Version 1.05
04.04.2019

KOBRA STICK

encrypted USB-C secure flash drive

für Unternehmen und Behörden
for business and governmental use

Benutzerhandbuch
User Manual

PLEASE READ THIS MANUAL AND FOLLOW THE INSTRUCTIONS CAREFULLY.

INCORRECT OPERATION CAN CAUSE DAMAGE TO THE KOBRA STICK AND LOSS OF DATA.

The digital version of the manual can be downloaded from www.digittrade.de in the Download Center.

Product version:	Kobra Stick (Encrypted USB-C Stick) Version 1.0
Benutzerhandbuch Version:	1.05 (04.04.2019)

Contents

1. About the KOBRA Stick

The KOBRA Stick is an encrypted USB-C stick in a sturdy, metal casing. It enables the storage, safekeeping and secure transport of sensitive business and private data for public authorities and companies in accordance with data protection regulations. It was developed in accordance with the "Technical Guidelines" of the BSI, has the quality marque "IT Security made in Germany" and, due to its security functions, is a good option for securely storing data on the move.

The confidentiality of the data stored on the KOBRA Stick is protected against unauthorised access, for example if the data carrier is lost or stolen, or in the event of virtual or physical attacks.

In order to take full advantage of the security features of the KOBRA Stick, please follow the following steps:

- Ensure that there is adequate protection on your host system for all data accessed from the protected storage area of the KOBRA Stick
- Make sure that no malware can be transferred to the KOBRA Stick
- After receiving the KOBRA Stick, check that the delivery is complete and correct.
- After the first login, check the functions of the KOBRA Stick (chapter 5).
- Change the user PIN (Chapter 5.2)
- Change the admin PIN if you are the administrator responsible for managing the KOBRA Stick (chapter 5.3).
- Create new encryption keys (also called crypto keys or KS) on the KOBRA Stick (chapter 5.5).
- Keep your authentication data (user PIN and admin PIN) confidential

A detailed description of the above steps can be found in the referenced chapters of this user manual.

The serial number and the corresponding QR code can be found on the back of the KOBRA Stick. This information as well as the Vendor ID (VID) and Product ID (PID) can be read via the USB-C interface:

The KOBRA Stick guarantees the confidentiality of data through the following security mechanisms:

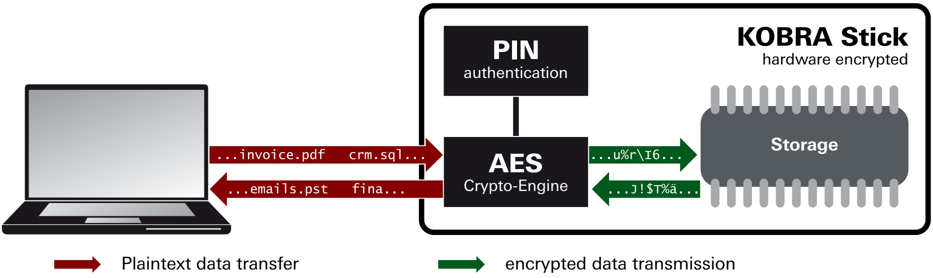
- Encryption
- Access control
- Cryptographic key management

1.1 Encryption

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

The encryption module integrated in the safety housing carries out a complete encryption of the KOBRA Stick. Every byte saved and each written sector on the storage device is encrypted in XTS mode, using two cryptographic keys according to the 256-Bit AES (Advanced Encryption Standard).

The KOBRA Stick also encrypts temporary data and areas that are often ignored by encryption software.



1.2 Access control

- Access is granted by entering a user PIN.

The KOBRA Stick automatically creates a new encryption key and resets the user PIN to the default setting as soon as the permitted number of incorrect PIN entries has been exceeded. Access to the data stored on the stick is then no longer possible.

1.3 Management of the cryptographic keys

The user can generate, change or destroy the cryptographic keys at any time. This process is irreversible. After the generation of new cryptographic keys, the old cryptographic keys and thus all data stored on the data carrier are irreversibly destroyed. Therefore, any information stored on the stick should first be saved on another encrypted data carrier, where necessary.

The two 256-bit encryption keys for the encryption and decryption of the data are generated by a hardware random number generator and stored within the stick. When the user PIN is entered correctly they are transmitted to the encryption module of the KOBRA Stick for the encryption and decryption of the data.

1.4 Overview of the most important features

- AES Full-disk hardware encryption in XTS mode with two 256-bit cryptographic keys
- Authentication via user PIN
- Hardware-based encryption module
- Data encryption of all saved bytes and written sectors
- Independent of operating system (supports all operating systems, multi-media devices, smartphones, and machines that support USB data carriers)
- Integrated write protection
- Adjustable number of incorrect attempts
- Compatible with USB 3.0 and USB 2.0
- No read and write speed restrictions
- Sturdy metal casing
- Time-out & quick-out functions
- Pre-boot authentication and bootability
- Internal power supply that allows authentication without connecting to a PC or USB hub.

Optional:

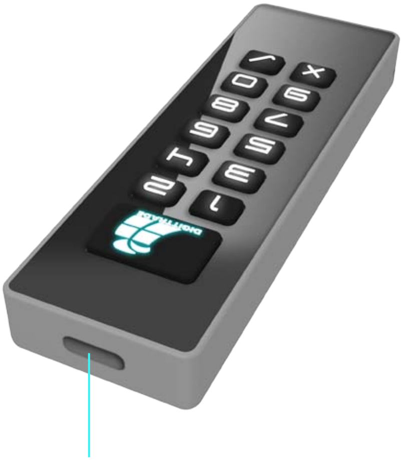
- USB VID, PID & serial numbers can be defined according to customer specifications
- Laser-engraved customer specific information on the back of the KOBRA Stick

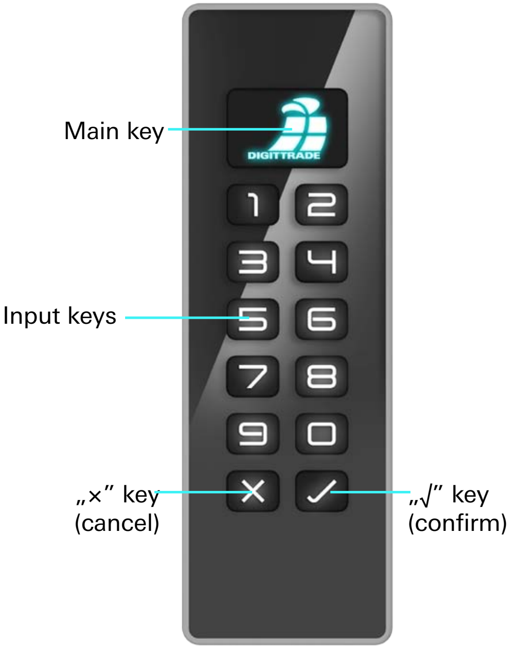
1.5 Advantages of the KOBRA Stick

- Private and business data is securely protected from unauthorised access
- Easy and secure handling due to hardware encryption: connect, login, use
- All data is immediately stored as encrypted
- No performance losses

2. USB port and input interface

The KOBRA Stick can be connected to a PC via a USB port.





On the front of the KOBRA Stick there is an input keyboard with a main key, two command keys ("×" cancel and "√" confirm) and ten input keys (0 to 9). Connection with a PC is via a USB-C 3.0 port.

3. Using the KOBRA Stick

To use the KOBRA Stick correctly, only two steps are necessary:

1) Connect the KOBRA Stick to the PC
2) Enter the PIN on the KOBRA Stick

It is also possible to carry out these steps in another order.

The power supply needed for the KOBRA Stick is generally provided via the USB port. In addition, this USB stick has an integrated autonomous power supply, which enables activation before connection to a PC as well as pre-boot authentication with subsequent PC start from the KOBRA Stick.

As long as the KOBRA Stick is not connected to a PC or with an external power supply (e.g. USB power supply or USB hub) it stays in sleep mode and all keys are deactivated.

The KOBRA Stick goes into authentication mode both after pressing the main key for approx. 3 seconds and immediately after being connected to a PC. The main key flashes green and the other keys are activated. Now the user PIN can be entered to unlock the KOBRA Stick.

All entries and commands are confirmed with the “√” key or cancelled with the “×” key. Every time the “×” key is pressed, the user returns to wait mode and can begin from there once again. The main key can also be used to confirm an input instead of the “√” key.

By pressing the main key in wait mode, the stick switches to menu mode. In this mode the main key lights up blue and all other entry keys are white. The lit-up input keys indicate that they are active and the relevant commands can be entered.

After pressing the “1“ key followed by the “√“ key, the user switches back to the authentication mode and can unlock the stick again by entering the user PIN. Following successful authentication the main key lights up green. The other keys are activated and access to the data is enabled.

If an incorrect PIN is entered, the main key flashes red according to the number of times an incorrect PIN has been entered (but not more than the maximum number of failed attempts permitted). Then the KOBRA Stick automatically switches back to wait mode. The authentication process can be repeated from this point as described above. PIN entry attempts of less than 4 digits are not considered failed attempts and are therefore not counted.

After the permissible number of failed attempts has been exceeded, the main key flashes red and yellow three times alternately. The KOBRA Stick then switches into authentication mode. At the same time the KOBRA Stick automatically deletes the old crypto keys, generates two new crypto keys and sets the user PIN back to the default setting.

Following successful authentication with a new user PIN the KOBRA Stick formats the data storage. The main key flashes blue continuously during formatting. Then the main key lights up green or purple depending on the write protection setting previously selected. The other keys are deactivated and access to the KOBRA Stick is enabled. The stick partition shows up on the desktop and can then be used.

All data previously stored is erased during this process!

If no further entries are made within 20 seconds of starting a command process, the KOBRA Stick connected to a PC automatically switches to wait mode. In battery mode, the stick returns to sleep mode after 20 seconds.

This function does not apply to the authenticated KOBRA Stick if it is already connected to a PC or is connected at the latest within 20 seconds after successful authentication. The time for a possible automatic locking of the authenticated KOBRA Stick connected to a PC is controlled by the time-out settings, if any have been set (Chapter 5.7).

In addition to the classic “logoff” mechanisms such as “safe removal” via the PC taskbar and the physical disconnection of the USB, the KOBRA Stick also has a quick-out function for quick logoff. This function is performed by double clicking the “×” button within 2 seconds.

Note:
To ensure the security of your data, it is essential to change the default user PIN. You should also change the user PIN at regular intervals in future. The user PIN must be kept secret.

4. Roles and authorisations

The KOBRA Stick allows roles and authorisations to be managed with regard to the administration and operation of the data carrier.

The user knows the user PIN. This PIN enables the user to change the PIN, to log in to the stick (authentication), to activate or deactivate the write protection function or to destroy the current encryption keys and generate new ones. The user PIN enables authentication on the KOBRA Stick and allows access to the stored data.

The administrator knows the Admin-PIN. He/she can change the Admin-PIN, define the time-out settings and set the number of permitted failed attempts. The administrator is not authorised or able to access the data stored on the KOBRA Stick.

5. Menü-Modus: Authentisierung und Verwaltung

The authentication and management of the KOBRA Stick is done via the menu mode by entering numbers and commands. Switching to menu mode is generally carried out from wait mode by pressing the main key. In menu mode, the main key lights up blue and all other input keys white.

To execute the commands, the KOBRA Stick usually requires a connection to a PC or another external power supply (e.g. USB power supply or USB hub). Exceptions to this are during authentication on the KOBRA Stick, the activation or deactivation of the write protection as well as the generation of new crypto keys. These functions can also be performed in battery mode.

In menu mode all inputs and commands should be confirmed with the "√" key. Alternatively, they can also be cancelled with the "×" key. Each time the "×" key is pressed, the main key briefly lights up orange and then white. Then the KOBRA Stick switches to wait mode. The procedure can be repeated from this position.

After starting a menu function, the main key starts flashing green when the user PIN has to be entered. If the admin PIN is required, the main key flashes purple. All other keys are active at this moment. If entry is confirmed with the "√" key, the main key lights up green if the PIN is correct.

If an error occurs, the main key flashes red briefly and then lights up white. Then the KOBRA Stick switches to wait mode. The procedure can be repeated from this position.

If the PIN entry was incorrect during one of the operations, the main key flashes red once or several times according to the number of unsuccessful attempts (but not more than the set number of permitted failed attempts). Then the KOBRA Stick switches to wait mode. The scheduled process can be restarted from this point.

After each successful execution of a command, the KOBRA Stick returns to wait mode.

The only exception is successful authentication.

Note:
For all functions and settings that require the user PIN to be entered, the main key flashes green continuously and all other keys remain active. To enter the admin PIN, however, the main key flashes purple continuously.

5.1 User authentication

User authentication is required to enable access to the data carrier.

For authentication:

1) Make sure that you are in menu mode. (The main button lights up blue and the other buttons white.
2) Press the keys “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 key lights up green, the other keys are deactivated and access to the data is enabled.

5.2 Changing the user PIN

On the KOBRA Stick the user PIN is needed to carry out authentication (login), to activate write protection and to deactivate, destroy or generate encryption keys.

In the KOBRA Stick factory settings the user PIN is “1- 2-3-4-5-6-7-8”. The stick will also have this PIN when the permitted number of failed attempts to login has been exceeded and the user PIN has been reset to the factory settings. The user PIN can be created using a combination of 4 - 16 digits.

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press “3” followed by “√”. The main key flashes green continuously and the other keys stay activated.
3) Enter the old user PIN and confirm with “√“
4) Enter a new user PIN and confirm with “√“
5) Enter the new user PIN again and confirm with “√“

If changing the PIN has been completed successfully the main key blinks green briefly and the data carrier switches back to wait mode.

5.3 Changing the administrator PIN

The administrator PIN (also called device PIN) is needed to set the time-out function and the number of failed log-on attempts that are permitted. This PIN can be 4 - 16 characters long, is purely for administration and does not allow access to the data stored on the device.

In the KOBRA Stick factory settings, the administrator PIN is “8-7-6-5-4- 3-2-1”. When entering the admin PIN, 16 failed attempts are allowed. If this number is exceeded, the admin PIN is irreversibly blocked and the above functions can no longer be changed. The user functions can still be operated independently of this.

To change the administrator PIN:

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press “9” followed by “√”. The main key flashes purple continuously and the other keys stay activated.
3) Enter the old admin PIN and confirm with “√“
4) Enter a new admin PIN and confirm with “√“
5) Enter the new admin PIN again and confirm with “√“

If the PIN has been changed successfully, the main key blinks green briefly and the data carrier switches back to wait mode.

5.4 Write protection function

Activated write protection offers you additional protection against viruses and trojans while you are using the stick on an unknown PC. It also prevents sensitive information from a PC or server being accidentally stored on the stick.

Even before authentication, the user can check whether write protection is activated by pressing the “2” key. If the main key lights up purple, write protection is activated. If the main key lights up green, write protection is deactivated.

To activate or deactivate write protection:

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press the “2” key. If the write protection is activated, the main key lights up violet, if the write protection is deactivated, it lights up green.
3) Then press the “√” key. The main key flashes green and all other keys remain active.
4) Then enter the user PIN and confirm with “√”. After a successful switch, the main key flashes green or violet twice and the data carrier switches back to wait mode.

5.5 Generating new crypto keys

When new crypto keys are generated, the old crypto keys are destroyed and thus all of the data stored on the data carrier is irreversibly erased. Therefore, all saved data should be previously stored on another approved data carrier, where necessary.

To generate or change the encryption keys:

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press the “7” key. The main key lights up red, this indicates that after carrying out this function all data stored on the stick will be irreversibly erased.
3) Press the “√” key, if you really wish to carry out this function. The main key flashes green and all other keys remain active.
4) Enter the user PIN and confirm with “√“.

After the crypto key has been successfully generated or changed, the main key flashes green briefly and the KOBRA Stick switches back to wait mode.

During the next authentication, the main key flashes blue until the formatting has been completed. Depending on memory size, this process can take several minutes. The main key then 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 stick is no longer possible.

5.6 Deleting the crypto keys

Deleting and/or destroying the crypto keys can be carried out in two ways.

a) Destruction by generating new cryptographic keys.

During this process the old encryption keys are irreversibly overwritten. Access to previously stored data is no longer possible.

This method is a quick way to destroy the data stored on the stick without having to connect it to a PC.

b) Destruction of the cryptographic keys by exceeding the permitted number of unsuccessful attempts to enter the user PIN.

During this process, in addition to resetting the user PIN back to the factory settings, the old cryptographic keys are irreversibly destroyed and new ones generated. Access to all previously stored data is also no longer possible in this case.

5.7 Time-out and quick-out functions

The administrator can define after how many minutes the activated KOBRA Stick is automatically locked if neither reading nor writing access to the stick takes place within the specified time. The lock time can be selected between 1 and 30 minutes. To remove the lock, press “0”.

To set the time-out function:

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press the “8” key, then press “√”. The main key flashes purple and all other keys remain active.
3) Enter the admin PIN and confirm with “√”
4) Enter a number from 0 to 30 and confirm with “√”.

If the process was successful, the main key flashes green briefly and the KOBRA Stick switches back to the wait mode.

The quick-out function allows you to log off quickly. It is executed by double-clicking the "×" key within 2 seconds

5.8 Permitted number of failed attempts for entering the user PIN

The original factory settings allow the user to make 8 failed attempts to enter the user PIN. The administrator can change this number to 1 to 16 failed attempts. After exceeding the specified number, the KOBRA Stick automatically deletes the old crypto keys, generates new crypto keys and resets the user PIN to the factory settings.

All available data is permanently destroyed.

1) Make sure that you are in menu mode. (The main key lights up blue and the other keys white.)
2) Press the "8" key, then press "√". The main key flashes purple and all other keys remain active.
3) Enter the admin PIN and confirm with "√".
4) Enter a number between 1 and 16 and confirm with "√".

If the process was successful, the main key flashes green briefly and the KOBRA Stick switches back to wait mode.

Note:
The reduction of permitted failed attempts is valid immediately. An increase of permitted attempts only becomes effective after the user PIN has been successfully entered, even if this entry is made for the first time after the stick has been reset to the factory settings.

6. Formatting

The KOBRA Stick comes with a FAT32 file system as standard. 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 content.

The user can reformat the KOBRA Stick according to the application scenario. For Windows users, it is recommended to use NTFS, for example. HFS+ is the most powerful file system for Mac OS X and EXT4 can be used for Linux.

Extension programs can also be used to write data to file systems where this would not otherwise be possible. Of course, it is also possible to format the KOBRA Stick with any other file system. This does not affect the encryption of the data and the settings already made.

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

	NTFS	FAT32	HFS+	EXT4
Windows 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

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

7. Applications

The KOBRA Stick features offer a wide range of possibilities for the safe storage, archiving and transmission of personal and sensitive data. In the following you can also find some specific scenarios.

7.1 Increasing the level of protection for KOBRA Stick in a company

The administrator in a company or public authority can determine how restrictive a user's KOBRA Stick should be. The administrator can define the number of permitted failed attempts and the time-out period for the user.

The administrator can use the time-out setting to determine after how many minutes the activated KOBRA Stick is automatically blocked if neither reading nor writing access to the stick takes place.

The user is not permitted to change these settings. This is not even possible after the number of permitted failed attempts has been exceeded and the user PIN has been reset to the factory settings.

7.2 Secure and more cost-effective data transport

The KOBRA Stick can be used to transport sensitive data. For this purpose, new encryption keys are first generated and the user PIN is changed. The number of permitted unsuccessful attempts can be reduced to the minimum value, e.g. 1 to 3 attempts. Write protection can also be activated after the data to be transported has been saved. The sender then only needs to send the KOBRA Stick by post or courier.

The sender and the recipient must also ensure that they can detect any attempted manipulation of the KOBRA Stick that might have taken place during data transport. The use of sealed security bags is recommended for this purpose. This also applies to all other data transport options using the KOBRA Stick.

When the data carrier has been received, its authenticity must be checked. For this purpose, the serial number of the data carrier is also transmitted to the recipient using a separate secure method. The serial number is located both on the housing and in the stick’s device information, which can be read via the USB connection. The user PIN is not transmitted to the recipient until this information matches.

This method enables the KOBRA Stick to deliver sensitive data to the recipient safely and cost-effectively using an insured parcel or courier service.

7.3 Use of fewer data carriers with a large customer base

For data processing companies, data centres of large companies or public authorities, which are, for example, constantly exchanging data with many data recipients, the KOBRA Stick is perfect for transporting data securely and cost-effectively as only a few storage media are then required.

This is because, for each data transport to a different recipient, the crypto keys of the

KOBRA Stick are generated anew and the user PIN is redefined. The number of permitted failed attempts can also be reduced for these purposes to the minimum values of, e.g. 1 to 3. The data can then be stored on the KOBRA Stick and sent by post or courier (see chapter 7.2).

Complex data deletions and repeated overwriting of the data carrier are no longer necessary, as the original data is encrypted with the previous crypto keys and all old crypto keys are deleted after new ones have been created. The memory is automatically formatted when new crypto keys are created.

The KOBRA Stick therefore reduces the number of data carriers needed, as a personalised KOBRA Stick is not required for each data recipient.

Note:
It is recommended to delete the data on the data carrier by creating new crypto keys, as this puts less of a strain on the lifespan of the memory than completely overwriting the entire memory several times.

7.4 Use of fewer data carriers in the field and with public authorities

For activities outside the company, an employee receives a KOBRA Stick that was previously used by another employee, for example, and which was then formatted by exceeding the permitted number of unsuccessful attempts to enter a PIN.

During this process the user PIN is reset to the factory settings, the two old crypto keys are deleted, new encryption keys are generated, and the data carrier is formatted. All these processes run in the background after the employee or administrator has exceeded the number of permitted failed attempts.

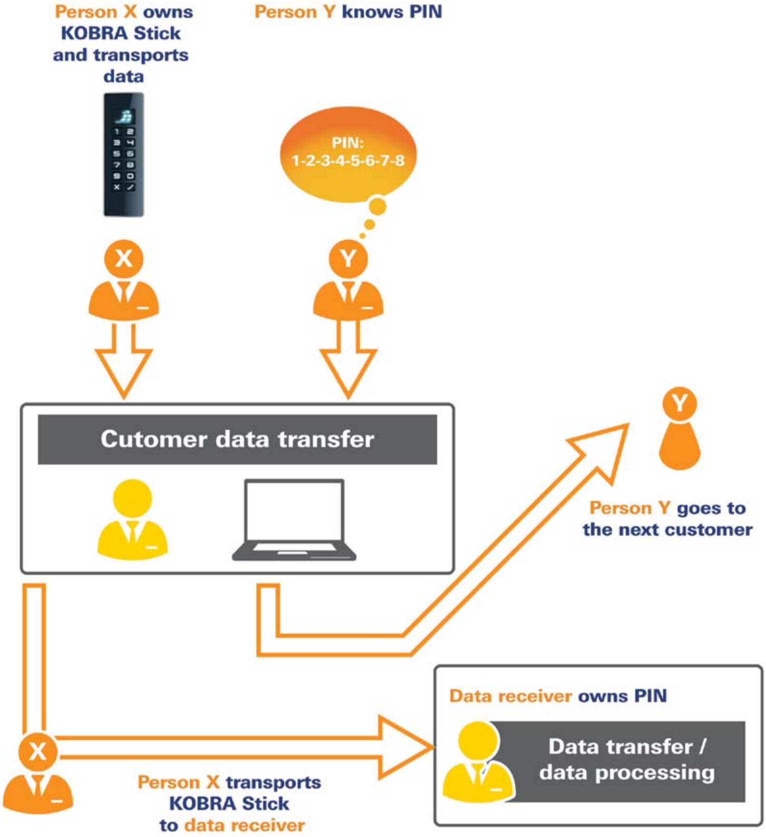
The new employee then changes the user PIN and can use the KOBRA Stick to store his or her data securely. If presentations have to be made on external PCs or if the saved files are to remain unchanged for other reasons, write protection can also be activated.

The employee then returns the KOBRA Stick after use. Before returning it, he or she destroys the current encryption keys and the data stored on the KOBRA Stick by creating new encryption keys. (Chapter 5.5)

Within a few minutes, the KOBRA Stick is then ready for use by the next colleague, as described above. This means a separate KOBRA Stick is not required for each employee and the number of data carriers needed in the company can be reduced.

7.5 Separation of data carrier from authentication

Access to the data can be regulated in such a way that it is only possible by bringing two particular people together, for example. Person X (e.g. courier) has the crypto key, person Y knows the user PIN. The two people only come together to transfer data at the receiving point and then separate again. Persons X and Y do not have individual access to the data.


Person X owns KOBRA Stick and transports data
Person Y knows PIN
PIN: 1-2-3-4-5-6-7-8
X
Y
Cutomer data transfer
Y
Person Y goes to the next customer
Data receiver owns PIN
Data transfer / data processing
X
Person X transports KOBRA Stick to data receiver

7.6 Use as an encrypted boot device

The integrated autonomous power supply enables authentication of the KOBRA Stick to take place before a PC is started (pre-boot authentication). This feature allows operating systems to be stored in encrypted form on the KOBRA Stick and then started directly from the stick.

Operating systems such as Windows To Go, Linux, ECOS Secure Linux and others, as well as the required data, can be stored on the stick. This application is suitable for both stationary and mobile computers. The minimum storage capacities required must be observed. The Windows To Go operating system can only be used with the KOBRA Stick with a memory capacity of 32 GB or more and requires special configuration of the stick, which must be carried out before delivery.

7.7 Use on different operating systems and smartphones

The KOBRA Stick works through its hardware encryption independently of the operating system and can be used on almost any device that supports USB media.

The optimized power consumption also allows the KOBRA Stick to be used for data exchange with a smartphone or tablet.

7.8 Integration von bestehenden Softwarelösungen

All existing software solutions in the organization can continue to be used to enhance the security features and methods of use. The integrated battery allows authentication to take place in advance of connecting the stick to a PC or other external power supply (e.g. USB power supply or USB hub). This feature of the data carrier is called pre-boot authentication (Chapter 3).

The KOBRA Stick can also be used as a boot medium with an installed operating system. When the stick is connected to any PC, the operating system installed on the stick starts. When the KOBRA Stick is disconnected from a PC, the data, programs and temporary files remain encrypted on the KOBRA Stick and are inaccessible to unauthorized persons.

7.9 Using the VID and PID to protect company data

As an option, the implementation of the Vendor ID (VID) and Product ID (PID) can be customized. This information allows the KOBRA Stick to be assigned to different departments and user groups. They may also have different authorizations for USB connections in the company’s internal network.

This makes it possible to determine which KOBRA Stick can be connected to which USB interfaces in the company. The connection of other “unauthorized” USB data carriers can thus be prevented.
Additional software may be required to control the USB ports on the host systems

7.10 Use as a data diode

The activated write protection of the KOBRA Stick data carriers provides secure protection from the unwanted flow of information from higher-rated systems to lower-rated systems.

To achieve this, the data from the source system is written onto the data carrier and then the write protection is activated on the stick. Then the data carrier is connected to the higher-rated system and the required data is transferred from the KOBRA Stick to the host system. Afterwards, the data carrier can be used normally in the source system again.

Any further security measures such as a virus-scan are still required. Optionally, the data carrier can be deleted fast and securely before and afterwards by regenerating the encryption keys.

8. Technical specifications

Transfer rate:	USB 3.0 max. 5 GBit/s USB 2.0 max 480 MBit/s The actual write and read rate that can be achieved depends on the selected memory size, memory type, USB port and host system.
Encryption:	256-Bit AES hardware encryption, XTS mode, with 2 x 256-bit crypto keys
Storage:	4 GB, 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Storage type	3D TLC, MLC and pSLC

9. Data security and disclaimer

We recommend that you also regularly back up the data on the KOBRA Stick on other storage media. This will protect you from complete data loss. DIGITTRADE GmbH is not liable for the loss of data or costs and damages resulting therefrom. In addition, the aforementioned company is not responsible for the stored data with respect to data protection law.

10. Safe termination after use of the KOBRA Stick

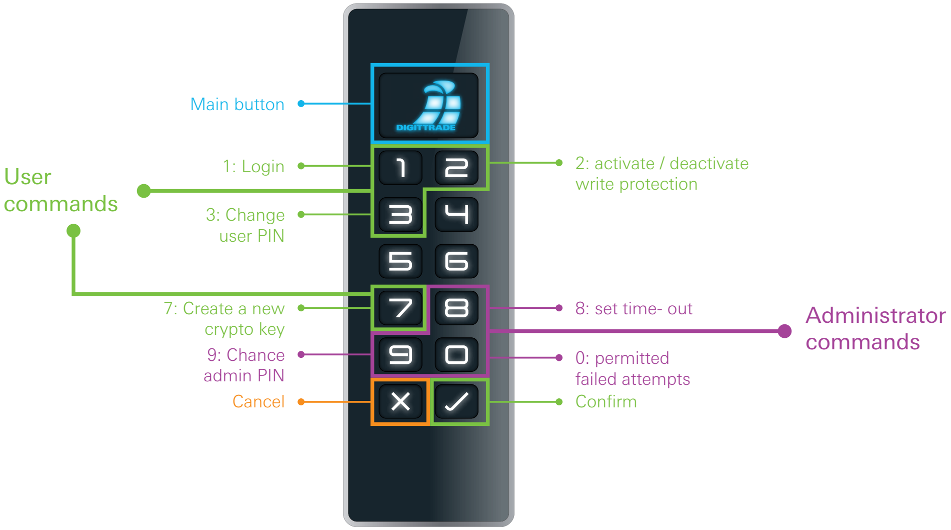
For security reasons, the stick must be separated virtually or physically from the host system after use. This is recommended especially in the case of termination, short-term interruptions or when leaving the workplace. When activated the time-out function can help to provide effective data protection.

You can also log out quickly by double-clicking the X button within 2 seconds (quick-out function).

To ensure secure physical separation, the USB cable must be completely removed from the KOBRA Stick.

Note:
To prevent data loss, make sure that data transmission and access to the KOBRA Stick are complete before disconnecting.

11. Menu overview, commands and factory settings



User	Key 1 - Login Key 2 - write protection Key 3 - change user PIN Key 7 - create new crypto keys

Administrator	Key 8 - set time-out Key 9 - change admin PIN TKey 0 - permitted failed login attempts
User PIN	1-2-3-4-5-6-7-8
Admin PIN	8-7-6-5-4-3-2-1
PIN length	8 characters (adjustable: 4 - 16)
Failed login attempts User PIN	8 times (adjustable: 1 - 16)
Failed login attempts Admin PIN	16 times (not adjustable)
Time- out	0 minutes (adjustable: 0 - 30)

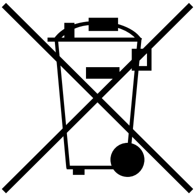
12. Product contents

- KOBRA Stick (externally encrypted USB-C stick) Version 1.0
- 3 USB cables (USB-C to USB-C, USB-C to USB-A, USB-C to USB Micro-B)
- Packaging

13. Hinweis zum Schutz und Erhalt der Umwelt

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

As a result of these measures, the materials in your product can be reused in an environmentally friendly way.



Ihre Notizen / Your Notes

DIGITTRADE GmbH
Ernst-Thälmann-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**