

iKey™ 3000

Digital Signatures, PKI and Network Security Preliminary Document



Enhancing Security:

The iKey 3000 is a powerful and portable two-factor authentication USB token 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; secure storage of X.509 digital certificates and PGP keys; with digital authentication and signing operations all performed on-board. The iKey 3000 contains a highly secure processor chip and operating system that has been ITSEC E4 High certified.

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 token 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 Windows Authentication:

The iKey 3000 seamlessly integrates with both 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 client when disconnected from the corporate network
- Secure VPN client logon and RAS logon for remote access to corporate network
- Secure eMail signing with Microsoft Outlook
- eMail encryption with Microsoft Outlook

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.

Enhancing the security of Digital Signatures:

The iKey 3000 contains a highly secure processor chip and STARCOS® operating system that have been ITSEC E4 High certified together with the StarCert applications. In addition to the on-board key generation and authentication, 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.

Ease of Use:

- iKey 3000 token 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

Secure:

- 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

Return on Investment:

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

iKey 3000 package contents:

Five iKey 3000s
USB cable
CD-ROM with iKey 3000 drivers and documentation

iKey 3000 Specifications:

Hardware	
PKI	8-bit processor, ITSEC E4 High certified G&D® STARCOS® SPK 2.3 O/S, ITSEC E4 High certified with StarCert applications AET SafeSign On-token Cryptographic generator for fast RSA-based Key pair generation On-token key signing 32K bytes EEPROM (up to 20Kbytes available for certificates and key storage)
USB 1.1 & 2.0 compliant	Windows Plug and Play supported
Software Interfaces	
	Microsoft CAPI (CSP) PKCS#11 (V2.01), 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
Electrical	
	ISO 7816-3 and 7816-4 compliant FCC and CE certified

Applications:

Microsoft Windows:

- Secure user authentication for: Windows 2000 Workstation, Network, VPN and RAS
- Secure eMail with Microsoft Outlook (signing and encryption)

PKI Systems and Applications:

- AddTrust
- Alcatel (Timestep VPN)
- Baltimore (SelectAccess, UniCERT)
- Check Point (VPN)
- Computer Associates (eTrust)
- Digital Signature Trust
- Entrust (PKI)
- GlobalSign
- Kyberpass
- NCP (VPN)
- Netscape/iPlanet
- Network Associates (PGP)
- Novell (NMAS and GroupWise)
- RSA (SecurID, Keon)
- SecGo (VPN)
- Secure Computing (SafeWord)
- SSE/Guardeonic (TrustedMIME)
- Utimaco (SafeGuard)
- VeriSign and affiliates (Certificates)
- Vordel (TalkXML)
- WiseKey (Certificates)



www.uk.rainbow.com/ikey3000

4 The Forum, Hanworth Lane, Chertsey, Surrey KT16 9JX United Kingdom tel. +44 1932 579200 fax. +44 1932 570743

Rainbow Corporate
Rainbow Technologies, Inc.
50 Technology Drive
Irvine, CA 92618
Tel: +1 949 450 7300
Fax: +1 949 450 7450
www.rainbow.com

Germany
Rainbow Technologies GmbH
Streiflacher Str. 7
D-82110 Germering
Tel: +49 (0) 89 3217980
Fax: +49 (0) 89 32179850
www.de.rainbow.com

France
Rainbow Technologies
122, Avenue Charles de Gaulle
92522 Neuilly sur Seine Cedex
Tel: +33 (0) 1414 32900
Fax: +33 (0) 1462 47691
www.fr.rainbow.com

Additional offices in the United States, Australia, The Netherlands, China, India, Brazil, Japan and Taiwan. Distributors located worldwide.