Version 1.21
22.02.2021

Kobra VS storage devices

encrypted USB-C secure flash drive and hard disk

for business and governmental use

User's Guide

PLEASE CAREFULLY READ THE MANUAL AND FOLLOW THE INSTRUCTIONS.

IMPROPER OPERATION MAY RESULT IN DAMAGE TO THE KOBRA VS STORAGE DEVICE AND LOSS OF DATA.

The digital version of the manual can be downloaded from the DIGITTRADE GmbH download center:
www.digittrade.de/download

Product version:	Kobra Drive VS, Kobra Stick VS (1FF) and Kobra Stick VS (2FF) - (Kobra VS STORAGE DEVICE) Version 1.0
Users's Guide:	Version 1.21 (as of 22.02.2021)

Contents

1. About the Kobra VS storage devices: Kobra Drive VS and Kobra Stick VS

The external encrypted data storage devices Kobra Drive VS as well as Kobra Stick VS (1FF) and Kobra Stick VS (2FF) are an external USB-C storage device (HDD/SSD) and USB-C memory stick with hardware-based encryption in stable, elegant metal housings with integrated keypad. The storage devices provide the same security features and differ only in their form-factor, design and storage capacities. For this reason, they are all referred to as Kobra VS in this Administrator's Guide.

The Kobra VS storage devices enable the GDPR/EU-DSGVO data protection compliant storage and safekeeping as well as secure transport of sensitive, personal and confidential information up to the classification level NATO Restricted, EU Restricted and VS-NfD (classified information - for official use only). These data carriers were developed in accordance with the "Technical Guidelines" of the German Federal Office for Information Security (BSI) and bear the quality mark "IT-Security made in Germany". They correspond to the current "state of technology" (German: Stand der Technik) and, due to their security functions, are currently one of the safest ways to store and transport data on mobile devices.

The data stored on the Kobra VS data carrier is protected against unauthorized access with regard to the confidentiality of the information, for example if the Kobra VS storage device is lost, misplaced or stolen. In doing so, it resists logical and physical attacks.

Thanks to the built-in storage in 2.5" format, the Kobra Drive VS is already small and handy as an HDD. The optional SSD version offers additional protection against shocks and vibrations. The data transfer and power supply are provided via the USB-C port. The Kobra Stick VS (1FF) and Kobra Stick VS (2FF) offer the same security features as the Kobra Drive VS, only in an even more compact format.

Kobra VS devices can be delivered in a PKI-based or stand-alone environment. There are two basic application scenarios. In the PKI-based variant, only Kobra VS devices are provided. These are set up by the user's administrators. Therefore, the PKI-related properties of the Kobra VS are also regulated by the administrator's IT security concepts.

This mainly concerns the generation and storage of the key pair (consisting of a public and a private key), the User-PIN and SO-PIN specifications (length and number of failed attempts) and other organizational measures. For this reason, the properties of the Kobra VS storage device are described in detail below, mainly regarding the stand-alone environment.

The stand-alone scenario, on the other hand, involves the delivery of the Kobra VS together with two Digittrade smartcards (Atos Card OS 5.3, CC EAL 4+) in the completely preset state. This Kobra VS can basically be used immediately in case of urgent need. In the VS-NfD approved configuration, however, the user may only put the Kobra VS into operation after changing the User-PIN and SO-PIN and generating a new DEK (Data Encryption Key) on the Kobra VS device itself.

In order to use the security features of the Kobra VS storage devices to the full extent and within the scope of the VS-NfD approval, the following steps are required:

- Ensure that your host system has adequate protection for all data accessed from the protected area of the Kobra VS
- After receiving the Kobra VS, check the completeness and correctness of the delivery (Chapter 10)
- Check via the host system that the USB properties of the device match the model name and serial number on the back of the Kobra VS (chapter 1.12)
- Change the User-PIN and SO-PIN on both Digittrade smartcards (chapter 4.3, 4.5)
- Change the Admin-PIN if you have administrator rights (Chapter 4.6)
- When selecting the Admin-PIN, User-PIN and SO-PIN, trivial PINs should not be considered and standard PINs should be excluded
- Create a new DEK (Data Encryption Key) on the Kobra VS storage device (Chapter 4.7)
- Check if the registration is possible with all activated Digittrade smartcards (or your PKI card)
- Protect your authentication features (smartcard and PIN), they must remain confidential

For a detailed description of the above steps, refer to the appropriate chapters in this Administrator's Guide. The model name and serial number can be found on the back of each Kobra VS. This information can be obtained using the supplied Kobra Client VS software and the USB device information on the host system.

The Kobra VS storage device ensures the confidentiality of the data through the following security mechanisms:

- Encryption
- Access control
- Key management
- User administration

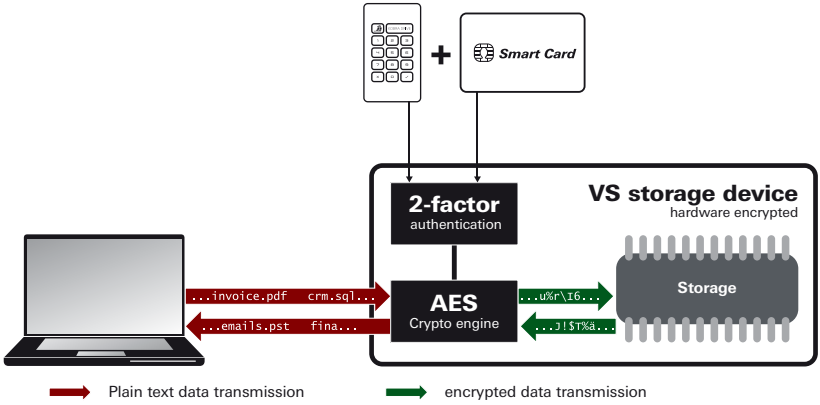
1.1 Encryption

- 256-Bit AES full-disk encryption in XTS mode

The encryption module integrated in the security housing carries out a complete encryption of the Kobra VS storage device. Each byte stored and each sector written on the Kobra VS is encrypted in XTS mode according to 256-Bit AES (Advanced Encryption Standard) using two cryptographic keys with 256-Bit each.

The Kobra VS also encrypts the entire partition. This also includes temporary files and boot sectors written to the partition, which are often ignored by encryption software.

The hardware encryption allows the Kobra VS to be used independently of the user operating system and is transparent. The data is accessed without restrictions on the read and write speed.



1.2 Access control

Access control is based on the principle of “possession and knowledge”: To access the data, the user must possess the smartcard and know the correct User-PIN.

The Digittrade smartcard is automatically blocked as soon as the allowed number of incorrect PIN entries is exceeded. Blocked Digittrade smartcards can be unblocked by entering the SO-PIN. The Digittrade smartcard will be irrevocably blocked as soon as the number of incorrect SO-PIN entries is exceeded. Afterwards the access to the data is only possible with another smartcard enabled for this specific Kobra VS storage device and the correct PIN entry.

For PKI cards, these features are regulated by the IT security concepts and internal guidelines of the administrators

1.3 Key management

The two 256-Bit encryption keys responsible for encrypting and decrypting the data are directly linked to the DEK (Data Encryption Key). Therefore, the key management focuses on the generation, storage, modification and destruction of the DEK (Data Encryption Key). It is generated on the Kobra VS by using a random number generated on the Digittrade smartcard and stored in a secure area encrypted in such a way that it can only be decrypted by the authorized smartcards.

To encrypt and decrypt the data, the encrypted DEK (Data Encryption Key) is decrypted after the correct entry of the User-PIN using the smartcard and made available to the encryption module of the Kobra VS. With the Digittrade smartcard (or PKI card) and the User-PIN, the user can create, change and destroy the DEK (Data Encryption Key) for the Kobra VS device at any time (chapters 4.7, 4.8).

These processes are irreversible. After a new DEK (Data Encryption Key) has been generated, the old DEK (Data Encryption Key) and thus all data stored on the Kobra VS, are permanently destroyed. Therefore, the stored information may have to be backed up on another device approved by the German Federal Office for Information Security (BSI) and/or NATO beforehand.

1.4 User administration

Several users can be released for a VS data carrier. The description of this function can be found in the Administrator's guide.

1.5 Smartcard

As a standard, the Kobra VS is delivered with two Digittrade smartcards certified according to Common Criteria EAL4+ (Atos Card OS 5.3, CC EAL 4+). In the stand-alone environment, only these Digittrade smartcards are approved for use according to VS-NfD approval for the time being. In addition, the user's own PKI cards can be used. In this way it is possible to integrate the Kobra VS storage devices as a component into the user's PKI infrastructure. In special cases it can be checked whether other customer-specific smartcards or PKI cards can also be integrated. If the PKI cards are based neither on Atos Card OS 5.0 nor Card OS 5.3, it is necessary to consult the German Federal Office for Information Security (BSI) whether these smartcards provide sufficient protection for VS-NfD.

The Digittrade smartcards are supplied for the Kobra VS storage devices Kobra Drive VS and Kobra Stick VS (1FF) in EC-card format. The Kobra Stick VS (2FF) is supplied with the Digittrade smartcards in mini-SIM-card format. They will be referred to as "Digittrade smartcard" in the following chapters. The Digittrade smartcard allows access to the data on the Kobra VS storage device as well as the creation, modification and destruction of the DEK (Data Encryption Key) and the encryption and decryption of the DEK (Data Encryption Key). The DEK (Data Encryption Key) is managed on the Kobra VS using the Digittrade smartcard (or PKI card) and the User-PIN, completely independent of a PC.

For the log-in to the Kobra VS both Digittrade smartcards have a User-PIN and SO-PIN with standard values at delivery (chapter 8). All Digittrade smartcards have different serial numbers and stored key pairs consisting of public and private keys. On the front of the Digittrade smartcard, the model name and the serial number of each smartcard is written.

With the help of the software Kobra Client VS the administrator can release up to 10 Digittrade smartcards or PKI cards for an individual Kobra VS storage device and define the authorization of the respective users differently. This is done by entering the Digittrade smartcards (or PKI cards) into the smartcard table of the Kobra VS storage device. (Chapter 4.14)

1.6 User-PIN and SO-PIN

The User-PIN and SO-PIN are available to the user and can be changed by them at any time. In combination with a valid Digittrade smartcard they enable authentication on the Kobra VS storage device and consequently access to the stored data.

With the help of the User-PIN, the user can authenticate (log-in) to the Kobra VS storage device, create a new DEK (Data Encryption Key) and change the User-PIN. In addition, he can activate and deactivate write-protection if he has write permission.

The SO-PIN is needed for the change of the SO-PIN as well as for the activation of the Digittrade smartcard after locking the User-PIN. This can happen if the number of allowed failed attempts to enter the User-PIN is exceeded. The Digittrade smartcard will be locked permanently, if the number of allowed failed attempts for entering the SO-PIN is also exceeded.

The Digittrade smartcard is delivered with the User-PIN 1-2-3-4 and the SO-PIN 1-2-3-4-5-6-7-8-9-0. The factory settings for the User-PIN allow a length of 4 to 12 digits and three attempts to enter the User-PIN. For the SO-PIN, ten input attempts and a length of 4 to 12 digits are also permitted. In the PKI scenario, these settings are controlled by the PKI administrators.

Important:
The passing on of the SO-PIN to the user can be regulated differently by the internal guidelines of the respective company.

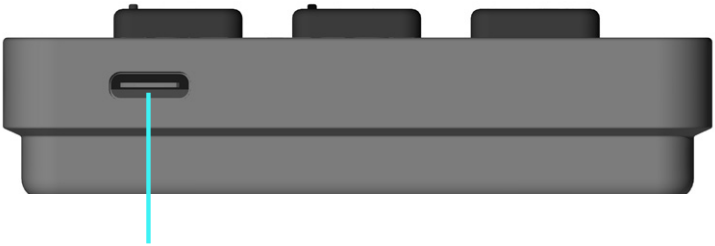
1.7 Admin-PIN

The description of this function can be found in the Administrator's guide.

1.8 USB connection, smartcard slot and input interface

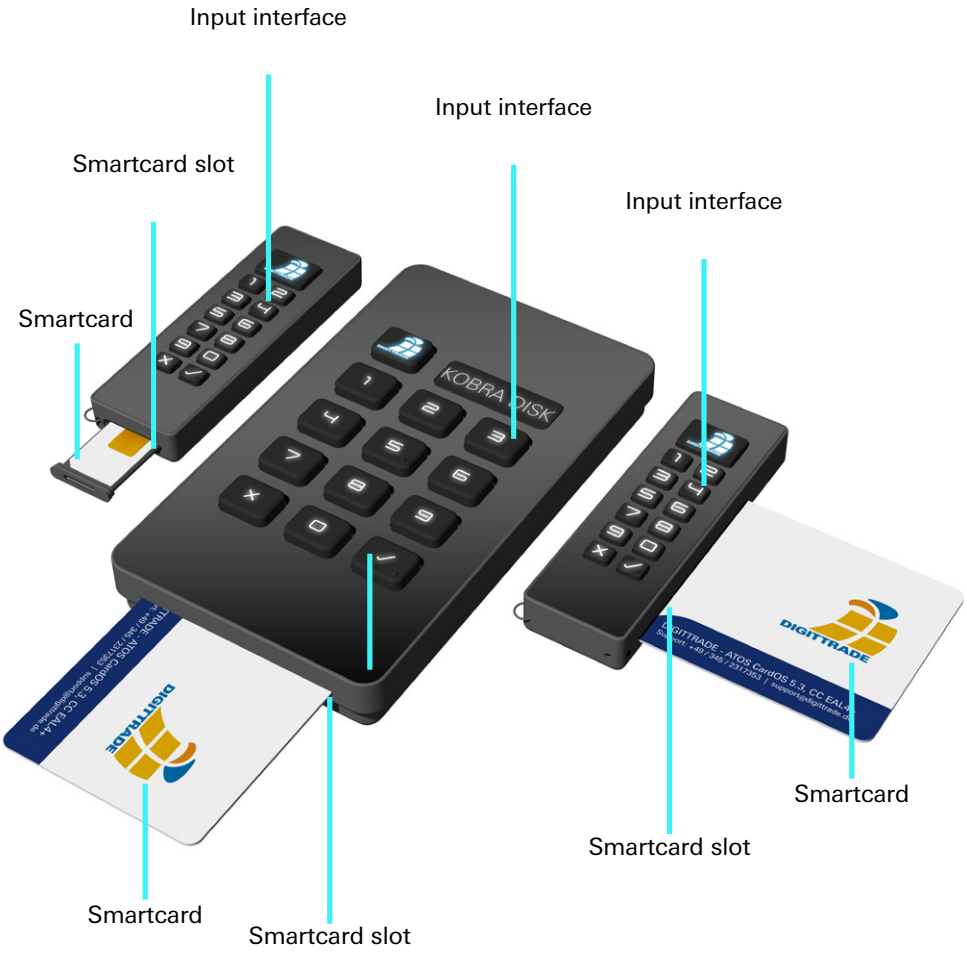
USB-C 3.0 port
Kobra Stick VS (2FF)

USB-C 3.0 port
Kobra Stick VS (1FF)



USB-C 3.0 port
Kobra Drive VS

Kobra Stick VS (2FF) **Kobra Drive VS** **Kobra Stick VS (1FF)**



1.9 Integrated battery as internal power supply

The Kobra VS has an integrated battery. This ensures the internal power supply and execution of the following functions without connecting the Kobra VS to a PC / Notebook or other external power supply (e.g. USB power supply or hub):

- Checking, activating and deactivating the write-protection
- Authentication before connection to a PC/Notebook (e.g. as pre-boot authentication) and booting from the Kobra VS after connection to a PC / Notebook (e.g. Windows To Go or other operating systems)
- Changing the User-PIN without connection to a PC
- Destroying a valid DEK (Data Encryption Key) and consequently deleting all data on the Kobra VS without connection to a PC

The Kobra VS is in sleep mode as long it is not connected to the PC / Notebook or another power supply. To turn it on, press and hold the Menu button for about 3 seconds.

If all keys remain unlit, this may be due to an empty battery. The battery is charged via the USB-C port after connecting the Kobra VS to a PC / Notebook or other external power supply (e.g. USB power supply unit or hub).

1.10 Features - Summary

Encryption

- 256-bit AES full-disk hardware encryption in XTS mode with two cryptographic keys
- 2-factor authentication by Digittrade smartcard (or PKI card) and PIN entry
- External storage of the key for decrypting the DEK (Data Encryption Key)
- Creation, modification and destruction of the DEK by the user
- Hardware based encryption module (data encryption of all stored bytes and described sectors)

Complimentary Security Features

- Integrated write-protection mechanism
- Time out function
- Quick-Out function
- Lock-out function

Interoperability

- Pre-Boot-Authentication and Bootability
- Operating system independent (compliant to all operating systems, multimedia devices and machines with USB slots)
- Compatible with USB 3.0 and USB 2.0
- Device usage does not reduce the read and write speed
- Internal power supply, which enables authentication without connection to a PC / Notebook or USB hub

PKI compatibility

- Support of various PKI cards
- Can be used as smartcard reader with PIN pad (CCID)

Mechanical protection

- Sturdy metal housing

Personalization

- USB VID, PID & serial number definable according to customer specifications
- High-quality laser engraving on the back of the Kobra VS storage devices

1.11 Advantages of the Kobra VS

Easy and safe handling
Connecting, log-in, usage

Secure storage of classified information
Confidential information from authorities and companies up to the VS-NfD, NATO Restricted and EU Restricted classification level can be stored on the Kobra VS device in a compliant manner.

Transparent insert
The hardware encryption implies all data is automatically and immediately stored in encrypted form, without any loss of performance.

GDPR / EU-DSGVO Compliance
Data can be stored according to the current state of technology (Stand der Technik) in accordance with the requirements of EU-DSGVO/GDPR and BDSG (German federal law of data protection).

PKI integration
Possibility of integration into already existing PKI infrastructures at authorities and companies.

1.12 Authentication

After receiving your Kobra VS it must be checked for Its authenticity. It is essential to compare the serial number and model designation in the delivery note with the engraved information on the housing of the Kobra VS and with the digital information which can be read with the aid of the supporting Kobra Client VS software.

For an additional authenticity check during operation, it is recommended to use a so-called authenticity file. This file can be selected in such a way that it is unique and can be easily verified by the owner as soon as they access the Kobra VS storage device.

In case of discrepancies, immediately contact your supplier or administrator.

1.13 Firmware Update

The description of this function can be found in the Administrator's guide.

2. Commissioning of the Kobra VS storage device

Only three steps are required for the correct commissioning of the Kobra VS storage device:

1) Connect to the PC/Notebook
2) Insert smartcard (or PKI card)
3) Enter User-PIN

The necessary power supply for a Kobra VS is always provided via the USB-C connection. For this reason, it should be connected to a PC / Notebook or USB hub with a power supply for commissioning the device. The Kobra VS also has an integrated battery. This allows you to perform certain functions without connecting the Kobra VS to an external power supply.

As long as the Kobra VS storage device is not connected to a PC or an external power supply (e.g. USB power supply or hub), it is in sleep mode. All buttons are switched off.

The Kobra VS switches to authentication mode immediately after connecting it to a PC / Notebook or other external power supply if a Digittrade smartcard (or PKI card) intended for this Kobra VS storage device is correctly inserted. The main key flashes green and the User-PIN can be entered. If there is no smartcard inserted into the Kobra VS or if it is wrongly inserted, the main key flashes red or yellow continuously until a

Digittrade smartcard (or PKI card) intended for this device is correctly inserted. If no further commands or entries are made within 20 seconds, the Kobra VS automatically switches into the waiting mode.

Pressing the main key switches from the waiting mode to the menu mode. In this state, the main key lights up blue and all other input keys light up white. The illuminated input keys indicate that they are active and that the corresponding commands can be entered. After pressing the „1“ key and then „√“, the user switches back to authentication mode. The main key flashes green and all other keys are still active. The User-PIN can be entered at this point. If the User-PIN or SO-PIN is already locked, the main key flashes alternately yellow-red-yellow-red after the PIN has been entered and confirmed by the „√“ key and then lights up white. The Kobra VS then switches into the waiting mode. Authentication is not possible in this case. The locked User-PIN can be reset with a valid SO-PIN. Digittrade smartcards with locked User-PIN and SO-PIN can no longer be used.

If there is a smartcard in the smartcard slot, that has not yet been entered into the smartcard table of the Kobra VS, the main key lights up red briefly immediately after pressing the „1“ key, and then it lights up permanently white. The Kobra VS then changes to the wait mode. Authentication is not possible in this case either.

All commands are confirmed with the „√“ key or cancelled with the „X“ key. Each time the „X“ key is pressed, the user switches to wait mode and can restart his planned steps. The main key flashes orange once and then lights up white.

After a successful authentication, the main key lights up continuously in green when the write-protection is deactivated and violet when the write-protection is activated. The other keys are unlit and access to the data on the device is enabled.

If the PIN entry was faulty, the main key will flash red once or several times according to the number of failed attempts (but no more than the number of allowed failed attempts) and the Kobra VS will switch back to wait mode. The authentication process can be repeated from this point as described above. When the permitted number of failed attempts has been exceeded, the main key flashes yellow-red-yellow-red and then lights up white. The Digittrade smartcard locks itself automatically and can only be unlocked afterwards by entering the SO-PIN. PIN entry attempts under 4 digits are generally not counted as failed attempts (chapter 4.4).

The faulty input of the SO-PIN leads to the final blocking of the Digittrade smartcard after exceeding the failed attempts. Accessing the data is then only possible with another Digittrade smartcard enabled for this specific Kobra VS device and correct entry of the User-PIN. In this case the existing smartcard table on the Kobra VS must be deleted and a new smartcard table created with the help of the Kobra Client VS software. This is done automatically and then a new DEK (Data Encryption Key) is generated. All previously stored data is irreversibly destroyed. (Chapter 4.14)

If there are no other Digittrade smartcards authorized for this specific Kobra VS storage device, the only possibility is to initialize a new Digittrade smartcard for this Kobra VS. This task is done by the administrator by deleting the current smartcard table and creating a new one. All previously stored data is irrevocably destroyed during this process.

Authentication can also be performed without connection to a PC / Notebook or other external power supply (e.g. USB power supply or hub). In this case the power supply is ensured by the integrated battery. After pressing the main button for approximately 3 seconds, the Kobra VS switches to authentication mode. The user then inserts his smartcard and enters the corresponding User-PIN. After the successful authentication the Kobra VS can be connected to a PC / Notebook within 20 seconds.

If no further commands or entries are made within 20 seconds, the Kobra VS automatically switches to wait mode if it is connected to a PC / Notebook or another external power supply (e.g. USB power supply or hub). In case there is no external power supply, the Kobra VS returns to sleep mode after 20 seconds. However, this does not apply to the authenticated Kobra VS if it is already connected to a PC / Notebook.

For security reasons, a logical or physical separation of the Kobra VS from the host system, after use, must be performed. This is especially recommended when terminating, interrupting for some time or leaving the workplace.
In this context, the activated time-out function provides good support for effective data protection. This setting can also be used to configure an automatic time-out for the connected data carrier in case of inactivity. (Chapter 4.9)

In addition, the Kobra VS storage device also has the Quick-Out function for quick log-out in addition to the classic „log-out" mechanisms such as „safe removal" via the PC task bar and physical disconnection of the USB connection. This function is performed by double-clicking the „×" button within 2 seconds.

For safe physical separation, the USB cable must be completely removed from the Kobra VS storage device.

Important:
To avoid data loss, make sure that the data transfer and access to the Kobra VS are completely finished before disconnecting the connections.

Important:
To ensure the security of your data, it is absolutely necessary to change the preset User-PIN and SO-PIN (chapters 4.3, 4.5). Also change the User-PIN at regular intervals in the future. Additionally, it is recommended to use different User-PIN for different Digittrade smartcards. The User-PIN and SO-PIN must be kept confidential.

3. Role and permissions

The Kobra VS allows the distribution of roles and authorizations regarding the administration and use of the storage device.

The user has the smartcard and knows the User-PIN and SO-PIN. He can change the User-PIN and SO-PIN, authenticate (log-in) to the Kobra VS storage device, create a new DEK (Data Encryption Key) and unlock the Digittrade smartcard after the lock due to an incorrect User-PIN entry. In addition, he can activate and deactivate the write-protection if he has write-permission.

The administrator knows the Admin-PIN. They can change the Admin-PIN and make time-out and lock-out settings. They can also add to, delete or create a new list of the authorized Digittrade smartcards of the Kobra VS storage device (also called smartcard table). In addition, they can define whether the user is only authorized to read or to read and write data onto the Kobra VS device.

The administrator has no possibility to access the stored data of a Kobra VS on the basis of his permissions. However, during the activation of an additional Digittrade smartcard for a Kobra VS device they might get knowledge of a User-PIN, because it has to be entered when adding. It is therefore imperative that the user changes the User-PIN after this process.

Using the Kobra Client VS software, the administrator can quickly transfer the above settings to other Kobra VS devices. Furthermore, they can deactivate or activate the entry of the Admin-PIN via the keypad of the Kobra VS device. The entry of the Admin-PIN via the Kobra Client VS software is still possible in any case. In this way the incorrect entry of the Admin-PIN by the user and thus the irrevocable blocking of the Admin-PIN can be avoided. Once the Admin-PIN has been locked, it is no longer possible to change the settings made by the administrator.

The conception of the PKI cards and the passing on of the SO-PIN to the user can be individually regulated by internal guidelines and security concepts of the respective companies or authorities.

Warning:
It must be assumed that the administrator may have access to the data stored on the Kobra VS device. Therefore, the administrator must be trustworthy. If there is any doubt about trusting the administrator, the user must become the administrator himself and manage the smartcard table on his own.

4. Menu mode: authentication and management

The authentication and administration of the Kobra VS storage device is done via the menu mode by entering numbers and commands. Switching to the menu mode is generally done from the wait mode by pressing the main key. In the menu mode the main key lights up blue and all other input keys are white.

To execute the commands, the Kobra VS usually requires connection to a PC / Notebook or other external power supply (e.g. USB power supply or USB hub). Exceptions are authentication on the Kobra VS, activation or deactivation of write protection and the creation of a new DEK (Data Encryption Key). These functions can also be performed in the battery mode.

In menu mode, all inputs and commands are confirmed with the "√" key or canceled with the "X" key. Each time the "X" key is pressed, the Kobra VS switches to wait mode. The process can be repeated from this point.

After starting a menu function, the main key starts flashing green when the User-PIN has to be entered. However, the main button flashes continuously purple for the Admin-PIN and light blue for the SO-PIN. All other keys are active at this moment. If the entry is confirmed with the "√" key, the main key lights up green if the PIN is correct.

When an error occurs, the main key flashes red briefly and then lights up white. The Kobra VS will switch to wait mode. The process can be repeated from this point.

If the PIN entry was faulty during one of the operations, the main key will flash red once or several times according to the number of failed attempts (but at most the number of allowed failed attempts) and the Kobra VS will switch to wait mode. The scheduled operation can be restarted from this point.

In addition, the Kobra VS switches to wait mode after each successful execution of a command (except user authentication).

4.1 User authentication

User authentication is required to enable access to the Kobra VS device.

For authentication:

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key, key "1" and then "√". The main key flashes green and all other keys remain active.
3) Enter the User-PIN and confirm with "√".

After successful authentication, the main button will be permanently lit in green if the write protection is disabled or purple if it is enabled. The other keys are deactivated and access to the data is enabled.

Note: *If the user has already inserted a valid smartcard into the Kobra VS device during sleep mode (all keys were switched off), the Kobra VS will immediately switch to authentication mode after pressing the main key for a long time or after connection to a PC/ Notebook. In this case, the User-PIN can be entered directly.*

4.2 Write-Protection Mechanism

The activated write-protection offers you additional protection against viruses and trojans while using the Kobra VS on a foreign PC/Notebook. In addition, it can prevent sensitive information from being accidentally stored on the Kobra VS from a PC / Notebook or server.

Even before authentication, the user can check whether the write-protection is activated by pressing the "2" key. The main key, which is permanently illuminated in violet, indicates that write-protection is activated. If the write-protection is deactivated, the main key lights up green

For activating or deactivating the write protection:

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key and the key "2". When the write-protection is activated, the main key lights up violet, when write protection is deactivated it lights up green
3) Then press the "√" key if you want to change the status. The main key flashes green and all other keys remain active.
4) Then enter the User-PIN and confirm with "√".

After a successful switchover, the main button flashes green or purple twice and the Kobra VS switches back to wait mode.

The administrator can use the Kobra Client VS software to define whether the user is authorized to read only or also to write.

4.3 Changing the User-PIN

The user can choose a combination of 4 to 12 digits for the User-PIN.

For changing the User-PIN:

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key, the key "3" and then "√". The main key flashes green continuously, and all other keys remain active.
3) Enter the current User-PIN and confirm with "√".
4) Enter the new User-PIN and confirm with "√".
5) Repeat the new User-PIN and confirm with "√".

After a successful PIN change, the main key flashes green briefly and the Kobra VS switches back to wait mode.

4.4 Activating/Resetting the User-PIN

After exceeding the permitted number of failed attempts, the Digittrade smartcard locks itself automatically and can only be unlocked again by entering the SO-PIN. This function allows the user to replace the locked User-PIN with a new one.

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key, the key "4" and then "√". The main key flashes light blue and all other keys remain active.
3) Enter the SO-PIN and confirm with "√".
4) Enter the new User-PIN and confirm with "√".
5) Repeat the new User-PIN and also confirm with "√".

After a successful activation of the Digittrade smartcard, the main key flashes green briefly and the device switches into the waiting mode.

The faulty entry of the SO-PIN leads to the final blocking of the Digittrade smartcard after exceeding the permitted number of failed attempts. Access to the data is then only possible with another smartcard enabled for this Kobra VS and correct a PIN entry.

4.5 Changing the SO-PIN

The user can select a combination of 4 to 12 digits for the SO-PIN.

For changing the SO-PIN:

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key, the “5” key and then “√”. The main key flashes light blue and all other keys remain active.
3) Enter the current SO-PIN and confirm with “√”.
4) Enter the new SO-PIN and confirm with “√”.
5) Repeat the new SO-PIN and also confirm with “√”.

After a successful PIN change, the main key flashes green briefly and the Kobra VS switches back to wait mode.

4.6 Changing or switching of the Admin-PIN

The description of this function can be found in the Administrator’s guide.

4.7 Creating a new DEK (Data Encryption Key)

With the help of an initialized Digittrade smartcard (or PKI card) and User-PIN, the user can create, change and destroy the DEK on the corresponding Kobra VS at any time. These processes are irreversible. After a new DEK has been generated, the old DEK and thus all data stored on the Kobra VS will be permanently destroyed. For this reason, the stored information may need to be backed up on another VS-NfD-approved device beforehand.

When deleting the data, you should refrain from overwriting the data several times, as this will considerably reduce the life of the Kobra VS. The data is deleted safely and efficiently by generating a new DEK or by deleting the smartcard table. (Chapter 4.8)

To create or modify the DEK:

1) Make sure that the Kobra VS is connected to a host system and that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key and the key “7”. The main key lights up red permanently, indicating that all data stored on the Kobra VS has been

permanently destroyed after this function has been carried out.

3) Press the "√" button if you want to perform this function. The main key flashes green and all other keys remain active.
4) Enter the User-PIN and confirm with "√".

After the DEK has been successfully created or modified, the main button first lights up yellow and then permanently white. The Kobra VS switches back to wait mode. This process can take several seconds. Especially if several smartcards are entered in the smartcard table.

At the next authentication, the main key will flash blue until formatting is complete. This process may take a few minutes depending on the memory size. Afterwards, the main button lights up green or purple, depending on whether the write protection is activated (purple) or deactivated (green). Access to the data previously stored on the Kobra VS is no longer possible from this point on.

4.8 Deleting a DEK (Data Encryption Key)

There are three ways to delete and/or destroy the DEK.

A: Destruction of DEK without generating a new DEK (occurs without connection to a host system)

The user can perform this method with the help of the User-PIN. During this process, the old DEK is irrevocably deleted. Access to all previously stored data is no longer possible from this point on. This method allows the data stored on the Kobra VS to be quickly destroyed without connecting the data carrier to a PC.

1) Make sure that you are in wait mode. (The main key lights up white and all other keys are hidden)
2) Then press the main key and the key "7". The main key lights up red permanently, indicating that all data stored on the Kobra VS has been permanently destroyed after this function has been carried out.
3) Press the "√" button if you want to perform this function. The main key flashes green and all other keys remain active.
4) Enter the User-PIN and confirm with "√". The main key initially lights up green, then flashes yellow-red-red and then lights up white.

This process deletes the current DEK. For further use of the Kobra VS, a new DEK must then be generated after connection to a host system. (Chapter 4.7)

B: Destruction by generating a new DEK (done with connection to a host system)

The user can only perform this method after connecting to a host system using the User-PIN. During this process, the old DEK is irrevocably overwritten. Access to all previously stored data is also no longer possible from this point on. (Chapter 4.7)

C: Destruction of the DEK by deleting the smartcard table

The description of this function can be found in the Administrator's guide.

4.9 Time-out functions

The administrator can define after how many minutes the unlocked Kobra VS is automatically locked if there is neither read nor write access to the Kobra VS within the specified time.

4.10 Quick-Out Function

The Quick-Out function enables a quick locking of the Kobra VS. It is performed by double clicking the "×" button within 2 seconds.

4.11 Lock-Out Function

With the Lock-Out function the administrator can determine whether the Digittrade smartcard (PKI card) should remain inside the Kobra VS after authentication or whether it can be removed. If the lock-out mode is deactivated, access to the data is immediately interrupted after removing the Digittrade smartcard (PKI-card) from the Kobra VS.

The description of this function can be found in the Administrator's guide.

5. Formatting

The Kobra VS storage device already has the FAT32 file system when delivered. This format can be read and written by almost all operating systems (Windows, Mac OS and Linux). The maximum file size in this format is up to 4GB and is therefore sufficient for most contents.

The user can reformat the Kobra VS according to the application scenarios. For Windows users, it is recommended to use NTFS, for Mac OS X, APFS is the most powerful file system and for Linux, EXT4 can be used.

If necessary, you can use extension programs to write data to file systems where this is otherwise not possible. Of course it is also possible to format the Kobra VS device with any other file system. This does not affect the encryption of the data or the protection performance of the Kobra VS. The table below shows the compatibility between the operating and file systems.

	NTFS	FAT32	APFS	EXT4
Windows XP, Vista, 7, 8, 10	L, S	L, S	X	X
Mac OS X	L	L, S	L, S	X
Linux	L	L, S	X	L, S

Title: L - Read, S - Write, X - No compatibility

6. Possible applications

The features of the Kobra VS offer extensive possibilities for the secure storage, archiving and transmission of sensitive, personal and confidential information up to the classification level VS-NfD, NATO Restricted and EU Restricted. The following application scenarios are also within the scope of the VS-NfD approval. Deviations from the described procedures must be approved by the German Federal Office for Information Security (BSI).

6.1 Strengthening the level of protection of data within a company or public office

The description of this function can be found in the Administrator's guide.

6.2 Secure and cost-efficient data transport

The Kobra VS device can be used to transport confidential data. For this purpose, the Digittrade smartcards of the sender and receiver are entered into the smartcard table of the Kobra VS device. The sender sends the Kobra VS without the smartcards. In this way a regular data exchange between two locations can be organized.

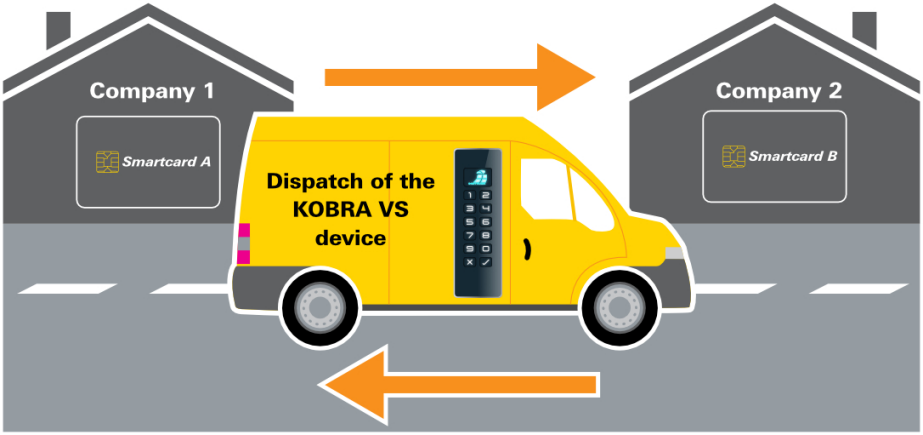
In the stand-alone version the user has two Digittrade smartcards which are already entered in the smartcard table. In this case they can give their second Digittrade smartcard to the receiver to decrypt the data. The administrator can also add an additional Digittrade smartcard to the smartcard table of the Kobra VS for the receiver. The Kobra VS and the Digittrade smartcard are sent to the recipient on separate ways. The transmission of the User-PIN and (if applicable) the SO-PIN is also done separately and only after receipt of the Digittrade smartcard.

When using PKI cards, the administrator enters the serial number and the public key of the PKI cards of the sender and the recipient into the smartcard table of the Kobra VS using the Kobra Client VS software. To do this, the administrator must physically possess the Kobra VS, but the smartcards can remain with the users.

During the physical transport of the Kobra VS device, a suitable packaging must be used to ensure that attempts at tampering are detected. The use of sealed DIGITTRADE security bags is recommended for this purpose. (For information on the security features to be checked on the Kobra VS, see Chapter 1.12 and on the security pouches in Chapter 7.2)

Upon receipt of the Kobra VS, its authenticity must be checked. For this purpose, the serial number of the Kobra VS device is sent along with it via a separate secure channel and a file with a specific identification is stored within the device. The serial number can be found both on the case and on the USB registration of the device. The Kobra Client VS conveniently displays the model name and serial number of the Kobra VS device immediately after connecting to a PC.

This method allows the Kobra VS to be used as transport device of confidential data to be delivered to the recipient cost-effectively and insured by a parcel service or courier.

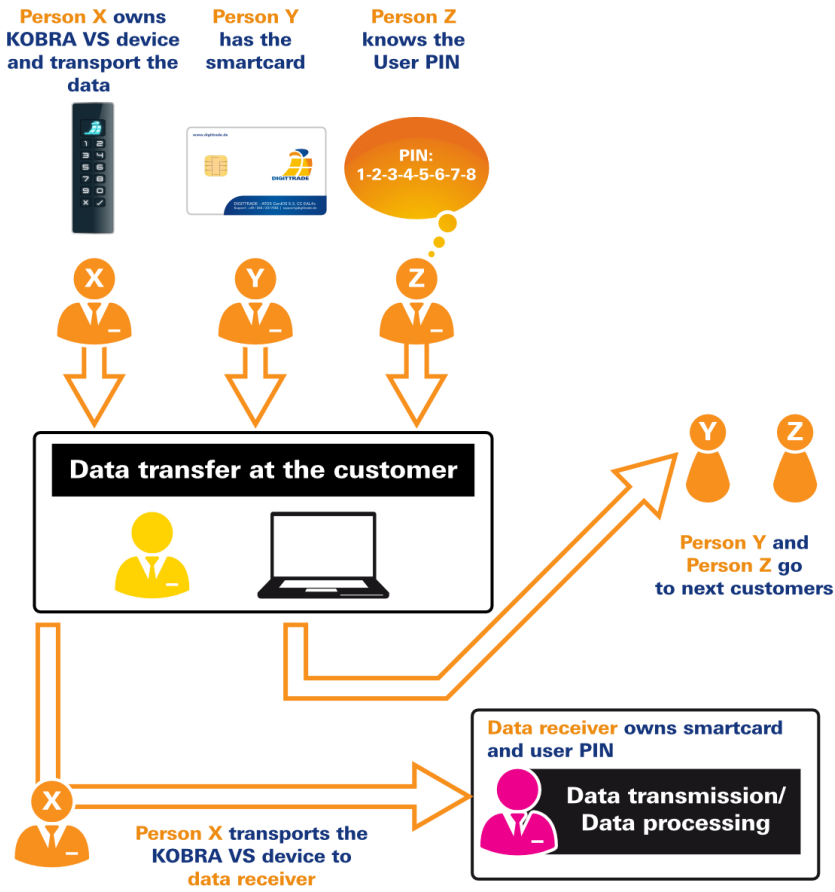


Warning:
If manipulation attempts have been made during transport, the Kobra VS may no longer be used within the scope of the VS-NfD approval.

6.3 Separation of Kobra VS device and authentication features

Access to the data may be regulated in such a way that it is only possible by bringing together three people. Person X (e.g. courier) physically owns the Kobra VS, person Y has the released Digittrade smartcard and person Z knows the User-PIN. The three people meet only for data transfer at the receiving point and separate again afterwards. The people X, Y and Z do not have the possibility to access the data individually.

Warning:
If manipulation attempts have been made during transport, the Kobra VS may no longer be used within the scope of the VS-NfD approval.



6.4 Use of fewer Kobra VS devices with a large customer base

If a company (e.g. a data processing company or a data-center of large companies/ authorities) or public office regularly exchanges data with several different users, the data can be transported cost-effectively and securely with a few Kobra VS devices.

Each user receives an individual smartcard. The serial number and public key of all smartcards are created at the data-center. For each data exchange with another user the smartcard table of the Kobra VS device is deleted first. The next step is to create a new table with the smartcard information of the sender and receiver (Admin-PIN required). Afterwards the data can be stored and sent secured on the Kobra VS storage device.

The administrator deletes the old smartcard table after receiving the Kobra VS from an employee and creates a new one with the smartcard information of the following user. Time-consuming data deletion and repeated overwriting of the data carrier is no longer necessary, the remaining data was encrypted with the previous DEK. It cannot be reconstructed after deleting the smartcard table and therefore there is no possibility to access the previously stored data.

If data is to be sent to the same recipient several times at short intervals, it is not necessary to wait for a personalized Kobra VS device to be returned, any Kobra VS device available in the company may be used. To do this, the smartcard table of the first Kobra VS can be imported into another Kobra VS device. (Chapter 4.14)

Thanks to this feature, the number of required Kobra VS devices can be significantly reduced, since a personal Kobra VS device is not required for each user. It is irrelevant which of the Kobra VS devices is available in the company and used for the data transport. The decisive factor is which Digittrade smartcards (or PKI cards) are entered in the smartcard table of the Kobra VS device.

Important:
When deleting the data, you should refrain from overwriting the data several times, as this will considerably reduce the life of the Kobra VS device. The data is deleted safely and efficiently by generating a new DEK or by deleting the smartcard table. (Chapter 4.8)

Warning:
If manipulation attempts have been made during transport, the data carrier may no longer be used within the scope of the VS-NfD approval.

6.5 Use of fewer Kobra VS devices in the field and by authorities

In a company, every sales representative has his personalized smartcard (or PKI card) with their own specific cryptographic features. For work outside the company, the employee may receive any Kobra VS device that has been prepared in advance for use by this employee. The administrator deletes the old smartcard table and creates a new one with the smartcard information of this employee. The field service employee then stores the data with his or her own cryptographic keys.

After use, the employee returns the Kobra VS device. This is then made ready for the next colleague to use in the same way within a few minutes. The data of the previous user is automatically and irrevocably deleted. Therefore, a separate Kobra VS device is not required for each employee and the number of required devices in the company can be reduced.

Important:
In addition, it is recommended to delete the current DEK before returning the Kobra VS device. This will destroy the data on the Kobra VS device even before it is returned to the administrator.

6.6 Operating several Kobra VS devices with only one smartcard

For the operation of several Kobra VS devices with only one smartcard, the smartcard table is stored with the samesmartcard information (serial number and public key) on several Kobra VS devices with the support of the Kobra Client VS software.

This scenario is of particular interest when working with data volumes that exceed the capacity of a Kobra VS device. In this case, the data can be distributed across several Kobra VS devices.

Even if data is sent very frequently, e.g. daily, it is advisable to use several devices in this way. A new Kobra VS device with the same smartcard table can be sent daily without having to wait for a personalized Kobra VS device. The sender and the recipient can always access the Kobra VS device with the same smartcard.

Important:
When sending the Kobra VS device, further measures are necessary, which are described in 6.2.

6.7 Use as an encrypted boot device

The integrated autonomous power supply enables authentication of the Kobra VS before starting a PC / Notebook (pre-boot authentication). This feature offers the possibility to store operating systems encrypted on the Kobra VS and then start them directly from the Kobra VS device.

In this context, operating systems such as Windows-To-Go, Linux, ECOS-OS and others, as well as user data can be stored. This application scenario is suitable for both stationary and mobile computers. The minimum memory capacities required must be considered. The Windows-To-Go operating system can only be used on Kobra VS devices with storage capacities of at least 32 GB. In addition, Kobra VS devices with pSLC memory are recommended for these purposes, in order to ensure the longest possible lifespan of the device.

When the Kobra VS is disconnected from the PC, the data, programs and operating systems, including temporary files, remain stored encrypted exclusively on the Kobra VS device and are inaccessible to unauthorized persons.

Important:
Windows-To-Go compatibility can be configured by the administrator via the Kobra Client VS.

6.8 Use on different operating systems and smartphones

With its hardware encryption and hardware authentication, the Kobra VS works independently of the operating system and can be used on almost any device that supports USB media.

The optimized power consumption allows the Kobra VS device to be used for data exchange with a smartphone or tablet.

Important:
Provided that VS-NfD classified information is on the data carrier, its use is only permitted on the devices approved for processing VS-NfD information within the scope of the approval. The deletion of VS-NfD information on the data carrier must be carried out according to the procedures in chapter 4.8.

6.9 Use as data diode

The activated write-protection of the Kobra VS device offers a safe protection against the unwanted flow of information from higher-rated systems to lower-rated systems.

To do this, the data from the source system (e.g. VS-NfD) is written to the Kobra VS device and then the write-protection is activated on the Kobra VS. In a next step, the Kobra VS is connected to the higher-rated system (e.g. secret) and the required data is transferred from the Kobra VS to the host system. Afterwards, the device can be used again normally in the original system.

Possible further security measures such as virus scanning are still required. As an option, a quick and secure deletion of the Kobra VS can be carried out before and after by regenerating the DEK.

For the implementation of the data diode function, the administrator can also define two smartcards as follows: One smartcard is for working in the VS-NfD area and the second smartcard is for the secret area. The smartcard for the VS-NfD area enables reading and writing. The smartcard for the secret area is read-only.

Afterwards the smartcard "VS-NfD" remains exclusively in the IT area for VS-NfD. The smartcard "Secret" is exclusively in the IT area Secret. If data is transferred from the VS-NfD area to the secret area using the Kobra VS, it is automatically ensured that the Kobra VS is read-only when used on the secret system. Neither consciously nor unconsciously can sensitive information classified as secret be transferred to the Kobra VS.

6.10 Use as authentication medium

The Kobra VS allows the secure storage of authentication features such as user names, very complex passwords, digital certificates, key pairs and others. However, the use of USB devices is prohibited in some companies and organizations to prevent unwanted data leakage.

Similar to its use as a data diode, the Kobra VS can be configured so that the user only has read access after the authentication component has been saved. These Kobra VS devices can then be released by the administrator for use within the company IT. In this way, every employee can receive a secure authentication device, without endangering the IT security of the company.

6.11 Use as Smartcard Reader with PIN-Pad

The Kobra VS can also be used as a smartcard reader with keypad for PIN entry or as an authentication token with PIN pad. This function enables the user to use their smartcard with digital certificates to sign digital documents, without having to purchase another card-reader for this purpose.

For example, the smartcard can be set up for e-mail encryption, VPN access, Windows or Linux log-on and for general 2-factor authentication with digital certificate by the manufacturer. For more information, please contact your supplier.

6.12 Integration within existing smartcard and PKI infrastructures

If a company already uses the smartcard Atos Card OS 5.0 or 5.3, CC EAL 4+ (e.g. for access management, user authentication etc.) or other smartcards that meet the security requirements for VS-NfD, the integration of the Kobra VS is possible. In addition, the Kobra VS device can be integrated into the PKI infrastructures of public authorities or companies. In this case, for example, users can use their employee ID card to unlock the device.

6.13 Integration of existing software solutions

All existing software solutions for external devices in the company can continue to be used as a supplement to extend the security features and methods in use.

6.14 Use of the VID and PID for the protection of company data

Optionally, the USB Vendor-ID (VID) and Product-ID (PID) can be implemented customer-specific. With this information the Kobra VS can be assigned to different departments and user groups. These may also have different authorizations for USB connections in the company's internal network.
In this way it can be determined which Kobra VS device may be connected to which USB interfaces in the company. The connection of other "unauthorized" USB devices can thereby be prevented.

Additional software may be required to control the USB ports on the host systems.

7. Optional accessories

Additional smartcards and security packaging are offered as optional accessories to implement user-specific tasks.

7.1 Additional Smartcards

If required, additional approved Digittrade smartcards can be purchased. These are delivered with generated key pairs and have a pre-set User-PIN and SO-PIN with standard values. For commissioning these please refer to chapter 2.

7.2 Safety packaging

In order to detect unauthorized tampering, a special Digittrade security packaging is recommended for the dispatch of the Kobra VS devices and Digittrade smartcards (PKI cards). This packaging can also be ordered from suppliers as optional accessories.

The contents of the security packaging are described on the packaging itself. Upon receipt, the recipient checks the integrity of the security lettering "DIGITTRADE SECURITY" on the sides. In addition, there is a special seal at the top end to indicate any attempts at tampering.

Possible indicators:

The blue stripe under the upper area of the seal closure and the pale yellow thermal stripe indicate that the safety packaging is correctly closed and has not been reopened.

In extreme cold areas (e.g. use of cold spray) the blue sealing tape separate from the backing material. The warning “STOP” becomes legible.

Strong heat (e.g. from a hairdryer) turns the pale yellow thermal strip red.

When solvents are used, the blue colour of the seal dissolves. The tampering is immediately visible.

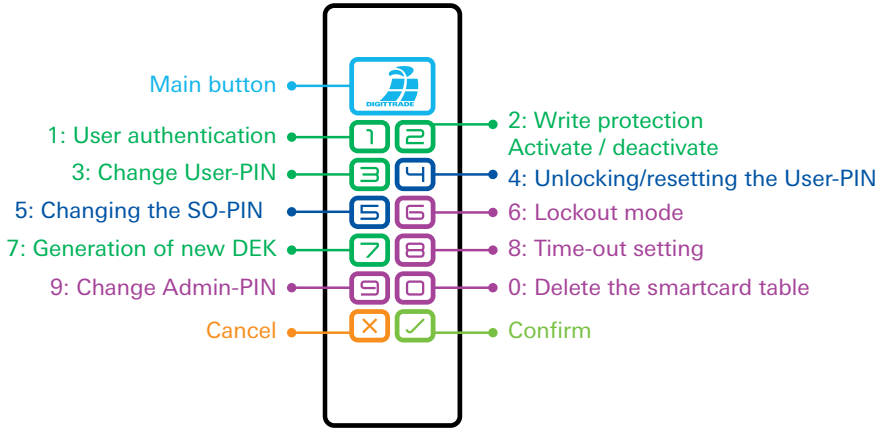
Upon receipt, make sure that these indicators have not been triggered.

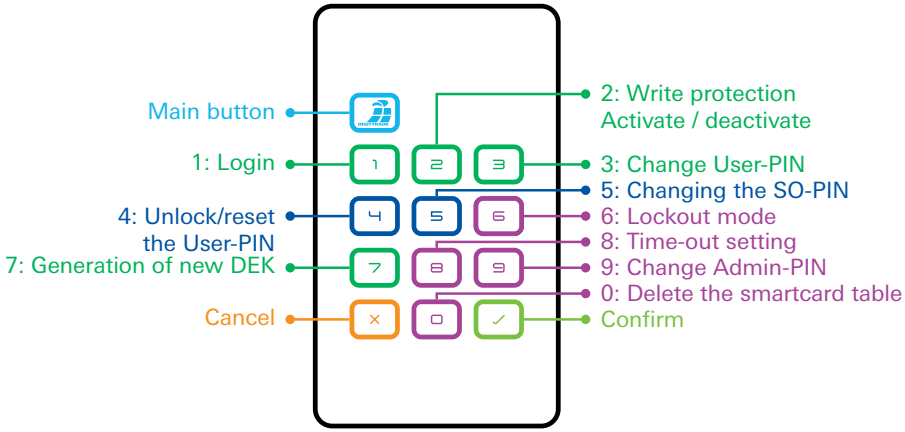
8. Menu overview, commands and factory settings

User	Button 1 - Log-in key 2 - Write-Protection * Key 3 - Change User-PIN Key 4 - Activating the User-PIN Key 5 - Changing the SO-PIN Key 7 - Create new DEK
Administrator	Key 6 - Setting Lock-Out Key 8 - Setting time-out Key 9 - Change Admin-PIN key 0 - delete the smartcard table
Confirmation of the entries	Key √ or main key
Cancel	X button
Quick logout	2 x key X within of 2 seconds press
User-PIN (standard)	1-2-3-4
Failed attempts (User-PIN)	3
Number of digits (User-PIN)	4 to 12
SO-PIN (default)	1-2-3-4-5-6-7-8-9-0
Failed attempts (SO-PIN)	10
Number of digits (SO-PIN	4 to 12
Time out	Adjustable: 0 to 30
Time out (default)	switched off*
Lock-Out (standard)	switched off*
Write protection (standard)	deactivated*

* – The administrator can block these settings before delivery to the user.

User-Commands
SO-PIN-Commands
Administrator Commands





9. Technical specifications

Transfer rate:	USB 3.0 max. 5 GBit/s USB 2.0 max. 480 MBit/s The actual write- and read-rate to be achieved depends on the the selected memory size, memory type, the USB port and the host system.
Encryption:	256-Bit AES hardware encryption, XTS mode, with 2 x 256-Bit crypto keys

Kobra Stick VS

Memory sizes:	4 GB, 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Memory types:	3D TLC, MLC and pSLC

Kobra Drive VS

Memory sizes:	250 GB, 500 GB, 1 TB, 2 TB, 4 TB, 8 TB
Memory types:	HDD, SSD

10. Scope of delivery

- Kobra VS storage device version 1.0
- 3 USB cables (USB-C to USB-C, USB-C to USB-A, USB-C to USB Micro-B)
- 2 Digittrade smartcards (optional)
- Packing

11. Data security, data availability and exclusion of liability

The Kobra VS storage devices offer you a high level of data security according to the current state of technology. They ensure data protection (GDPR, EU-DSGVO) compliant storage and safekeeping as well as secure transport of sensitive, personal and confidential information up to the classification level VS-NfD, NATO Restricted and EU Restricted.

To achieve the same high data availability level, we recommend that you regularly back up the data on the Kobra VS onto another Kobra VS device. This will protect you from complete data loss in unforeseen situations.
DIGITTRADE GmbH is not liable for the loss of data or for any costs and damages incurred

as a result. In addition, the company mentioned does not bear any responsibility for the stored data in terms of data protection law.

12. Secure exit after using the Kobra VS storage device

For security reasons, a logical or physical separation of the Kobra VS from the host system, after use, must be assured. This is especially recommended when terminating, interrupting for a short time or leaving the workplace. In this context, the activated time-out function offers significant support for effective data protection.

The quick log-out can be done by double clicking the X button within 2 seconds. (Quick-Out function)

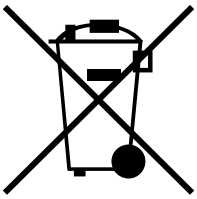
For safe physical separation, the USB cable must be completely removed from the Kobra VS device.

Important:
To avoid data loss, make sure the data transfer and access to the Kobra VS device are completely finished, before disconnecting.

13. Note on the protection and preservation of the environment

According to the EC directive, waste electrical and electronic equipment may not be disposed of as municipal waste. In order to avoid the spreading of the contained building substances in your environment and to save natural resources, we ask you to return this product at the end of its service life exclusively to a local waste collection point in your vicinity.

Thanks to these measures, the materials of your product can be reused in an environmentally friendly way.



Since a possible zero-day attack could significantly reduce the security of large user numbers, it is essential that this is kept secret until a firmware update can be provided to a user majority and they have installed it onto their devices. In this context, any

Ihre Notizen / Your Notes

Ihre Notizen / Your Notes

DIGITTRADE GmbH
Ernst-Thälmann-Str. 39
06179 Teutschenthal

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