



System Description

High Density Devices AS


	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

Table of Content

- 1 Introduction 5**
 - 1.1 General5
 - 1.2 Summary.....5
 - 1.3 Company Background.....6
- 2 [hiddn] Encryption Technology 7**
 - 2.1 Introduction to [hiddn]™7
 - 2.2 Concept.....8
 - 2.3 Role Definition8
 - 2.3.1 Crypto Officer Role.....8
 - 2.3.2 User Role9
 - 2.4 Encryption Keys9
 - 2.5 Capabilities and Characteristics.....10
 - 2.5.1 Normal Mode10
 - 2.5.2 Forensic Use case10
- 3 [hiddn]™ Product Line 11**
 - 3.1 Overall Structure11
 - 3.2 [hiddn]™ Crypto Module (CM) 11
 - 3.2.1 Introduction 11
 - 3.2.2 Features..... 12
 - 3.2.3 Key Differentiators 13
 - 3.3 [hiddn]™ Product Portfolio14
 - 3.3.1 [hiddn]™ Laptop..... 14

Date: 26.02.2010	Revision: 1.6	Author: TF/AV/BN/OSt	Approved: OSt	Doc. No: 2009/9/Specifications/4
---------------------	------------------	-------------------------	------------------	-------------------------------------

- 3.3.1.1 [hiddn]™ Laptop Solutions 15
- 3.3.1.2 [hiddn]™ Laptop with Smart Card – Typical Installation 16
- 3.3.1.3 Optional Token Types – Contactless Reader 16
- 3.3.2 [hiddn]™ Desktop 18
- 3.3.3 [hiddn]™ SATA Adapter 19
- 3.3.4 [hiddn]™ Crypto Adapter 20
- 3.3.4.1 [hiddn]™ Crypto Adapter – Optional Hard Drive Extension 21
- 3.3.5 [hiddn]™ Smart Card 21
- 3.4 [hiddn]™ - Versatile & Modular Encryption Module 22**
- 3.4.1 [hiddn]™ OEM Technology 22
- 3.4.2 [hiddn]™ Serverpark Application 22
- 3.4.3 [hiddn]™ Surveillance Application 23
- 3.5 [hiddn]™ Key Management System (KMS) 24**
- 4 Work 25**
- 4.1 Sample Upgrade Operation in User Organisation 25
- 4.1.1 Issues Related to Upgrade of Existing PCs 25
- 5 Related Documentation and Abbreviations 27**
- 5.1 Applicable Documents 27

List of Figures

- Figure 1 [hiddn]™ Architecture 12
- Figure 2 [hiddn]™ Crypto Module with Smart card reader 12
- Figure 3 [hiddn]™ Laptop Concept 14

Date:	Revision:	Author:	Approved:	Doc. No:
26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

Figure 4 [hiddn]™ Laptop – SATA 15

Figure 5 [hiddn]™ Laptop installed in Laptop with side-mounted disk drive..... 16

Figure 6 [hiddn]™ Laptop with Contactless smart card interface 17

Figure 7 [hiddn]™ Desktop PCI card 18

Figure 8 [hiddn]™ Desktop 18

Figure 9 [hiddn]™ SATA Adapter – Standalone 19

Figure 10 [hiddn]™ SATA Adapter – w/ Disk & w/ Disk in Enclosure 19

Figure 11 [hiddn]™ Crypto Adapter – w/ Memory Stick and Smartcard 20

Figure 12 [hiddn]™ Crypto Adapter..... 20

Figure 13 [hiddn]™ Crypto Adapter w/ Hard Drive Extension 21


Figure 13 [hiddn]™ Serverpark Application 22

Figure 14 [hiddn]™ Surveillance Application 23

Figure 15 [hiddn]™ Key Management System – GUI & Standard Installation 24

Figure 16 [hiddn]™ KMS & Unit Architecture 24

Figure 17 Sample upgrade procedure in organisation..... 26

	Date: 26.02.2010	Revision: 1.6	Author: TF/AV/BN/OST	Approved: OST	Doc. No: 2009/9/Specifications/4
----------------------------------------------------------------------------------	---------------------	------------------	-------------------------	------------------	-------------------------------------

1 Introduction

1.1 General

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

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

1.2 Summary

[hiddn][™] 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][™] 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][™] 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, versatile, and flexible [hiddn][™] Crypto Module (CM) serves in solutions for data protection for laptops, desktops, memory sticks, external storage media, serverparks, and UAVs.

[hiddn][™] 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][™] provides for several additional functionalities and features unique to the full disk encryption market (ref. Contactless optional solution).

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/Ost	Ost	2009/9/Specifications/4

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 AES 256-bit individual encryption key(s).


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][™] 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][™] 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 were part of a project group with the chief goal of certifying and validating the encryption already developed 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][™] 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+.

To secure further commercialization and industrialization of the patented and HDD-owned technology, additional equity was raised September 2009. HDD then went through a process with new external investors, securing 24 MNOK in new fresh capital. The investment included 14 MNOK from Incitia Ventures II AS, 3 MNOK from HDD’s Management Team and 7 MNOK from existing owners. In addition, a previous debt of 3 MNOK was converted into shares, and the participants in this capitalization secured an option (subscription right / warranties) to raise an additional 10 MNOK in future equity. Following this capitalization, the company is valued at 45 MNOK (2009). Incitia Ventures II AS is now the largest single shareholder, with more than 34 % of HDD’s overall shares.

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

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. The [hiddn]™ encryption technology will cater for all 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:
	26.02.2010	1.6	TF/AV/BN/OSt	OSt	2009/9/Specifications/4

2.2 Concept

[hiddn][™] is a hardware based data encryption device designed for the encryption of user data stored in a computer storage device (Hard Drive). **[hiddn]**[™] 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]**[™] 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][™] is a self-contained hardware encryption engine. It resides in the data path between the computer motherboard and the storage device. **[hiddn]**[™] 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]**[™] 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]**[™]. 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]**[™]. 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]**[™].

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

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

2.3.2 User Role

The normal user of the services provided by [hiddn][™] is referred to as the User. The User will use [hiddn][™] 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.

2.4 Encryption Keys

[hiddn][™] 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.

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

2.5 Capabilities and Characteristics

2.5.1 Normal Mode

In the normal mode of operation, [hiddn][™] 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][™] 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][™] 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].

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][™]. [hiddn][™] 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][™] 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:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

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 (ZIF/LIF, SSD, 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 3.3.1.3.

hdd High Density Devices	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

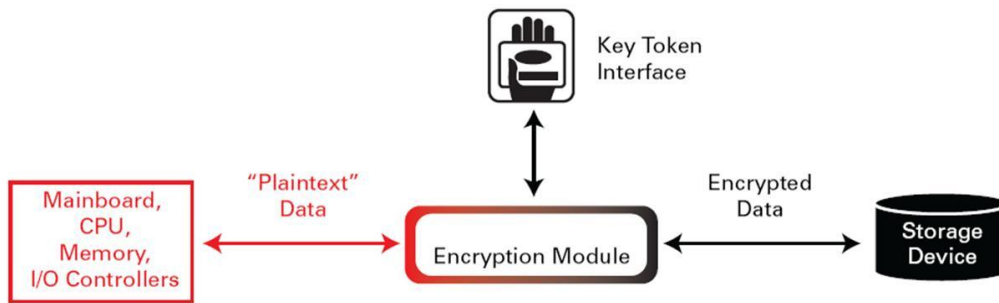



Figure 1 [hiddn]™ Architecture



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

	Date: 26.02.2010	Revision: 1.6	Author: TF/AV/BN/OSt	Approved: OSt	Doc. No: 2009/9/Specifications/4
-----------------------------------------------------------------------------------	---------------------	------------------	-------------------------	------------------	-------------------------------------

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, Crypto Adapter, serverparks, UAVs 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:
	26.02.2010	1.6	TF/AV/BN/OSt	OSt	2009/9/Specifications/4

3.3 [hiddn]™ Product Portfolio

[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 is a presentation of current solutions available based on the highly versatile Crypto Module.

3.3.1 [hiddn]™ Laptop

The unit 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 an 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.

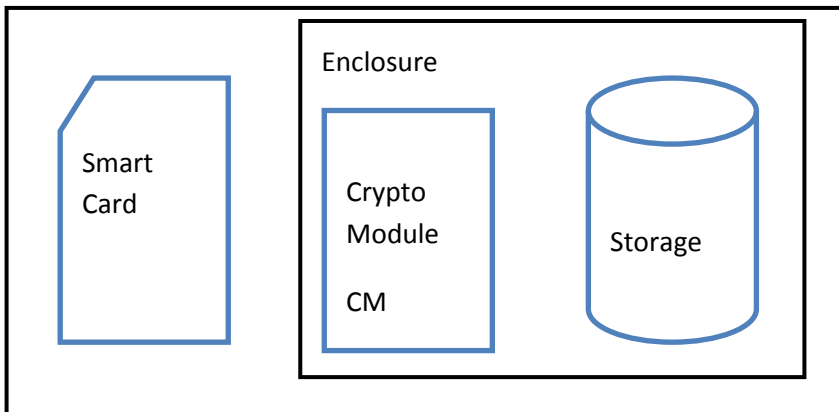



Figure 3 [hiddn]™ Laptop Concept

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.1.1 [hiddn]™ Laptop Solutions

[hiddn]™ Laptop 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:

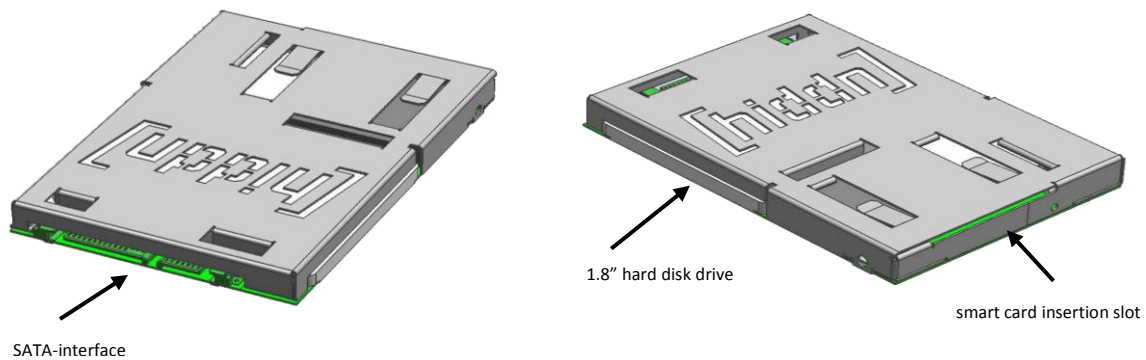


Figure 4 [hiddn]™ Laptop – SATA

hdd High Density Devices	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.1.2 [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 installed in Laptop with side-mounted disk drive

3.3.1.3 Optional Token Types – Contactless 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 an alternate solution:

- i) 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]™ 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]™ CM. In addition, an RF-antenna is mounted on top of the Enclosure. Thus, to activate the disk, an RF-based [hiddn]™ 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.

hdd High Density Devices	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

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

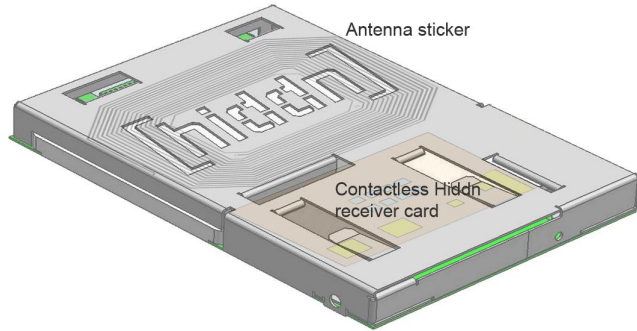



Figure 6 [hiddn]™ Laptop with Contactless smart card interface

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.2 [hiddn]™ Desktop

The [hiddn]™ Desktop unit is a PCI card with the [hiddn]™ Crypto Module mounted on, in addition to interfaces for data in/data out, power, and smart card reader. With [hiddn]™ CM installed, one internal disk in the PC can be connected and encrypted. The PCI card opens up for having two [hiddn]™ CM units installed on the same card, allowing for encryption of two hard drives simultaneously, e.g. for backup purposes.

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

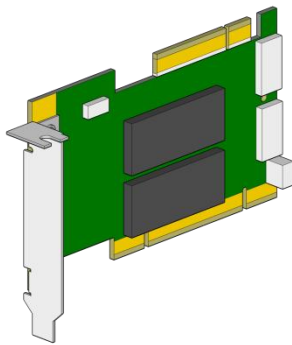



Figure 7 [hiddn]™ Desktop PCI card

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



Figure 8 [hiddn]™ Desktop

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.3 [hiddn]™ SATA Adapter

Incorporating the [hiddn]™ Crypto Module, this compact application enables full-disk encryption of any SATA drive. The unit consists of the [hiddn]™ Crypto Module mounted on a carrier board with integrated smart card reader(s) and a “USB-to-SATA” conversion card, enabling the user to connect any SATA drive to the board and then connect the unit to a computer using USB-cable.

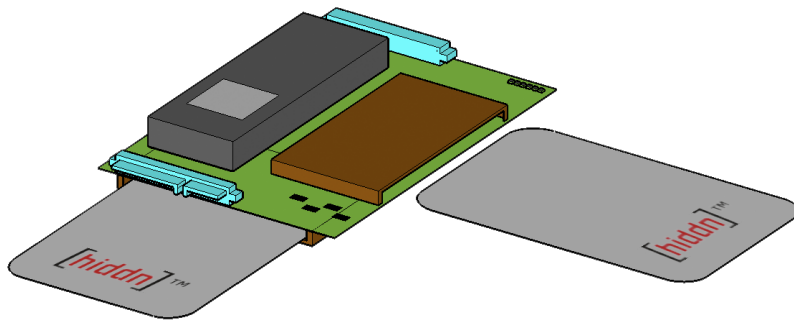


Figure 9 [hiddn]™ SATA Adapter – Standalone

The SATA Adapter can be delivered either as standalone application for OEM into third party products, as a unit with hard drive mounted for insertion into third part enclosures or as a complete [hiddn]™ external hard drive end-product. Versatility and flexibility is a keyword for describing this unit, as it offers a certified and robust encryption solution for both OEM partners and end-users.

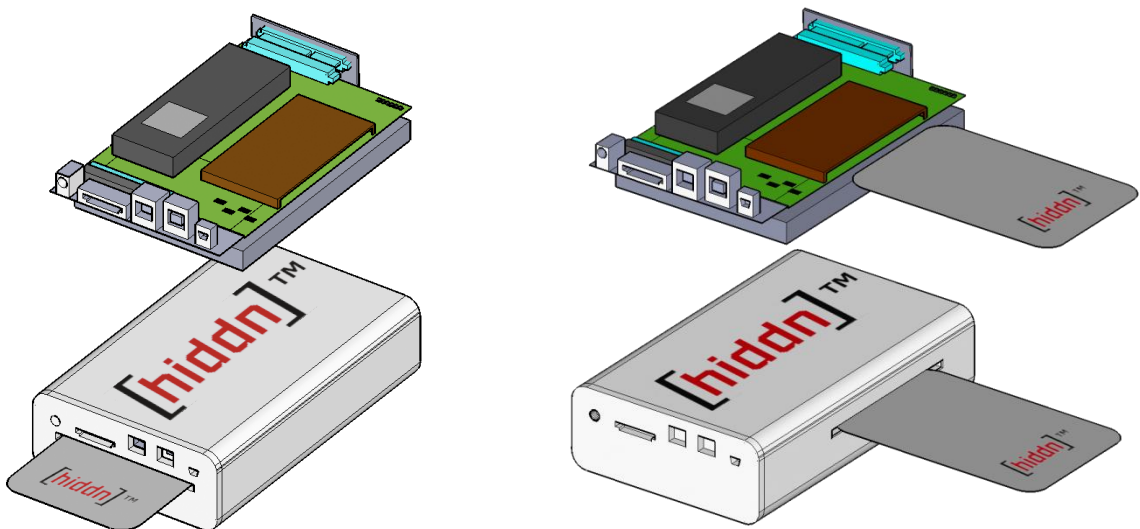



Figure 10 [hiddn]™ SATA Adapter – w/ Disk & w/ Disk in Enclosure

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.4 [hiddn]™ Crypto Adapter

The [hiddn]™ Crypto Adapter is a unique and exclusive product for encryption of all USB-connected external storage media. The Crypto Adapter contains all encryption functions, including the [hiddn]™ CM, smart card reader, and input for two-way authentication (PIN). It connects to a PC northbound and a storage device southbound both using standard USB2.0 interfaces.




Figure 11 [hiddn]™ Crypto Adapter – w/ Memory Stick and Smartcard

Encryption of memory sticks has never been easier with the [hiddn]™ Crypto Adapter, and the cost of losing data stored on a memory stick is effectively reduced to the minimal cost of losing a low-price memory stick – i.e., it demolishes the need for expensive encryption memory sticks as [hiddn]™ encrypts any storage media!



Figure 12 [hiddn]™ Crypto Adapter

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.3.4.1 [hiddn]™ Crypto Adapter – Optional Hard Drive Extension

The [hiddn]™ Crypto Adapter is also available with an optional hard drive extension. With this extension, the [hiddn]™ Crypto Adapter connects to any SATA 2.5” hard drive. Simply mount the drive in the enclosure and connect it to the Crypto Adapter for full-disk encryption. Ideal for backup purposes and for processing larger amounts of data, the extension can easily be disconnected and stored as all data on the drive will be inaccessible without the correct smart card and PIN code.



Figure 13 [hiddn]™ Crypto Adapter w/ Hard Drive Extension


3.3.5 [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.

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

3.4 [hiddn]™ - Versatile & Modular Encryption Module

The highly versatile and modularly designed Crypto Module can be applied to address a vast number of data protection needs, from the end-user solutions presented above to more complex encryption solutions and systems. The following sub-sections will highlight some of the opportunities presented through the patented and certified technology.

3.4.1 [hiddn]™ OEM Technology

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

- [hiddn] Crypto Module – the certified Crypto Module FPGA-module (dimensions: 70mm x 30mm x 8mm)
- [hiddn] ASIC – to be released low-cost chip solution ASIC-chip (dimensions: 10mm x 10mm)
- [hiddn] 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.

3.4.2 [hiddn]™ Serverpark Application

The [hiddn]™ Crypto Module can be incorporated into a Serverpark solution for full-disk encryption of enterprise servers, based on the very same principles as for the end-user products – installing the [hiddn]™ Crypto Module in-between the data path. Such a scenario will be based on a customer specification process, but is viable with the FIPS & Common Criteria certified module, providing for a rigorously tested and easy-to-use solution for protection of server data.



Figure 14 [hiddn]™ Serverpark Application


	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OSt	OSt	2009/9/Specifications/4

3.4.3 [hiddn]™ Surveillance Application



Figure 15 [hiddn]™ Surveillance Application

The same [hiddn]™ Crypto Module as used in all other applications documented, is also ideal for encryption of “video-on-the-fly”, such as encryption of UAVs and CCTV footage. The UAV encryption case will for example provide the UAV with on-board encryption of all data stored on the unit, in case of it ending up in the hands of the wrong people, or if it is lost. CCTV footage is stored in large amounts throughout the world, and this footage will be far better protected if it was encrypted by the [hiddn]™ encryption technology – ***Safeguarding all data at rest, anywhere!***

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

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 16 [hiddn]™ Key Management System – GUI & Standard Installation

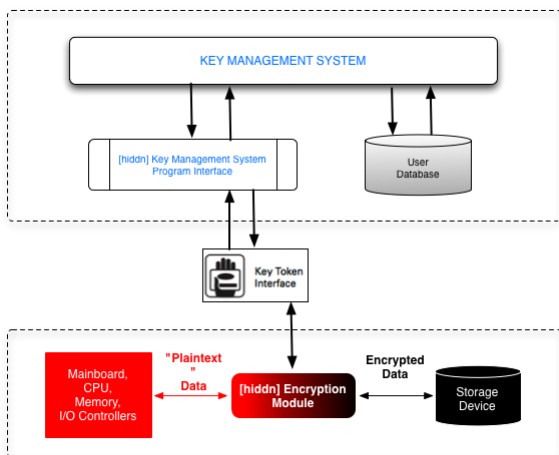



Figure 17 [hiddn]™ KMS & Unit Architecture

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OSt	OSt	2009/9/Specifications/4

4 Work

The instructions required to install and operate [hiddn][™] 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][™] 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][™] USB enclosure as an external transportable encrypted disk, serving e.g. as a secure local back-up solution.

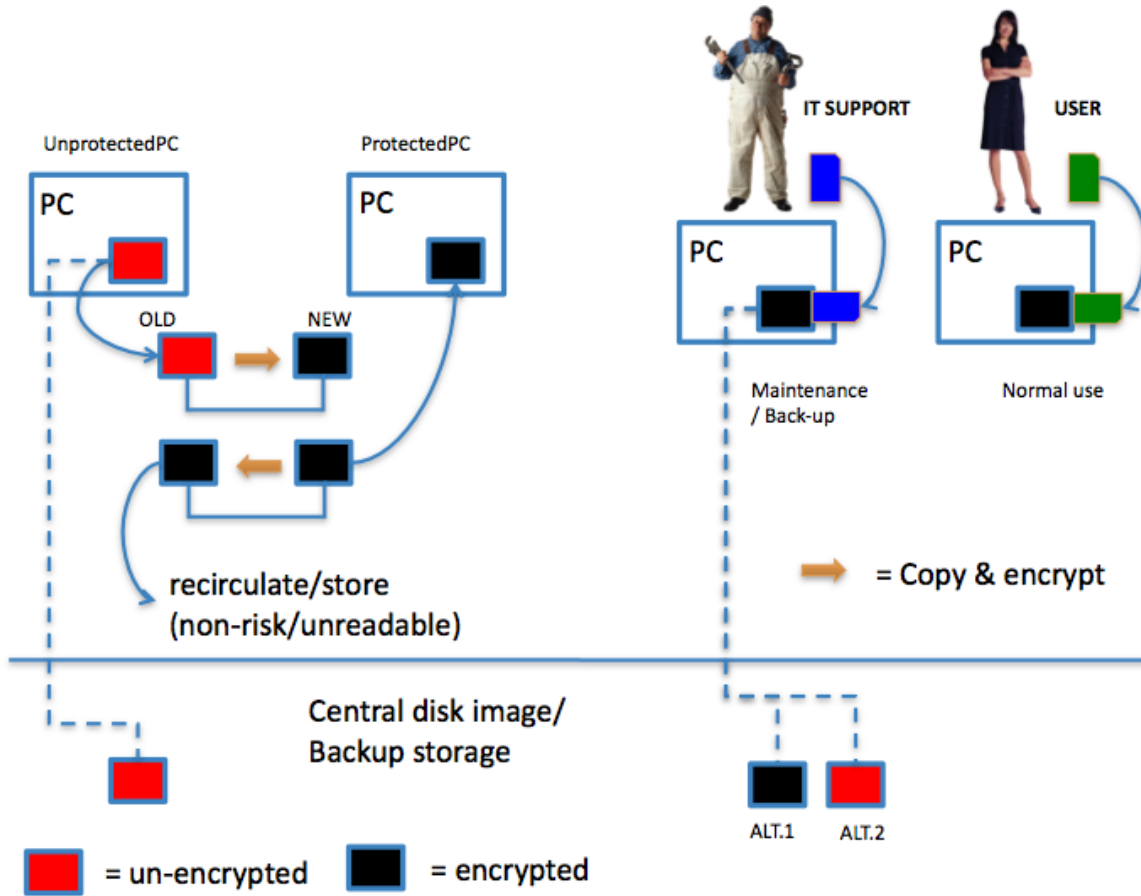



Figure 18 Sample upgrade procedure in organisation

	Date:	Revision:	Author:	Approved:	Doc. No:
	26.02.2010	1.6	TF/AV/BN/OST	OST	2009/9/Specifications/4

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.