

What is the iKey 1000?

The iKey 1000 hardware token is an integrated circuit housing a processor, non-volatile random access memory and a USB interface to a PC. The iKey 1000 is a memory token designed primarily as a password replacement device.

What is the difference between a memory token and a cryptographic token?

A memory token provides storage capability and an input/output interface. It does not have any hardware level cryptographic ability. A cryptographic token allows for the supported cryptographic algorithms to be performed on the hardware itself. An example of a cryptographic token is the iKey 2000. Cryptographic tokens are generally more expensive than memory tokens.

What is PKCS #11 and what is MS-CAPI and what are the differences between the two?

RSA Laboratories has developed, in cooperation with representatives of the industry, academia and government, a family of standards called Public Key Cryptography Standards or PKCS for short. PKCS #11 or “cryptoki” is designed to present to applications a logical view of the device called the “cryptographic token.” MS-CAPI is Microsoft’s Cryptographic API, also designed to isolate the application from the details of the cryptographic device. Most applications that support hardware cryptographic devices comply with one or both of these standards. As would be expected, all Microsoft products that support crypto tokens use MS-CAPI. Rainbow Technologies has both a PKCS #11 and an MS-CAPI interface that allows applications that support these standards to use the iKey 1000.

How do I integrate the iKey 1000 with my VPN solution?

Rainbow Technologies works with vendors to integrate the iKey with product offerings that will make it as seamless as possible to implement for end-users. However, some VPN solutions (for e.g. Windows 2000 VPN) allow for secure connections using public key cryptography. Since the iKey 1000 supports the two most common standards, PKCS #11 and MS-CAPI, in most cases it can be used with VPN software that support either or both of these standards.

With What VPN solutions is the iKey 1000 integrated?

The iKey 1000 is OPSec certified by CheckPoint to work with SecuRemote and VPN-1.

Does the iKey 1000 work with Windows 2000 logon?

Yes it does. Smart cards are a key component of the public-key infrastructure that Microsoft is integrating into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure e-mail.

Rainbow Technologies provides software that allows the iKey 1000 to be recognized as a smart card by Windows 2000 and used wherever a smart card can be used.

Does the iKey 1000 work with Entrust?

Yes. The iKey 1000 can be used to store an entire Entrust profile thereby giving users a portable, secure solution at a low cost. Rainbow Technologies has libraries that work with Entrust 4 and 5.

Can I store multiple key pairs on the iKey 1000?

The iKey 1000 has 8K of memory, which can be used to store multiple key pairs. The iKey1032 has 32K of total storage, although at present only 8K is available for certificate storage. The number of key pairs that can be stored varies on the size of the key pairs.

Can I delete a single certificate from the iKey 1000 without formatting the token?

Yes you can. This can be done either by software provided by Rainbow Technologies or through a capable browser such as Netscape or Internet Explorer. All certificates on the iKey can be displayed and deleted. However, in order to erase all the memory from the token, the best practice is to initialize/format the token.

I want to secure data on my desktop/laptop using a physical token. Does the iKey 1000 support this?

Yes. Rainbow Technologies has several solution partners that offer different forms of security solutions. Our partner page on the Rainbow Technologies web site (<http://www.rainbow.com/partners>) has more information. Solutions include log-on security using the iKey as a password replacement and file encryption using the iKey as a secure key container.

Can I send secure e-mail with a digital ID on my token? What, if any, additional software do I need?

Yes you can. Any e-mail client that supports S/MIME can send and receive secure e-mail over the Internet. Rainbow Technologies provides libraries that support the PKCS #11 (cryptoki) and MS-CAPI standards. Any e-mail client that works with either of these two standards can use the iKey 1000 to send signed e-mail. All Microsoft applications use MS-CAPI. Netscape Messenger uses PKCS #11.

What platforms does the iKey 1000 support?

The iKey 1000 works on Windows 95, Windows 98, Windows NT and Windows 2000. Since Windows NT does not inherently support USB, Rainbow Technologies uses a USB stack on top of which we have built an iKey class driver that enables the iKey to be recognized by NT. On Windows 95 only the version that supports USB will work with the iKey.

What do I need to do to enable Microsoft programs to use the certificate on my iKey?

The certificate must be registered in the Microsoft certificate store. Certificates requested by Internet Explorer will automatically be registered.

I obtained a certificate using my Netscape browser, but I cannot sign my mail through Outlook. Why?

Certificates requested via Netscape Communicator will have to be registered on the system. This will enable all Microsoft applications to use the key pair on the iKey. This is due to the fact that Netscape uses PKCS #11 whereas Microsoft applications use MS-CAPI. Rainbow Technologies provides utilities that will register the certificates on the iKey to the system.

Does the iKey 1000 work in a terminal server environment?

There is no solution yet that works directly with a terminal server. Rainbow Technologies has partners that have applications to allow secure, encrypted client server communication in a terminal server environment using the iKey. Please refer to the partner page on Rainbow's website.