be carried out on-board.

Ease of Use

- iKey 3000 Smart Key fits into any existing USB port - no need to carry around additional smart card readers
- Simply plug in your iKey and enter its PIN code to logon
- Users no longer have to memorize complex multiple passwords

The iKey™ 3000 is a powerful and portable two-factor authentication USB Smart Key that enhances the security of Public Key Infrastructure (PKI) systems and other high security applications. The iKey 3000 specifically supports PKI and digital signature needs by providing: on-board cryptographic key generation and secure storage of X.509 digital certificates with all the digital authentication and signing operations performed on-board.

Enhancing the security of Windows Authentication

The iKey 3000 seamlessly integrates with Windows® 2000 Certificate Services (PKI) and the Windows Smart Card Logon service enabling strong two-factor authentication that can be deployed for Windows 2000 services and applications:

- Secure user authentication to the Windows 2000 domain
- Secure user authentication for the Windows 2000 or XP client when disconnected from the corporate network
- Secure VPN client logon for remote access to corporate network
- Secure eMail signing with Microsoft Outlook
- eMail encryption with Microsoft Outlook

Enhancing the Security of Digital Signatures

The iKey 3000 can securely store three or more key pairs and support multiple PINs to fully meet the requirements of the EU Digital Signature Directive and German Digital Signature Law.



Benefits of Smart Key-Based PKI

Security Enhancements

- Password sharing between users is eliminated
- The iKey 3000 can perform on-token key pair generation and application signing
- The user's private key never leaves the iKey

Lower TCO

- No need to purchase or deploy additional reader hardware
- Decreases costs of Administration and Management of User passwords

iKey 3000 Specifications

Hardware—PKI

- On-token Cryptographic generator for fast RSA-based Key pair generation
- On-token key signing
- 32k bytes EEPROM (up to 20k bytes available for certificates and key storage)

Package Contents

- Two iKey 3000s
- CD-ROM with iKey 3000 drivers and documentation

Electrical

- ISO 7816-3 and 7816-4 compliant
- FCC and CE certified

Software

- AET Safesign Software
- Interfaces supported:
 - Microsoft CAPI (CSP)
 - PKCS#11 (V2.11), PKCS#12, PKCS#15
 - Microsoft PC/SC

O/S Support

- Microsoft Windows 2000
- Microsoft Windows NT (Rainbow USB drivers supplied on CD-ROM)
- Microsoft Windows ME
- Microsoft Windows 98
- Microsoft Windows XP Professional

USB 1.1 & 2.0 Compliant

- Windows Plug and Play supported

Applications

Microsoft Windows

- Secure user authentication for: Windows® 2000/XP Workstation to Windows 2000 domain, Network and VPN
- Secure eMail with Microsoft Outlook (signing and encryption)

PKI Systems and Applications

- Baltimore (SelectAccess, UniCERT)
- Cisco Systems (VPN Client)
- Checkpoint (Firewall-1 NG)
- Computer Associates (eTrust)
- GlobalSign
- NCP (VPN)
- NetScreen
- Netscape/iPlanet
- PGP
- RSA (SecurID, Keon)
- SafeNet
- Utimaco (SafeGuard)
- VeriSign and affiliates (Certificates)
- WiseKey (Certificates)



www.safenet-inc.com

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410.931.7500 or 800.533.3958 eMail: info@safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111

India +91 11 26917538
Japan +81 3 5719 2731
Japan(Tokyo)+81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore (1) +65 6274 2794

Singapore (2) +65 6297 6196
Taiwan +886 2 6630 9388
UK +44 1932 579200
UK (Basingstoke) +44 1256 345900
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500

U.S. (Irvine, California)
+1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers located worldwide.