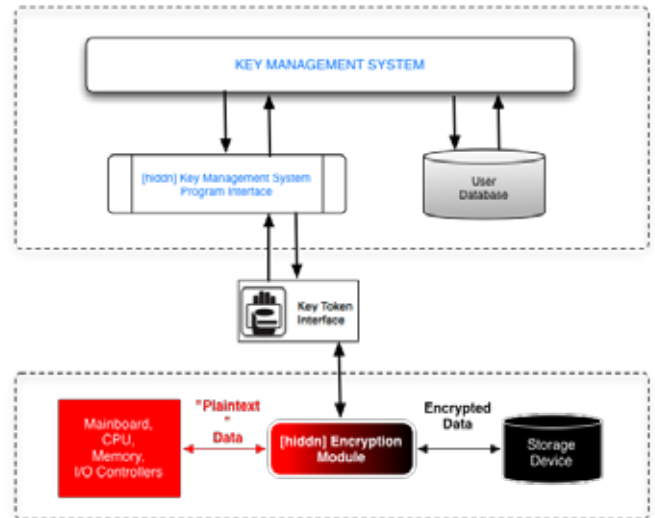


[hiddn]™ Key Management System

Management of encryption keys and Key Token lifecycle for organisations

- For volume deployment of [hiddn]™ products or for implementation of [hiddn]™ solutions into larger organisations
- [hiddn]™ KMS allows for programming of [hiddn]™ encryption keys onto existing corporate ID-cards and other smart cards
- Delivered readily installed on a Laptop with [hiddn]™ encryption
- Software only (option)
- Provides for increased overview of tokens and users (Security Officer)
- Extensive functionalities
 - Create, retire, change, duplicate, and backup smart cards
 - Set pre-boot authentication PIN
 - Manage user-token-unit relations
 - Manage multiple smart cards per unit, multiple users per unit
- Configure multi-user set-up with shared or individually encrypted partitions



[hiddn]™

Safeguarding Your Data Anywhere

[hiddn]TM Encryption

- Safeguarding your data anywhere



The [hiddn]TM technology provides for hardware encryption of all data at rest, where the keys used for protection and encryption are all stored in a separate, physical Key Token (smart card). This quality data protection solution is both PC and operating system independent, requires no software as it is all implemented in hardware, places no restraints on the CPU, operates transparently, and requires no user intervention of any kind. Supplementing this flexibility and user friendliness is a rigorously tested and validated encryption.

Robust & Versatile Data Protection

[hiddn]TM's versatile hardware-based encryption technology has been rigorously tested, and is certified with FIPS 140-2 Level 3 and Common Criteria EAL4+ certifications. To add to the strength of the technology, the Norwegian NSA passed [hiddn]TM for protection of data classified NATO RESTRICTED.

The [hiddn]TM Crypto Module can be installed on any brand computer and on any operating system, making it easy for an organization to standardize its data protection tools. There are no annual licensing fees, no end-user training is required, and it operates transparently to users; not generating any logs, errors or messages.

[hiddn]TM's transparent and independent operation enables IT professionals to upgrade operating systems and application software without stopping or uninstalling [hiddn]TM. Furthermore, fully-encrypted disks make computer repairs and disk retention (recycling) far safer, more assured and less expensive.

- **High security:** No encryption keys are stored on the hard drive or in the unit
- **Simple to audit and prove compliance:** Without the Key Token, the drive is inaccessible
- **Low total cost of ownership:** No licensing fees, no maintenance, no need for upgrades or services, and zero end-of-life disposal cost
- **Blazing fast:** no SW affecting CPU
- **Works with all PCs:** Invisible to all Operating Systems and File Systems

- **Validated and verified:** Holds the highest commercially viable certifications
- **Strong and secure encryption:** AES 256-bit encryption algorithm
- **Authentication:** All encryption keys stored on a separate, physical smart card, with encrypted key transfer
- **Performance:** Real-time encryption with no delay (transparent)
- **Plug and play:** No drivers or software required

[hiddn]TM

Patented and certified technology

The qualified and validated design of the patented [hiddn]TM technology caters for a vast array of data protection needs through its differentiated implementations.

[hiddn]TM **Crypto Module** – the certified Crypto Module FPGA-module (dimensions: 70mm x 30mm x 8mm)

[hiddn]TM **ASIC** – to be released low-cost chip solution ASIC-chip (dimensions: 10mm x 10mm)

[hiddn]TM **VHDL** – certified and well-documented code for licensing and integration with third party solutions

The modular [hiddn] IPR is well-documented, and the design opens up for OEM-implementation into third party solutions.

Contact Details

Trond Erik Bognø – Chief Sales Officer
teb@hdd.no // +47 415 08 148

Tormod Fjellgård – Chief Marketing Officer
tormod@hdd.no // +47 959 63 504

[hiddn]TM

hdd
High Density Devices