hiddn

SAFEDISK **M2**

Capacity
128 - 256 GB SSD

Protocols
SATA III

Operating systems
Linux and Windows

Form factor
M.2 | 2280-D3-B-M

MODELS

SafeDisk M2

Dimensions (mm)
SafeDisk: L22 x W80

PRODUCT FEATURES

Total protection of data
SafeDisk is an internal laptop hard drive with an embedded, tamper-proof crypto module performing full-disk AES encryption using 256-bit keys transferred from a smart card.

It uses 256 GB SSDs in a M.2, and communicates over the SATA III protocol.

Use case
A typical use case for the SafeDisk suite is organisations with very strict safety requirements for carrying sensitive information, e.g. a national security agency or a health care unit.

SafeDisk can be customized to meet your individual or organisational demands.

Card Management System (CMS)
The optional CMS enables the IT department to keep control of keys, units and users. Hiddn's CMS is a software application that allows the IT administrator to generate encryption keys and certificates, and to manage the various user profiles and encryption devices in an organization.

TECHNICAL SPECIFICATIONS

Encryption algorithm	AES-256 XTS
Interface	SATA III
SATA compliance	Rev 3.1
SATA speed	3 Gbps
Capacities	256 GB
Sustained read	up to 180 MB/sec
Sustained write	up to 140 MB/sec
Operating temperature range	0 to 60 °C
Storage temperature range	-40 to 85 °C
Supply voltage	3.3V +/- 5%
Power consumption	570 mA (max) @ 3.3V
Connector type	75-pin SATA-based M.2 module pinout
Form factor	M.2 2280 form factor / Dimensions: 80.00 mm x 22.00 mm x 3.80 mm
ROHS Recast compliant	Complies with 2011/65/EU standard
ESD (Electrostatic)	Passed (at relative temp/ humidity 23 °C, 33-35% RH)
Resistant to keyloggers	✔
Encryption key stored separately	✔
Authentication mode	7-16 characters PIN + smart card (2-factor authentication)
Tamper-proofed	✔
Brute-force defence	✔

DATA ENCRYPTION KEY

The Hiddn SafeDisk uses a Data Encryption Key (DEK) to encrypt/decrypt data on a disk.

The DEK is transferred to the Hiddn SafeDisk from a user smart card after the user has been authenticated.

Transport Layer Security (TLS) is used to provide a secure and authenticated transfer of the DEK, and in this lies the use of a number of additional keys and digital certificates. Before the Hiddn SafeDisk can receive a DEK from a user card, it must first be initialized by a Crypto Officer smart card.

The initialization procedure will load onto the Hiddn SafeDisk a set of keys including a Key Encryption Key (KEK) that is used to decrypt the DEK received from a User Card, since the DEK itself is encrypted. Along with the keys, certificates are also loaded onto the Hiddn SafeDisk used to prove the authentication and ownership of the keys.

ADDITIONAL FEATURES

- No software or drivers required.
- FIPS 140-2 Level 3 physical tamper-resistance and identity-based authentication.
- FIPS 140-2 Level 4 tamper-responsive.
- Encryption key cleared when the PC is powered off (including hibernation mode).
- Works with most laptops integrated smart card readers or with a Hiddn USB token.
- «Read-only» functionality will soon be introduced.

hiddn

SAFEDISK **M2**

Capacity
128 -256 SSD

Protocols
SATA III

Operating systems
Linux and Windows

Form factor
M.2 | 2280-D3-B-M

MODELS

SafeDisk M2

HIDDN'S ADVANTAGE
DESIGNED, DEVELOPED AND ASSEMBLED IN NORWAY

SECURITY FEATURES

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.

PIN and PUK administration
Users can change passphrase. A PUK can reopen the smart card and the user can set a new PIN/PUK. To many failed attempts to enter PUK will permanently lock the smart card and erase all data.

Data Recovery
An unfortunate user entering the wrong 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.

Smart cards
Hiddn's smart cards are effectively small, secure computing devices that contain advanced key management and transfer technology. The smart cards are tamper-proofed in accordance with Common Criteria-principles for physical security (CC EAL5+).

Password attack protection
All data encryption keys are encrypted, stored in Common Criteria EAL 5+ certified tokens (Smart Cards) and protected by PIN security measures.

External encryption key
The unique feature of Hiddn's solution is that the encryption key is actively deleted from the SafeDisk when the system is shut down. Instead, it is stored encrypted on a separate, tamper-proof smart card. This provides an unmatched level of security which has been approved and applied by various military, governmental and national security agencies to store highly sensitive information.

GDPR-PROOF GUARANTEE

APPROVED SUPPLIER TO THE NORWEGIAN ARMED FORCES

hiddn.no/support | sales@hiddn.no