USB flash drive

[hiddn]™ coCrypt

- **Replacable micro SD card encryption**
- **USB host port encryption**
- **PIN or Password Authentication**
- **Data recovery using PUK**

Total Protection of Data

All [hiddn]™ products utilizes secure Smart Card technology for storing data encryption keys, thus when the system is shut down, there is **no keys** that can be compromised.

Enabling a safe USB environment

The [hiddn]™ coCrypt is the perfect solution for transportation of data between the office and home, for traveling with sensitive data, for working between office braches, and for moving sensitive data between systems/platforms.

Replaceable microSD storage

The microSD memory card resides in a slot and can easily be exchanged with another card providing the user with a virtually unlimited storage capacity. By supporting the SDXC standard, up to 2TB of storage is addressable.

USB storage device support

The coCrypt includes a USB 2.0 Host Controller enabling encryption of memory sticks and external USB hard drives. The coCrypt provides additional security for the user by blocking autorun of applications that might infect a PC with backdoors or malware.

Passphrase Authentication

As an alternative to PIN authentication, the coCrypt supports true entry of passphrase (not only used to memorize digits). This enhances security by expanding the character set to include not only digits, but also letters and special characters.
Using a passphrase is an essential contributor to security and user friendliness. The user can change the passphrase at any time and as often as required.

Data recovery

An unfortunate user entering the wrong PIN/passphrase too many times, does not have to face erased data, but may still recover from the situation of a locked storage device by entering the PUK.

Easy to use

Instead of complicated LED light encoding the coCrypt provides a bright, easy to read OLED display that informs the user about the status of the device reducing the risk of operator errors.

The coCrypt offers a full alphanumeric keyboard enabling the user to enter passphrases in a T-9 style as known from mobile phones.

Key Management

For larger organizations the IT-department may use the [hiddn]™ Key Management System to keep control of keys, units and users. The administrator can define authentication policies and facilitate key escrow, a proactive solution anticipating the future need for access to secret keys.

Security Features

- **Authentication.** The system administrator might define the policy for passphrase and PUK. The latter for recovery of locked devices. Users can change their own passphrase. All data encryption keys are stored in Common Criteria EAL 5+ certified key tokens (Smart Cards).
- **Password Attack Protection.** The embedded Smart Card is automatically locked after a predefined number of failed passphrase attempts. A PUK can reopen the Smart Card and the user can set a new passphrase. Too many failed attempts to enter a PUK will permanently lock the Smart Card.
- **Policy based passphrase and PUK.** The system administrator defines passphrase and PUK minimum length. The passphrase character set requirements can be defined to form a security policy. The maximum number of incorrect passphrase and PUK entries adds to the security policy definition.

hdd
High Density Devices

High Density Devices AS
www.hiddn.no // sales@hdd.no
Twitter @hiddnhdd