PC / Laptop encryption

[hiddn]™ LapTop

- **AES-256 Full Disk Encryption**
- **Strong Two-factor Authentication**

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** stored in your laptop or the disk drive.

Strong Two-factor Authentication

The Smart Card and the secret passphrase are the two factors required to be granted access to the data. Something you have and something you know – the same security level commonly used for access to your bank account e.g. via an ATM. Why settle for less?

Key Recovery

If you forget the passphrase, the data is not lost. By means of a PUK a new passphrase can be defined and you are back in business immediately. This is a much more friendly approach than deleting the data encryption keys, which will require system reinstallation and backup recovery.

Key Management

The [hiddn]™ Key Management System 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 keys.

Ultrabook compatible

The [hiddn]™ Laptop 1+ is an ideal drop-in replacement for your laptop's 2.5" disk. Only 7mm thick, this disk will fit in even the slimmest Ultrabook.

Security Features

- **Full Disk Encryption.** All data stored on the [hiddn]™ Laptop 1+ is encrypted, including the Master Boot Record, the OS and all temporary files. The encryption is turned on before any sensitive data ever is written to the media, facilitating secure cryptographic erase.
- **Cryptographic Erase**. Removing and destroying the Smart Card provides an effective end-of-life drive sanitization and disposal. Even just removing the Smart Card and powering off the laptop clears all data encryption key material in the device. The net result is reduced classification level and handling requirements for your data. Keys and computer might travel separately to provide secure transportation of sensitive data.
- **Two-factor Authentication.** The system administrator defines the policy for passphrase and PUK. The latter for recovery of locked Key Tokens. 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 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.
- **Anti-Clone.** Cloning a drive is supported by means of a special Key Token available for the administrator only. This facilitates efficient system deployment and at the same time protects the device from unauthorized copying of data.
- **Network Image Deployment.** By defining the boot order to first look for a local drive and secondly network boot, installation of OS from a central server on the LAN works seamlessly.
- **SSD Technology.** Solid State Drives offers very low access time to data resulting in a very responsive experience for the user. In addition, there are no moving parts, no noise and very good resistance to shock and vibrations.
- **Endpoint security software compatible.** The [hiddn]™ Laptop 1+ operates comfortably with endpoint security software needed to form a complete protection solution.

hdd
High Density Devices

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

[hiddn]™ Safeguarding your data anywhere

Additional Features:

- Operating System independent - no software or drivers required.
- FIPS 140-2 Level 3 physical tamper-resistance and identity-based authentication.
- Up to 32 different data encryption keys per user.
- Flexible data encryption key options:
  - Key lifetime
  - Read-only mode
  - Media resident split keys
- MBR shadowing functionality allows tailored partition tables for individual users and/or multi-boot OS.
- Works with most laptop's integrated smartcard reader.
- Direct zeroization resets unit to factory default state.

The [hiddn]™ KMS offers centralized lifecycle management of keys. A perfect administration tool for an organization. Confidentiality, regulatory compliance and accountability of crypto keys, all in one user-friendly product.

Technical Specifications:

CAPACITIES:	128GB, 256GB, 512GB
SIZE:	7.0 x 69.85 x 100.45 mm (according to SFF-8201 std)
DATA INTERFACE:	SATA Rev 2.6
DIRECT KEY INTERFACE:	ISO 7816-3 (Mini-SIM 2FF)

Designed in Norway
Assembled in EU

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