[hiddn]® LapTop1+

Installation Manual

VERSION 1.8.8

Date: 04-March-2016

Hiddn Security AS http://www.hiddn.no // support@hiddn.no

1. Introduction

This document will explain what is delivered, how units are initialized (keys are loaded) and some alternatives for installing an operating system.

The Key Management System (KMS) Administrator is responsible for providing the required keys for initialization of the [hiddn]® LapTop1+ units. For guidance on how to use the KMS to program User Key Tokens, please see the KMS manual.

When working with the [hiddn]® LapTop1+ product it is important to remember that once the PIN/password is accepted and keys are loaded, the keys stay active until powered off. This means the keys will survive a reboot, which might occur frequently during installation of operating system or restoring backups. However, the slightest loss of power to the drive will cause the encryption keys to be cleared.

2. Overview

The [hiddn]® LapTop1+ system consists of the following:

- [hiddn]® LapTop1+ unit
    - 2.5” form factor, 7mm tall encrypted SSD
- [hiddn]® Smart Cards
    - One (or more) User Key Token
    - Optional Backup Key Token
    - Optional Zeroize card
    - Optional User Key Token in miniSIM form factor (2FF)

All smart cards come loaded with the [hiddn]® applet, ready for key loading using your KMS, if not being preprogrammed from the factory.

3. Physical Installation of the [hiddn]® LapTop1+

Prior to initializing the [hiddn]® LapTop1+, the original hard drive of the computer must be removed and replaced with the [hiddn]® LapTop1+ unit. Please consult your computer manufacturer’s manual for instructions on how to remove and replace hard drives.

1. Make sure the computer is powered off
2. Remove the hard drive cover from the outside of the computer
3. Remove the original hard drive from the computer
4. Move any rubber or plastic parts from the original drive to the [hiddn]® LapTop1+
5. Gently insert the [hiddn]® LapTop1+ unit
6. Press firmly at the end of the [hiddn]® LapTop1+ unit to ensure that the connector is properly inserted.
7. Reattach the hard drive cover and fasten any screws

The physical installation is now completed.

4. BIOS Configuration

Before the [hiddn]® LapTop1+ is ready for use you need to ensure that the SATA mode is set right.

1. Power on your computer
2. Enter BIOS, usually by pressing F2.
3. Set the SATA mode to AHCI or IDE (native). RAID mode is not supported.
4. Save settings and EXIT

When installing a preconfigured Windows image, selecting a SATA mode different from the one selected when building the image, will result in blue-screen when booting. This is a well-known Windows problem and is not related to the [hiddn]® LapTop1+.
As an alternative to BIOS the [hiddn]® LapTop1+ supports UEFI with Secure Boot disabled.

5. Defining boot order

When the computer is powered on, the BIOS configuration determines in which order to look for connected bootable media. A new installed [hiddn]® LapTop1+ unit will be recognized as an unformatted disk drive without any boot sector. For successful installation of an operating system, the boot order must be set correctly.

There are two ways of making the computer boot from a specific installation media:

1. Configure BIOS to boot from a connected USB, DVD or network bootable media if no bootable disk is found.
2. Most computers will let you enter a boot menu by pressing F12 during startup. Some manufacturers use another key. You can then select the correct boot media from a list.

After installing the OS, you might remove other boot devices than the disk from the list of boot devices in the BIOS settings. A CD-ROM in the boot list might introduce delays during boot.

6. First-time Initialization

The first time you are using the [hiddn]® LapTop1+, you must go through an *Initialization procedure*, where you enable the unit to recognize the *User Key Token* and load your keys into the unit. This is called a “Crypto Officer” operation.

1. Power on your computer
2. Wait for the message “Waiting for Key Token. Please insert…” to appear on the screen
3. Insert the Key Token
4. Follow on-screen instructions, and when prompted “New Officer Token. Press enter key to start initialization.”, use the computer keyboard and press “enter”
5. Enter your PIN/password and confirm with Enter
6. The message “Initialization started. Please Wait…” appears on the screen
7. Wait for the message “Initialization completed. Press a key to continue…”
8. Press a key on the computer keyboard and wait for the computer to reboot
9. Remove the Key Token
10. The [hiddn]® LapTop1+ is now ready for normal disk operation. The unit will stay in normal operation (with encryption keys loaded) until powered off. *Note that sleep mode will cut power to the [hiddn]® LapTop1+ if not disabled (ref chapter 12).*

11. While keeping the [hiddn]® LapTop1+ powered, the next step is normally one of the following:
    - **Install an operating system on the unit from a USB or DVD drive**. Insert the installation media and reboot the laptop with Ctrl+Alt+Del. Normally, the laptop should automatically boot from the installation media. If not, select the installation media manually when rebooting the computer. This is normally done by pressing F12 during startup, but varies between computer manufacturers.
    - **Install an operating system on the unit over network (PXE)**. Connect the laptop to a network with a configured boot server. Reboot the laptop by pressing Ctrl+Alt+Del. Normally, the laptop should automatically boot over network. If not, select network boot manually when rebooting the computer. This is normally done by pressing F12 during startup, but varies between computer manufacturers.
    - **Clone an existing disk to the [hiddn]® LapTop1+**. This procedure involves copying data from an existing disk over to the [hiddn]® LapTop1+. Refer to section 11 for details on cloning.
12. After installation is completed, your [hiddn]® LapTop1+ is ready for normal operation.

7. The Backup Key Token

If you lose the User Key Token, you can use the Backup Key Token to get access to your data.

1. Power on the computer
2. Observe that the message “Waiting for Key Token. Please insert…” appears
3. Insert the Backup Key Token
4. Observe that the message “New User Key Token detected. Press any key to continue…” to appear
5. Enter your PIN/password and confirm with Enter
6. Wait for the computer to reboot
7. Remove the Backup Key Token
8. The computer will boot as normal and is ready for use
9. Make a backup of your data.
10. Zeroize the module using the Zeroize card or the zeroize button on the [hiddn]® LapTop1+ unit
11. Obtain a new set of Smart Cards, reinitialize the [hiddn]® LapTop1+ unit and restore your data from the backup media.

8. Zeroization

The [hiddn]® LapTop1+ has a small opening to the right side of the miniSIM reader. Inserting a paper clip 2-3mm will activate the zeroize button which clears all keys and reverts the unit’s settings to factory default state.

If it is not desirable to open the computer, use the optional Zeroize Card delivered with the unit or ask your local KMS administrator to make one.

9. Change PIN/password

If not blocked by your KMS Administrator, the PIN/Password can be changed by the user in the following way:

1. Make sure the Key Token is **not** inserted in the reader.
2. Turn on the computer

3. The message “Waiting for Key Token. Please insert…” appears on the screen 4. Press the F1 key to change password
5. Insert Key Token in reader
6. Enter old PIN/Password
7. Enter new PIN/Password
8. Re-enter new PIN/Password
9. If the operation succeeds, “PIN code successfully changed” appears on the screen. Press any key to finish authentication.
10. If the PIN/password do not comply with the policy defined by your local administrator, it will be rejected and you will be asked to enter a stronger PIN.

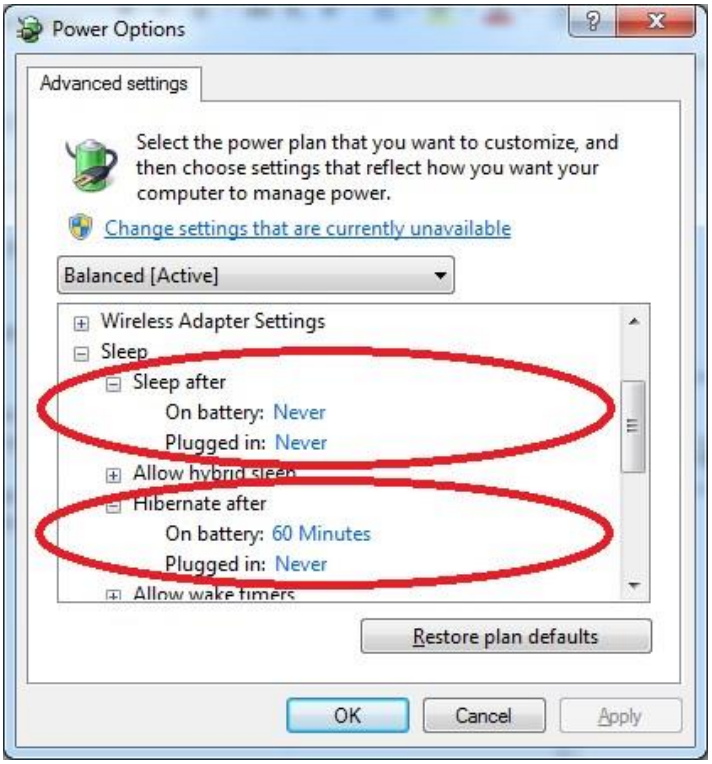
10.Display status information

Information about the installed unit can be obtained as follows:

1. Make sure the Key Token is **not** inserted in the reader.
2. Turn on the computer
3. The message “Waiting for Key Token. Please insert…” appears on the screen
4. Press the F2 key to display version information and serial numbers
5. Press T to display the temperature of the Crypto Module

11.Power Settings

One of the main security features with the [hiddn]® LapTop1+ is that the data encryption keys are cleared when the unit is powered off. This renders the unit useless for an attacker not having the User Key token and the PIN/passphrase.
However, to avoid that the unit inadvertently loses power, **and the encryption keys**, make sure to remove all options for entering sleep mode under “Power Options” in the Control Panel.



Sleep mode is under all circumstances a security risk, hence most security aware organizations already have deactivated sleep mode as a corporate policy.
Hibernation with a fully encrypted drive should be acceptable from a security point of view and is supported by the [hiddn]® LapTop1+.

Trademark Disclaimers

Hiddn Security AS, HDD, [hiddn], and the HDD [hiddn] logo and graphics are trademarks of High Density Devices AS.

Disclaimer

High Density Devices 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 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.

All [hiddn] Laptop parts are High Density Devices' parts, and High Density Devices does not accept any liability for any direct or indirect loss related to the handling and/or mishandling of any of the parts and/or a combination of the parts provided in this package.

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

Note:

HDD has the responsibilty that this equipment complies with the FCC criteria for radiation and any user made changes or modifications to this equipment that is not expressly approved by HDD could void the user's authority to operate this equipment.

Contact Information:

E-mail: support@hiddn.no
Website: http://www.hiddn.no