

CyProtect Drive Encryption

Drive-Encryption with 512 Bit PMC

Secure ♦ Easy ♦ Fast

Secure with polymorphic encryption
„Made in Germany“

Easy through intuitive and simple user interface

Fast without loss of Security

How do you secure your confidential data on your PC or Laptop from unauthorized access? Do you rely on simple password protections of conventional office products? Or do you count on single files security with the time consuming and annoying cycle „Decryption - Using - Encryption“?

You can only reach efficient working by using of a totally encrypted volume, which can be integrated into the file-system of a PC, if needed.

CyProtect Drive Encryption offers the creation of encrypted container-files, which can be used like normal drives of the system.

Instead of entering a password there can be used **CyProtect Key Administration** with a SafeNet iKey (USB-Token) to store the secret.

The encryption method in use is the sophisticated Polymorphic Cipher (short **PMC**) with 512 bit key length. PMC is based on a self-modifying code and holds against all sorts of known hacker attacks. The algorithm was developed and patented in Germany and is working much faster as normal available encryption methods.

Highlights

- ✓ Easy installation and handling
- ✓ Encrypted drives > 2 GB possible
- ✓ Fast, even on older hardware
- ✓ Network-compatible (container files on network drives)
- ✓ Secure encryption without masterkey
- ✓ Integration with SafeNet iKey (optional)
- ✓ 512 Bit polymorphic algorithm (PMC)
- ✓ Optional also AES/Rijndael (256 bit)

Requirements

- x CPU: Intel x86 or compatible
- x Operation system: Microsoft Windows 2000/XP

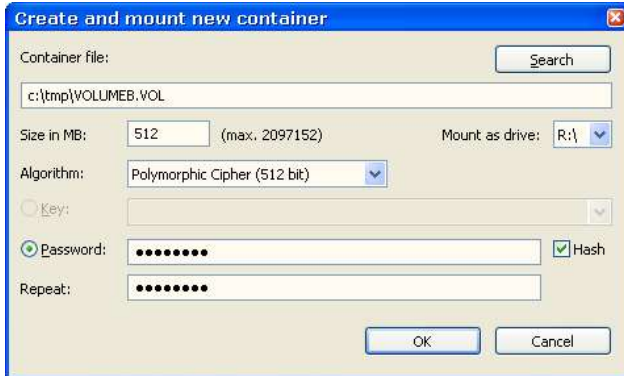


CyProtect AG

A company of IT & More GmbH
Schatzbogen 58
D-81829 Munich
Phone: +49 (0)89 420447-0
Fax: +49 (0)89 420447-79
E-Mail: info@cyprotect.com
Internet: www.cyprotect.com

-CyProtect-

Internet Security



With few mouse clicks and a password (or iKey) you can create a virtual drive.

Your data is saved into a container file, which is connected to the system as a normal volume.

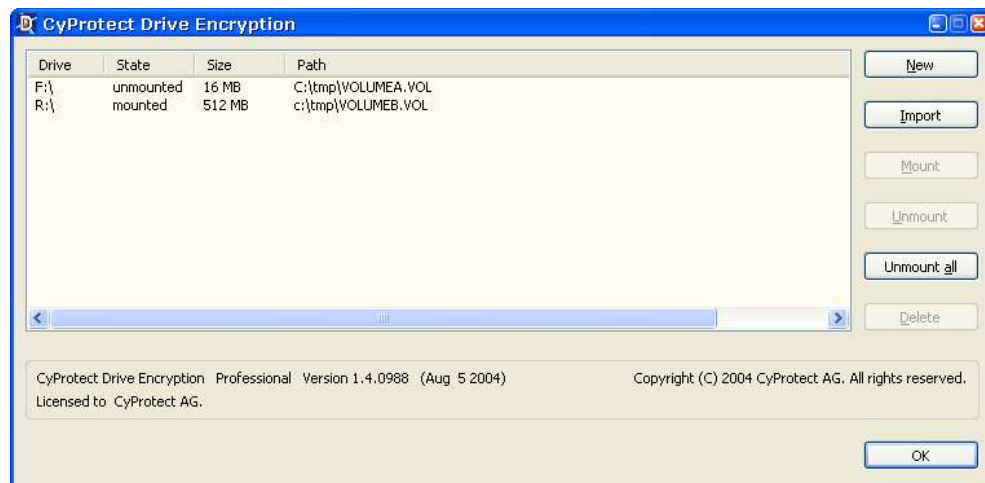
You can choose where the container file will be saved and how big it should be.

Choose a drive-letter and which encryption algorithm should be used.

Choose a password, from which a real 512 bit key will be generated.

Secure yourself against a mistype of the password

by using a hashcode as verification.



You can manage multiple encrypted drives.

If drives are unmounted, your data is secured against unauthorized access.

Connect your drives again by entering your correct password or by plugging your SafeNet iKey. Then your data will be available again for you.

Use SafeNet iKeys together with **CyProtect Key Administration** as secure alternative instead of entering a password.

