hiddn

KRYPTODISK 2

User primary card and data restore card

User Manual

English

Copyright © Hiddn, 2018. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder. Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder. Documentation is provided as is and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid.

KD02-UM-SK1-01.02-ENG-21.11.18

1. Introduction

The KryptoDisk 2 is the perfect solution for securely transporting data between the office and home, travelling with sensitive data, working between office branches and moving sensitive data between systems and platforms.

There are two ways of using the KryptoDisk 2 - either as a generic external storage disk, or as a bootable external disk. As an external storage disk, it provides you with a secure USB environment for file storage, while using it as a bootable disk enables you to use virtually any computer and still work in a secure environment.

The KryptoDisk 2 features a superior level of security and offers a GDPR – proof guarantee that secures you against GDPR breaches and potential fines if your KryptoDisk 2 is lost or stolen. Your data is protected with military grade AES 256-bit hardware encryption and a two-factor authentication. The data encryption key is stored on a Common Criteria EAL 5+ certified smart card and is deleted from the KryptoDisk 2 when the device is powered off.

NB: The GDPR-proof guarantee is only valid when the Smart Card is kept separate from the device.

The KryptoDisk 2 comes with a user primary card, a user data restore card and a PIN/PUK card. The user data restore card is in case your primary card is lost, stolen or broken. Please remember to keep the user data restore card and the card with PIN and PUK information in a secure place.

Upon first use, simply insert your user primary card into your KryptoDisk 2, enter the pre-set PIN code printed on your PIN/PUK card and connect the device to any computer. For a detailed walkthrough, please refer to section - Passphrase, PIN and PUK requirements.

The package includes the following:

- KryptoDisk 2
- USB Cable
- User primary card
  This is your primary user card, with a pre-set PIN code found on your PIN/PUK card. The PIN code can later be changed from the Admin menu.
- User data restore card
  The user data restore card is your back up if you have lost or invalidated your primary user card. Using the user data restore card requires the original PIN from the PIN/PUK card.
- PIN / PUK card

2. First time use

This section contains instructions on how to set up the KryptoDisk 2 during first use. Before you can start using the KryptoDisk 2, you must initialize (i.e. pair) the device and the user primary card (included), and format the hard drive from your computer's operating system.

Unlike most other drives on the market, Hiddn's two-factor encryption products cannot be pre-formatted. This is a security feature and a consequence of how the encryption module inside the KryptoDisk 2 is designed. When you pair the KryptoDisk 2 with the user primary card, the data encryption key is transferred to the device for the first time. That means that any pre-installed data (e.g. partition tables) would be unreadable. To be able to use the KryptoDisk 2 with your computer, the KryptoDisk 2 therefore needs to be formatted upon first use.

When the KryptoDisk 2 is initialized and formatted, it is ready to be used with your preferred device.

Initialize the KryptoDisk 2 encryption module

1. Insert the user primary card in your KryptoDisk 2
2. Connect the device to your computer using the included USB cable
3. The device will prompt you to confirm initialization using the user primary card. Press the "9"-key followed by the '#'-key to confirm.
4. Enter your PIN, do not unplug device.
5. Wait until the device prompts you to restart, then unplug the device from your computer
6. Connect the device to your computer again with the user primary card still inserted
7. The device will prompt you to enter a PIN code. The code can be found on the PIN/PUK card included with the user primary and user data restore cards

The device is now initialized and successfully paired with the user primary card. Please note that if you insert the user data restore card from this point onward, the user primary card will be invalidated, and you will have to order a new set of cards.

Please contact support@hiddn.no for purchasing new cards.

Initialize and format the KryptoDisk 2 hard drive

Before you can start using the KryptoDisk 2, the hard drive must be initialized and formatted. For instructions on this step, please refer to section 9**Error! Reference source not found.**.

Change PIN code

We strongly recommend that you change the pre-set PIN code. For instructions on this step, please refer to section 8 - Admin menu.

3. Daily use

This section contains instructions on the ordinary operation of KryptoDisk 2.

NB: We strongly recommend that you remove the user primary card from the KryptoDisk 2 when the authentication process is complete and the "Disk Unlocked" message appears in the display, especially when you are working in public spaces.

1. Power on the KryptoDisk 2
2. Insert the user primary card
3. Enter your PIN code
4. Connect the KryptoDisk 2 to your computer (or similar device) using the included USB cable. It is now unlocked and ready for use
5. Remove the user primary card from the KryptoDisk 2

4. How to respond in case of emergency [FAQs]

This section contains procedures for emergency situations like a lost, stolen or malfunctioning card or device, as well as information on how to use the user data restore card.

My user primary card was lost or stolen

If you have lost control of your user primary card, you should zeroize the KryptoDisk 2 immediately. Please refer to section 8 – Admin menu and follow the procedure *Zeroize without the user primary or user data restore card inserted.* This does not change or delete any data on the KryptoDisk, but only invalidates the currently accepted card. To regain access to the data on the KryptoDisk 2 initialise using the user data restore card.

NB: If your user primary card is lost or stolen, we advise you to order a new set of cards immediately. Please contact support@hiddn.no for a new set of cards.

My KryptoDisk 2 was lost or stolen

The tamper-proof hardware encryption module in the KryptoDisk 2 provides a level of security that is sufficient for the Norwegian Army and GDPR requirements, amongst others. The AES-256 encryption keeps your data safe against brute force attacks.

We strongly recommend that you destroy the user primary card and user data restore card by properly cutting through the smart card chip, the small and golden on your keycard.

My KryptoDisk 2 and user primary card was lost or stolen

In addition to being tamper-proof, the user primary card contains a secure retry-counter that protects the PIN code. After 5 unsuccessful attempts the user primary card will lock, and the only way to reactivate it is to enter the PUK code (which we recommended that you keep separately from the KryptoDisk 2). After 10 unsuccessful PUK entries the user primary card will be permanently locked.

If your KryptoDisk 2 is lost together with the user primary card, we strongly recommend that you destroy the user data restore card immediately, and eliminate any record of the PIN and PUK codes. If you follow these measures, the data on your device can be considered secure even though the user primary card was lost along with the device.

I forgot PIN code for my user primary card

If you forget your PIN code, you can use the PUK code to restore your PIN and regain access to your KryptoDisk 2. Please refer to section 8 – Admin menu for information on how to reset your PIN code.

1. Enter a wrong PIN code 5 times to trigger a prompt to enter the PUK code
2. Restart device
3. Find the PUK code from your PIN/PUK card and enter PUK, you will then be redirected to create a new PIN

I need to zeroize my card immediately

Some situations might require you to instantly zeroize your user primary card. The *emergency zeroize* function allows you to do this without entering the Admin menu.

1. While not connected to USB cable, insert your user primary card into the KryptoDisk 2

2. Power on the device
3. Press and hold the '3', '*' and '#'-keys for at least 1 second until "Card Zeroized" is shown
4. Connect the USB cable and "Zeroize Completed is shown followed by "Please restart.
5. Remove and reconnect the USB cable to verify that the KryptoDisk 2 is reset to Factory Default by observing that the KryptoDisk 2 shows "Initialize [Y/N]".

The KryptoDisk 2 stops responding when set up as a bootable disk

1. If booting from the KryptoDisk 2, the operating system might cut power to the USB bus during start-up. To prevent the KryptoDisk 2 from becoming unresponsive it might be necessary to set Keep Alive to 1 second. This will enable retransmitting the encryption key from the Card to the KryptoDisk 2 after the short loss of power.
2. Please refer to section 8 – Admin menu for further instructions.

5. Security recommendations

This section contains our recommendations on how to fully utilise the KryptoDisk 2's security features. The KryptoDisk 2 is an advanced security product capable of providing a very high level of data protection. However, as with any other product, security can be compromised by human error and wrong use. In this section, we have outlined some recommendations on how to establish good security habits.

Store the KryptoDisk 2 and the smart cards separately when not in use

The KryptoDisk 2 relies on a two-factor authentication scheme using a PIN code and a smart card. Effective protection requires that the authentication factors are kept separate from the device they protect when it is not in use. To ensure that you do not compromise this protection, we strongly recommend that the smart cards are stored separately from the KryptoDisk 2.

Keep PIN/PUK card and user data restore card in a secure place

The PIN/PUK card contains one the two factors to access the KryptoDisk 2, and should always be stored securely and separate from the device, except during initialization. It should also be kept separate from the user data restore card, as an attacker would be able to unlock the KryptoDisk 2 using the PIN/PUK card and the user data restore card together.

Change the PIN code on first use

We recommend that you change the PIN code that is printed on the PIN/PUK card upon first use of the KryptoDisk 2, and that you don't write down the new code. The PIN code can easily be changed from the admin menu, please refer to section 8 – Admin menu for instructions.

Remove the user primary card from KryptoDisk 2 when in use

We recommend that you remove the user primary card from the KryptoDisk 2 after the authentication process is complete, especially when working in a public place. As soon as the "Disk Unlocked" message shows in the display you can remove the card and store it separately from the KryptoDisk 2.

Back up your data

Make sure that you have a secure backup of your data, in case your device is lost, stolen or malfunctions.

Understand the concepts of zeroizing

Zeroizing is a key security feature in the KryptoDisk 2, which allows the user to disable communications between the device and the paired smart card. For an introduction to the concept of zeroizing, please refer to section 6 – Important information about Hiddn's security principles.

For information on how to zeroize and which method to use, please refer to section 8 – Admin menu.

Understand the principles behind Hiddn's unique security technology

To increase your familiarity with the security concepts underpinning the KryptoDisk 2, please refer to section – 6 - Important information about Hiddn's security principles.

6. Important information about Hiddn's security principles

This section contains information on the key principles of Hiddn's encryption and authentication technology, the core of the KryptoDisk 2's encryption module.

The KryptoDisk 2 derives its matchless security from a two-factor authentication scheme, where the factors are something you *know* – a PIN code – and something you *have* – a smart card. The key used to decrypt the data on the KryptoDisk 2 is stored on the smart card, and it is only transferred to the device if the correct PIN code is entered. Thus, the data on the device is impossible to access unless both factors are present.

The encryption solution used in the KryptoDisk 2 uses two Common Criteria EAL5+-approved smart cards (the user primary card and the user data restore card), each of which contains two different keys.

The *data encryption key* ("DEK") is the key that is used to encrypt and decrypt the data stored on the device. Without the DEK, the data is completely unreadable and impossible to interpret. Because of this, the key is identical in the user primary card and the user data restore card.

The *communication key* is the key that allows the KryptoDisk 2 and the smart card to communicate securely, which is necessary for the DEK to be transferred safely. The communication key is unique for each user primary card and user data restore card.

During initialisation, the communication key is copied from the smart card to the KryptoDisk 2 in a non-repeatable process, thus opening a secure communication channel between the device and that specific smart card. Because the encryption module can only hold one communication key, it is impossible to unlock the KryptoDisk 2 using another smart card, unless the device or card is zeroized.

Each time you use the KryptoDisk 2, the DEK is transferred from the user primary card to the device, allowing you to decrypt and access the data on the drive. If the device is unplugged from the computer, the DEK is deleted and must be transferred from the smart card again. This ensures that the data is secure even if the KryptoDisk 2 is lost or stolen.

Zeroizing is the process of disabling communications between the KryptoDisk 2 and its matching smart cards, and the opposite process of initialising. It is a key security feature, because the communication key can only be transferred once from a smart card. Thus, zeroizing the KryptoDisk 2 ensures that a lost or stolen smart card can never be used to access the data on the device. Please refer to section 8 – Admin menu for information on how to zeroize your KryptoDisk 2 safely according to your needs.

NB: Zeroizing must be performed with care, as it can possibly make all the data on the device unrecoverable if no user data restore card exists or while user data restore card is the active card.

7. Passphrase, PIN and PUK requirements

This section contains information on the requirements for PIN and PUK codes on your KryptoDisk 2 device.

- Between 7-15 digits in length
- Cannot contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Cannot contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- After 5 unsuccessful PIN entries the device is locked and PUK entry is required
- After 10 unsuccessful PUK entries the user primary card will lock, and you have to insert the data restore card to access your data. Please use the PIN / PUK from the PIN/PUK card when restoring data with the data restore card.

You can create a memorable word, name, phrase or any other alphanumerical PIN combination by simply pressing the key with the corresponding letters on it. Examples of alphanumerical PIN codes include:

PIN code “Password”:

7 (PQRS) **2** (ABC) **7** (PQRS) **7** (PQRS) **9** (WXYZ) **6** (MNO) **7** (PQRS) **3** (DEF)

PIN code “HIDDN”:

4 (GHI) **4** (GHI) **3** (DEF) **3** (DEF) **6** (MNO)

8. Admin menu

This section contains information on the Admin menu on the KryptoDisk 2, which is used for customization and administration of the device. Some of the controls in the Admin menu are only visible with the smart card inserted – these are marked with  a symbol in the list below. Others are only available on battery power – these are marked with 

To enter the Admin menu, press and hold the "0"-key while powering on the device. To navigate the menu, press the "0"-key , and press the "#"-key to select an option. Select the "Exit" option to leave the menu.

System info

This provides a list of version numbers and serial numbers for your device, which is useful if you must contact customer support for any reason. The smart card must be inserted for smart card information to be displayed.

Change PIN code

This allows you to change the PIN code of your card. You will be prompted to input your old PIN code, followed by a prompt to enter the new code, and finally a prompt to confirm the new code. The PIN code must comply with the requirements outlined in section 7 – Passphrase, PIN and PUK requirements.

 Set name

This allows you define a name for your KryptoDisk 2. The device name will appear in the display during start-up, allowing you to easily distinguish between multiple devices. If you assign a name to your device, the start-up process will be 2 seconds delayed allowing the name to appear.

You will be prompted to enter a device name. The KryptoDisk 2 uses alphanumeric inputs for this function, allowing you to input letters as well as numbers using the keypad. Confirm by pressing the "0/enter" key. To remove a stored name, simply erase all the characters using the "*" key and save an empty name.

Zeroize KryptoDisk 2

This allows you to zeroize your KryptoDisk 2 and smart cards.

Both the KryptoDisk 2 and the corresponding smart card can be zeroized, either separately or together. This disables all communication between the KryptoDisk 2 and the paired smart card. After a zeroization, the smart card is useless and must be replaced with either the user data restore card or a new user primary card.

There are various alternatives for zeroizing, and which to use depends on what your objective is. The alternatives, their uses and their consequences are listed below.

NB: If you zeroize after initialising the KryptoDisk 2 with the user data restore card, all data on the device will be lost. Make sure that you have backed up your data before doing this.

Zeroize without the user primary card or user data restore card inserted

This method is used if your user primary card is lost, stolen or malfunctioning.

When you zeroize without a smart card inserted, the encryption module in the KryptoDisk 2 deletes the communication key stored in the device, thus making it permanently unable to communicate with the smart card it was paired with during initialisation. To access the data on the device, you must use the user data restore card.

To zeroize without a smart card inserted, power up your device by connecting the KryptoDisk 2 to USB power and enter the Admin menu. Select the Zeroize option and confirm by entering "Y" (press the 9-key). If you want to cancel, enter "N" (press the 6-key). The device will confirm and prompt you to restart the device. Disconnect and reconnect the USB cable to complete the zeroize process.

To regain access to the data on the KryptoDisk 2 follow the procedure **Initialize the KryptoDisk 2 encryption module explained in** section**Error! Reference source not found.** 2 when replacing user primary card with user data restore card.

Zeroize both the smart card and the KryptoDisk 2

This method is used if you are replacing your smart cards.

NB: Be sure to have a verified backup of the contents of the KryptoDisk 2 before zeroizing both the smart card and the KryptoDisk 2.

When you zeroize both the smart card and the KryptoDisk 2, the encryption module in the KryptoDisk 2 deletes both the communication key stored in the device, and the communication key stored on the smart card. Deleting the communication key from the smart card adds another layer of security, as compared to deleting the key from the KryptoDisk 2 only.

To zeroize both the smart card and the KryptoDisk 2, power up your device with the smart card inserted and enter the Admin menu. Select the Zeroize option and confirm by entering "Y" (press the 9-key). If you want to cancel, enter "N" (press the 6-key).

If running on USB power, the KryptoDisk 2 will confirm and prompt you to restart the device. Disconnect and reconnect the USB cable, and the device will confirm that the zeroization was successful.

If running on battery power, the KryptoDisk 2 will only zeroize the smart card. You will then be prompted to connect the device to a computer. When connected to USB power, the device will confirm that the KryptoDisk 2 is also zeroized.

To regain access to the data on the KryptoDisk 2 follow the procedure **Initialize the KryptoDisk 2 encryption module** in the section 2 when using the user primary card from a new card set and restore data from backup.

Admin Battery Status

This displays the voltage (V) and charge (%) of the battery in the KryptoDisk 2.

Set Keep Alive

This allows you to activate and set the timer for *keep alive* mode. This mode allows you to establish a pre-set timer that keeps the KryptoDisk 2 unlocked after the device is unplugged (the timer can be set to maximum 240 seconds). This can be useful if the KryptoDisk 2 is to be moved from one computer to another in a secure environment. Keep alive has to be used if you are booting from the KryptoDisk 2 and the operating system cuts power to the USB bus during start-up.

To activate this mode, enter the Admin menu. If the KryptoDisk 2 is connected to a computer, you will be prompted to disconnect it. The display will reveal whether keep alive mode is currently active, where "0" means inactive. Enter how long (in seconds) you want the device to be unlocked after unplugging. The "*"-key functions as a backspace key. Press the "#"-key to save.

To disable the feature, enter "0" or simply delete the current setting and confirm.

NB: This functionality, while practical, can be a severe security liability if misused. If someone were to gain access to your KryptoDisk 2 while it is open and connected, they can steal it, connect it to their own computer and gain access to your data.

Only activate this feature if you are certain your environment is safe and that you understand the possible ramifications.

9. Initialising and formatting the hard drive

Formatting a hard drive in Windows

NB: Formatting in Windows requires admin access.

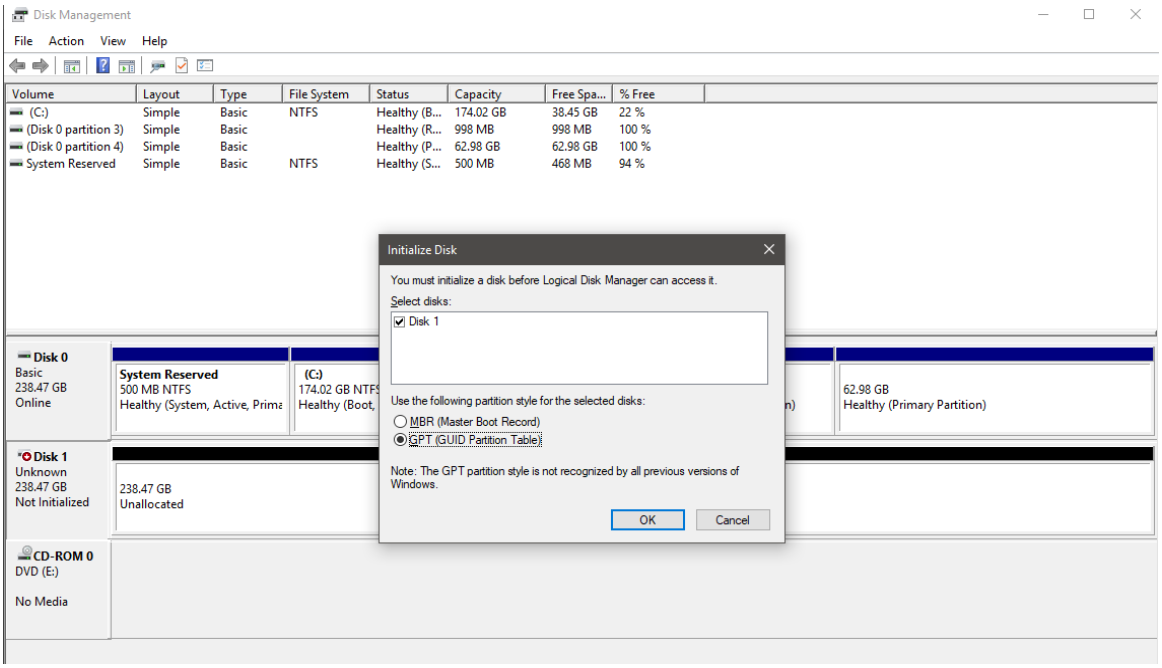
1. Open Disk Management

Open the Disk Management tool. How to do this depends on your version of Windows, but usually you can press the Windows key and type “Run” (consult Microsoft help pages to find the corresponding command if you have a native language installation of Windows). In the resulting dialogue box, enter *diskmgmt.msc*

The disk management tool will open and you can start formatting the disk.

2. Initialise disk

Disk initialisation should appear automatically. If it doesn’t, right-click on the icon and follow the instructions.



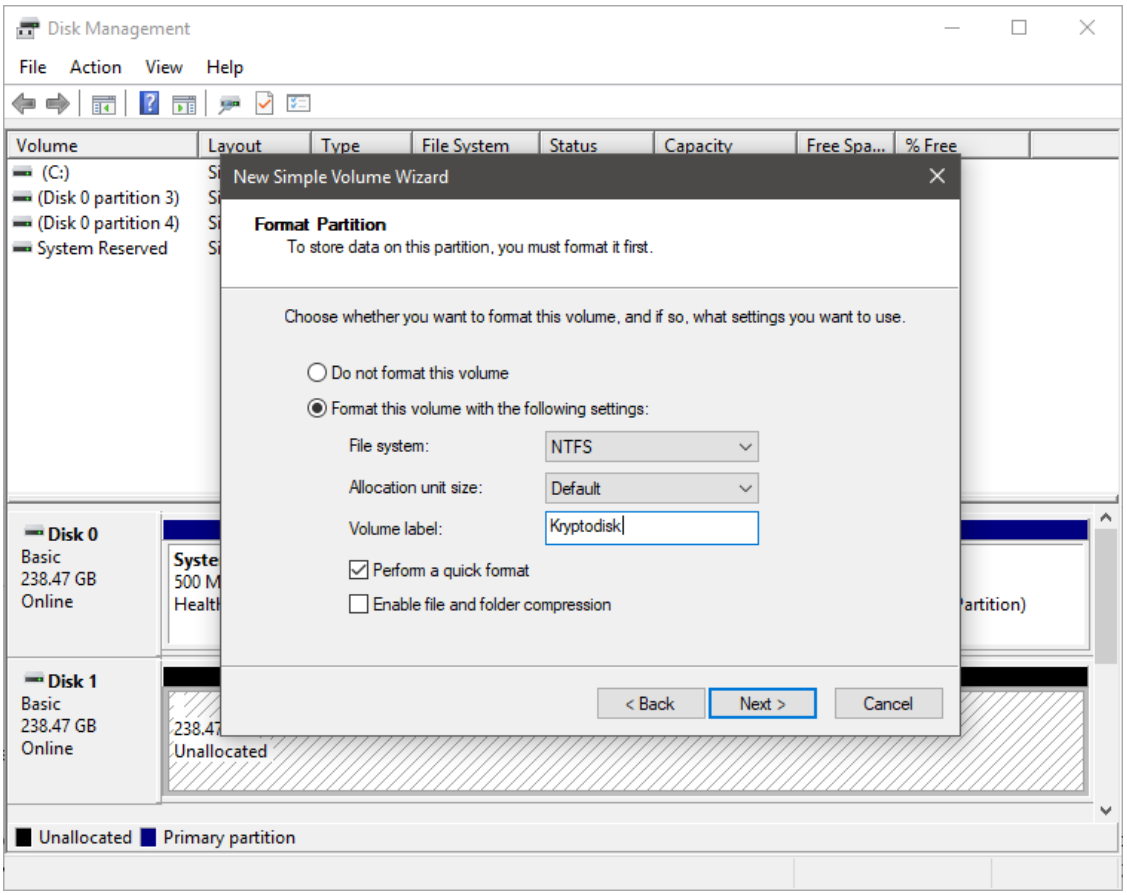
3. Partition and format disk

Once Disk Management opens, look for the new drive in the list.

NB: KryptoDisk 2 is a new hard drive that needs to be partitioned before use. In Windows, partitioning needs to be done before a hard drive can be formatted. The KryptoDisk 2 will probably be on a dedicated row labelled Disk 1 (or 2, etc.) and will say Unallocated.

- Tap-and-hold or right-click anywhere on it and choose New Simple Volume.
- Tap or click Next > on the New Simple Volume Wizard window that appears.
- Tap or click Next > on the Specify Volume Size step to confirm the size of the drive you're creating.
- Tap or click Next > on the Assign Drive Letter or Path step

Windows will now partition the drive, a process that will only take a few seconds on most computers. In Windows 10, Windows 8, and Windows 7 you will be asked to format the disk.



NTFS is the most recent file system available for Windows systems, and is recommended if you only intend to use your KryptoDisk 2 with Windows computers. If you want to move data between computers with different operating systems, e.g. Mac or Linux computers, select exFAT.

Our suggested settings for Windows-exclusive use are as follows:

File System	Allocation unit size	Volume label	Perform a quick format	Enable file/folder compression
NTFS	Default	[Your choice]	Yes	No

Our suggested settings for inter-platform use are as follows:

File System	Allocation unit size	Volume label	Perform a quick format	Enable file/folder compression
exFAT	Default	[Your choice]	Yes	No

Formatting a hard drive on Mac

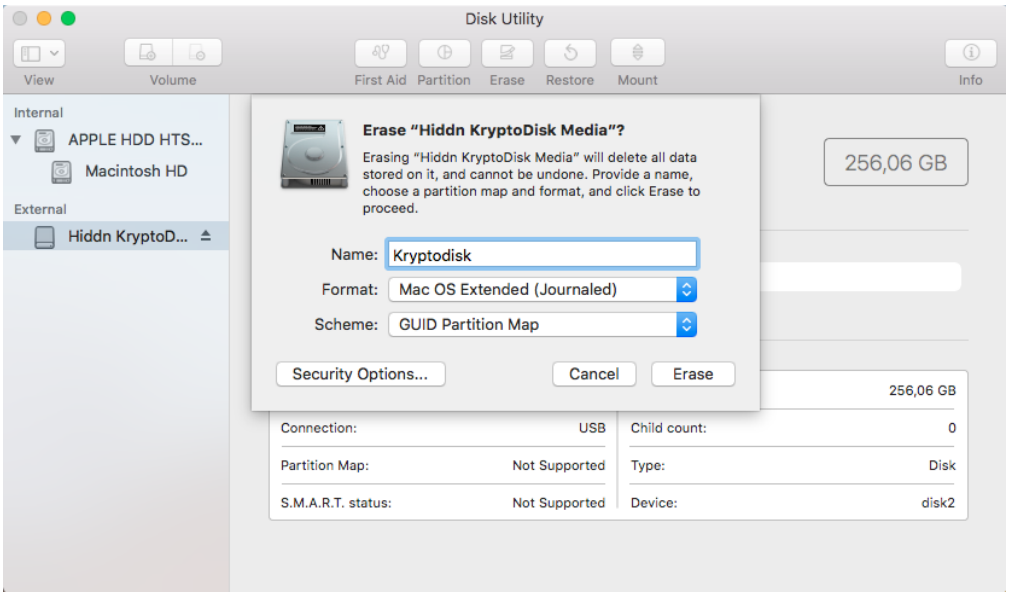
Launch Disk Utility, located in /Applications/Utilities.

1. Initialise disk

Disk initialisation will most likely pop up automatically. If not please click on the disk icon and a wizard will take you further.

2. Partition and format disk

From the left-hand pane, select the drive you wish to format. Click the Erase button at the top of the Disk Utility window, or select Erase from the Edit menu. A window should pop up resembling the image below.



Mac OS Extended (Journaled) is the default MacOS file system, and is recommended if you only intend to use your KryptoDisk 2 with Apple computers. If you want to move data between computers with different operating systems, e.g. Windows or Linux computers, select exFAT.

Our suggested settings for Mac-exclusive use are as follows:

Name	Format	Scheme
[Your choice]	Mac OS Extended (Journaled)	GUID Partition Map

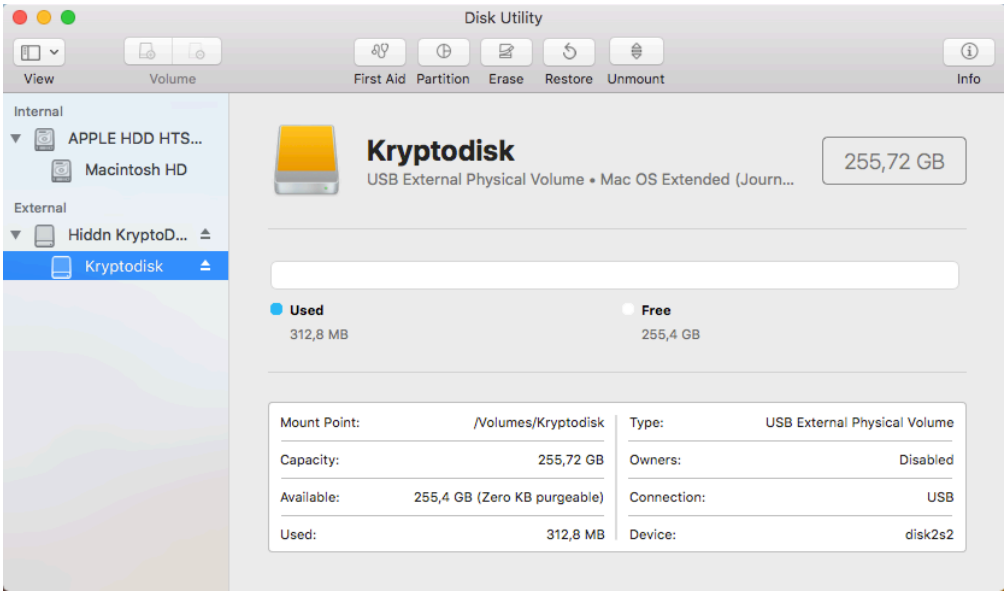
Our suggested settings for inter-platform use are as follows:

Name	Format	Scheme
[Your choice]	exFAT	GUID Partition Map

When you have configured your settings, click the Erase button.

Disk Utility will erase and format the selected drive, resulting in a single volume being created and mounted on your Mac's desktop.

Click the Done button.



10. Warranty and RMA Information

Two Year Warranty:

Hiddn offers a 2-year warranty on the KryptoDisk 2 against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from Hiddn or an authorised reseller.

Disclaimer and terms of warranty:

The warranty becomes effective on the date of purchase and must be verified with your sales receipt or invoice displaying the date of product purchase. Hiddn will, at no additional charge, repair or replace defective parts with new parts or serviceable used parts that are equivalent to new in performance. All exchanged parts and products replaced under this warranty will become the property of Hiddn.

This warranty does not extend to any product not purchased directly from Hiddn or an authorised reseller or to any product that has been damaged or rendered defective: 1) as a result of accident, misuse, neglect, abuse or natural or personal disaster, or any unauthorised disassembly, repair or modification or failure and/ or inability to follow the written instructions provided in this instruction guide: 2) by the use of parts not manufactured or sold by Hiddn; 3) by modification of the product; or 4) as a result of service, alternation or repair by anyone other than Hiddn and shall be void. This warranty does not cover normal wear and tear.

No other warranty, either express or implied, including any warranty or merchantability and fitness for a particular purpose, has been or will be made by or on behalf of Hiddn or by operation of law with respect to the product or its installation, use, operation, replacement or repair.

Hiddn is not liable for, and does not cover under warranty, any costs associated with servicing and/or the installation of the Product/s.

Hiddn Security AS
Oslo
Norway
www.hiddn.no

Compatible
with Windows,
macOS and
Linux

ALL TRADEMARKS AND BRAND NAMES ARE THE
PROPERTY OF THEIR RESPECTIVE OWNERS