	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OSt	OSt	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.



# System Description

## High Density Devices AS


Date:	Revision:	Author:	Approved:	Doc. No:
02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4

# System Description

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## Table of Content

<b>1</b>	<b>INTRODUCTION</b>	<b>4</b>
1.1	General	4
1.2	Summary	4
1.3	Company Background	5
<b>2</b>	<b>[HIDDEN] ENCRYPTION TECHNOLOGY</b>	<b>6</b>
2.1	Introduction to [hiddn] <sup>TM</sup>	6
2.2	Concept	7
2.3	Role Definition	7
2.3.1	Crypto Officer Role	7
2.3.2	User Role	7
2.4	Encryption Keys	8
2.5	Capabilities and Characteristics	8
2.5.1	Normal Mode	8
2.5.2	Forensic Use case	9
<b>3</b>	<b>[HIDDEN]<sup>TM</sup> PRODUCT LINE</b>	<b>10</b>
3.1	Overall Structure	10
3.2	[hiddn] <sup>TM</sup> Crypto Module (CM)	10
3.2.1	Introduction	10
3.2.2	Features	11
3.2.3	Key Differentiators	11
3.3	[hiddn] <sup>TM</sup> Enclosures	12
3.3.1	[hiddn] <sup>TM</sup> Laptop Enclosure	12
3.3.2	Enclosure Interface - [hiddn] <sup>TM</sup> Laptop Solutions	12
3.3.3	[hiddn] <sup>TM</sup> Laptop with Smart Card – Typical Installation	13
3.3.4	Optional Token Types – External Reader	13
3.3.5	[hiddn] <sup>TM</sup> Desktop Enclosure	14
3.3.6	[hiddn] <sup>TM</sup> USB Enclosure	16
3.3.7	[hiddn] <sup>TM</sup> Crypto Adapter	17
3.3.8	[hiddn] <sup>TM</sup> Smart Card	18
3.4	Storage	18


	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

3.4.1	[hiddn]™ Laptop Enclosure.....	18
3.4.2	[hiddn]™ USB Enclosure.....	18
3.5	[hiddn]™ Key Management System (KMS) .....	19
4	<b>WORK .....</b>	<b>20</b>
4.1	<b>Sample Upgrade Operation in User Organisation .....</b>	<b>20</b>
4.1.1	Issues Related to Upgrade of Existing PCs.....	20
5	<b>RELATED DOCUMENTATION AND ABBREVIATIONS.....</b>	<b>22</b>
5.1	<b>Applicable Documents .....</b>	<b>22</b>

## List of Figures

Figure 1	[hiddn]™ Architecture .....	10
Figure 2	[hiddn]™ Crypto Module with Smart card reader .....	11
Figure 3	[hiddn]™ Laptop Concept.....	12
Figure 4	[hiddn]™ Laptop Enclosure (SATA).....	13
Figure 5	[hiddn]™ Laptop Enclosure in Laptop with side-mounted disk drive.....	13
Figure 6	[hiddn]™ Laptop Enclosure with Contactless smart card interface .....	14
Figure 7	[hiddn]™ Desktop Concept.....	15
Figure 8	[hiddn]™ Desktop .....	15
Figure 9	[hiddn]™ USB Concept .....	16
Figure 10	[hiddn]™ USB.....	16
Figure 11	[hiddn]™ Crypto Adapter Concept.....	17
Figure 12	[hiddn]™ External Hard Drive Enclosure.....	17
Figure 13	[hiddn]™ Key Management System .....	19
Figure 14	[hiddn]™ KMS & Unit Architecture.....	19
Figure 15	Sample upgrade procedure in organisation .....	21

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OSt	OSt	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 1 Introduction

### 1.1 General

The System Description describes in detail the [hiddn]<sup>TM</sup> encryption technology, the [hiddn]<sup>TM</sup> product line, and the work offered by High Density Devices.

**NOTE: [hiddn] was previously known as Secured and has recently been renamed due to trademark considerations.**

### 1.2 Summary

[hiddn]<sup>TM</sup> Hard Disk Protection from High Density Devices AS (HDD) safeguards your data anywhere by patented, verified and certified encryption solutions and products for Full Disk Encryption, applicable to laptop computers, desktop computers and external storage media.

High Density Devices has for years cooperated with the US DoD on verification and certification of the [hiddn]<sup>TM</sup> technology for military purposes and has received very favourable feedback from warfighters who has demonstrated the technology's simplistic operation and verified that the system performed well during, and outside of, scheduled test events.

Operator comments quoted include:


- *"Stable, simple, deployable."*
- *"Extremely reliable and predictable."*
- *"Simple technology that anyone could understand and use."*
- *"This is a quality product."*

[hiddn]<sup>TM</sup> is among **the highest certified** and most user friendly encryption technologies available on the market today, and key features include being completely independent of PC Operating System (Windows XP, Windows Vista, Windows7, MacOS, Linux, etc.), independent of hardware manufacturers (SW drivers, etc.) and the unique and flexible [hiddn]<sup>TM</sup> Crypto Module (CM) serves in solutions for laptops, desktops and external USB disks.

[hiddn]<sup>TM</sup> does – as opposed to SW solutions - not use resources in a PC that will degrade overall performance such as CPU or memory, and requires no further competence by the user operating the PC other than that of using the provided smart card.

**In addition, [hiddn]<sup>TM</sup> provides for several additional functionalities and features unique to the full disk encryption market (ref. Contactless optional solution).**

HDD has also developed a proprietary Key Management System (KMS) that allows organisations to effectively manage and administer users and the smart cards storing the AES256 individual encryption key(s).

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OSt	OSt	2009/9/Specifications/4
<b>System Description</b>					


© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 1.3 Company Background

High Density Devices AS is the sole owner of the patented technology behind its products (US Patent No. 7,434,069), and was established in 1998 by a team of computer-industry veterans who saw a growing need to protect valuable data where it is most vulnerable – at rest on storage media like hard disk drives. The privately owned company based in a Norwegian town southwest of Oslo then spent the next four years dedicated to developing and enhancing leading edge encryption technologies. Gradually, as the market woke up to news of data breaches, **[hiddn]**<sup>TM</sup> as we know it today came into shape.

In 2002, the company’s breakthrough technologies caught the attention of the US Department of Defence, and through carefully selected partners, the DoD was introduced to the encryption technology. Having learned about the possibilities of hardware encryption, the DoD recognized that the **[hiddn]**<sup>TM</sup> technology provided strong enough encryption for military purposes, and in a form factor that could be easily adopted for Commercial Off-the-Shelf (COTS) applications. As a result, High Density Devices AS has received over \$8 million from the US Defence Budget to certify and validate the encryption technology platform under the internationally renowned Common Criteria standard and the US Federal Information Processing Standards (FIPS).

This detailed and thorough validation process was completed in late 2005 and **[hiddn]**<sup>TM</sup> is now one of very few commercially available technologies for encryption of data at rest that is validated at both FIPS 140-2 level 3 and Common Criteria EAL 4+. HDD, the sole owner of the patented **[hiddn]**<sup>TM</sup> encryption technology, has 10 employees and hired consultants, all working with the commercial launch of **[hiddn]**<sup>TM</sup> in the rapidly growing market for data protection.

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 2 [hiddn] Encryption Technology

### 2.1 Introduction to [hiddn]™

[hiddn]™ is a patented technology that offers the unparalleled flexibility of keying material including key lifetime, read/write only keys, forensic capabilities, split key functionality etc. This technology comes with top of the line security, validated by certification authorities both governmental and military.


The [hiddn]™ technology is Operating System and Platform independent, which makes it easy to deploy in a variety of scenarios expected in large organizations. Management becomes much easier since there is just one product organization has to relate to for securing data at rest. [hiddn]™ works on laptops, desktops, servers, external USB drives etc., and one solution will cater for all your data protection needs. Deploying [hiddn]™ technology in your organization releases you from dependency on hardware and software manufacturers as the [hiddn]™ technology works with all of them.

The [hiddn]™ technology is built on a simple but very robust “bump in the wire” approach. Operating on the ATA protocol level enables [hiddn]™ technology to encrypt all user data sent to the hard disk while maintaining Operating System and Platform independency. Physically and logically separated data and key interface prevents cross-contamination between user data and keying material.

All encryption keys are erased from the [hiddn]™ module during power-off using validated mechanisms. If your computer is lost or stolen you may rest assure that no attacker can retrieve your encryption keys because they are simply not residing on the [hiddn]™ module in power off state. Certified two-way authentication mechanisms keep the unauthorized persons away from trying to access your data with false Smart cards.

The [hiddn]™ technology builds on three basic principles:

- **Robust** – FIPS, Common Criteria and NATO certifications, and passed NSA extended vulnerability analysis
- **Flexible** – [hiddn]™ devices support up to 32 different encryption keys per user, provides support for multiple clearance levels on the same computer, and has a shadowed Master Boot Record, two-way authentication, and split keys.
- **Simple** – transparent true Full Disc Encryption that encrypts ALL outgoing data and decrypts ALL incoming data.

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 2.2 Concept

**[hiddn]**<sup>TM</sup> is a hardware based data encryption device designed for the encryption of user data stored in a computer storage device (Hard Drive). **[hiddn]**<sup>TM</sup> is logically and physically separated from the computer processor unit, and placed directly in the data path between processor unit and storage device.

The objective of **[hiddn]**<sup>TM</sup> is to protect data at rest from disclosure by applying robust encryption. Encryption is performed on the entire disk, including boot-up information, swap space and temporary files. As users work, real-time and transparent encryption is performed on all user data as it is written to the hard disk.

**[hiddn]**<sup>TM</sup> is a self-contained hardware encryption engine. It resides in the data path between the computer motherboard and the storage device. **[hiddn]**<sup>TM</sup> uses AES [3][4] to encrypt and decrypt data being transferred between the computer and the storage medium. Up to 32 different keys can be used, each key allocated a non-overlapping sector range on the storage medium. The AES keys for the encryption/decryption are loaded into **[hiddn]**<sup>TM</sup> from an interface physically and logically separate from the data path. Only the key interface is provided. The Smart card and the key management system responsible for generating keys are not part of **[hiddn]**<sup>TM</sup>. Any type of Smart card satisfying the requirements of the Key Interface can be used. The AES keys are encrypted with 168-bit TDEA [5][6] when transferred over the patented Key Interface.

## 2.3 Role Definition

The concept recognizes two different roles:

- Crypto Officer
- User


### 2.3.1 Crypto Officer Role

The purpose of the Crypto Officer is to change the TDEA communication keys in **[hiddn]**<sup>TM</sup>. For authentication, the Crypto Officer will have a Smart card with a valid Crypto Officer Key. The Crypto Officer may also change the Crypto Officer Key. When AES split keys are used, the Crypto Officer is responsible for downloading the resident part of the AES keys into **[hiddn]**<sup>TM</sup>.

The resident parts of the AES keys are stored in **[hiddn]**<sup>TM</sup>, and merged with the user part whenever a User Smart card is introduced.

### 2.3.2 User Role

The normal user of the services provided by **[hiddn]**<sup>TM</sup> is referred to as the User. The User will use **[hiddn]**<sup>TM</sup> for encryption and decryption of user data. For authentication, the User will have a Smart card with a valid set of TDEA keys for communication over the Key Interface.

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 2.4 Encryption Keys

[hiddn]<sup>™</sup> supports up to 32 different encryption keys per user. Encryption keys are valid on administrator's predefined addressable non-overlapping part of the disk. This enables the users to encrypt different parts of the drive with a different encryption key.

**This way of utilizing addressing features of the storage medium in relation to the selection of keys is a central part in HDD's US patent 7,434,069, describing this feature in details.**

One can enforce different clearance levels for different users on the same hardware using Smart cards with different sets of encryption keys.

**Multiple Users case:** Three users on a laptop with installed Windows on partition 1 encrypted with encryption key 1, user partition encrypted with encryption key 2 and user partition encrypted with encryption key 3.

The Crypto Officer can then produce three different Smart cards:

1. **"Commander"** Smart card contains all three encryption keys and has the access to all partitions.
2. **"Officer 1"** Smart card contains encryption keys one and two. MBR stored on the Smart card conceals partition no. 3. User has access to partitions one and two and is totally unaware of partition number three. Any possible attempt to address the disk area defined as partition three ends in an ATA error message as Windows cannot access this area. Any attempt to format this area will end up in Windows indicating error, because no data can be written or read.
3. **"Officer 2"** Smart card contains encryption keys one and three. MBR stored on the Smart card conceals partition nr. 2. User has access to partitions one and three and is totally unaware of partition number two. Any possible attempt to address the disk area defined as partition three ends up in an ATA error message as Windows cannot access this area. Any attempt to format this area will end up in Windows indicating error, because no data can be written or read.

## 2.5 Capabilities and Characteristics


### 2.5.1 Normal Mode

In the normal mode of operation, [hiddn]<sup>™</sup> will encrypt data being written from the host computer to the storage device, and decrypt data being read from the storage device to the host computer. [hiddn]<sup>™</sup> will interface directly to the IDE/ATA bus of the host computer and the storage device.

The encryption process is transparent to the user, and no particular requirements are put on the host system or storage unit apart from the fact that they must use the IDE/ATA bus. Both the [hiddn]<sup>™</sup> ATA interfaces and the encryption algorithm support the maximum data rate given by the ATA/ATAPI-6 specification [1].

The AES keys for the process are downloaded from the User Key Token. The AES keys are protected by TDEA [5][6].




	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	Ost	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 2.5.2 Forensic Use case

By setting the key range covering the whole drive but not associating any encryption key to the range, the user can read clear text data from the drive but can not write anything to the drive due to the no clear write policy implemented in [hiddn]<sup>TM</sup>. [hiddn]<sup>TM</sup> enters the state defined by the Federal Information Processing Standard FIPS 140-2 as “Exclusive Bypass Mode”. This feature is verified through the FIPS Operational Evaluation Test. Once again, [hiddn]<sup>TM</sup> does not allow clear write to the disk under no circumstances.

This feature can be used by organizations requiring reading data from a drive, but having to make sure that they have not altered any data on the drive.

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3 [hiddn]™ Product Line

#### 3.1 Overall Structure

A [hiddn]™ end-user solution comprises of five elements:

- One [hiddn]™ Crypto Module
- One [hiddn]™ enclosure unit
- One storage unit with capacity to suit user need
- Minimum one [hiddn]™ smart card for storing encryption keys
- Optionally, the [hiddn]™ Key Management System can be acquired for encryption key escrow and management and generation of [hiddn]™ smart cards

***[hiddn]™ Hard Disk Protection includes the [hiddn]™ Crypto Module and the appropriate enclosure, thereby providing the end-user with a standard disk interface (ZIF/LIF, SATA, PATA) for easy integration with a suitable optional storage unit.***

#### 3.2 [hiddn]™ Crypto Module (CM)

##### 3.2.1 Introduction

[hiddn]™ is a hardware encryption module with well-defined red and black interfaces. The data interfaces obey the ATA specification, and the module is inserted in the data path between motherboard and storage device. The key interface is encrypted and playback protected. HDD uses the Atmel smart card for its [hiddn]™ Smart cards.

There are three options to read the smart card information into the [hiddn]™ CM:

1. The standard practise is to connect directly to the integrated card reader of the [hiddn]™ CM.
2. [hiddn]™ CM can also use an external smart card reader instead of the integrated reader, as signals for this are available on the [hiddn]™ CM-to-board connector.
3. As an option, the [hiddn]™ CM can be equipped with a special interface replacing the integrated card reader that will connect it to a small loop antenna enabling the use of contactless (RF) smart card technology.

For more information regarding these options, consult section 3.3.4.

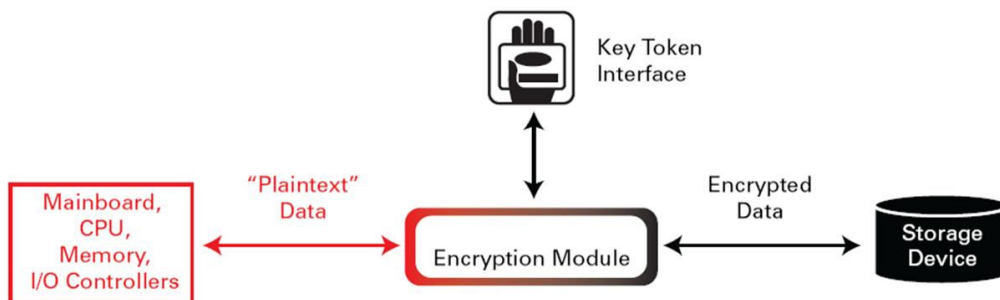



Figure 1 [hiddn]™ Architecture

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.




Figure 2 [hiddn]™ Crypto Module with Smart card reader

### 3.2.2 Features

- Transparent operation at full ATA speed
- ALL user data encrypted on drive providing the true Full Disk Encryption
- No software involved
- Operating System independent (No transition cost for introduction of new OS)
- Integrated card reader for smart card
- Up to 32 different encryption keys per user
- Flexible key policies – multiple keys, lifetime setting, split key
- Keys stored in controlled environment and zeroized at power-off by validated mechanisms
- Supports multiple clearance levels on the same drive
- Support for shadowed Master Boot Record
- Periodic self-tests of all cryptographic functions

### 3.2.3 Key Differentiators

- The only FIPS Level 3 module for protection of data at rest on PCs
- No Encryption keys stored on module after power off
- Completely transparent use with no need for user intervention
- 256 bits AES encryption
- Certified by US certification authorities (NIST/NSA) & laboratories (SAIC/InfoGard)
- Unparalleled user flexibility enforced by encryption key attributes
- KMS allows Crypto Officer to set and change all the attributes and consequently enable all features and capabilities embedded within the [hiddn]™ Crypto Module
- Operating System and Platform independent
- Hardware manufacturer independent
- One module (CM) serves laptops, desktops and USB external hard drive
- [hiddn]™ does not use PC resources such as CPU and memory as software does

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3.3 [hiddn]™ Enclosures

[hiddn]™ Crypto Module is a general module implementing strong encryption for multiple purposes. To utilise the [hiddn]™ CM in connection with the PC, it will have to be combined with an enclosure and a storage unit internal or external to the PC.

Below are enclosures suitable for introduction in laptop computers, desktop computers and USB units functioning as secure external storage for both laptop and desktop PCs.

#### 3.3.1 [hiddn]™ Laptop Enclosure

The enclosure has the overall form factor similar to that of a 2.5" hard disk drive utilised by most laptops. By mounting the [hiddn]™ CM on the enclosure together with a 1.8" hard disk drive (ZIF), the components form a complete unit that can be inserted directly into the drive bay of a laptop.

The [hiddn]™ CM is placed in front of the unit (away from the disk connector) and makes it possible to insert a [hiddn]™ Smart card into the enclosure for key transfer.

The figure below shows a [hiddn]™ laptop enclosure with [hiddn]™ CM and disk fitted.

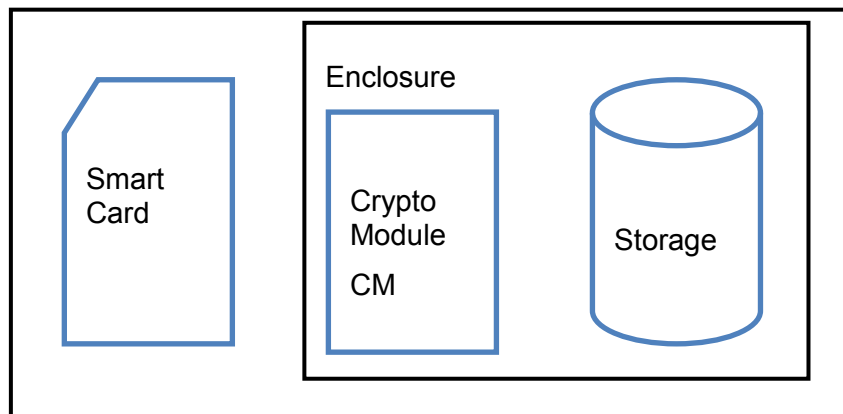


Figure 3 [hiddn]™ Laptop Concept

#### 3.3.2 Enclosure Interface - [hiddn]™ Laptop Solutions


The [hiddn]™ Laptop enclosure is provided in two different versions:

i) **PATA**-version supporting IDE-type (standard parallel) hard disk drive interface towards the host laptop (total 48 pins)

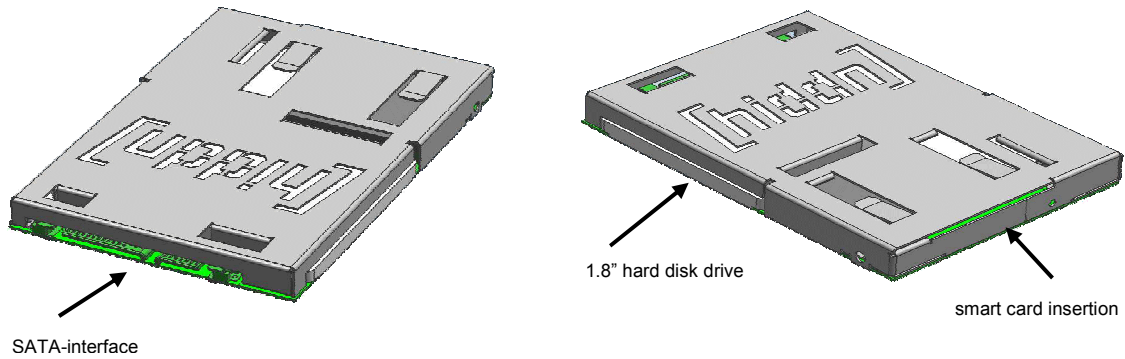
or

ii) **SATA**-version supporting SATA-type (standard serial) hard disk drive interface towards the host laptop.

The most recent version of the **SATA-based** enclosure is as shown below:

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	Ost	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.



**Figure 4 [hiddn]™ Laptop Enclosure (SATA)**

### 3.3.3 [hiddn]™ Laptop with Smart Card – Typical Installation


The following figure illustrates a typical installation, with the [hiddn]™ solution installed in the hard drive bay of the Laptop, replacing the original hard drive with the encryption solution along with a hard drive.



**Figure 5 [hiddn]™ Laptop Enclosure in Laptop with side-mounted disk drive**

### 3.3.4 Optional Token Types – External Reader

As a number of Laptop models only allows for its hard disk drives to be mounted internally (in the “crate”) in the Laptop, not allowing for side-mounted access to the integrated smart card reader in the [hiddn]™ Crypto Module, HDD has developed two alternate solutions:

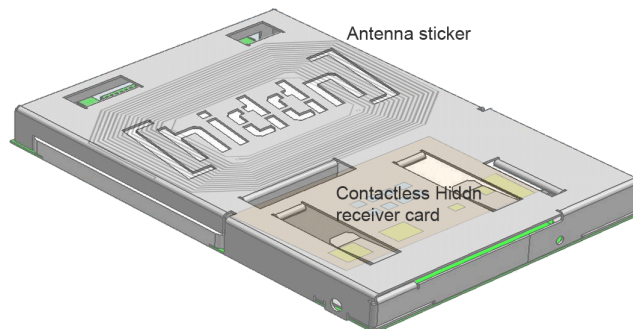
	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

- i) PCMCIA/PCCard/ExpressCard (54 mm) with smart card reader provided for insertion into the appropriate PCCard/ExpressCard (54 mm) slot of the PC/Laptop. This external reader is an HDD-design and only uses the slot for physical placement of the reader. There is no electrical connection to the Laptop/PC (the reader cannot be used for any other purpose than the FDE from HDD), but a separate connection to the carrier board of the Laptop enclosure to connect this external reader to the [hiddn]<sup>TM</sup> CM.
- ii) A brand new design by HDD providing Contactless smart card access to the Full Disk Drive Protection solution from HDD. This solution provides for a secure RF-based contactless interface to the [hiddn]<sup>TM</sup> Crypto Module. This solution is based on a small card being inserted into the smart card “bay” of the Laptop Enclosure ensuring/providing a contactless interface to the [hiddn]<sup>TM</sup> CM. In addition, an RF-antenna is mounted on top of the Enclosure. Thus, to activate the disk, an RF-based [hiddn]<sup>TM</sup> Smart card (with a combined physical terminal / RF-interface/antenna) is placed above / on to the keyboard allowing for the PIN-code to be verified and keys to be transferred to the CM.

**This solution is unique to HDD, provides extreme ease of installation and use, and is equally secure.**

The most recent version of the **SATA-based** enclosure with the Contactless feature installed is as shown below:



**Figure 6 [hiddn]<sup>TM</sup> Laptop Enclosure with Contactless smart card interface**

### 3.3.5 [hiddn]<sup>TM</sup> Desktop Enclosure

The enclosure has the overall form factor similar to that of a CD drive unit to be installed in a drive bay available in most desktop PCs. By fitting a [hiddn]<sup>TM</sup> CM in the enclosure, one internal disk in the PC can be connected and encrypted.

The enclosure has one SATA channel and one PATA channel available for interconnection to existing internal disks in a desktop PC.

Date:	Revision:	Author:	Approved:	Doc. No:
02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4

## System Description

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

In front of the enclosure is a slot for insertion of the [hiddn]™ Smart card for key transfer to the [hiddn]™ CM. The module is placed in front of the unit (away from the disk connector) and makes it possible to insert a [hiddn]™ Smart card.

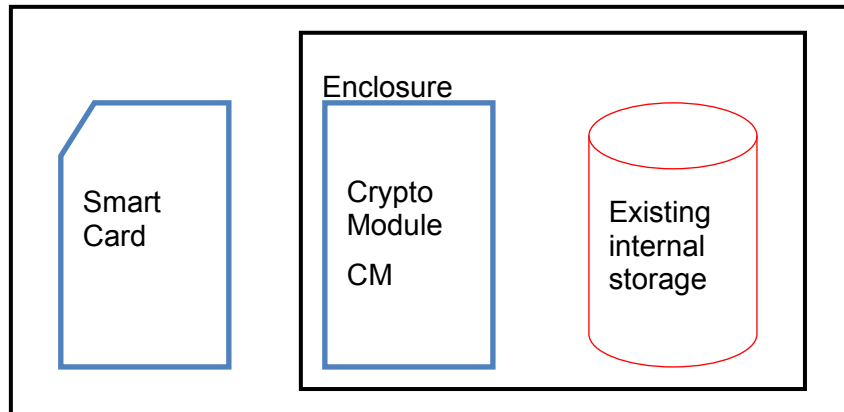


Figure 7  
Desktop

[hiddn]™  
Concept

The figure below illustrates how the [hiddn]™ Desktop is installed in a generic workstation.

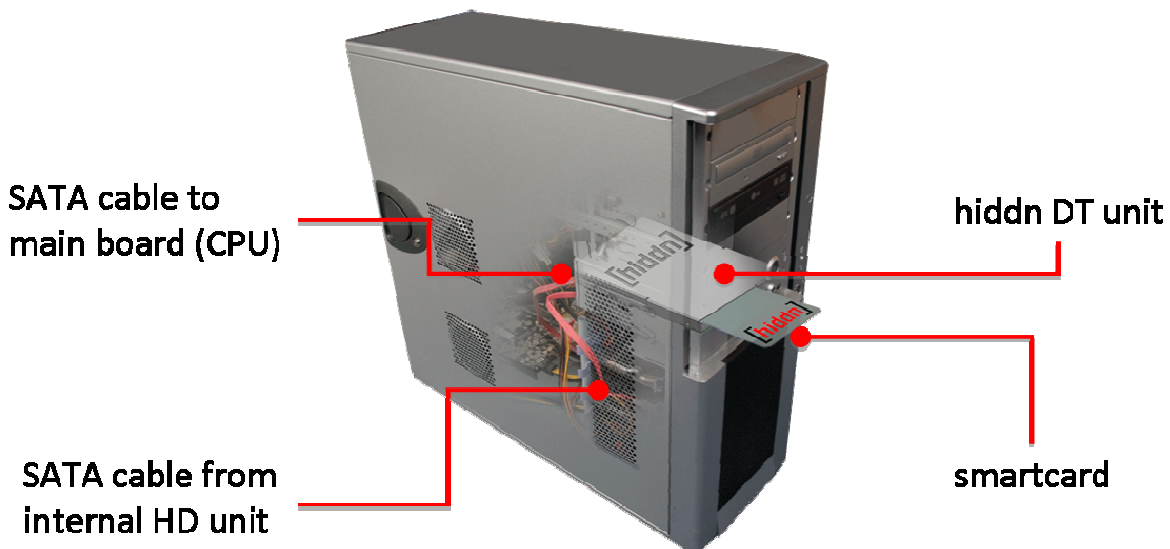



Figure 8 [hiddn]™ Desktop

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3.3.6 [hiddn]™ USB Enclosure

The enclosure can, in addition to a CM module, accommodate a standard 2.5" hard disk drive with SATA interface. The card reader integrated on the CM module interfaces with a smart card for key transfer. The unit then offers a standard USB 2.0 interface for connection to host computer.

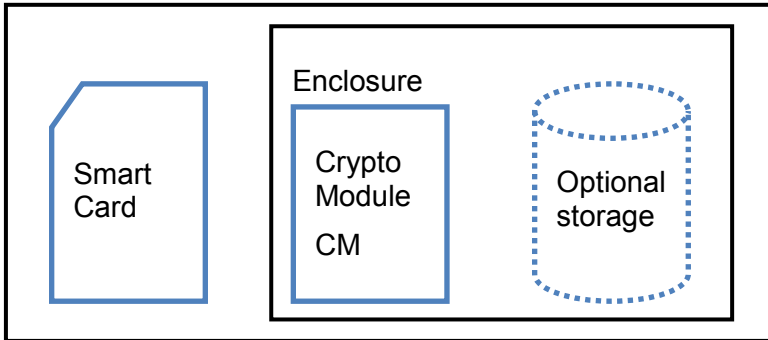


Figure 9 [hiddn]™ USB Concept

The unit can be equipped with a numeric keypad for PIN entry thus providing two-factor authentication. The SecureD USB unit is an encrypted hard drive designed to provide secure, portable, external data storage. It connects to a PC via a standard USB2.0 cable.

The figure below illustrates the various components that make up the [hiddn]™ USB unit.

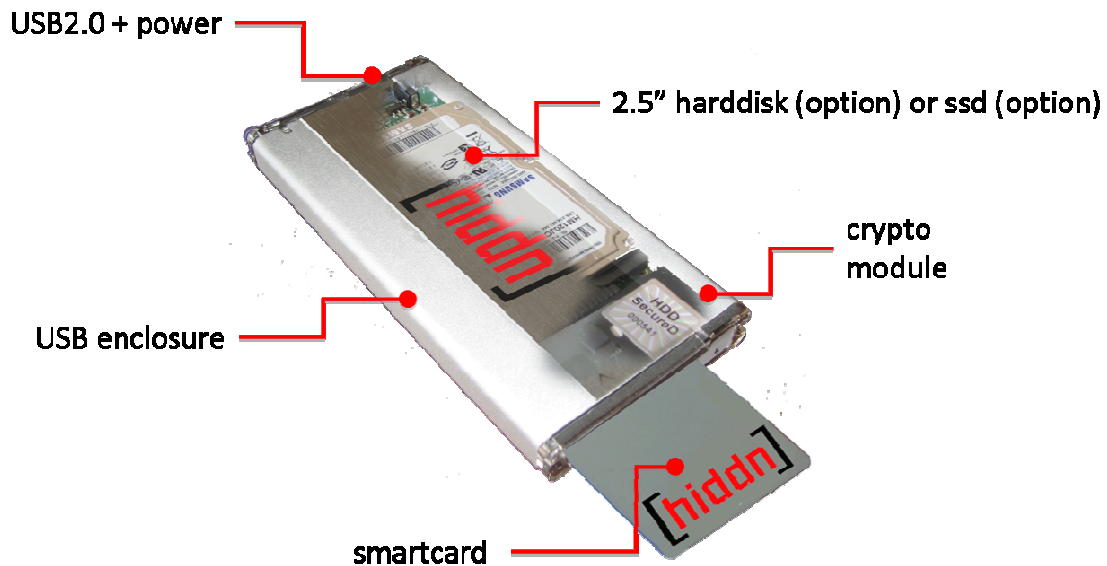



Figure 10 [hiddn]™ USB



	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3.3.7 [hiddn]™ Crypto Adapter

This latest system consists of a unique adapter for encryption of external storage media, and an add-on unit for encryption of hard drives:

- [hiddn]™ Crypto Adapter
- [hiddn]™ External Hard Drive Enclosure

[hiddn]™ Crypto Adapter contains all encryption functions, including the [hiddn]™ CM, smart card reader, and input for two-way authentication (PIN, fingerprint). It connects to a PC northbound and a storage device southbound both using standard USB2.0 interfaces.



- 1 – USB connection to PC
- 2 - Connection of USB storage (e.g. memory stick)
- 3 - PIN entry
- 4 - Smartcard with encryption key
- 5 – Indicator lights for operator

Figure 11 [hiddn]™ Crypto Adapter Concept

The Adapter can be combined with [hiddn]™ External Hard Drive Enclosure and equipped with any standard 2.5" SATA disk, comprising a complete Full Disk Encryption for external hard drives.

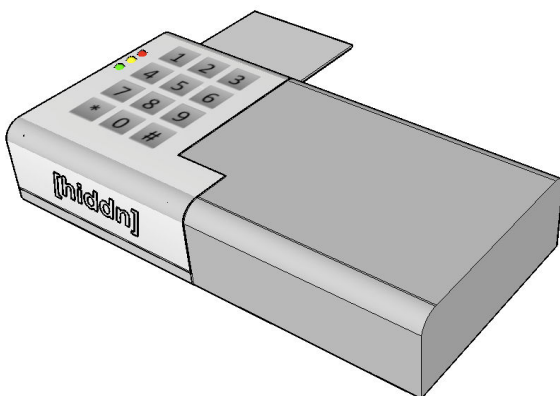



Figure 12 [hiddn]™ External Hard Drive Enclosure

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OSt	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3.3.8 [hiddn]™ Smart Card

The smart card store encryption keys used to encrypt and decrypt the data to and from hard drive. These keys are downloaded to the [hiddn]™ Crypto Module through an encrypted Key Interface. The smart card also contains a pre-boot Master Boot Record with sufficient code to transfer a PIN number entered by the user from the computer keyboard back to the smart card where the PIN is verified.

On initial boot-up, the pre-boot Master Boot Record is verified by the [hiddn]™ Crypto Module and loaded by the host computer before the operator is prompted for the PIN number. Only the correct PIN will release the media encryption keys from the FIPS certified smart card chip. The keys are transferred to the [hiddn]™ Crypto Module, and the laptop can reboot using the proper boot sector.

The combination of the PIN number request and the smart card provides two factor authentication. The smart card used in the [hiddn]™ solution implements a number of safety features including protection from DPA/SPA attacks, side channel attacks as well as physical protection of encryption material.

## 3.4 Storage


Storage is added to the different enclosures together with a [hiddn]™ Crypto Module to form a complete unit. Physical size and capacity of the storage unit will vary according to customer requirements and the different capabilities of the enclosure. Suitable storage can be delivered as options with the different enclosures or purchased from local dealers.

### 3.4.1 [hiddn]™ Laptop Enclosure

Uses any HDD approved 1.8" hard disk drive with ZIP/LIF.

### 3.4.2 [hiddn]™ USB Enclosure

Uses any 2.5" hard disk drive with SATA interface.

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<h2>System Description</h2>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

### 3.5 [hiddn]™ Key Management System (KMS)

The [hiddn]™ KMS is installed and delivered on a dedicated computer along with a smart card reader/writer. For security reasons, it is always recommended to install a [hiddn]™ Crypto Module on the KMS and store it in a physically secured room. A designated Crypto Officer should be the only person authorized to use the KMS.

The [hiddn]™ Key Management System utilizes the following functionality:

- Create, manage, and retire encryption keys and Communication Key Set
- Create and manage the encryption keys' attributes
- Key escrow
- Management of roles and services

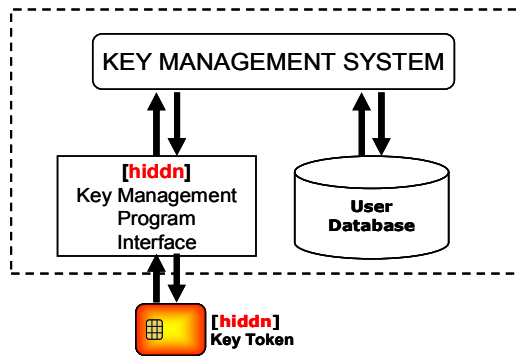


Figure 13 [hiddn]™ Key Management System

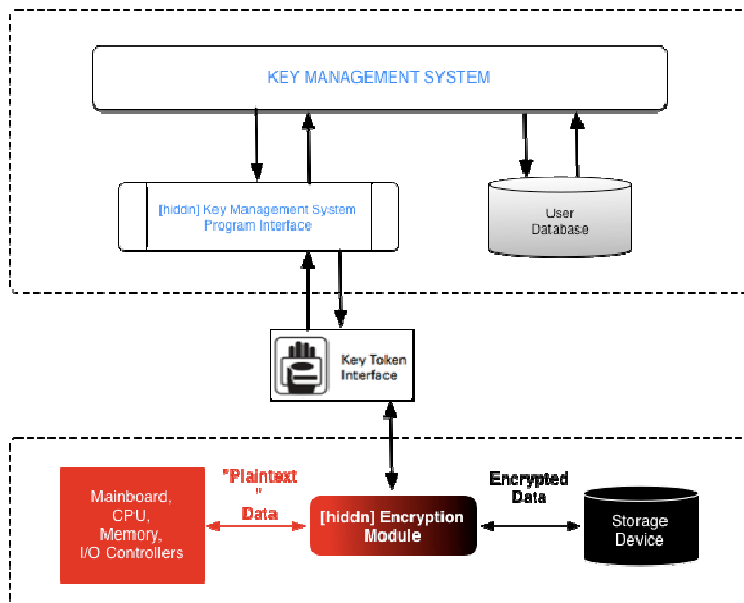



Figure 14 [hiddn]™ KMS & Unit Architecture

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 4 Work

The instructions required to install and operate [hiddn]<sup>TM</sup> solutions are included in the respective product's user documentation. The following sub-sections will thus focus on the labour considered with installation and configuration of the units prior to end-user operation.

### 4.1 Sample Upgrade Operation in User Organisation

Upgrading PCs in a large organisation requires strict procedures for converting unprotected data to become protected data. Also disposal or reuse of existing hard disks must be taken into account.

As part of the scope of delivery this operation will be handled in cooperation with the customer.

#### 4.1.1 Issues Related to Upgrade of Existing PCs

Upgrading a laptop PC in use will require a change of hard disk from the original 2.5" hard drive to the 1.8" hard drive mounted on the [hiddn]<sup>TM</sup> Laptop unit. This replacement will leave the customer with an added security since the original 2.5" can be used as a master for producing the 1.8" encrypted (new) disk. After completion of the data transfer the customer can either store the original disk as an extra precaution or the disk can be erased and reused in an [hiddn]<sup>TM</sup> USB enclosure as an external transportable encrypted disk, serving e.g. as a secure local back-up solution.

# System Description

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

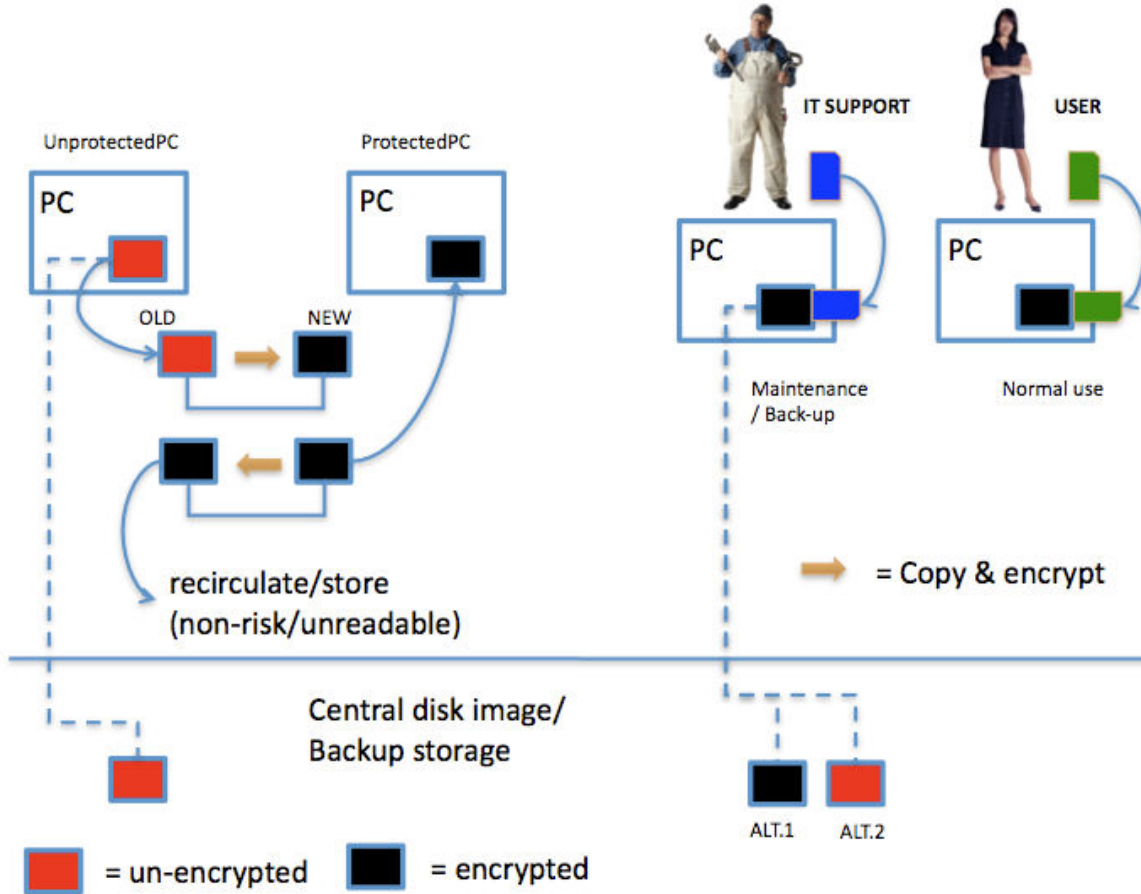



Figure 15 Sample upgrade procedure in organisation

	Date:	Revision:	Author:	Approved:	Doc. No:
	02.11.2009	1.5	TF/AV/BN/OST	OST	2009/9/Specifications/4
<b>System Description</b>					

© 2008 High Density Devices AS. Passing or copying of this document, use or communication of its contents is not permitted without written authorization.

## 5 Related Documentation and Abbreviations

### 5.1 Applicable Documents

#### Ref. # Document Title

- [1] ANSI INCITS 361-2002  
Information Technology – AT Attachment with Packet Interface – 6 ATA/ATAPI-6
- [2] ANSI INCITS XXX T10/1545-D (Draft)  
Information Technology – Multimedia Commands – 4 (MMC-4)
- [3] Advanced Encryption Standard (AES), FIPS Publication 197.  
National Institute of Standards and Technology, November 2001,  
<<http://cs-www.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf>>,  
viewed 08 September 2003.
- [4] Recommendation for Block Cipher Modes of Operation - Methods and Techniques, Special  
Publication 800-38A, 2001 Edition.  
National Institute of Standards and Technology, December 2001,  
<<http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>>,  
viewed 11 September 2003.
- [5] Data Encryption Standard (DES), FIPS Publication 46-3.  
National Institute of Standards and Technology, October 1999,  
<<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>>,  
viewed 29 November 2004.
- [6] Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52-1998.