KRYPTODISK **2**

Capacity
SSD 128 GB-2TB

Interface
USB 3.1

Operating systems
Linux, Windows, MacOS

Package includes
KryptoDisk 2
USB cable
Quick installation guide
Smart cards
Protective case

MODELS

PRODUCT	CAPACITY	CODE
KryptoDisk 2 User primary	128GB SSD	KD02-0SK0
KryptoDisk 2 User primary	256GB SSD	KD02-0SK1
KryptoDisk 2 User primary	512GB SSD	KD02-0SK2
KryptoDisk 2 User primary	1TB SSD	KD02-0SK3
KryptoDisk 2 User primary	2TB SSD	KD02-0SK4
KryptoDisk 2 Selfkey	128GB SSD	KD02-0SG0
KryptoDisk 2 Selfkey	256GB SSD	KD02-0SG1
KryptoDisk 2 Selfkey	512GB SSD	KD02-0SG2
KryptoDisk 2 Selfkey	1TB SSD	KD02-0SG3
KryptoDisk 2 Selfkey	2TB SSD	KD02-0SG4

PRODUCT FEATURES

KryptoDisk 2 – Selfkey (B,S)
This is the ideal product if you want to be in control of your data, PIN and PUK.

KryptoDisk 2 - User primary and user data restore
With this solution you have an extra set of cards with PIN/PUK that you can keep in a safe place in case your key card is lost or stolen.

KryptoDisk 2 KMS
By replacing the Hiddn "Selfkey" smart card with a managed smart card the IT department can keep control of keys, units and users.

Enabling a safe USB environment
KryptoDisk 2 is the perfect solution for transportation of data between the office and home, for travelling with sensitive data, for working between office branches and for moving sensitive data between systems and platforms.

Easy to use
KryptoDisk 2 comes with a bright, easy to read OLED display that informs the user about the status of the device.

Plug and Play
KryptoDisk 2 can be used straight out of the box and does not require any software or drivers to be installed prior to use. It is compatible with various operating systems (OS). Before first time use you will need to format the KryptoDisk 2. Our installation guide will guide you through this process.

Two-factor authentication
The smart card and the secret passphrase (PIN) are the two factors required to be granted access to the data. Something you have and something you know.

Key management system
With KryptoDisk 2 KMS the administrator can define authentication policies and facilitate key escrow.

Bootable secure environment
KryptoDisk 2 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.

TECHNICAL SPECIFICATIONS

Encryption algorithm	AES-256
Interface	USB 3.1
Approvals in process	FIPS 140-2 LEVEL 3
Capacities	SSD 128 GB, 256 GB, 512 GB, 1 TB, 2TB
Authentication mode	7-16 digit PIN + smart card
Read / Write	✓
Tamper-proofed	✓
Brute-force defence	✓
2-factor authentication	✓
Bootable	✓
Resistant to keyloggers	✓
Encryption key stored separately	✓
Transfer speed	80 MB/s

Dimensions (mm): L122xW79xH16

KRYPTODISK 2

Capacity
SSD 128 GB-2TB

Interface
USB 3.1

Operating systems
Linux, Windows, MacOS

Package includes
KryptoDisk 2
USB cable
Quick installation guide
Smart cards
Protective case

MODELS

KryptoDisk 2 | Selfkey (B,S)
KryptoDisk 2 | User primary and user data restore
KryptoDisk 2 | KMS

SECURITY FEATURES

HIDDN'S ADVANTAGE
DESIGNED, DEVELOPED AND ASSEMBLED IN NORWAY

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.

PIN/PUK administration
Users can change PIN/PUK. A PUK can reopen the smart card and the user can set a new PIN/PUK.

Too many failed attempts to enter PUK will permanently lock the smart card and erase all data.

Password attack protection
All data encryption keys are stored in Common Criteria EAL + certified tokens (smart cards).

GDPR-PROOF GUARANTEE

APPROVED SUPPLIER TO THE NORWEGIAN

hiddn.no/support | sales@hiddn.no