ClipGuard BIO

EDGELYNC

Client Based - IWC Authentication Engine

The EdgeLync software is our core and highly scalable security product, offering unprecedented security. EdgeLync software resides on client hardware (such as a PDA, Handheld PC, Laptop or Desktop PC, Secure Digital or PCMCIA card).

EdgeLync allows users to lock applications, folders and files as well as encrypting folders and files. The nClose icon makes it easy for the user to identify encrypted objects. The authentication process allows the user to use one or multiple methods depending on what devices are installed and available For users who wish to further augment security, both biometrics and smart card devices may be combined.

In addition to implementing to it's cryptographic security features, EdgeLync has several other key product differentiators geared to provide maximum functionality for both individual and corporate environments, which include:

- MMC Based Administration,
- Support for multiple authentication methods,
- E-mail encryption,
- File wiping,
- Single Sign On,
- Biometric GINA

ClipDrive Bio™
USB Flash Drive

The ClipDrive Bio™ Series delivers the ultimate in security for portable USB drive technology. Use your fingerprint and password to control access to the hidden encrypted partition.

Public and Secure Partitions

The ClipDrive Bio™ contains two storage partitions (like a small hard disk). There is a PUBLIC partition and a SECURE partition.

The public partition is visible as soon as you plug the device into a USB port. This partition is meant to contain data that does not need to be protected. You can easily go from computer to computer without the need of any special programs to handle the fingerprint protection. For ease of portability, and to maximize flexibility, the software needed to use the fingerprint security, on other systems other than your own, can be saved on this public partition.

The secure partition is hidden initially. Windows® does not detect it. This drive is only made visible to Windows® when the appropriate fingerprint has been authenticated.

There are two levels of protection to the data on the secure partition

1. The drive is hidden from Windows® so that the data on it cannot be accessed without the appropriate fingerprint (and optional password) authentication.
2. The data stored on the drive itself is encrypted using state of the art AES based encryption technology. This provides data security in the event the drive is disassembled and a direct attack to the flash memory chip is attempted.

Access Levels

Once the secure partition has been unlocked with a fingerprint it appears to Windows® as a normal drive. Applications can access the data as a standard storage device. The encryption and decryption of the data is done seamlessly, “on the fly”, so that it is transparent to Windows®

and the user. There is no cumbersome copying of the file, decrypting it, using it, and re-encrypting the result.

There are two levels of access on the ClipDrive Bio™.

1. **User** - This corresponds to a user who has had a fingerprint enrolled into the secure hidden encrypted fingerprint database on the ClipDrive. When the ClipDrive Bio™ Unlock utility program is run, the user applies the fingerprint (and optional password) and is granted access to the secure partition. This is known as the authentication procedure.
2. **Administrator** – The administrator is responsible for adding users to the fingerprint database. The administrator is also responsible for certain administrative tasks as are described in this manual.

Passwords

There are two passwords that will be potentially used in the ClipDrive Bio™ Unlock utility program.

1. **Administrator** – This password grants access to the administrative tools for enrolling new users, passwords, etc.
2. **User Logon** – As an additional security feature, a password can be required along with the fingerprint providing additional security to the secure partition.

Passwords are case sensitive, may contain any character on the keyboard, and can be up to 32 characters in length.

Up to 16 fingerprints can be stored in the fingerprint database. **It is strongly advisable that the administrator enroll more than one finger in case of unanticipated medical problems**.