COCRYPT KP

Capacity
Flash 8 GB - 128 GB

Interface
USB 3.1

Operating systems
Linux, Windows and Mac

Package includes
coCrypt,
Quick installation guide

MODELS

PRODUCT	CAPACITY	CODE
coCrypt KP	8GB	CCS1-0SD0
coCrypt KP	16GB	CCS1-0SD1
coCrypt KP	32GB	CCS1-0SD2
coCrypt KP	64GB	CCS1-0SD3
coCrypt KP	128GB	CCS1-0SD4

SECURE AND EASY TO USE

The coCrypt KP is an easy to use, hardware encrypted portable hard drive.

Simply connect coCrypt KP to any computer and enter a 7-15 digit PIN to access all data stored on the drive.

The coCrypt KP will be encrypted and not accessible until the correct PIN is entered.

To lock the drive and encrypt all data, simply eject coCrypt KP from the host computer and the entire contents of the drive will be encrypted (full disk encryption) using military grade AES 256-bit hardware encryption (XTS mode).

If the drive is lost or stolen all data is protected by military grade encryption and cannot be accessed without the 7-15 digit PIN.

Hiddn's encrypted products are already in use by and suitable for several industries;

- The Military
- Governments
- Educational institutions
- Healthcare providers
- Crypto industry
- Lawyers
- Financial institutions
- Entertainment

PRODUCT FEATURES

OS and Platform independent
The coCrypt KP works on any host operating system (MS Windows, MacOS, iOS, Linux, Chrome, Thin Clients, Zero Clients, Android & Embedded Systems).

The coCrypt KP incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN onto the on-board keypad before connecting the drive to a USB port.

There are no drivers or software to update, all encryption and authentication is performed directly on the drive.

Bootable Drive
KryptoDisk KP operates either as a generic external storage or as a bootable external disk. A secure bootable disk make it possible to use virtually any computer and still operate in a secure environment.

Saving boot files and drivers required to load a PC, laptop or workstation on the KryptoDisk KP will keep your system image fully encrypted until you're ready to load the machine.

TECHNICAL SPECIFICATIONS

Capacity	8 GB - 64 GB
Data transfer speed	Up to 116 MB per second read. Up to 43MB per second write
Approvals	FIPS 140-2 Level3 / CESG CPA / NLNCSA / FIPS PUB 197 certified
Authentication method	On-board keypad
Authentication mode	7-15 digit PIN
Interface	USB 3.1
Hardware data encryption	Real time military grade AES – XTS 256-bit Full-Disc
Waterproof	MIL-STD-810F, IP57 Certification pending
Tamper-proofed	✓
Brute-force defence	✓
Immune to Bad USB	✓
Read only & Read and write	✓

Dimensions with sleeve (mm): 80mm x 20mm x 10.5mm
Dimensions without sleeve (mm): 78mm x 18mm x 8mm
Weight: 25 grams

RoHS Compliant

COCRYPT KP

Capacity
Flash 8 GB - 128 GB

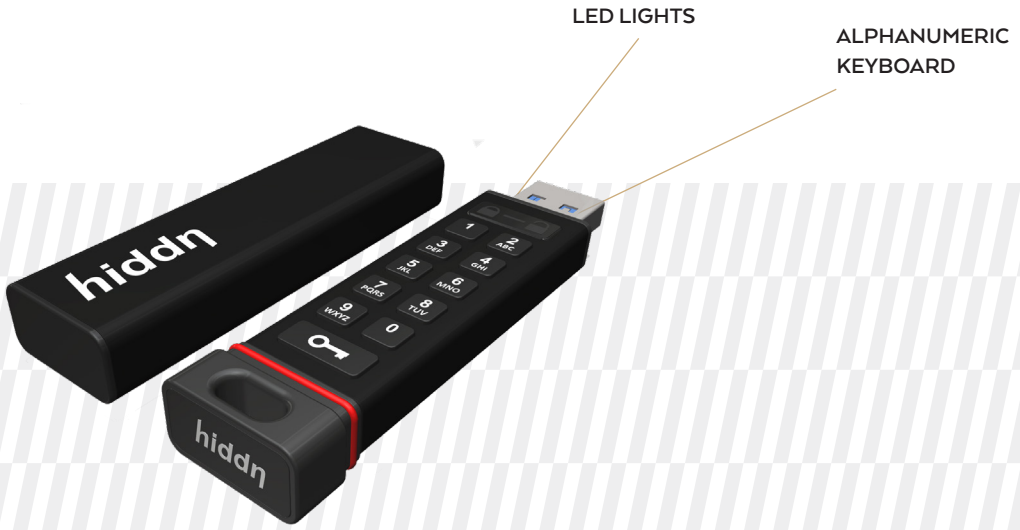
Interface
USB 3.1

Operating systems
Linux, Windows and Mac

Package includes
coCrypt,
Quick installation guide

MODELS

coCrypt | KP



SECURITY FEATURES

HIDDN'S ADVANTAGE
A NORWEGIAN TECHNOLOGY COMPANY

Brute force hack defence mechanism
Entering an incorrect password ten consecutive times will trigger the brute force hacking detection which will crypto-erase the passwords, all user data and drive formatting. The drive will remain functional but will require reformatting and all data which resided on the device including any identifiable user parameters will be unrecoverable.

IMPORTANT
If the user PIN is forgotten there are no techniques to retrieve the key. There are absolutely no backdoors and all data will be erased permanently.

Auto-lock feature
To protect against unauthorized access when the drive is connected to a host computer and unattended, the coCrypt KP can be set to automatically lock after a pre-set amount of time of inactivity. This feature can be set to activate (lock) at predefined times between 1 and 60 minutes.

Tamper proof and evident design
In addition to incorporating a secure microprocessor, encrypting the data and the encryption key, The coCrypt KP adds another barrier between your data and a hacker. Every vital piece of electronics is covered with a tough epoxy coating cementing the critical components in an indistinguishable solid capsule.

FIPS-compliant design
In addition to impenetrable hardware design, all user data and crypto parameters are encrypted as well.

The coCrypt KP contains an independent processor, crypto processor as well as other security components to create a unique and patent pending design.

Wear resistant keypad
Special coating covers the keys on the keypad which masks key usage that can be used to aid a potential attacker guess the most commonly used keys.

Admin and User modes
Setting up an Admin PIN will allow the Admin to regain access to the data if the User is no longer available

APPROVED SUPPLIER TO THE NORWEGIAN ARMED FORCES

hiddn.no/support | sales@hiddn.no