

HardKey/EG Pro - unique data security architecture



- NEW - Easy to use data encryption device
- Single PC - Multi User Support
- Windows Compatible Software
- Screen Saver Function
- Lock Out Function - internet, files, directories, disk drives or the entire PC

HardKey™ is an innovative new, personal data security solution, combining *MS Windows compatible software with a USB hardware "key" which provides powerful data encryption, transparent to the end user. **HardKey™** requires no password and is easy to use.

What is **HardKey™**?

HardKey™ is a small USB device which will fit on any keyring with your keys. All encryption information is tamperproof, stored digitally on the **HardKey™**, only accessible via **HardKey™** Administrator software.

Easy to use

Load the software, plug in the USB "key", select the files you wish to protect and encryption is just a mouseclick away. It's as easy as using *WinZip! **HardKey™** controls access to your data - remove the key and your files can no longer be accessed. Plug in the key and **HardKey™** takes care of decryption, on the fly as you open your documents.

Security

All encryption/decryption information is safely held on the key, so even if your PC is stolen your data remains secure. **HardKey™** is ideal for industries where information is an asset, eg government, military and law enforcement agencies research, customer databases; or portable users where transportation increases the risk of theft.

File Transfer

HardKey™ is network and internet friendly and incorporates Public Key/Private Key technology for secure transfer of information. Share your Public Key signature with other **HardKey™** users, safe in the knowledge that your Private Key details remain confidential. When you're ready to encrypt data to send to other **HardKey™** users, their Public Key information is used in the encryption. Files transfer is entirely secure, as only the matching Public Key holders can open it.

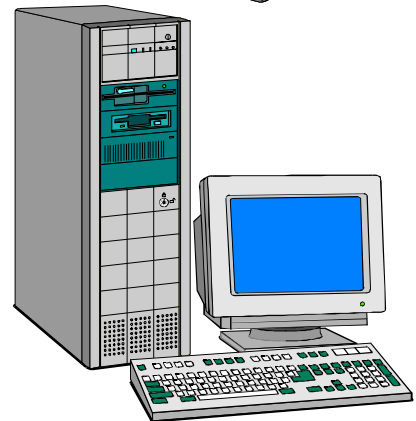
Multiple Users

Multiple keys can be used on the same PC - **HardKey™** is the answer for modern "hot desk" offices. **HardKey™** can also be used to 'lock out' access to the Internet, applications, directories, disk drives or other peripherals.

One Size Fits All

HardKey™ has been designed for all computer users, small business, corporate and home use, with powerful Administrator functions for both a single PC or multi-user network. Administrator functions include: selection of encryption algorithms from six popular standards depending on speed and complexity; lockout of peripherals and autologon to *MS Windows; user management on an individual PC; and the ability to recreate a lost or damaged **HardKey™** USB device.

*WinZip & MS Windows are Trade Marks of Microsoft Corporation





HardKey/EG Pro
Actual Size



unique data security architecture

How does **HardKey™** Work?

The **HardKey™** system incorporates both software and hardware, providing a superior solution to data security as it requires both to encrypt and decrypt information. When **HardKey™** software encrypts a file, it references the key information from the **HardKey™** USB device for file "ownership" and access information, and includes this in the encryption. Vital details of the encryption process are retained on the **HardKey™** USB device and without it, decryption is impossible.

HardKey™ combines three wellknown means of data security in one user-friendly application: software encryption, token-based identification and public/private key technology to ensure your peace of mind and complete safety for your files.



Software Encryption

Since man has been able to write, encryption of one form or another has been used to protect sensitive information or guarantee the authorship of documents, from the basic alpha-numeric substitution to highly sophisticated single-use systems used by intelligence in World War II. Software encryption alone is vulnerable to "brute force" attacks. Technological advance has made all but the most complex encryption algorithms breakable: codes which might have taken a lifetime of manhours to break manually via traditional means can be broken in a matter of minutes by a powerful PC running the appropriate software. **HardKey™** offers a range of high level industry standard encryption algorithms and the added security of a USB hardware "key".

Technical Specification

Dimensions:

- 54 x 15 x 7 mm
- (including hook for keyring)
- Fits all standard PC USB ports.

Minimum Configuration:

- Pentium PC
- 32 Mb RAM
- 10 Mb disk space*
- MS Windows 98 SE

Recommended Configuration:

- Pentium PC
- 64 Mb RAM
- 20 Mb disk space*
- MS Windows 2000 or higher

* These figures are intended as a guide only - disk space requirement is directly related to the size of the file to be encrypted.

Encryption Standards:

- RC5 - RC6
- TDES - DES
- IDEA - TwoFish

Token-Based Identification

Many proprietary data security devices are "tokenbased", where a hardware "key" contains identification details and controls access to specific PC applications and peripherals. Key details may be stored on a swipe card or plugin device of some sort (a "dongle"), and are "matched" against a file on the PC to allow access. Token-based security systems can usually be bypassed, since they are reliant on a file held somewhere on the PC itself. **HardKey™** USB hardware device operates as a token - when you plug it in it identifies the individual user and grants access privileges. However, **HardKey™** goes beyond the average token-based security system, as the **HardKey™** USB device is essential to software encryption operations.

Public/Private Key Technology

Public/Private Key Systems (PKI) are standard for secure transfer of encrypted files, across local area networks or the internet. In a PKI system, two key files are generated for the user - a Public Key and a Private Key. Private Keys contain password and identification information about the individual user, and are kept private. Each individual Private Key has a corresponding Public Key which may be shared with other users as they are referenced in the encryption process to grant another user access to an encrypted file - a kind of addressee list to the encryption. **HardKey™** stores the individual's Private Key information digitally on the USB device itself, in tamperproof format. The Public Key is a 2K file, stored on the hard disk and easy to share with other **HardKey™** users. When encrypting a file to be sent securely to another **HardKey™** user, their Public Key information must be included in the encryption or they will not be able to open it. Public Keys may be safely shared - they're ASCII files, and it's impossible to obtain a corresponding Private Key from them. Since **HardKey™** PKI key feature guarantees the identity of both sender and recipient, it can also be used as a digital signature.

Industry Standard Encryption

HardKey™ offers a range of industry standard software encryption algorithms up to 256-bit encryption. The user can select whichever they prefer, according to the level of security required and time available - some algorithms may take longer to encrypt and decrypt than others, which may be significant with larger file sizes. For added security, you can compress the encrypted file with proprietary software, and then re-encrypt it, using a different algorithm - nested encryption in "Russian Doll" fashion. The exact method of nesting and series of algorithms used is unimportant: **HardKey™** records all the details within the encrypted file, and decrypts it transparently as the file opens. It is very important to decrypt any encrypted files before you uninstall the **HardKey™** software as the files cannot be decrypted after the software and hardware are gone.

Creating a Personal Hardkey

The USB **HardKey™** device ships blank, ready for personalisation with **HardKey™** Administrator software. All you need to activate the **HardKey™** is your name, a password and your eMail address which is stored on the device itself. The **HardKey™** Administrator should keep a copy of each user's key information in a safe place, to replicate a lost key.