COCRYPT BT

Capacity
Flash 8 GB - 64 GB

Interface
USB 3.1

Operating systems
Linux, Windows and Mac

Package includes
coCrypt,
Quick installation guide

MODELS

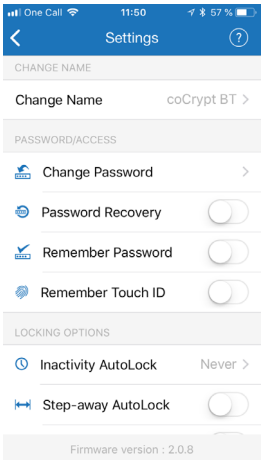
COCRYPT BT

PRODUCT FEATURES

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

Simply download the App and follow the user guide to pair your coCrypt BT with your smartphone.

The coCrypt BT are easily managed from your mobile phone and blue-tooth connection.



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

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

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	PIN authentication from smartphone
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	✓

Remote management ready
The admin can take full control of where/when the drive can be unlocked as well as remotely wiping the data and disabling access even if the user has a drive PIN.

Avoid fatal data leaks due to mis-placed portable drives with Hiddn's remote management solution, compatible with the coCrypt BT.

Hiddn's Remote Management can be added to the coCrypt BT any time after the purchase.

- App availiable in App-store and Google play.

ANDROID APP ON Google play

Available on the App Store

RoHS Compliant

hiddn

COCRYPT **BT**

Capacity
Flash 8 GB - 64 GB

Interface
USB 3.1

Operating systems
Linux, Windows and Mac

Package includes
coCrypt,
Quick installation guide

MODELS

COCRYPT BT

SECURITY FEATURES

HIDDN'S ADVANTAGE
A NORWEGIAN
TECHNOLOGY
COMPANY

APPROVED SUPPLIER TO THE NORWEGIAN ARMED FORCES

GDPR-COMPLIANT

Brute force hack defence mechanism
Entering an incorrect password 10 (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 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 back-doors and all data will be erased permanently.

Inactivity auto-lock feature
To protect against unauthorized access when the drive is connected to a host computer and unattended, the coCrypt BT 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.

Step – away auto lock
The Step-away auto lock will lock the coCrypt BT (disappear from the file Explorer/Finder) when the iOS/Android device is moved about 3 m away from the coCrypt BT for longer than 5 seconds. When returned to the coCrypt BT it unlocks automatically if the function "Remember Password" option is activated.

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

The coCrypt BT 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 and well as set policies such as Read-Only and Inactivity AutoLock.

Tamper proof and evident design
In addition to incorporating a secure microprocessor, encrypting the data and the encryption key,
The coCrypt BT 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.

RoHS Compliant

hiddn.no/support | sales@hiddn.no