

# **[hiddn]<sup>TM</sup> Crypto Adapter**



## **User Guide**

Off-the-shelf version with two random generated Smartcards (keys) included

**VERSION 1.4**  
(Software version 1.x)

Thank you for purchasing the **[hiddn]™ Crypto Adapter!**

Please take the time to read this Guide carefully as it contains important information on how to use the **[hiddn]™ Crypto Adapter**.

## 1. About USB Storage Devices and the famous **[hiddn]™ Crypto Adapter**.

The **[hiddn]™ Crypto Adapter (CA)** is based on the **[hiddn]™ CryptoModule (CM)** and is designed to allow for encryption/decryption of general purpose and low cost USB Storage Devices like USB memory sticks, thumb drives, etc.

The **[hiddn]™ Crypto Adapter** supports in theory any type of USB storage devices with any capacity. However, as the market is packed with a variety of USB storage devices, HDD cannot make any guarantees the **CA** will work with every device on the market. Thus, the **CA** owner and user are urged to test devices properly before deploying data full-scale. Please also observe normal procedures for back-up of important information, etc.

In addition, the **CA** is in theory compliant with any operating system supporting USB 2.0. However, HDD cannot make any guarantees the **CA** will work with every operating system available. The **CA** has been tested in a large number of such configurations to the satisfaction of HDD. Please also observe that some operating systems can lead to slightly different behavior of the **CA** (e.g. having to re-insert the cable between USB memory stick sessions).

The **CA** does not require any **CA**-specific software drivers within the PC, and is based on utilizing the PC's (operating system's) standard **USB generic disk drivers** and **USB mass storage drivers**.

The **CA** does not support specific functionality (based on e.g. specific software drivers provided by the various vendors of such units) offered by some USB storage devices like built-in launch platforms (e.g. U3), CD drives, encryption, etc. The **CA** only supports the USB mass storage device part of such storage devices (in some cases a removal tool would have to be applied to achieve **CA**-support (e.g. removing unwanted parts of the U3 launch platform). Thus, HDD strongly recommends standard plain USB storage devices (also ensuring low cost and cost-efficiency).

The **CA** is designed to operate within a highly secure environment and adheres to a strict security regime utilizing the overall powerful features of the **[hiddn]™ CryptoModule**. Thus, this **User Guide** should be read in detail to allow efficient and secure use of the USB storage devices.

The **CA** provides for hardware based full-disk encryption of the connected USB storage devices, and all such units need to be formatted as the first step. Once formatted, the units store encrypted data fully transparent to the operating system's file system (with close to real time performance) as long as the **CA** is involved. However, if such an encrypted device is connected directly to a PC it will pop-up as an un-formatted drive with no identification on the encrypted data stored on the device.

Enjoy!

## 2. Introduction

**[hiddn]™ Crypto Adapter (CA)** safeguards your data anywhere. Connect a thumb drive or an external hard disk (USB) and begin protecting your data. With the **[hiddn]™ CA** you can be assured that all data will be encrypted and only accessible when accessed through the **[hiddn]™ CA**.

All data stored on the storage media will be encrypted, and the only way to read it in decrypted form is to connect the storage media to the **[hiddn]™ CA** and authenticate using your smartcard and PIN-code.

## 2.1. Box Contents

- 1 [hiddn]™ Crypto Adapter
- 1 USB-cable
- 1 “User Smartcard”, 1 “Backup Smartcard” , 1 “ZEROING” Smartcard (not to be used) and your PIN-code & PUK-code.

### Please note!

**The Backup Smartcard, the “ZEROING” Smartcard, the PIN-code and the PUK-code must be kept in a secure place. Without your PIN-code, you cannot retrieve data from a storage media that is encrypted.**

## 3. System Requirements and Physical connections

The [hiddn]™ CA requires normally only to be connected to one USB port on your computer. One port is normally sufficient, providing necessary power is provided by the computer’s USB port. However, if power is not sufficient, the second USB plug needs to be connected to another USB port on the PC (the USB plug with the thinnest lead (USB power plug)).

Any storage device with a USB-connection can normally be used together with the unit.

## 4. Installation

1. **Connect** the [hiddn]™ CA with the attached **USB-cable** to your computer and observe the Status LED turn red & green .
2. **Insert** the User Smartcard and observe the PIN LED blinking green (chip facing down)



## 5. Normal operation

- Make sure the cable is properly connected and **fully inserted at all times**.
- The USB-storage device can be connected before or after the Smartcard is inserted.
- Insert the User Smartcard and observe the PIN LED blinking green. Type your **PIN-code** and complete with #. A correct PIN-code will be confirmed with a steady green light on the PIN LED.
- Observe the Status LED going from green/red to a steady green light when a memory stick is inserted.
- When both LEDs show a steady green light the Crypto Adapter is ready to protect your data.
- Your computer will normally automatically detect any connected removable storage device. If not, you may have to initialize and format the device (consult your operating system manual for procedures on initializing and formatting external USB storage devices).
- If the device has been used before with the [hiddn]™ CA, your computer will detect and identify the unit and present the file system and the files on the storage device.
- To stop (remove) using the USB storage device, follow procedures for safe removal of external storage media, in accordance with the operating system in use.
- If you want to connect a new USB storage device, remove the first device and insert the new device. Normally, it's not required to remove and re-insert the USB cable to the PC (however, some operating systems require this).



**NOTE: Always store the User Smartcard, the Backup Smartcard, the “ZEROING” Smartcard and the PIN/PUK-code in a safe place when not in use.**

## 6. Trouble shooting

### 6.1. General

1. After entering the PIN-code the PIN LED shows a red light and starts to blink green again.
  - Wrong PIN-code has been typed. Make sure you use correct PIN-code.
2. After inserting a Smartcard the PIN LED is blinking red.
  - Wrong PIN-code has been typed 3 times and the Smartcard is locked. To unlock the Smartcard use the PUK-code received with your PIN-code. Follow the instructions on the enclosed printed card.
3. The connected storage device is not visible in my computer's file system overview (e.g. Windows Explorer).  
You may have to initialize and format the device.

**Please observe:** By performing this sequence, all data on the connected storage device will be permanently erased. Please perform backup of data you want to keep before you start initialization - process.

To initialize the device, consult your operating system's manual.

For e.g. MS Windows:

- In Windows, click "Start" - then select "Control Panel".
- Select "Administrative Tools" and double click "Computer Management".
- From the "Console Tree" select "Disk Management".
- Right click the disk you want to initialize, and then click "Initialize Disk".
- The "Initialize Disk" dialog box will appear - perform initialization.

When initialization is completed, right click on the disk you have initialized and select "Format". Any type of file system can be selected according to your preferences (we recommend "default" settings).

4. The Status LED is consistently rapidly blinking red
  - The encryption hardware failed the self-test – please restart the CA. If the error persists – contact your dealer.

### 6.2. LED interpretation – PIN LED (user interface error codes)

**At initial processing of the inserted Smartcard:**

Reason	PIN LED
Un-readable Smartcard	Red (after approx. 200 ms)
Not valid Smartcard (type, format, lacking PIN-code, etc.)	Red (immediately)
Wrong PIN-code	Red (for about 2 second)

**After approved Smartcard and accepted PIN-code:**

Reason	PIN LED
Un-readable/un-supported USB storage device	Green/Red blink (green & red, i.e. yellow)
Lack of sufficient power	Green/Red (steady)

## 7. Use of the Backup Smartcard

If you ever lose the *User Smartcard*, you can use the *Backup Smartcard* to get access to your data. The PIN-code for the *Backup Smartcard* is identical to the PIN-code for *the User Smartcard*.

## **IMPORTANT**

Please note the following when using your **[hiddn]<sup>TM</sup> CA**:

- The **[hiddn]<sup>TM</sup> CA** is delivered with two Smartcards (and a separate “ZEROING” card – not to be used before you eventually purchase and receive a new set of Smartcards) containing random generated encryption keys.
- HDD can IN NO CASE reproduce either of these Smartcards, if lost or rendered unusable by customer.
- If the User Smartcard is lost or becomes unusable, it is strongly recommended to use the Backup Smartcard to make a backup of your data stored on the device to another storage device. Then a new set of Smartcards should be ordered (see below).
- A NEW set of User and Backup Smartcards can be ordered from HDD. This will NOT give access to any data stored prior to using this new set of Smartcards (all data stored with previous Smartcards will be lost unless you have made a backup that can be restored onto your storage device after the new set of Smartcards is initialized). To enable this – according to a separate guide provided together with the new set of Smartcards – you will need to use the “ZEROING” card in conjunction with the last set of Smartcards eventually purchased and received.
- If your organization has access to **[hiddn]<sup>TM</sup> Key Management System (KMS)**, lost or unusable cards can be substituted (reproduced) if originally provided by your **KMS**.
- HDD accepts no responsibility for any data lost or left inaccessible due to loss or misuse of Smartcards or for any other reason.

HDD offers a **Key Management System (KMS)**. This proprietary administrative utility system is for managing lifecycle functions of **[hiddn]<sup>TM</sup> Smartcards** and the accompanying **[hiddn]<sup>TM</sup> products**. It is designed for larger organizations, value added resellers, IT managers of business units and military units deploying **[hiddn]<sup>TM</sup> technology**. The KMS is delivered as a dedicated workstation.

## **Trademarks / Trademark Disclaimers**

High Density Devices, HDD, **[hiddn]<sup>TM</sup>** and the HDD **[hiddn]<sup>TM</sup>** logo and graphics are trademarks and property of High Density Devices AS, Norway. All other trademarks are the property of their related companies.

## **Disclaimer**

High Density Devices AS accepts no liability for any consequential, incidental, direct or indirect damage (including loss of business profits, business interruption, loss of business information and similar events causing losses to business) arising from any action and/or inaction based on information contained in this document.

High Density Devices AS does not accept any liability for any loss of data and/or company and/or personal information that may result from any action and/or inaction based on information contained in this document. Users are instructed to make backups of all data prior to installation of any device or product described herein.

High Density Devices AS reserves the right to at any time and without notification, change its offer and/or price and/or availability of parts.

## **Contact High Density Devices AS**

E-mail: [support@hdd.no](mailto:support@hdd.no)  
Website: <http://www.hiddn.no>