

iKey™ 1000 Series – Smart Devices for Two-Factor Authentication

“A secure alternative to user names and passwords”

For businesses seeking a secure way to authenticate users, Rainbow Technologies offers the iKey 1000 Series smart token solution. Designed to overcome the limitations of traditional user name and password authentication methods, iKey 1000 Series products are portable devices that can effectively deter fraud and unauthorized access to confidential information.

iKey 1000 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 1000 Series provides secure storage of shared secrets used to authenticate the user to a server. Available as a USB smart token, the iKey 1000 Series supports international encryption and authentication standards for a wide range of global requirements. The iKey 1000 Series solution is ideal for secure authentication requirements such as remote access and secure system logons.

Unique product benefits:

- Replaces user name and password
- Securely stores the shared secret
- Stores shared secrets securely within iKey
- Connects to computers via a USB bus – a PC standard since 1997
- Highly robust and portable
- Supports all major PKI cryptographic algorithms
- Ideal for remote access and secure logons



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.



The iKey 1000 smart token is a two-factor authentication product

iKey 1000 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 an 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.

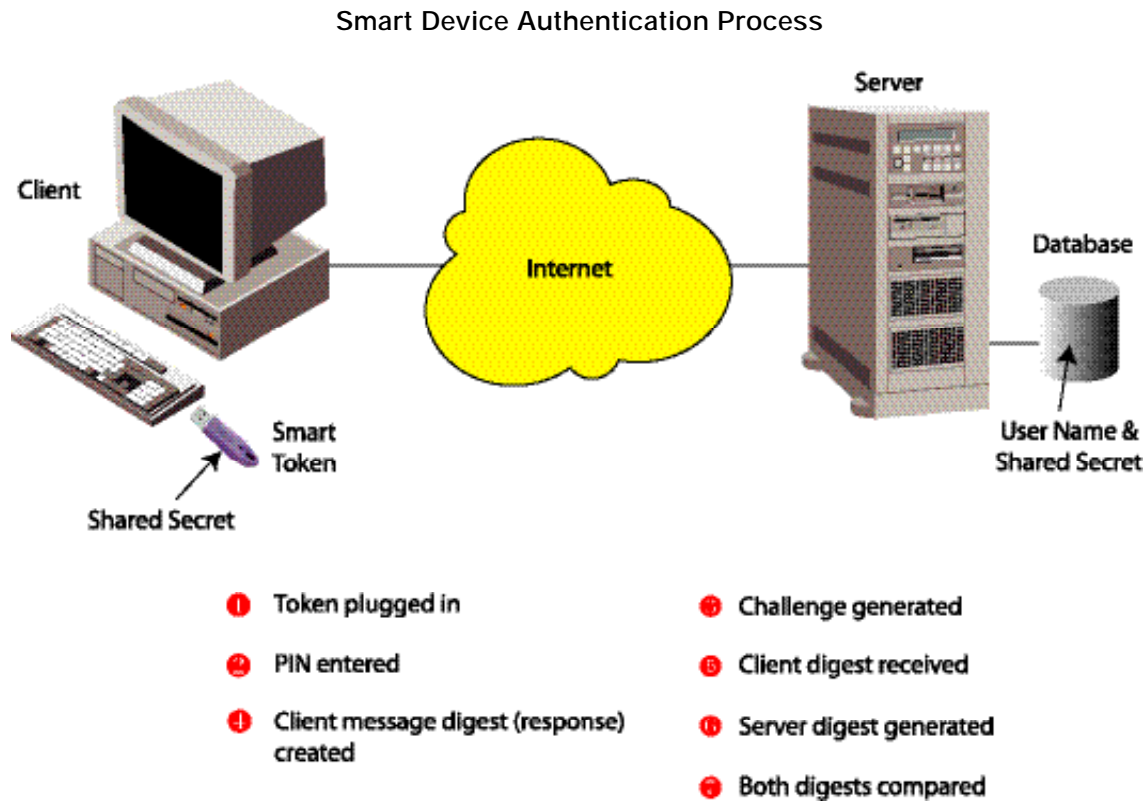
Smart USB Tokens

The iKey 1000 Series is a smart token that contains a tiny computer chip for securely storing information. 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 keychain. Studies have shown that when presented with a choice between a smart card or a smart token, 95% of users prefer the smart token.



How the iKey 1000 Works: Challenge and Response

When a smart token is initialized, a shared secret or key is generated from a server and placed in the token. The shared secret is an electronic piece of data that plays an important role in authenticating the user and is not known by the user. When the user receives the smart token, he or she activates it with a custom PIN. The shared secret stored within the token creates the first factor. The PIN creates the second factor. Authentication will only be granted when both factors are present.



The smart token authentication process begins when a user plugs his or her smart token into a spare USB port. This represents the first factor: something the user *has*. The second factor is accomplished when the user enters his or her PIN: something the user *knows*. Next, the server reads the user's unique token user name to determine if it is a known token. If the token is located within the server's database, the server then sends the client a random string of data as a challenge, designed to help authenticate the user's identity.

The client processes the challenge data with his or her shared secret – stored within the iKey – creating a message digest. The client digest, also known as a *response*, is then transmitted to the server. The server locates within its database a copy of the user's shared secret and uses the secret to process the challenge data it sent to the client. The resulting calculation is known as a *server digest*. If the client and the server digests match, the client is authenticated and access is granted.

Applications: Desktop Security and Remote Access

Desktop Security

To gain access to most computers, a user name and password must be entered. In a non-iKey environment, that information is transmitted over a network to a server that verifies the data and grants access. The problem with this traditional authentication method is that it is very easy to compromise the password. Keyboard monitoring, sharing passwords and network snooping are just a few of the threats to this type of system.



The iKey 1000 overcomes these limitations. User name and password, or a shared secret, can be securely stored within the iKey's private storage area, which is DES encrypted to block access to unauthorized parties. With an iKey 1000 solution, the iKey is inserted into the computer's USB port. At startup, instead of a user name and password, the user simply enters a PIN. The PIN authorizes the creation of a message digest using the shared secret located within the iKey. That digest is sent to the server for comparison to the server's digest. If they match, access is granted.

The advantages to iKey's desktop security application include:

- Secret never leaves the iKey
- Secret cannot be shared by user
- Secret is encrypted
- Secret is unknown to the user

Remote Access

Similar to desktop security, the iKey 1000 Series can be used to authorize remote access to the enterprise and prevent unauthorized users. Check Point™ VPN-1 SecuRemote™ and SecureClient™ are currently the only environments which are supported for secure remote access. With the iKey 1000 series software, integration can be done on additional remote access applications.

With an iKey 1000 Series solution, hacking into the enterprise can be reduced because:

- Users cannot share login data
- Access requires the presence of an iKey at all times
- Session information is only valid for a single session, minimizing the value of captured data

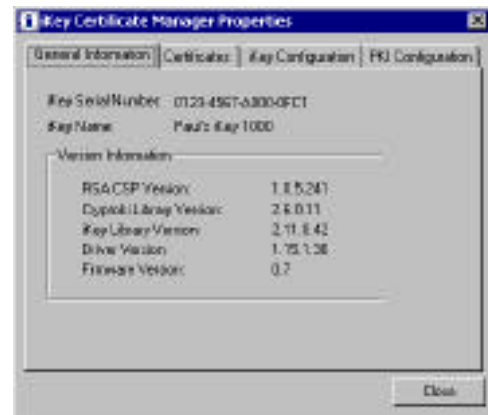


iKey 1000 Series Software

The iKey 1000 Series includes a certificate and token management application for managing important aspects of the iKey. The Certificate Manager application lists all certificates in the iKey 1000. In addition, the certificate manager allows a user to name, copy or delete certificates.

In addition, the iKey software performs a series of functions related to the operation of the smart token. Functions include:

- Setting the PIN
- Setting security officer PIN (management function only)
- Naming the token
- Testing the token
- Formatting the token
- Importing key pairs and digital certificates in PKCS#12 format
- User management of certificates and private data
- Selecting default Windows 2000 logon certificate (for Windows 2000 PKI)



The iKey software allows a user to customize the iKey 1000 Series functionality

OS and Interface Support

The iKey 1000 Series solution is Windows 32-bit compatible and supports, Windows 95, 98, NT, 2000 and Me. Macintosh is only supported through API. 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, and in some cases, creating key pairs and performing cryptographic operations.



The iKey 1000 Series supports the following interface standards:

- PKCS#11: The token interface used by most major PKI vendors including Netscape, VeriSign, Baltimore, Entrust and others.
- PKCS#12: Enables remote transmission and storage of key pairs and digital certificates into the iKey.
- 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.
- iKey API: Rainbow's iKey 1000 API allows file, directory and password manipulation within the token for custom applications.

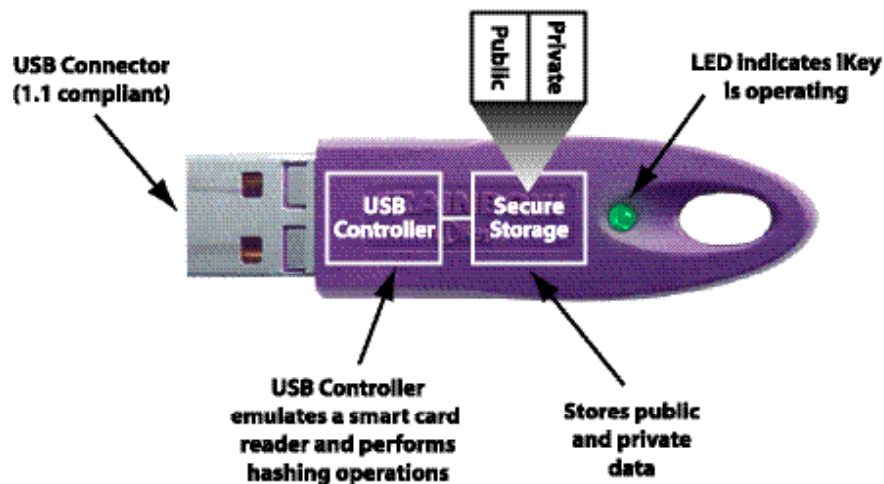
iKey 1000 Series Family Overview

Rainbow Technologies iKey 1000 Series includes two models to meet a variety of security authentication needs for today and the future. With highly reliable secure storage capabilities from 8KB to 32KB, software-based encryption support up to 1024-bit and a firmware based MD5 hashing capability, the iKey 1000 Series supports a wide range of requirements.

iKey Product	Secured Storage	Hashing Performed in Firmware	Software-Based RSA Support
iKey 1000 USB Smart Token	8KB	MD5	1024-bit Encryption
iKey 1032 USB Smart Token	32KB	MD5	1024-bit Encryption

iKey 1000 Hardware

The USB smart token is USB 1.1-compliant device that supports transfer rates up to 1.5 MB per second. The onboard USB controller within the iKey 1000 Series smart token performs the same function as a smart card reader, converting data for use in the controller. The USB controller also performs data hashing operations. The storage within the iKey 1000 is split between public and private storage. The private storage is a secure and encrypted place where shared secrets and keys can be stored. The public storage area is where certificates, cookies and other unprotected data can be stored.



iKey 1000 Series Specifications

Basic specifications:

- iKey 1000 8K memory
- iKey 1032 32K memory
- PKCS #11 middleware (v2.01)
- Microsoft CAPI/CSP middleware
- Browser-based access to iKey via Active X and Java components
- 1024-bit RSA (software)
- X.509 digital certificate storage
- MD5 hashing algorithm (hardware)
- Three security levels of file access
- Two-level file directory
- 64-bit unique serial number
- Application-controllable LED
- USB 1.1 compliant
- Low power USB device
- Write time for 4KB file = 3s
- Windows 95/98/2000/NT 4.0, Service Pack 4 or later
- ISO 7816-4 compliant
- FCC/CE certified
- Windows 2000 PC/SC compliant
- Approved for Windows 2000

Applications:

- Workstation security through Windows 2000 smart card logon, iKey-enabled partner solutions and Intel IPAA
- E-mail signing and encryption through Netscape Navigator and Microsoft Outlook / Express and Internet Explorer
- Secure Web access through Netscape Communicator and Microsoft Internet Explorer
- OPSEC certified with Check Point™ VPN-1 SecuRemote™/ SecurClient™ Software (iKey VPN Solution Series v 1.1.1CP)
- PKI compatibility with Windows 2000, Netscape Navigator and Microsoft Internet Explorer

The iKey 1000 Series Software 2.0: (optional)

Rainbow Technologies' iKey 1000 was originally designed with the developer in mind. Consequently, the iKey 1000 has a robust and well-documented Software Developer's Kit appropriate for integrating the iKey into client/server and browser-enabled applications. The iKey 1000's drivers and support software are modular in design allowing for hassle-free post-sales support.

Software Specifications:

- Windows 95/98/2000/NT 4.0, Server Pack 4 or later
- Delivered as Win32 DLL and ActiveX components for easy integration and post-sales support
- Supports Visual Basic, C++, Java
- Component installer included
- Middleware: PCKS #11 (128 bit), MS-CAPI/CSP (128 bit) and iKey Proprietary API
- Royalty-free distribution license

