

DIGITTRADE High Security HS256 S3

external encrypted HDD/SSD



For Enterprise and Government Use

Benutzerhandbuch
User Manual



PLEASE READ THE USER MANUAL CAREFULLY AND FOLLOW THE INSTRUCTIONS.

MISUSE CAN LEAD TO DAMAGE AND/OR DATA LOSS OF THE DIGITTRADE HIGH SECURITY HS256 S3 (EXTERNAL ENCRYPTED HDD/SSD).

PLEASE MAKE SURE THAT THE WARRANTY SEAL AND THE SECURITY PACKAGING HAVE NOT BEEN DAMAGED. ESPECIALLY PAY ATTENTION TO THE SECURITY LETTERING “DIGITTRADE SECURITY” ON THE SIDES OF THE SECURITY PACKAGING (SEE CHAPTER 1.8)

The digital copy of the user manual can be downloaded from www.digittrade.de at the download-center.

product version:	DIGITTRADE High Security HS256 S3 (encrypted HDD/SSD) version 1.0
user manual version:	1.8 (24.04.2017)

Content

1.	About the DIGITTRADE HS256 S3	55
1.1	Encryption	56
1.2	User authentication	56
1.3	Administrating the cryptographic keys	57
1.4	The smart card	57
1.5	Extra features	58
1.6	Overview of the most important features	58
1.7	DIGITTRADE HS256 S3 benefits	59
1.8	Security packaging and security seals	59
2.	Control panel and USB port	61
3.	Getting started with the HS256 S3	62
3.1	Inserting the smart card	63
3.2	Entering the smart card PIN	63
3.3	Changing the smart card PIN	65
4.	Administrating the cryptographic keys with the smart card	66
4.1	Creating the cryptographic keys	66
4.2	Deleting the cryptographic keys	67
5.	Device PIN features	69
5.1	Changing the device PIN	69
5.2	Activating/deactivating of the lock-out mode (Device PIN needed)	70
5.3	Copying the cryptographic keys (Device PIN needed)	71
5.4	Initialising a new smart card (Device PIN needed)	73
6.	Initializing/partitioning and formatting with Windows	74
7.	Initializing/partitioning and formatting with Mac OS X	80
8.	Initializing/partitioning and formatting with Linux	82
9.	The correct file system	85
10.	Possible usage of the DIGITTRADE HS256 S3	86
11.	Technical specifications	91
12.	Troubleshooting	92
13.	Data security and disclaimer	93
14.	Appropriate handling of the HS256 S3 for data privacy	94
15.	Safe shutdown after using the HS256 S3	96
16.	Smart card storage	96
17.	Product contents	97
18.	WEEE Statement	97
19.	Functions diagram	98

1. About the DIGITTRADE HS256 S3

The DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) enables the privacy-compliant storage and keeping as well as the safe transport of personal data. Thanks to the security features it is one of the safest solutions to save mobile data.

From the point of the stored data the DIGITTRADE HS256 S3 is secure from unauthorized access even in the case if it will be lost, misplaced or stolen as well as from digital and physical attacks.

The DIGITTRADE HS256 S3 is delivered completely pre-set and is ready to use for the data storage. In the BSI-certified configuration, the user is only allowed to use the hard drive, after he has changed the smart card PIN, the encryption key on the smart card has been generated by himself and the smart card has been initialized.

To use the whole security properties of the HS256 S3 and according to the BSI certification, the following steps are besides necessary:

- Ensure that your host system has a proper protection of all data retrieved from the protected storage of the DIGITTRADE HS256 S3
- Make sure that no malware can be transferred to the hard drive
- Check the security package after the receiving (chapter 1.8)
- Check the range, the completeness and the correctness of the delivery (chapter 17)
- Check all functions of the device after the first start (chapter 3)
- Change the smart card PIN (chapter 3.3)
- Change the device PIN (chapter 5.1)
- Create a new cryptographic keys (chapter 4.1)
- Initialize the smart card with the new cryptographic keys on the HS256 S3 and format the hard drive afterwards (chapter 5.4, 6-9)
- Copy the cryptographic keys on other delivered smart cards (chapter 5.3)
- Check if the login is possible with all smart cards
- Check continuously that the lock-out mode is activated (chapter 5.2)
- For effectively destruction of the encryption key the key must be deleted from all smart card that contains the key. Alternatively the whole hard drive must be overwritten by a new encryption key. (chapter 4.2)
- Keep your authentication data confidential
- The encryption key of the smart card must be used by one hard drive only

Detailed description of the above-named steps is outlined in relevant chapters of this manual.

The information about the type, version and serial number of the hard drive are located on the back of each HS256 S3. Because the hard drive is not updatable, this information is sufficient for determining the version of the delivered HS256 S3.

The DIGITTRADE HS256 S3 ensures the safety of the data through the following security mechanisms:

- Encryption
- User authentication
- Administration of the cryptographic keys

1.1 Encryption

- 256 bit AES full disk hardware encryption in XTS mode

The encryption module inside the secure casing encrypts the hard drive/SSD completely. Every saved byte and every written sector on the hard drive/SSD are encrypted according to 256 bit AES (Advanced Encryption Standard) in XTS mode with two 256 bit cryptographic keys.

The DIGITTRADE HS256 S3 encrypts additionally to all stored data temporary files as well as areas that would normally be unnoticed by encryption software.



1.2 User authentication

- 2-factor authentication using smart card and PIN

The user authentication is based on the principal “having and knowing”.

To get an access to the data the user must have the smart card and need to know the correct 8-digit PIN.

If the 8-digit PIN was entered incorrectly 8 times, the smart card is disabled and no longer usable. The cryptographic keys is also irreversibly deleted.

1.3 Administrating the cryptographic keys

With the device PIN the user can copy the cryptographic keys to another smart card, initialize new smart cards on the HS256 S3 and manage the lock-out mode. Instructions to this can be found in chapter 5.

In particular usage scenarios the knowledge of the smart card PIN and the device PIN can be split between two people, with the intention that only one person knows the device PIN and the other one smart card PIN. Knowledge of device PIN only will not enable the individual access to the data.

The cryptographic keys needed for de- and encrypting of the data is externally created and saved encrypted.

This means there is a physical separation between the encrypted data and the cryptographic keys, which makes it impossible to read the cryptographic keys from the DIGITTRADE HS256 S3. After the PIN has been correctly entered the cryptographic keys is transferred to the encryption module of the HS256 S3 to de-/encrypts the data. The external storage of the cryptographic keys enables a number of possible applications which are described in chapter 10.

1.4 The Smartcard

Serially the HS256 S3 works with two java based and Common Criteria EAL5 certified smart cards (NXP J2E081_M64 R3, CC EAL 5). For the use according with the BSI certification only these NXP smart cards are permitted.

These smart cards enable the creating, copying, changing and destroying of the cryptographic keys in use. The administration of the keys is supported by the DIGITTRADE HS256 S3 applet.

For the login on the hard drive are both smart cards needed with the the same cryptographic keys. The smart card PIN can be set differently for each smart card.

The type and the serial number of each smart card are displayed on the front of the smart card. The DIGITTRADE HS256 S3 version number is plotted on the back.

The permitted smart cards can be ordered separately at DIGITTRADE. These will be delivered without the cryptographic keys and have the factory set PIN (see chapter 3.2). To activate new smart cards, please refer to chapter 4.1, 5.3 and 5.4.

Warning: *If an invalid or defective smart card is inserted in the associated slot the “ERROR”-LED will flash three times and illuminate then permanently red. At these findings and accordingly if a smart card behave abnormally or if you identify defects during each operation, please contact DIGITTRADE.*

1.5 Extra features

The 2.5 inch built-in data storage device makes the HS256 S3 small and handy. The optional usage of SSD storage devices makes it shock proof. The data transfer and power supply are solved by USB. The hardware encryption method makes it possible to use the storage device on any OS and occurs transparently.

Accessing the data occurs without the loss of reading/writing speed.

1.6 Overview of the most important features

- 256 bit AES full disk hardware encryption in XTS mode with two cryptographic keys
- 2-factor authentication by smart card and 8-digit PIN
- external and encrypted storage of the cryptographic keys
- creating, copying and deleting the cryptographic keys by the user
- hardware based encryption module
- data encryption of all saved bytes and written sectors
- bootable and independent of the used OS (support for all operating systems, multimedia devices and machines with USB storage device support)
- compatible with USB 3.0 and USB 2.0
- without the loss of reading/writing speed
- handy 2.5 inch format and robust metal enclosure

1.7 DIGITTRADE HS256 S3 benefits

- private and business data are safe from unauthorized access
- easy and safe handling using hardware encryption: connect, log in, use it
- all data are immediately saved with encryption
- no performance loss
- integration into existing smart card infrastructures within companies

1.8 Security packaging and security seals

To avoid manipulation, a special security package is used for the delivery of the DIGITTRADE HS256 S3 and smart cards as well as for additional deliveries of smart cards. The contents will be described on the package.



After receiving, please check the inviolacy of the security lettering “DIGITTRADE SECURITY” on the sides. In addition there is a specific safety closure at the top which shows every manipulation attempts.

On the following images you can see possible indicators:



That's the safety closure when it has been properly closed and not opened again. The blue band at the top of the safety closure and the pale yellow thermal strip is undamaged.



In extreme cold conditions (e.g. use of cold spray) the areas of the blue tape will separate from the carrier material. The warning "STOP" is readable.



Through extreme heat (e.g. hair dryer), the pale yellow thermal strip turns red.



When using solvents, the blue color of the safety closure dissolves - manipulation is immediately visible.

Please check if these indicators have been damaged or removed when you receive the product. Contact your seller if the the security packaging have been manipulated, since the security of the HS256 S3 cannot be guaranteed in this case.

The components are sealed with epoxy resin. In addition there is a warranty seal placed on the opening point as seen below. This sealing is not evaluated by the BSI certification.

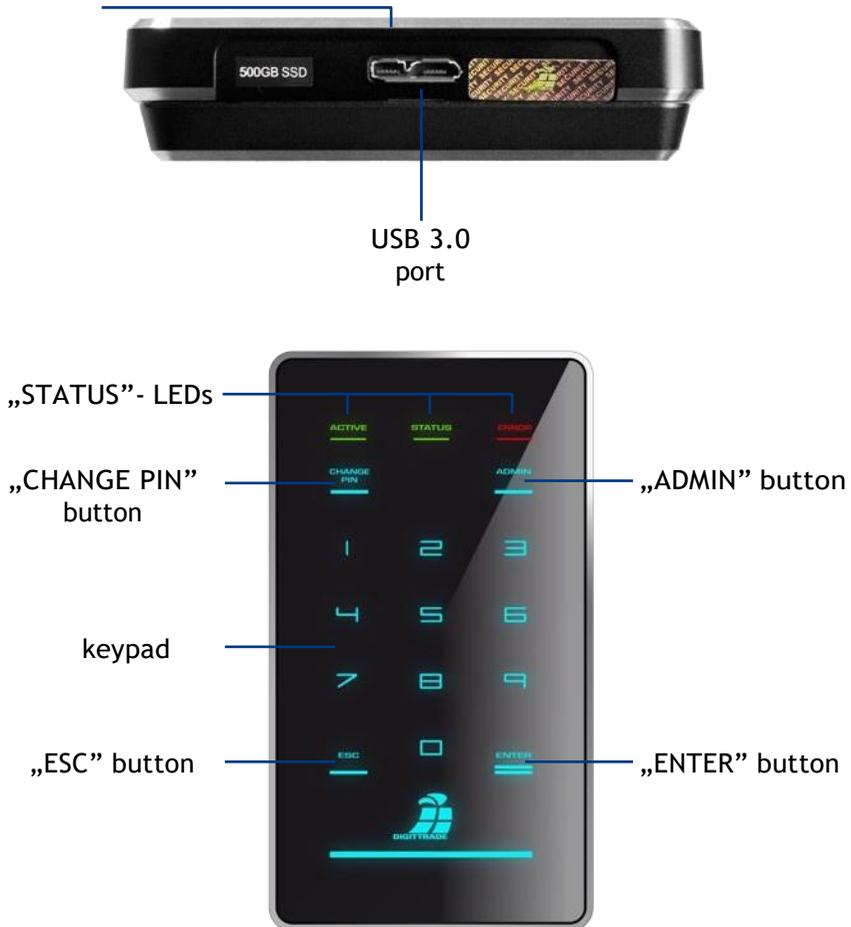


Additional warranty seals are inside of the HS256 S3.



2. Control panel and USB port

It is possible to connect the DIGITRADE HIGH SECURITY HS256 S3 either using USB to the computer.



The HS256 S3 has three status-LEDs: “ACTIVE”, “STATUS” and “ERROR”.

Possible colors:

“ACTIVE”-LED: green light

“STATUS”-LED: green or red light

“ERROR”-LED: red light

Connect the HS256 S3 to your PC or laptop using the USB cable included in the delivery.

Not only the data will be transmitted through the USB cable but also the HS256 S3 will be energized.

Please make sure that the HDD is connected at all times directly to the USB plug of the PC or laptop.



Note: Do not use the DIGITTRADE HS256 S3 via a buspowered USB hub or extension cable and ensure it has enough power.

3. Getting started with the HS256 S3

The necessary power supply for the HS256 S3 is provided by USB.

If the HS256 S3 is connected correctly to the computer, the LED “ACTIVE”, “STATUS” and “ERROR” will flash at the same time.

Now the DIGITTRADE HS256 S3 is ready for use, but still needs to get unlocked. For this, keep your smart card and smart card PIN ready.

Note: For security reasons please use only original accessories.

3.1 Inserting the smart card

After the DIGITTRADE HS256 S3 is ready for use it still needs to get unlocked.

To accomplish this, insert the smart card into the associated slot in direction of the arrow.



If an invalid or defective smart card is inserted in the smart card slot the “ERROR”-LED will flash three times and illuminates then permanently red. In that case please contact DIGITTRADE.

3.2 Entering the smart card PIN

After you have activated the DIGITTRADE HS256 S3 successfully and inserted a valid smart card, the keypad will be lighted and the HDD is ready for PIN entry.

Now you can type in the 8-digit PIN.

The preset factory PIN is:

“1-2-3-4-5-6-7-8”.

after you entered the PIN, press the “ENTER” button.



Note: To guarantee the safety of your data, it is very important to change the factory set PIN (page 65). Change the smart card PIN periodically. It is recommended to use different PINs for different smart cards. The numerical order must be kept confidentially.

After successful PIN entry, the cryptographic keys are transferred to the encryption module and the “STATUS“-LED illuminates red. The DIGITTRADE HS256 S3 will be identified by the operating system as a removable device and the lighting of the keypad goes out. The “ACTIVE“-LED flashes during the data transfer.

The access is enabled now. The smart card must remain in the DIGITTRADE HS256 S3 whilst in operation. If the smart card will be removed from the slot, the storage device is locked (lock-out mode).

If necessary this function can be deactivated, so that the smart card can be removed after the authentication and you still will have access to the HS256 S3. The “STATUS“-LED illuminates green after successful PIN entry. Please find more information in chapter 5.2. Upon removal of the smart card, the “STATUS” LED turns off and the “ACTIVE” LED is green.

If a wrong PIN was entered, the red “ERROR“-LED flashes and it sounds an acoustic signal. Press the “ESC“ button to restart the PIN entry.

Note: After the PIN was entered eight times incorrectly, the smart card will be irrevocably locked and cannot be used anymore. The cryptographic keys on the smart card are irreversible deleted in the process.

Note: In the activated status the HS256 S3 must not be unattended to prevent unauthorized access. Please note, if you are leaving your workplace and if you are not using the DIGITTRADE HS256 S3, it should be locked correctly. All data transfers must be completed and the HS256 S3 must be separated from the USB connector. If the lock-out mode is activated it is sufficient to remove the smart card from the associated slot.

For security reasons it is recommended to hide traces upon entry that could allow conclusions about the use of PIN numbers. Possible methods can be:

1. Frequent cleaning of the keypad, so no fingerprints are visible.
2. Frequent tapping of all buttons, so fingerprints are spread evenly.
3. Using special stylus pens that do not leave marks on the surface of the keypad, such as the DIGITTRADE stylus pen.

3.3 Changing the smart card PIN

Follow these steps to change your smart card PIN:

- 1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1).
The keypad illuminates.

Note: *If the keypad and the red “ERROR”-LED illuminate permanently, please initialize the smart card as described in chapter 5.4.*

- 2) Press the “CHANGE PIN” button and afterwards the “1” button.
- 3) Press “ENTER” to confirm. The “STATUS”-LED flashes green several times.
- 4) Type in the current 8-digit PIN and press “ENTER” to confirm the entry.
- 5) Type in the new 8-digit smart card PIN and press “ENTER” for confirmation.
- 6) To confirm, type in the new 8-digit smart card PIN again and press “ENTER”.

After a successful PIN change, the “STATUS”-LED flashes green several times and it sounds an acoustic signal at the end. The DIGITTRADE HS256 S3 will be identified from the system as a removable device, the “STATUS”-LED illuminates red (in active lock-out mode) and the lighting of the keypad disappears.

The access to the hard drive is enabled.

If the PIN change was not successful, the red “ERROR” LED flashes and it sounds an acoustic signal. Press the “ESC” button and start again with the first step of the PIN change.

You have 8 attempts for changing the smart card PIN. After this the inserted smart card is locked and no longer usable.

Note: *1. The DIGITTRADE HS256 S3 only accepts 8-digit PINs. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*

2. Please change the smart card PIN periodically during the use of the hard drive, plus after receiving the smart card and the transfer to another user.

4. Administrating the cryptographic keys with the smart card

The cryptographic keys are created and encrypted on a certified smart card. After the PIN has been correctly entered the cryptographic keys are transferred to the encryption module of the HS256 S3 to de-/encrypt the data. The cryptographic keys can be copied to other smart cards for using the storage device. The cryptographic keys can be created, changed or deleted using the smart card PIN.

The function of administrating the cryptographic keys (creating, destroying and copying) only works with smart cards that have the DIGITTRADE HS256 S3 Java Card Applet. The HS256 S3 is (by default) distributed with 2 of the following type of smart cards NXP J2E081_M64 R3, CC EAL 5.

Note: *The HS256 S3 is delivered preconfigured and ready-to-use. For security reasons it is very important that the cryptographic keys are changed and the smart cards are re-initialized for the HS256 S3.*

4.1 Creating the cryptographic keys

With the help of DIGITTRADE HS256 S3 the cryptographic keys can be created on a working smart card. The integrated certified random number generator creates random and safe cryptographic numbers.

Follow these steps to create cryptographic keys:

- 1) Insert a working smart card into the associated card slot (see chapter 1.4 and 3.1).
- 2) If the smart card has no cryptographic keys, the “ERROR“-LED as well as the “STATUS“-LED illuminate red.

If the smart card already has cryptographic keys that are not initialized for the HS256 S3, the red “ERROR“-LED and the keypad illuminate. The smart card is already initialized the key pad illuminates.

- 3) Press the “ADMIN“-button and afterwards “2“.
- 4) Press the “ENTER“-button. The “STATUS“-LED flashes green several times.
- 5) Type in your 8-digit smart card PIN and press “ENTER“ to confirm the entry.

Note: *If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC“ button and start again with the third step of creating the cryptographic keys. You have 8*

attempts for creating a new one. After this the inserted smart card is locked and no longer usable.

- 6) The “STATUS“-LED flashes green whilst the DIGITTRADE HS256 S3 is creating and writing the cryptographic keys to the smart card. If the process was successful, the “STATUS“-LED illuminates green and it sounds an acoustic signal.
- 7) Separate the USB connection to the DIGITTRADE HS256 S3 to exit this feature.

The cryptographic keys have been created or changed. Now the prior cryptographic keys have been irreversibly deleted. With this smart card you do not have a longer access to the prior stored data. It's necessary to create a data backup before. If you want to use these cryptographic keys with the HS256 S3, it has to be initialized for the HS256 S3. Please follow the steps in chapter 5.4.

Note: Please do not remove the smart card during the creation of the cryptographic keys (step 6 “STATUS“-LED flashes green several times), otherwise the smart card could be damaged.

4.2 Deleting the cryptographic key

1. There are two ways to delete the cryptographic keys.
 - a) Deleting the cryptographic keys by creating a new one

Please follow the steps in chapter 4.1. With this method the cryptographic keys can be quickly deleted without attracting attention in a dangerous situation as the process hardly differs from the normal log-on process. Now the access to the data with this smart card is even for the user impossible.

- b) Deleting the cryptographic keys by entering the 8-digit PIN incorrectly 8 times

This method is more complex but can be done intuitive and without the knowledge of the smart card PIN. Please follow these steps:

- 1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1).
- 2) Type in a wrong 8-digit PIN and press “ENTER“.
- 3) The red “ERROR“-LED flashes and it sounds an acoustic signal.

- 4) Press the “ESC”-button and execute the second step 7 times more.
 - 5) If the wrong PIN had been entered 8 times, the cryptographic keys are destroyed and this smart card is locked and no longer usable.
2. In both cases, only the cryptographic keys are deleted on the respective smart card. The remaining data on the hard drive is not damaged and still stored encrypted. If the user has the second smart card with the appropriate cryptographic keys and valid PIN, he can access this data easily.
3. If one of the smart cards is lost, misplaced or stolen, it is necessary to destroy the cryptographic keys completely. Please follow these steps:
- 1) Start running the DIGITTRADE HS256 S3 (see page 62 and 63).
 - 2) Back up all necessary data from the HS256 S3 to another storage device.
 - 3) After this process is completed, disconnect the HS256 S3 and connect it again.
 - 4) Now create new cryptographic keys (see chapter 4.1).
 - 5) Initialize the smart card (see chapter 5.3).
 - 6) Initialize and format the HS256 S3 with your OS (see chapter 6-8).
 - 7) Overwrite the HS256 S3 completely with random data. After this process is completed, you can delete the random data and use the DIGITTRADE HS256 S3 normally.

Now any copies of the old cryptographic keys on other smart cards are useless.

5. Device PIN features

The device PIN does not allow the access to the stored data. With the help of this PIN you can execute the following administrative features:

- change the device PIN
- activate/deactivate the lock-out mode
- copy cryptographic keys
- initialize a new smart card for the DIGITRADE HS256 S3

The preset factory device PIN is: “**8-7-6-5-4-3-2-1**”. For security reasons, we recommend that you should change it. The device PIN must be kept confidentially. Therefore avoid the execution of the above functions on your hard drive by unauthorized persons.

The number of attempts to enter the device PIN is not limited.

Note: *Bear your device PIN in mind. Without this PIN the initialization of new smart cards and thus the use of more HS256 S3 is not possible.*

5.1 Changing the device PIN

Follow these steps to change the device PIN:

- 1) Insert a working smart card into the smart card slot (see chapter 1.4 and 3.1)
Make sure that the keypad illuminates.

Note: *If the red „ERROR“-LED and the keypad illuminate, please initialize the smart card as described in chapter 5.4.*

- 2) Press the “CHANGE-PIN“ button on the keypad and afterwards “0“.
- 3) Confirm your entry with “ENTER“.
- 4) Type in the current 8-digit device PIN and press “ENTER“ to confirm the entry.
The “STATUS“-LED flashes green twice.
- 5) Type in the new 8-digit device PIN and confirm with “ENTER“.
- 6) For confirmation type in the new 8-digit device PIN again and press “ENTER“.
- 7) During the change, the “STATUS“-LED flashes green several times and it sounds an acoustic signal at the end.
- 8) The smart card can be removed now. Disconnect the USB connection of the

DIGITTRADE HS256 S3 to exit this features.

If the PIN change was not successful, the red “ERROR“-LED will flash. Press the “ESC“ button and start again with the first step of the PIN change.

English

Note: *The DIGITTRADE HS256 S3 only accepts 8-digit PIN. The PIN should be chosen at random. Do not use a trivial PIN like ascending or descing series of numbers or user-specific PIN like your phone number or date of birth.*

5.2 Activating/deactivating of the lock-out mode (Device PIN needed)

In the activated lock-out mode access to the data is instantly stopped if the smart card is removed.

The HS256 S3 is preset with activated lock-out mode. The “STATUS“- LED illuminates red during the access mode. For a safe use of the HS256 S3 the lock-out mode must be activated. Using the HS256 S3 with deactivated lock-out mode is outside the scope of the BSI certification.

The user can deactivate this feature in particular situations. This must be done when only one smart card has access to many different storage devices that are supposed to be unlocked at the same time with the same cryptographic keys. When the lock-out mode is deactivated the “STATUS“-LED illuminates green during the access mode.

In that case please use the physical separation after the end of the use (chapter 15) because the logical separation is not possible in the deactivated lock-out mode.

Follow these steps to activate/deactivate the lock-out mode:

- 1) Insert a working smart card into the associated slot (see chapter 1.4 and 3.1). Make sure that the keypad illuminates.

Note: *If the “STATUS“-LED flashes green shortly and the red “ERROR“-LED illuminates permanently, please initialize the smart card as described in chapter 5.4.*

- 2) Press the “ADMIN“-button and afterwards “1“.
- 3) Press the “ENTER“-button. The “STATUS“-LED flashes green several times.

- 4) Type in your 8-digit device PIN and press “ENTER“. If the PIN was entered correctly, the “STATUS“-LED flashes green several times and it sounds an acoustic signal.

Note: If the Keypad and the red “ERROR“-LED flashes press the “ESC” button and start again with the third step.

- 5) The lock-out mode is now activated/deactivated now. The “STATUS“-LED illuminates red if the mode is activated and green if it is deactivated.
- 6) Disconnect the USB connection of the DIGITTRADE HS256 S3 to exit this feature.

Note: The activated lock-out mode is preset. In this mode do **not** remove the smart card from the DIGITTRADE HS256 S3, as it can lead to data loss.

5.3 Copying the cryptographic keys (Device PIN needed)

With this feature you can copy the cryptographic keys from one smart card to another. For this at least two smart cards are needed: the smart card that has the cryptographic keys that should be copied and one or more smart cards the cryptographic keys should be copied on.

Follow these steps to copy the cryptographic keys:

- 1) Insert a working initialized smart card into the associated slot (see chapter 1.4 and 3.1).

If the smart card is already initialized, the keypad illuminates. If the smart card has already cryptographic keys that are not initialized with the HS256 S3, the red “ERROR“-LED and the keypad illuminate. Initialize this smart card. (see chapter 5.4)

- 2) Press the “ADMIN“-button and then the “3“.
- 3) Press “ENTER“. The “STATUS“-LED flashes entered several times.
- 4) Type in your 8-digit device PIN and press “ENTER“. The “STATUS“-LED flashes entered twice. Enter the 8-digit PIN from smart card A and press “ENTER“.

Note:

1. If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC” button and start again with the second step of copying the cryptographic keys.
2. The smart card A is automatically locked and rendered useless as soon as the 8-digit PIN was entered eight times incorrectly.

- 5) The “STATUS“-LED flashes green several times during the DIGITTRADE HS256 S3 reads the cryptographic keys from smart card A. After this process is completed the “STATUS“-LED illuminates green and it sounds an acoustic signal at the end.
- 6) Remove smart card A and insert smart card B into the smart card slot. Make sure that the keypad illuminates.
- 7) Enter the 8-digit PIN for smart card B and press “ENTER“.

Note:

1. If the PIN entry was not successful, the red “ERROR“-LED flashes. Press the “ESC” button and type in the PIN of smart card B again.

2. The smart card B is automatically locked and rendered useless as soon as the 8-digit PIN was entered eight times incorrectly.

- 8) The “STATUS“-LED flashes green several times when the HS256 S3 is writing the cryptographic keys to smart card B. If the process was successful, the “STATUS“-LED illuminates green and it sounds an acoustic signal.
- 9) To describe further smartcards with these cryptographic keys disconnect the hard drive and start again with step 1.

Note: Do not remove the smart card during the reading/writing process (steps 5 and 8, the “STATUS“-LED flashes green several times), otherwise the smart card could be damaged.

5.4 Initializing a new smart card (Device PIN needed)

Initialising a new smart card is necessary, if the cryptographic keys have been changed and the DIGITTRADE HS256 S3 has to operate with it (for example for security reasons if one or more smart cards are lost).

Whilst initialising a new smart card, the cryptographic keys are changed in the crypto-system. Therefore the HS256 S3 has to be reinitialized and reformatted by the user's OS afterwards. Now the access to the previous stored data is impossible with the new cryptographic keys.

Follow these steps to initialize a new smart card:

- 1) Insert a working smart card into associated slot (see chapter 1.4 and 3.1).
Make sure that the red "ERROR"-LED and the green and the keypad illuminate.
- 2) Press the "ADMIN" button and afterwards "0".
- 3) Press "ENTER" to confirm. The "STATUS"-LED flashes green several times.
- 4) Type in your 8-digit device PIN and press "ENTER".

Note: *If the PIN entry was not successful, the red "ERROR"-LED flashes. Press the "ESC" button and start again with the third step of initialising a smart card.*

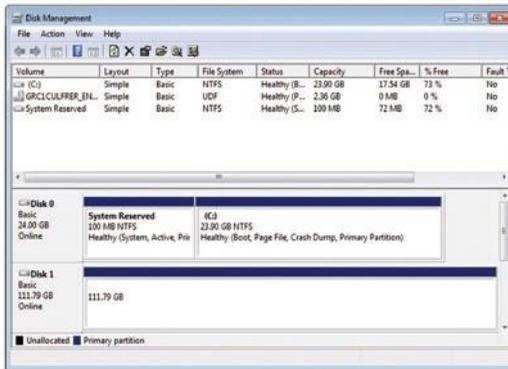
- 6) If the PIN was entered correctly, the "STATUS"-LED flashes green and it sounds an acoustic signal. The inserted smart card is initialized with this DIGITTRADE HS256 S3 now.
- 7) Disconnect the USB connection to the DIGITTRADE HS256 S3 to exist this feature.
- 8) Initialize and format your DIGITTRADE HS256 S3 with your OS.
Follow the instructions in the following chapters.

Note: *Keep your device PIN in mind. Without it the initialising of new smart cards is impossible as well as the regular use of your HS256 S3.*

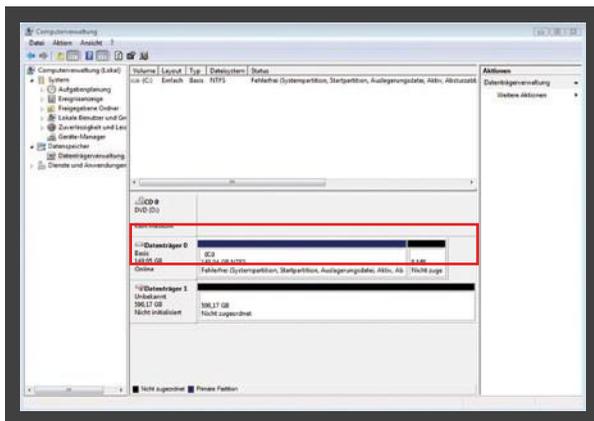
6. Initializing/partitioning and formatting with Windows

Follow these steps to initialize the DIGITRADE HS256 S3 with Windows:

- Start running the DIGITRADE HS256 S3 (see page 62 and 63).
- Enter Disk Management. Right-click on my computer and then click on manage. In Windows Vista or 7 click start, then right-click on my computer, choose manage and then click on Disk Management from the list.
- Here you will find an overview of the different drives:

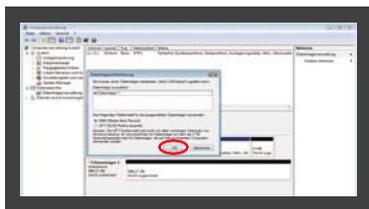


- After successfully initialization the HS256 S3 will be shown in the bottom area of the Disk Management window:



- If the Disk Management is opened for the first time since the HS256 S3 has been

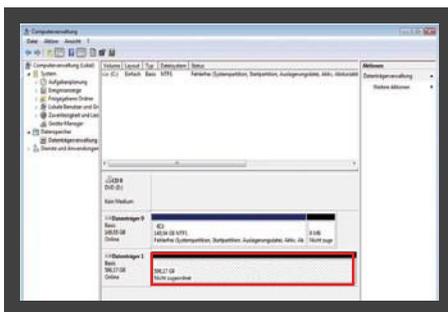
started, the following window will pop-up:



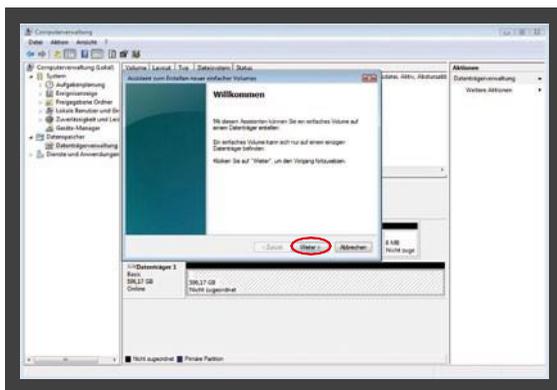
- Here you can initialize the drive by clicking “OK“.

Note: In case the initialisation window does not automatically pop up, or it was ended by clicking “Cancel“, you can initialize the disk by right clicking on it in the list.

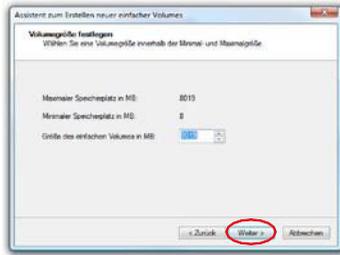
- The status should then change from “not initialized“ to “online“.



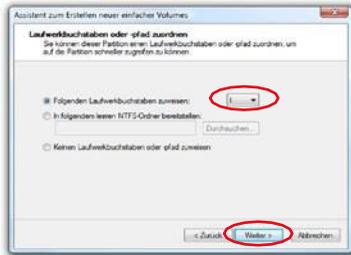
- Right click on the “unallocated“ area and choose “New simple volume“ in the menu. In the started assistant you can change all needed settings and format the drive.
- Click on “next“ to start the process



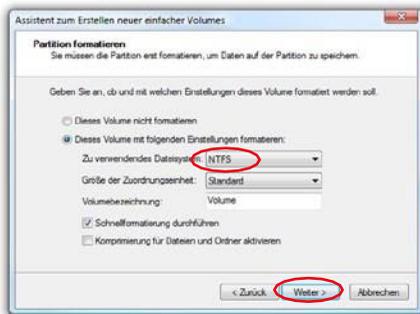
- Enter the desired size of the partition in MB and click “next“:



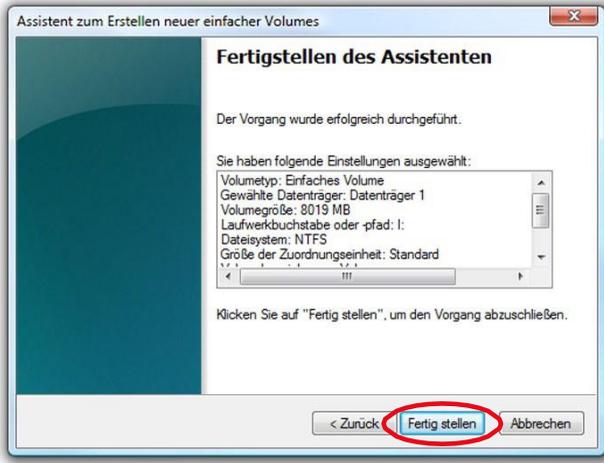
- You may assign a partition letter, then click on “next“:



- Now choose the file system and the type of formatting you would like to use and click “next“:

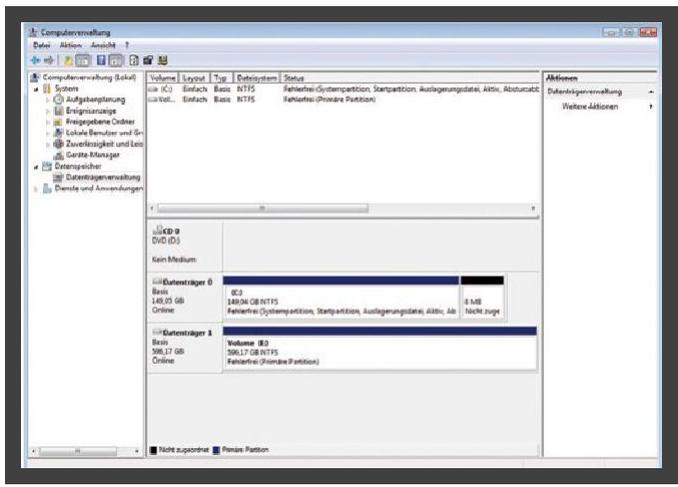


- Click “Done” to complete the formatting:



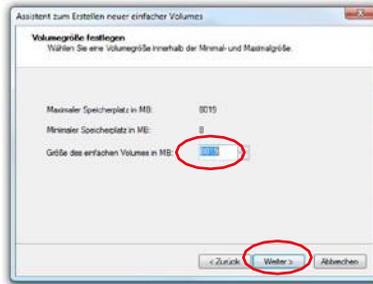
The duration of the formatting can vary depending on the size of the hard drive.

When formatting is completed the HS256 S3 will be shown as “healthy” and can be used now:

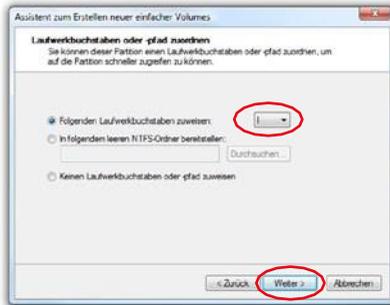


It is also possible to partition the DIGITRADE HS256 S3 in more than one partition using the Disk Management.

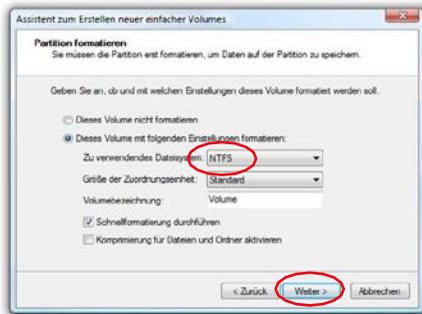
- Enter the desired size of the partition in MB and click “next“:



- You may give the partition a letter then click on “next“:



- Now choose the file system and the type of format you would like to use and click “next“:



- Then the format be complete, to continue click “done“:

Note: The newly partitioned area is being formatted. After successfully partitioning, the new partition is automatically recognised by the system.



7. Initializing/partitioning and formatting with Mac OS X

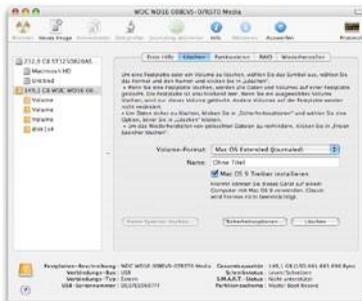
- Start running the DIGITRADE HS256 S3 (see page 62 and 63).

To manage external disks using a MAC you can use the “Disk Utility“. To open it go to “Programs“ and then “Utilities“.

- Choose the “Disk Utility“. The Disk Management for initialising, partitioning and formatting opens.



- Choose the HS256 S3 from the drive list on the left side. Under menu item “delete“ you can initialize and partition the HS256 S3.



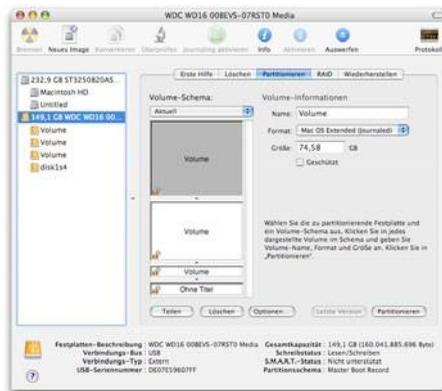
As well as giving the drive a name you can choose the file system to be used. For MAC

OS X you should use “Mac OS Extended (Journaled)” and for the classic MAC OS 9 the HFS Format (Mac OS Extended).

- Confirm the initialization/formatting by clicking the “DELETE” button.

To partition the HS256 S3 the “Disk Utility” is also used. Click on the HS256 S3 and choose ”Partitioning“ you may also choose the size of the partitions.

- In the middle you can see how the disk is currently partitioned. Click on the pulldown menu “current“ right under “volume scheme“.
- Now you may choose the number of partitions you would like to have.
- After you have applied all of the partitions, you can decide the name and size of every partition under “Volume Information“.



- Now you can apply the settings by clicking “apply“.

8. Initializing/partitioning and formatting with Linux

It is possible to partition the DIGITRADE HS256 S3 in more than one partition using Linux. For this the correct file system has to be initialized first.

The process which is described here based on YaST from Suse Linux. The process is similar on other Linux distributions.

- Start running the DIGITRADE HS256 S3 (see page 63 and 65).

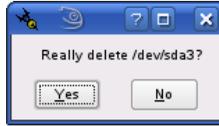
Then open YaST. If necessary, you will need to authenticate yourself.



- Choose from the left side “System” and from the right field “Partitioner”.
- For security reasons a window will open and you will be asked whether you are familiar with the partitioning. Confirm this with “Yes”.
- The volume table of your system will appear.



- Now you can choose the desired volume, partition it, edit or delete already existing partitions.
- To delete the standard NTFS partition please click on it and afterwards on “Delete”.



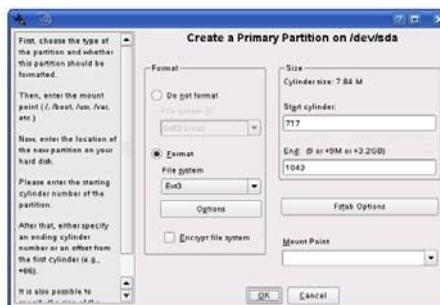
- You will be asked whether you really want to delete the partition. Make sure you have chosen the correct partition and confirm with a click on “Yes”.

Note: *If you delete the partition, you will delete irrevocably all files stored on it.*

- To create a new partition in the free space of your volume click on “Create”.



- Choose a volume to create the new partition.
- You will be asked which type of partition you want to create. It is recommended to use “Primary Partition”.

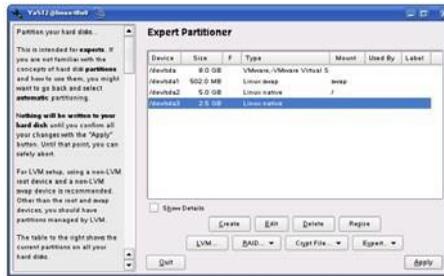


- In this window you configure all features of the partition. You can choose between

different file systems and sizes and if necessary you can configure a mountingpoint for Linux.

- Confirm your configuration with “OK”.
- Formatting works similarly. Choose the desired partition and click on “Edit”.
- Click on “Formatting” and choose the adequate file system. Confirm your configurations with “OK”.

English



- Click on “Apply” to operate your modifications.



- All modifications will be shown in a new window. Make sure that all modifications are correct and confirm the configurations by clicking on “Apply”.

Note: If you are not sure which file system or partition size you should choose, we recommend taking the automatically entered values.

9. The correct file system

The table below shows the compatibility between operating systems and file systems.

	NTFS	FAT32	HFS+	EXT3
Win 98	X	R, W	X	X
Win NT, 2000, ME, XP, Vista, 7, 8, 10	R, W	R, W	X	X
Mac OS X	R	R, W	R, W	X
Linux	R	R, W	X	R, W

description: R - read, W - write, X - no compatibility

You may be able to write data to file systems that are usually not compatible by using an external program.

At the time of the delivery the DIGITTRADE HS256 S3 is already formatted for you in the NTFS file system. In the chart above you can see the compatibility of the NTFS file system with your operating system. If NTFS does not work with your operating system, you will have to re-format the hard drive (chapter 6).

For Windows users we recommend NTFS. The most powerful file system for MAC OS X is HFS+ and for Linux you should use EXT3. The DIGITTRADE HS256 S3 can be formatted to any other file system, this does not affect the encryption of the data.

If you would like to use the hard drive with different operating systems, we suggest using the FAT32 file system, as it is supported by nearly all operating systems (Read/Write). However, there are restrictions to the file/partition size. Furthermore there are slight performance differences.

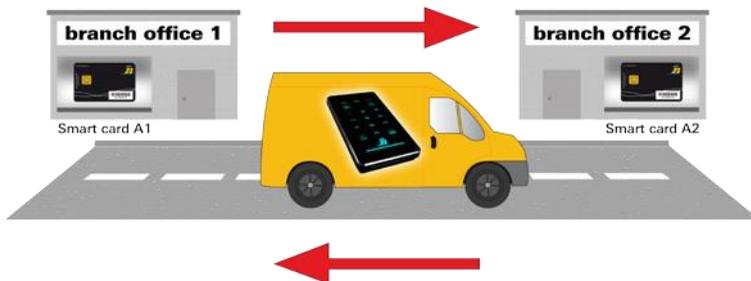
10. Possible usage of the DIGITTRADE HS256 S3

1) Secure and cost-efficient data transport

The HS256 S3 can be used to transport confidential data. For the dispatcher and recipient of the data, have a smart card with identical cryptographic keys. The dispatcher only sends the HS256 S3. As the cryptographic keys do not physically exist (it is on the smart cards), it cannot be read out during the transport. Additionally the HS256 S3 with confidential data can be sent cost-efficiently and insured by a postal service or courier.

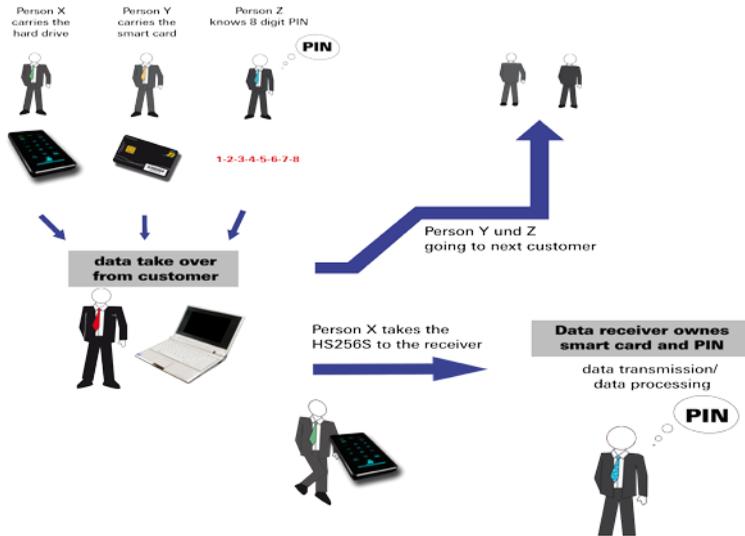
The dispatcher and recipient must check that the HS256 S3 has not been tampered during the transport. For this purpose it is recommended to use security packaging like described in chapter 1.8. This is also effective for all other transport possibilities of the HS256 S3.

For additional security, the use of multiple smart cards with different cryptographic keys, (deposited at the dispatcher and recipient) which can be used to decrypt or encrypt the data in a chosen sequence.



2) Data storage device & authentication separation

The access to the data can be regulated with help of three persons. Person X has the HS256 S3, Person Y has the smart card and person Z knows the smart card PIN. The three people only meet for the data transfer at the recipient and separate again afterwards. Persons X, Y and Z cannot gain access to the data on their own.



3) Using limited amount of storage devices for a wide range of customers

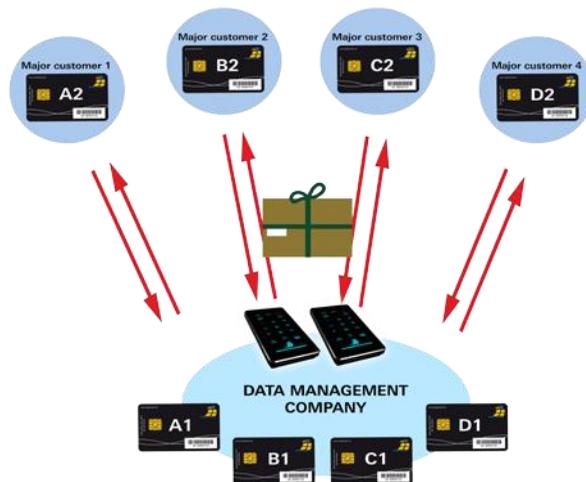
If a company (i.e. data processing company or data center for large companies or agencies) is in a constant exchange of data with many different data recipients, it can use the benefits of the HS256 S3 to transport data secure and cost-efficiently. Every recipient receives a smart card with his/her own cryptographic keys. The dispatcher has a copy of each of the cards with the cryptographic keys of every recipient.

For the transportation of data a smart card with the cryptographic keys of the recipient is initialized with the HS256 S3 (device PIN required).

Every HS256 S3 is suitable. Subsequently, the data dispatcher does a quick format of the HS256 S3 with the new cryptographic keys which only takes a few minutes. Complicated data deletion or overwriting is not necessary, as the data was encrypted with different cryptographic keys and could only be encrypted and restored by the owner of the old cryptographic keys provided the data has not already been overwritten.

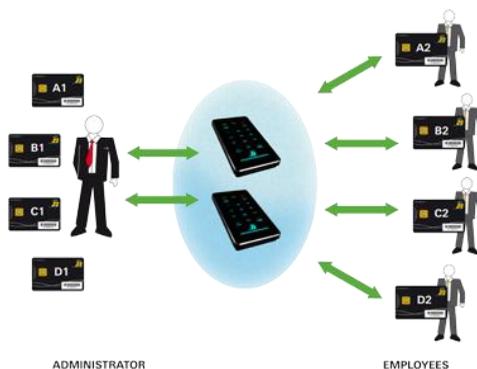
If data is supposed to be sent to the same recipient in short intervals there is no need to wait for a personalized HS256 S3 to return. Every HS256 S3 can be used. All you need to do is initialize it with the recipients cryptographic keys.

The amount can be reduced to the actual amount. Because not every recipient needs their own HS256 S3. It is irrelevant which of the company's HS256 S3 is available and used for transport. Crucial is which cryptographic keys have written the data to the HS256 S3.



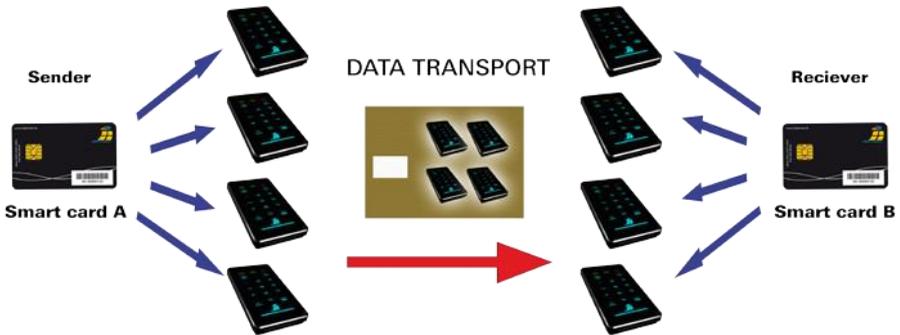
4) Using limited amount of storage devices in the field and public authorities

Within a company every Sales Representative can have his/her own personalised smart card (own cryptographic keys). For their work every employee receives their own HS256 S3 which has been priory initialized. The employee saves the data with his/her cryptographic keys. After usage the employee gives the HS256 S3 back. Then it goes through a quick configuration and within minutes it is ready for the next employee. Therefore there is no need for a HS256 S3 for every employee and the actual amount of required storage devices is reduced to a minimum.



5) Operating multiple storage devices with a single smart card

To accomplish this multiple HS256 S3 have to be initialized with identical cryptographic keys. It is possible to generate cryptographic keys for one smart card which allows the access to several different hard drives. It offers the advantage that one employee does not know various numeric codes for the different drives which he/she has an access for. It is only one PIN necessary. Even if the data are sent frequently, it provides a great solution for every time the data are dispatched and an other different HS256 S3 can be used. A Waiting for the return of personalies HS256 S3 is unnecessary.



6) Deleting the cryptographic keys

The user has the possibility to delete the key without attracting attention in dangerous situations, given that he/she knows the PIN. In order to do this three additional buttons must be pressed. (Chapter 4.2)

Now the access to the data is impossible with this smart card and therefore also for the user.

Provided the smart card PIN is unknown, the cryptographic keys are also deleted by entering the 8-digit PIN wrong 8 times.

7) Bootability

Operating systems, programs and data can be saved to the HS256 S3. This usage is compatible with stationary as well as mobile computers. By disconnecting the HS256 S3 from the pc, the data, programs and operating systems are saved and encrypted exclusively on the HS256 S3 and are inaccessible by unauthorized persons.

8) Usage with all operating systems

The HS256 S3 hardware encryption is standalone, which means it can be used on any device that supports data storage devices.

9) Integrating in existing smart card infrastructures within companies.

If a company is already using the smart card Smartcard NXP J2E081_M64 R3, CC EAL 5 (i.e. access management, user authentication) the integration of the HS256 S3 is possible. Further functions can also be implemented into the smart card.

10) Integrating in existing software solutions

All existing software solutions can still be used to additionally expand the security properties and methods of use.

11. Technische Spezifikationen

Data Transfer Rate: USB 3.0 max 5 Gbps
USB 2.0 max 480 Mbps

Smart Card: NXP J2E081_M64 R3, CC EAL 5
JCOP v2.4.2 R3, (NSCIB-CC-13-37761-CR2)
with installed DIGITTRADE HS256 S3 Java Card Applet v1.1.0

Supported Encryption: 256 bit AES hardware based encryption, XTS mode,
with two 256 bit cryptographic keys

Internal volume:

The encrypted data are stored on the internal 2.5 inch SATA HDD or SSD drive from Samsung (preferred), Seagate, Western Digital or Toshiba.

The following capacities are available: 120GB SSD, 160GB HDD, 250GB SSD, 320GB HDD, 500GB HDD/SSD, 640GB HDD, 750GB HDD/SSD, 1TB HDD/SSD, 1,5TB HDD/SSD, 2TB HDD/SSD, 4TB HDD/SSD

Computers and HDD manufacturers convert differently from Byte to KByte, MByte and GByte. HDD manufacturers calculate in the metric system (1 KByte = 10^3 Byte = 1000 Byte) and computers use due to their construction the dual system (1 KByte = 2^{10} Byte = 1024 Byte). The outcomes of this are the following differences in the representation of the memory capacity.

HDD manufacturer	available space
120 GB	111.76 GB
160 GB	149.01 GB
250 GB	232.80 GB
320 GB	298.08 GB
500 GB	465.66 GB
640 GB	596.03 GB
750 GB	698.49 GB
1,000 GB	931.32 GB
1,500 GB	1,396.98 GB
2,000 GB	1,862.64 GB
4,000 GB	3,725.29 GB

12. Troubleshooting

If any problems occur with your DIGITTRADE High Security HS256 S3 HDD/SSD please read the following checklist to find a solution. If further technical support is required, please feel free to contact our support team.

Problem	Symptom	Solution
The number pad is inactive	keypad light is turned off	Ensure that the USB connector is firmly connected to your computer's USB port.
	"ERROR" LED lights up	Ensure that a valid card is inserted and that the card orientation is correct by inserting the card with the contacts facing down.
Authentication fails	"ERROR" LED lights up	An incorrect PIN was entered. Press the "ESC" button to restart PIN entry (max. 8 trials).
The drive cannot be identified	no icon for the device is shown on the computer	Ensure that the HS256 S3 is not connected to a bus-powered USB hub or a USB extension cable. Please use the delivered USB cable.
	missing partition or file system cannot be detected	Please refer to Chapter 6 "Partitioning / Formatting", p. 41 et seqq.

Problem	Symptom	Solution
The drive cannot be identified	the wrong USB-cable is used	Please use the delivered USB cable and connect it to your computer.
The drive is performing very slowly	connection using USB	Please ensure your HS256 S3 is connected to a USB interface.
	the wrong USB-cable is used	Please use the delivered USB cable and connect it to your computer.
	wrong connection to the computer	Ensure the USB cable is connected to your computer.
	the HS256 S3 is plugged in an USB hub	Connect the HS256 S3 directly to your computer.
	other USB devices are connected to the same port	Disconnect any other USB devices and see if performance improves.

13. Data security and disclaimer

We recommend to frequently backup your data saved on the DIGITTRADE High Security HS256 S3 on another storage device. This will protect you from a total data loss. The DIGITTRADE GmbH is not liable for any data loss and/or resulting costs and damages and does not bear the responsibility of data privacy of the stored data.

14. Appropriate handling of the HS256 S3 for data privacy

Please note following principles and requirements of the Federal Data Protection Act (BDSG), State Data Protection Acts and the corresponding standards of the EU Data Protection Directive (95/46/EC) for storing personal data:

1) Lawfulness of data collection, processing and use

According to §4 para. 1 BDSG the collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.

The same is true in regard to Article 7 of the EU Data Protection Directive, according to which Member States shall provide that personal data may be processed only if:

- a) the data subject has unambiguously given his consent; or
- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- d) processing is necessary in order to protect the vital interests of the data subject; or
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

2) Data reduction and data economy (Section 3a)

Personal data shall be collected, processed and used as well as and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

Please consider this aspect during the creation of backup copies. The old backups should be replaced with the current data regularly instead of providing new ones. To delete the old data before creating a new backup completely before creating a new backup, it is recommended to change the cryptographic keys and afterwards please format the whole hard drive with a new key.

3) Transparency and purpose

The data subject is to be informed of collection, first-time storage or transmission of the personal data according to §48 Para. 3, §19 and §33 of the Federal Data Protection Act (BDSG). This is also regulated by Article 10 f. of the EU Data Protection Directive (95/46/EC). In addition to processing personal data the principle of the purpose must be regarded (see in particular Article 6 (b) of EU Data Protection Directive).

4) The processing of special categories of data Article 8:

Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life.

Processing is only allowed if e.g. this is required for the employment relationship or to protect the vital interests involved. Further data processing is allowed if the owner has published the data by himself/herself. It is required to assert claims in court or processing the data in the context of medical care / health care is needed.

Appropriate regulations can be found in § 28 para. 6-9 BDSG

5) Inalienable rights of the data subject

According to §19, 20, 34 and 35 BDSG the data subject has the right of access, rectification and erasure or blocking of the stored data concerning them.

The same also applies to Article 12 of the EC Data Protection Directive, in which any interested party has the right to information and, as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive.

Furthermore according to article 14 Member States shall grant the data subject the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him.

6) Section 42a Obligation to notify in case of unlawful access to data:

With very vulnerable data types referred to in §42a para.1 BDSG it is obligatory that the responsible authority informs all parties concerned of the data loss.

7) Administrative offences:

The unauthorized collection, processing and use of personal information can in accordance to §43 BDSG be punished with fines up to € 300,000.00. In the event of an intentional commission of certain offenses fines can therefore be according to §44 BDSG a criminal offense and can be punished with imprisonment up to two years or with a fine.

15. Safe shutdown after using the HS256 S3

For safety reasons, a logical or physical separation of the hard drive is executed from the host system after use. This is recommended especially at the end, short-term interruption and when leaving the workplace.

The logical separation is achieved by removing the smart card from the enclosure. This function is available in the active lock-out mode, which is preset by the manufacturer at the delivery and is the default mode for the safe use of HS256 S3.

For the safe physical separation all connections must be removed from the HS256 S3.

Note: *To prevent data loss, make sure that the data transfer and access are terminated on the hard drive before disconnecting all cables.*

16. Smart card storage

The DIGITTRADE HS256 S3 is delivered with 2 smart cards. Please keep your smart cards separated from the HS256 S3! Doing this guarantees additional protection of your data.

If a card is somehow broken, you can create a copy (DIGITTRADE certified smart card) of the working one using the HS256 S3. You can find tips in chapter 5.3 and compatible smart cards can be purchased at DIGITTRADE.

If lost, we recommend using the HS256 S3 with two new smart cards with new cryptographic keys. You can obtain new smart cards at DIGITTRADE. You can choose between a new one which is already written with cryptographic keys by DIGITTRADE or without new keys. In these case you are able to generate cryptographic keys by yourself for your HS256 S3. Furthermore it is necessary to destroy the cryptographic keys completely. Please follow the steps in Chapter 4.2 (3).

If the smart cards are lost or broken, there is no way of accessing the data. To continue using the hard drive you need at least two new DIGITTRADE certified smart cards. As described in chapter 4.1 then you can create a new cryptographic key pair and operate the HS256 S3 with it. During the process of initialising the hard drive is formatted and the data on the disk is irrevocably deleted. Please contact the support at DIGITTRADE GmbH for new smart cards and other questions.

Note: *Please keep your device PIN in mind. Without this PIN it is not possible to initialize new smart cards and hence to use the HDD.*

Please keep the locations and PINs of your smart cards always in mind, otherwise access to your data would not be possible any more. To use the HS256 S3 with new smart Cards according to the BSI-Certification it is necessary fulfill the procedure of chapter 1.

17. Product contents

- DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) version 1.0
- Two smart cards NXP J2E081_M64 R3 loaded with DIGITTRADE HS256 S3 Java Card Applet version 1.1.0
- User manual “DIGITTRADE High Security HS256 S3“
- USB cable
- Slim case

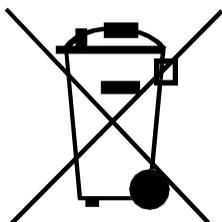
Note: For the exact identification, the components HS256 S3 (Device), smart cards and user manual are individual marked by the explicit product name and product version “DIGITTRADE High Security HS256 S3 Version 1.0”. The certified storage configurations of the DIGITTRADE HS256 S3 are available in chapter 11.

18. WEEE Statement

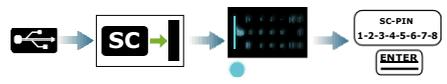
According to the EC directive, waste electrical and electronic equipment (WEEE) must not be disposed as municipal wastes.

To avoid the spread of the contained fabric components in your environment and to save natural resources we would like to ask you to hand this product after its economic life time only to a collecting point for WEEE in your area.

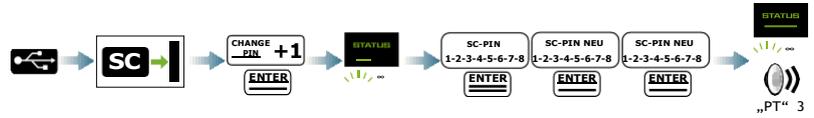
Thanks to these measures, materials of your product can be reused environmentally friendly.



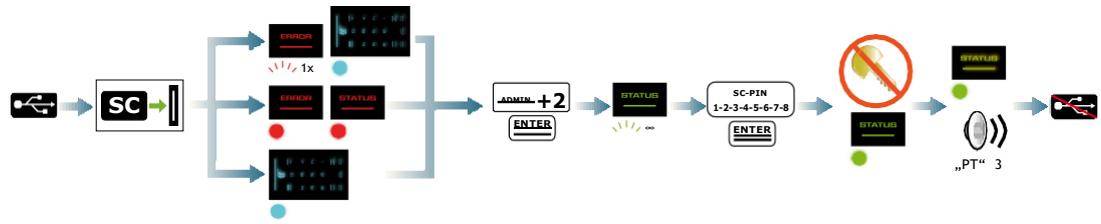
authentication on the HS256 S3



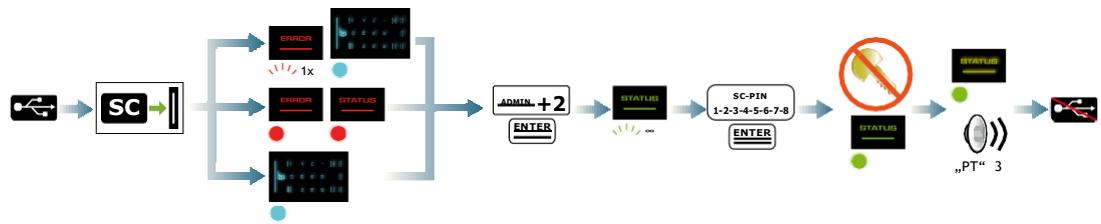
changing the smart card PIN



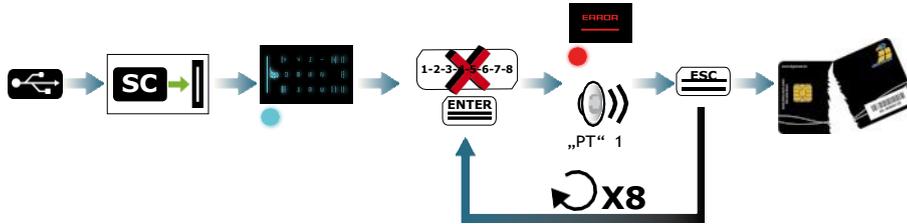
creating the cryptographical keys



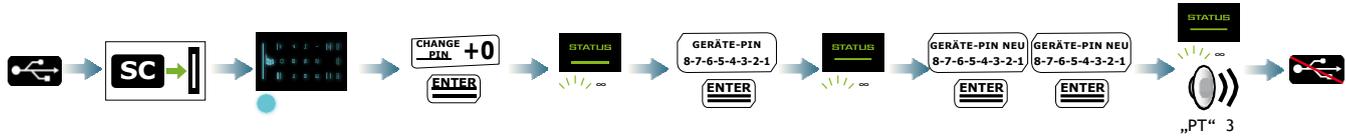
delete the cryptographical keys (PIN is be known)



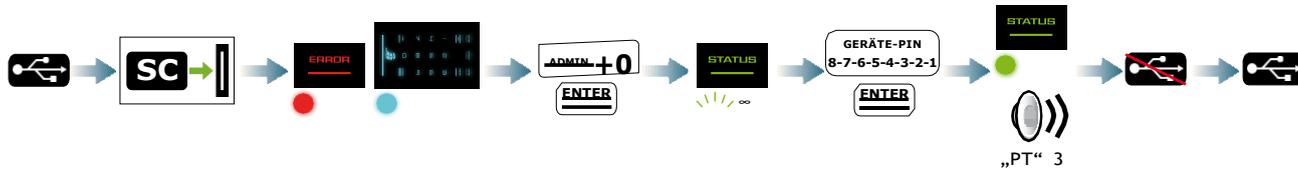
deleting of the cryptographic keys (unkown smart card PIN)



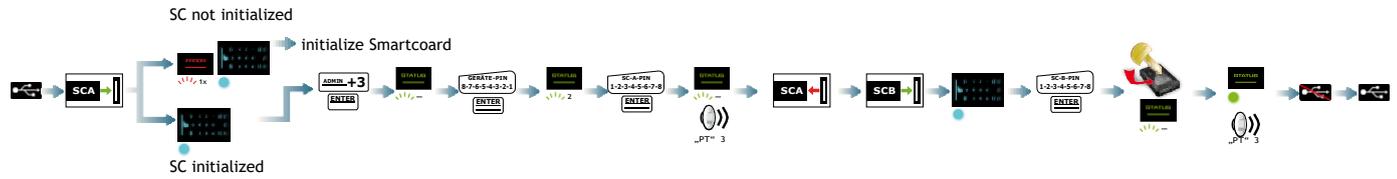
changing the device PIN



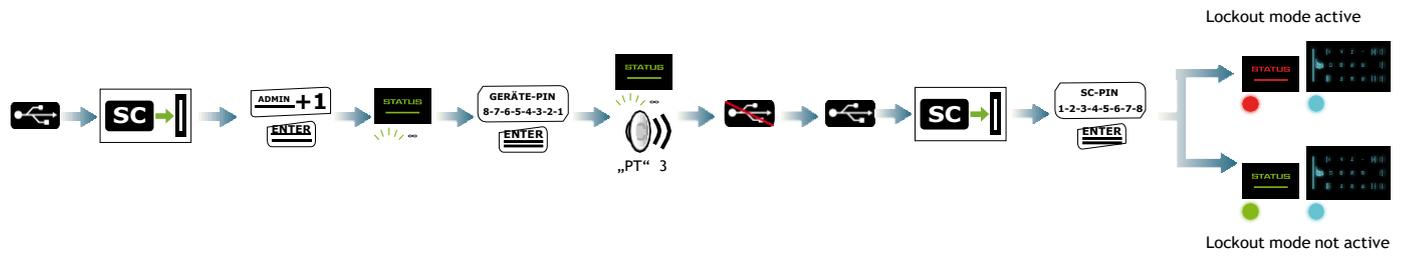
initialising a new smart card



Copying the cryptographic keys



activating/deactivating the lock out mode





Connect the HS256 S3 to the PC



Press „ENTER“



Disconnect the HS256 S3 from the PC



Press „ESC“



Connector



The keypad illuminates



Insert the smart card into the slot



Insert smart card A into the slot



Insert smart card B into the slot



Pull out smart card A



The smart card is locked and unusable



Enter the smart card pin by using the keypad



The „STATUS“-LED...



...flashes green for 1-times



...flashes green multiple times



...illuminates green



Enter the smart card PIN by using the keypad



The „STATUS“-LED and / or the „ERROR“-LED...



Enter the device PIN by using the device PIN



...flashes red for 1-times



Enter the new device PIN on the keypad



...illuminates red



Misentry of the smart card PIN



You will hear beep tones for x-times



Press „CHANGE PIN“ then „0“ (similar for 0 and 1)



The cryptographic keys will be written to the smart card



Press „ADMIN“ then „0“ (similar for 1,2,3)



The cryptographic keys will be destroyed



Do this step 8 times in a row

Ihre Notizen / Your Notes

© 2017 DIGITTRADE GmbH

Deutsch

Dieses Handbuch ist urheberrechtlich geschützt und darf nicht (auch nicht teilweise) ohne schriftliche Zustimmung der DIGITTRADE GmbH kopiert werden.

English

This user manual is protected by copyright. No part of this material may be reproduced, transcribed, used or disclosed to any third party in any form or by any means, without the written permission of the DIGITTRADE GmbH.

DIGITRADE GmbH
Ernst-Thalman-Strasse 39
06179 Holleben Germany

Fon +49 / 3 45 / 2 31 73 53
Fax +49/ 3 45/ 6 13 86 97
Web www.digittrade.de
E-Mail beratung@digittrade.de