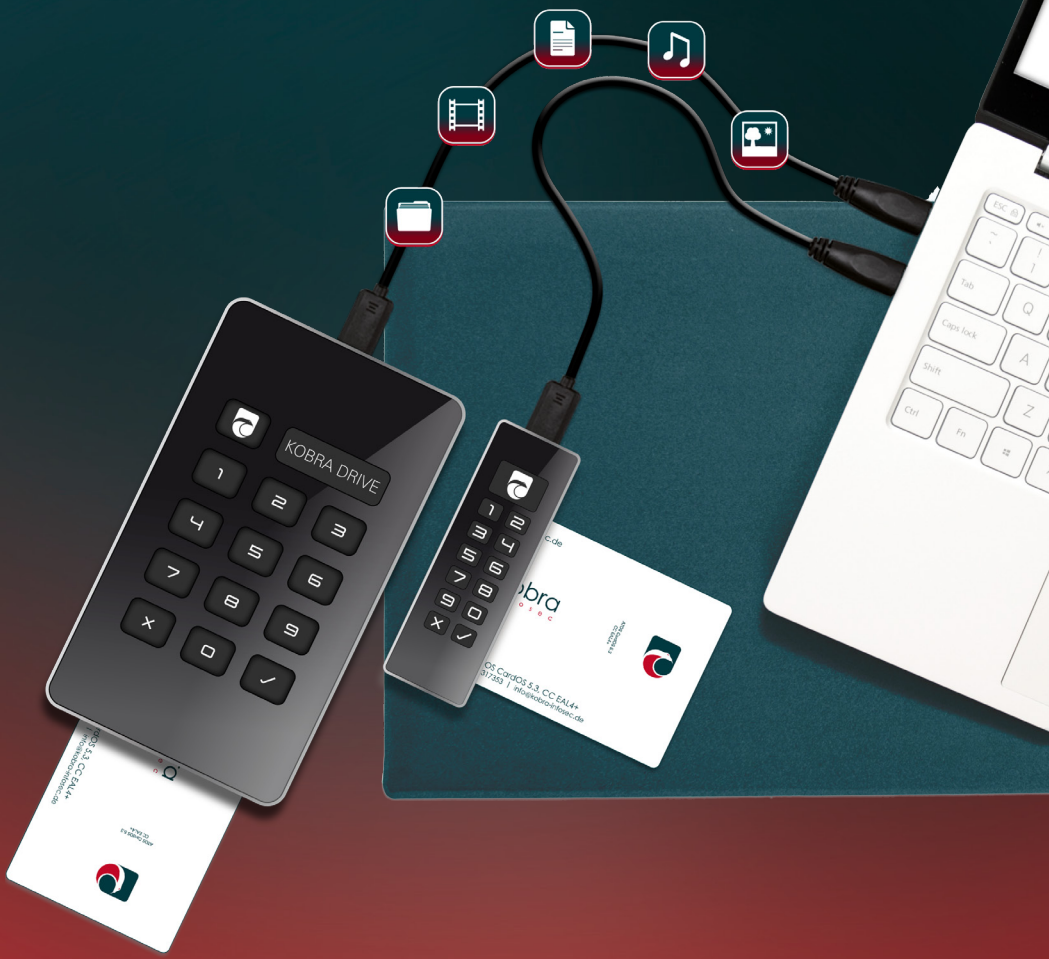
Kobra Infosec

User's Guide

Kobra VS storage devices

Encrypted USB-C secure flash drive and hard disk



Version 1.3
07.08.2026

for business and governmental use

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 Kobra Infosec GmbH Download Center:
https://kobra-infosec.de/de/all-support-sites/support.html

Product version:	Kobra Drive VS, Kobra Stick VS (1FF) und Kobra Stick VS (2FF) - (Kobra VS Storage Device) Version 1.0
User's Guide:	Version 1.3 (as of 07.08.2026)

Table of contents

1. About the Kobra VS Storage Devices: Kobra Drive VS and Kobra Stick VS

The Kobra Drive VS, Kobra Stick VS (1FF), and Kobra Stick VS (2FF) external encrypted storage devices are an external USB-C hard drive (HDD/SSD) and USB-C flash drive with hardware-based encryption, housed in sturdy, elegant metal enclosures with an integrated keyboard. The devices offer the same level of security and differ only in their design and available storage capacities. For this reason, they are referred to as Kobra VS storage devices in this Administrator's Manual.

Kobra VS data storage devices enable the data protection-compliant storage and retention, as well as the secure transport, of sensitive, personal, and confidential information up to the classification levels NATO Restricted, EU Restricted, and VS-NfD (Classified Information—For Official Use Only). These storage devices were developed and manufactured in Germany in accordance with the BSI's "Technical Guidelines." They bear the "IT-Security made in Germany" seal of approval and represent the current state of the art. Thanks to their security features, Kobra VS data storage devices are currently one of the most secure options for mobile data storage.

The data stored on the Kobra VS storage device is protected against unauthorized access to ensure the confidentiality of the information, for example, if the Kobra VS storage device is lost, misplaced, or stolen. It is designed to withstand both logical and physical attacks.

The Kobra Drive VS is available in both HDD and SSD versions. The option to use SSD storage devices with the Kobra Drive VS provides additional protection against shocks and vibrations. Data transfer and power are provided via the USB-C port. The Kobra Stick VS (1FF) and the Kobra Stick VS (2FF) offer the same security features as the Kobra Drive VS in an even more compact format.

Kobra VS storage devices can be deployed in either a PKI-based or a stand-alone environment. There are two fundamentally different application scenarios:

In the PKI-based version, only Kobra VS storage devices are provided. These are set up by the user's administrators. Therefore, the PKI-related properties of the Kobra VS storage device are also governed by the administrator's IT security policies.

This primarily involves the generation and storage of the key pair (consisting of a public and a private key), the User PIN and SO PIN (PUK), SO PIN settings (length and number of failed attempts), as well as other organizational measures. Therefore, the characteristics of the Kobra VS storage device, primarily with regard to the stand-alone environment, are described in detail below.
s
The stand-alone scenario (also known as the independent scenario), on the other hand, involves the delivery of the Kobra VS storage device together with two Kobra Infosec Smartcards (Atos CardOS 5.3, CC EAL 4+) in a fully preconfigured state. This Kobra VS storage device can generally be used immediately in case of urgent

need. However, in the VS-NfD-approved configuration, the user may not put the Kobra VS storage device into operation until they have first changed the user and SO PIN (PUK) and generated a new cryptographic key on the Kobra VS storage device itself.

To take full advantage of the security features of the Kobra VS storage device within the scope of the VS-NfD certification, the following steps are required:

- Ensure that your host system has adequate protection for all data accessed from the protected storage area of the Kobra VS storage device
- Upon receipt of the Kobra VS storage device, verify that the shipment is complete and correct (Chapter 15. Package Contents)
- Use the host system to verify that the USB properties of the storage device match the model number and serial number on the back of the Kobra VS storage device (Chapter 4. Authentication)
- Change the User PIN and SO PIN (PUK) on both Kobra Infosec Smartcards (Chapter 9.3 Changing the User PIN, Chapter 4.3.3 Changing the SO PIN/PUK in the Kobra Client VS Manual)
- Change the Admin PIN if you have administrator privileges (Chapter 9.6: Changing or Disabling the Admin PIN)
- When selecting the Admin, User, and SO PIN (PUK), avoid trivial PINs and exclude the default PINs.
- Generate a new cryptographic key on the Kobra VS storage medium (Chapter 9.7 Generating a New Cryptographic Key)
- Verify that you can log in with all activated Kobra Infosec Smartcards (or your PKI card)
- Keep your authentication credentials (Smartcard and PIN) confidential

A detailed description of the steps mentioned above can be found in the relevant chapters of this user‘s guide and the administrator´s guide. The model number and serial number are located on the back of the respective Kobra VS storage device. This information can be retrieved using the included Kobra Client VS software and via the USB device information on the host system.

2. Security mechanisms

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

- Encryption
- Access Control
- Key Management
- User Management

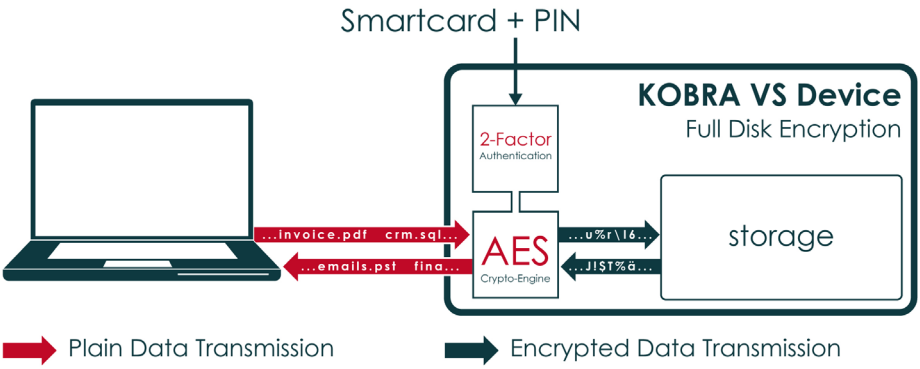
2.1 Encryption

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

The encryption module integrated into the security enclosure performs full encryption of the Kobra VS storage device. Every byte stored and every sector written to the Kobra VS storage device is encrypted using 256-bit AES (Advanced Encryption Standard) in XTS mode with two 256-bit cryptographic keys.

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

Hardware encryption allows the Kobra VS storage device to be used independently of the user's operating system and operates transparently. Data can be accessed without any restrictions on read or write speeds.



2.2 Access Control

Access control is based on the "possession and knowledge" principle: To access the data, the user must possess a valid Smartcard and know the correct User PIN.

The Kobra Infosec Smartcard is automatically locked as soon as the allowed number of incorrect PIN entries is exceeded. Locked Kobra Infosec Smartcards can be unlocked by entering the SO PIN (PUK). The Kobra Infosec Smartcard is permanently locked as soon as the allowed number of incorrect SO PIN (PUK) entries is also exceeded. Afterward, access to the data is only possible with another Smartcard that has been unlocked for this Kobra VS storage device and by entering the correct PIN

For PKI cards, these properties are governed by the IT security policies and internal guidelines established by the administrators.

2.3 Key Management

The two 256-bit encryption keys used to encrypt and decrypt the data are directly linked to the crypto key. Therefore, key management focuses on the generation, storage, modification, and destruction of the cryptographic key. It is generated on the Kobra VS storage device using a random number generated on the Kobra Infosec Smartcard and stored in an encrypted form in a secure area so that it can only be decrypted by authorized Smartcards.

To encrypt and decrypt data, the encrypted cryptographic key is decrypted using the Smartcard after the User PIN is entered correctly and made available to the encryption module of the Kobra VS storage device. Using the Kobra Infosec Smartcard (or PKI card) and the User PIN, the user can generate, change, and destroy the cryptographic key on the Kobra VS data storage device at any time (Chapter 9.7 Generating a New Cryptographic Key, Chapter 9.8 Deleting a Cryptographic Key).

These operations are irreversible. After a new cryptographic key is generated, the old cryptographic key—and thus all data stored on the Kobra VS storage device—is permanently destroyed. Therefore, under certain circumstances, the stored information must first be backed up to another VS-NfD- and/or **NATO-Restricted/ EU-Restricted**-approved storage device.

2.4 User Management

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

3. Properties and special features

Kobra VS storage device offer numerous unique features.

3.1. Features - Summary

Encryption

- 256-bit AES full-disk hardware encryption in XTS mode with two cryptographic keys
- 2-factor authentication by Kobra Infosec 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 reading and writing 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

3.2 Advantages of Kobra VS Data Storage Devices

Easy and safe handling
Connecting, log-in, using

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 compliant with classified information instruction.

Transparent use
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 the art in accordance with the requirements of EU-DSGVO/GDPR and BDSG (German federal law of data protection).

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

3.3 Smartcard

The Kobra VS storage device comes standard with two Kobra Infosec Smartcards certified to Common Criteria EAL4+ (Atos CardOS 5.3, CC EAL 4+). In a stand-alone environment, only these Kobra Infosec Smartcards are currently approved for use in accordance with the VS-NfD certification. In addition, the user's own PKI cards may be used. This allows the Kobra VS storage devices to be integrated into the user's PKI infrastructure. In special cases, it can be determined whether other customer-specific Smartcards or PKI cards can also be integrated. If the PKI cards are not based on Atos CardOS 5.0, CardOS 5.3, or a higher version, consultation with the BSI is required to determine whether these Smartcards provide sufficient security for VS-NfD.

The Kobra Infosec Smartcards are supplied in EC card format for the Kobra VS storage devices Kobra Drive VS and Kobra Stick VS (1FF). The Kobra Stick VS (2FF) is equipped with Kobra Infosec Smartcards in mini-SIM card format. They are referred to as "Kobra Infosec Smartcards" in the following chapters. The Kobra Infosec Smartcard enables access to the data on the Kobra VS storage device, as well as the creation, modification, and destruction of the cryptographic key, and the encryption and decryption of the Kobra VS storage device. The cryptographic key is managed on the Kobra VS data storage device using the Kobra Infosec Smartcard (or PKI card) and the User PIN, completely independently of a PC.

To log in to the Kobra VS storage device, Kobra Infosec Smartcards are shipped with a User PIN and SO PIN (PUK) set to default values (Chapter 3.7 Menu Overview, Commands, and Factory Settings). All Kobra Infosec Smartcards have unique serial numbers and stored key pairs consisting of a public

and a private key. The model name and serial number of each Smartcard are printed on the front of the Kobra Infosec Smartcard.

Using the Kobra Client VS software, the administrator can authorize up to 8 Kobra Infosec Smartcards or PKI cards for a Kobra VS storage device and define different permissions for each user. This is done by entering the Kobra Infosec Smartcards (or PKI cards) into the Smartcard table of the Kobra VS storage device. (9.14 Smartcard Table)

3.4 User PIN and SO PIN (PUK)

The User PIN and SO PIN (PUK) are available to the user, who can change them at any time. When used in combination with a valid Kobra Infosec Smartcard, they enable authentication on the Kobra VS storage medium and, consequently, access to the stored data.

Using the User PIN, the user can authenticate (log in) to the Kobra VS storage device, generate a new cryptographic key, and change the User PIN. In addition, the user can enable and disable write protection if they have the appropriate write permissions.

The SO PIN (PUK) is required both to change the SO PIN (PUK) and to unlock the Kobra Infosec Smartcard after the User PIN has been locked. This can occur if the number of allowed failed attempts to enter the User PIN is exceeded. The Kobra Infosec Smartcard is permanently locked as soon as the number of allowed failed attempts (10 attempts) to enter the SO PIN (PUK) is also exceeded.

The Kobra Infosec Smartcard is shipped with the User PIN 1-2-3-4 and the SO PIN (PUK) 1-2-3-4-5-6-7-8-9-0. The factory settings allow for a User PIN length of 4 to 12 digits and three entry attempts. For the SO PIN (PUK), ten entry attempts and a length of 4 to 12 digits are permitted. In a PKI scenario, these settings are managed by the PKI administrators.

Note:

The disclosure of the SO PIN (PUK) to the user may be governed by different internal policies depending on the company in question.

Warning:

Make a note of your SO PIN: Without it, you cannot unlock a Kobra Infosec Smartcard after the User PIN has been blocked, nor can you change the SO PIN.

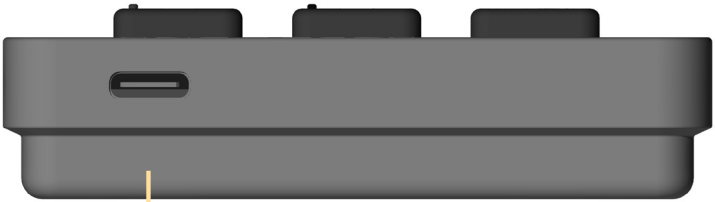
3.5 Admin PIN

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

3.6 USB connection, Smartcard slot and input interface

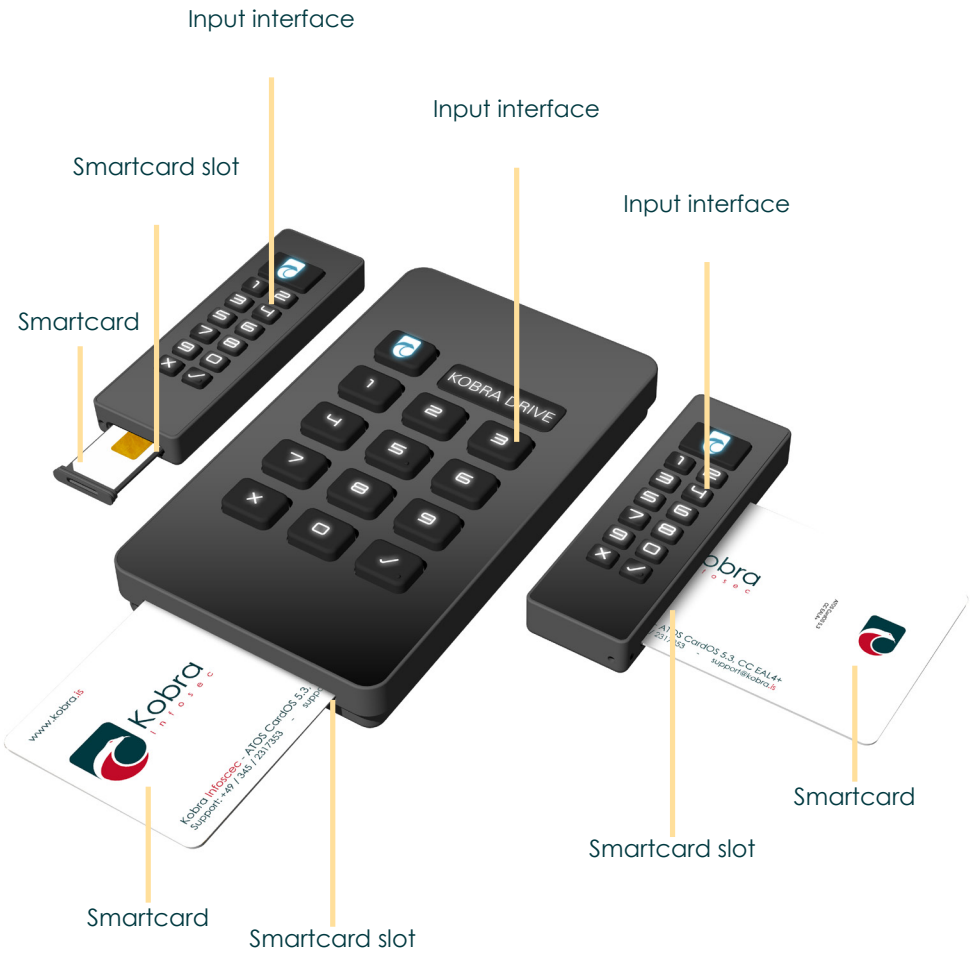
USB-C 3.0 port
Kobra Stick VS (2FF)

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)



3.7 Menu overview, commands and factory settings

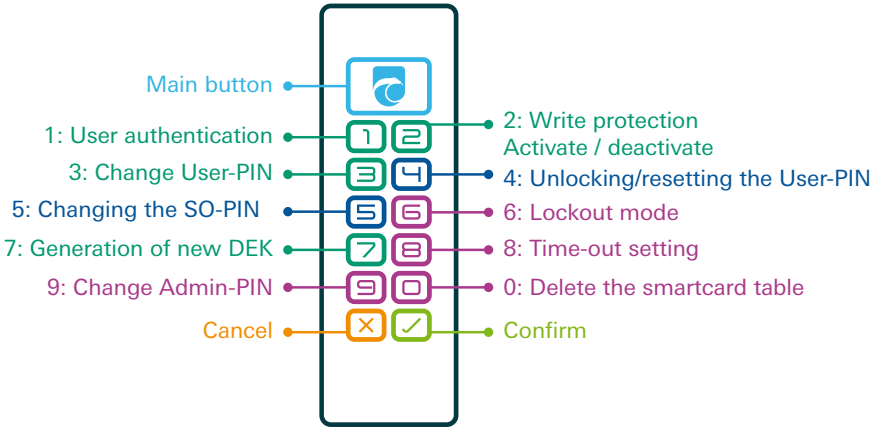
User	Taste 1 - Login Taste 2 - Write protection * * Taste 3 - Change User PIN Taste 4 - Enable the User PIN Taste 7 - Create new DEK
Administrator	Key 6 - Setting Lock-Out Key 8 - Setting time-out Key 9 - Change Admin PIN key 0 - delete the Smartcard table
Confirmation of the entries	Key √ or main key
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 (PUK) (default)	1-2-3-4-5-6-7-8-9-0
Failed attempts (SO PIN)	10
Number of digits (SO PIN	4 to 12
Admin PIN (default)	8-7-6-5-4-3-2-1
Failed attempts (Admin PIN)	16
Number of digits (Admin PIN)	4 to 16
Time-Out	Adjustable: 0 bis 30
Time-out (standard)	disabled*
Lock-Out (Standard)	disabled*
Write protection (standard)	disabled*
Admin PIN entry	enabled*
Drive type	Removable storage device

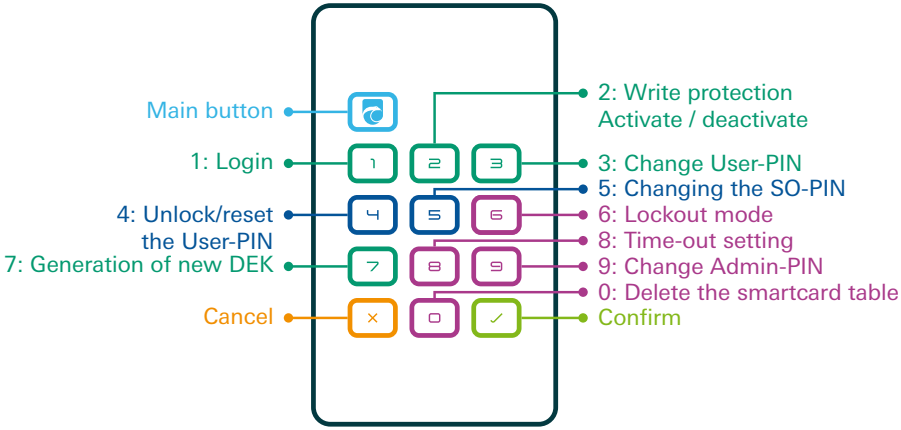
* – The administrator can block these settings before delivery to the user.

User-Commands

SO-PIN-Commands

Administrator Commands





3.8 Integrated battery as internal power supply

The Kobra VS data storage device has a built-in battery. This ensures an internal power supply and allows the following functions to be performed without connecting the Kobra VS data storage device to a PC or other external power source (e.g., USB power adapter or hub):

- Checking, Enabling, and Disabling Write Protection
- Both authentication before connecting to a PC (e.g., as pre-boot authentication) and booting from the Kobra VS storage device after connecting to a PC (e.g., Windows or other operating systems)
- Changing the User PIN without connecting to a PC
- Destruction of a valid cryptographic key or deletion of the Smartcard table, resulting in the deletion of all data on the Kobra VS storage device without connecting to a PC

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

If none of the buttons light up, this may be due to a dead battery. The battery can be charged via the USB-C port after connecting the Kobra VS storage device to a PC or another external power source (e.g., a USB power adapter or hub).

4. Authenticity Check

Every time a Kobra VS storage device is received, it must be verified for authenticity. A key step in this process is comparing the serial number and model designation on the delivery slip with the information engraved on the Kobra VS storage device's casing, as well as with the digital information that can be read using the supporting Kobra Client VS software.

For an additional authenticity check during operation, it is recommended to use a so-called authenticity file. Its purpose is to verify the authenticity and integrity of the data. The authenticity file can be chosen in any way that ensures it is unique and can be easily verified by the owner as soon as they access the storage device.

Depending on the application, an authenticity file can be generated and used in various ways. In the simplest form, it contains checksums—for example, using SHA256 or SHA512—of the original files. For a higher level of security, these hash values or even the complete files can be digitally signed using a private key, such as via GPG.

If you notice any discrepancies, please contact the supplier or your administrator.

5. Firmware Updates

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

6. Commissioning of the Kobra VS storage device

Only three steps are required to properly set up the Kobra VS storage device:

1) Insert the Smartcard (or PKI card)
2) Connect to the host system (e.g., PC)
3) Enter the User PIN

The Kobra VS data storage device is always powered via the USB-C port. Therefore, to set it up, connect it to a PC or a USB hub with a power supply. The Kobra VS data storage device also has a built-in battery. This allows certain functions to be performed without connecting the Kobra VS data storage device to an external power source.

As long as the Kobra VS data storage device is not connected to either a PC or an external power source (e.g., a USB power adapter or hub), it remains in sleep mode. All buttons are disabled in this state.

When connected to a PC or an external power source, the Kobra VS storage device immediately enters authentication mode if a Kobra Infosec Smartcard (or PKI card) designated for that Kobra VS storage device is correctly inserted. The main button flashes green, and the User PIN can be entered. If no Smartcard is present in the Kobra VS storage device, or if the card is invalid or not compatible, the main button flashes continuously in red or yellow until a Kobra Infosec Smartcard (or PKI card) designated for this storage device is correctly inserted. If no further commands or entries are made within 20 seconds, the Kobra VS storage device automatically switches to standby mode.

Pressing the main button switches the device from standby mode to menu mode. In this state, the main button lights up blue and all other input buttons light up white. The illuminated input buttons indicate that they are active and that the corresponding commands can be entered. After pressing the "1" key and then the "√" key, the user returns to authentication mode. The main button flashes green, and all other buttons remain active. At this point, the User PIN can be entered. If the User PIN or SO PIN (PUK) is already locked, the main button flashes alternately yellow-red-yellow-red after the PIN is entered and confirmed with the "√" button, and then lights up white. The Kobra VS storage device then switches to standby mode. Authentication is not possible in this case. The locked User PIN can be reset using the valid SO PIN (PUK). Kobra Infosec Smartcards with locked user and SO PINs (PUKs) can no longer be used.

If a Smartcard that has not yet been entered into the Kobra VS storage device's Smartcard table is inserted into the Smartcard slot, the main button will briefly light up red immediately after pressing the "1" button and then remain lit white: The Kobra VS storage device has entered standby mode. Authentication is also not possible in this case.

All commands are confirmed with the "√" button or the main button, or canceled with the "X" button. Each time the "X" button is pressed, the user enters standby mode and can restart their planned steps from this state of the Kobra VS storage device. The main button flashes orange once and then lights up white.

After successful authentication, the main button remains lit green when write protection is disabled and purple when it is enabled. The other buttons are unlit, and access to the data is enabled.

If the PIN entry was incorrect, the main button flashes red once or multiple times depending on the number of failed attempts (up to a maximum equal to the number of allowed failed attempts), and the Kobra VS storage device returns to standby mode. The authentication process can be repeated from this point, as described above. Once the maximum number of allowed failed attempts has been exceeded, the main button flashes yellow-red-yellow-red and then lights up white. The Kobra Infosec Smartcard automatically locks itself and can only be unlocked afterward by entering the SO PIN (PUK). PIN entry attempts with fewer than 4 digits are generally not counted as failed attempts (Chapter 9.4 Unlocking/Resetting the User PIN).

Entering the SO PIN (PUK) incorrectly will result in the permanent locking of the Kobra Infosec Smartcard once the maximum number of failed attempts has been exceeded. Afterward, access to the data is only possible with another Kobra Infosec Smartcard that has been activated for this Kobra VS storage device and by correctly entering the User PIN. In this case, you can use the Kobra Client VS software to delete the locked Smartcard from the Smartcard table on the Kobra VS storage device and register another compatible Smartcard.

If there are no other Kobra Infosec Smartcards authorized for this Kobra VS storage device, the only option is to initialize a new Kobra Infosec Smartcard for this Kobra VS storage device. The administrator performs this task by deleting the current Smartcard table and creating a new one. All previously stored data is irrevocably destroyed during this process.

Authentication can also take place without a connection to a PC or another external power source (e.g., USB power adapter or hub). In this case, power is supplied by the built-in battery. After pressing and holding the main button (for approx. 3 seconds), the Kobra VS storage device enters authentication mode. The user then inserts their Smartcard and enters the corresponding User PIN. After successful authentication, the Kobra VS storage device can be connected to a PC within 20 seconds.

If no further commands or inputs are made within 20 seconds, the Kobra VS storage device automatically switches to standby mode if it is connected to a PC or another

external power source (e.g., USB power adapter or hub). Without an external power source, the Kobra VS storage device returns to sleep mode after 20 seconds. However, this rule does not apply to an authenticated Kobra VS storage device if it is already connected to a PC.

For security reasons, the Kobra VS storage device must be logically or physically disconnected from the host system after use. This is particularly recommended upon completion of work, during brief interruptions, and when leaving the workstation.

In this context, the activated timeout function provides effective support for data protection. Using this setting, an automatic timeout due to inactivity can also be configured for the connected storage device (Chapter 9.9 Timeout Functions).

In addition to traditional "logout" mechanisms—such as "safely removing" the device via the PC's taskbar and physically disconnecting the USB connection—the Kobra VS storage device also features the Quick-Out function for rapid logout. This function is executed by double-clicking the "×" button within 2 seconds. For safe physical disconnection, the USB cable must be completely removed from the Kobra VS storage device.

Note:

To prevent data loss, make sure—before disconnecting the connections—that data transfer and access to the Kobra VS storage device are completely finished.

Note:

To ensure the security of your data, it is absolutely necessary to change the default User PIN and SO PIN (PUK) (see Chapter 9.3, "Changing the User PIN," and Chapter 4.3.3, "Changing the SO PIN/PUK," in the Kobra Client VS Manual). You should also change your User PIN at regular intervals in the future. It is also recommended that you use different User PINs for different Kobra Infosec Smartcards. The User PIN and SO PIN (PUK) must be kept confidential.

Note:

Please note that the "Kobra Client Software" (Chapter 8. Kobra Client VS) must be turned off as soon as you format the Kobra VS storage device.

7. Role and permissions

Kobra VS storage devices allow for the assignment of roles and permissions related to the management and use of the storage device.

The user has the Smartcard and knows the User PIN and OS PIN (PUK). They can change the User PIN and SO PIN (PUK), authenticate (log in) to the Kobra VS storage device, generate a new cryptographic key, and unlock or reset the Kobra Infosec Smartcard after it has been locked due to an incorrect User PIN entry. In addition, they can enable and disable write protection if they have write permissions.

The administrator knows the Admin PIN. He can manage the Kobra VS storage device and configure it in accordance with the company's security policy and the intended use cases. Among other things, he can change the Admin PIN, configure timeout and lockout settings, and add to, delete, or recreate the list of authorized Smartcards for a Kobra VS storage device. Furthermore, they can specify which users have read-only access and which also have write access, as well as whether a particular user is permitted to destroy or generate the cryptographic key. For more information, see Chapter 8 and the user guides for Kobra Client VS and Kobra Connect.

Based on their permissions, the administrator cannot access the data stored on a Kobra VS storage device. However, they may potentially learn a user's PIN while activating an additional Kobra Infosec Smartcard for a Kobra VS storage device, since the PIN must be entered during the addition process. Therefore, it is imperative that the user reset the User PIN after this process.

Using the Kobra Client VS software, the administrator can quickly transfer the above settings to other Kobra VS storage devices. Furthermore, the administrator can enable or disable the entry of the Admin PIN via the Kobra VS storage device's keyboard. Entering the Admin PIN via the Kobra Client VS software remains possible in any case. This prevents the user from entering the Admin PIN incorrectly and thus avoids the Admin PIN being permanently locked. Once the Admin PIN is locked, it is no longer possible to change the settings configured by the administrator.

The design of the PKI cards and the provision of the SO PIN (PUK) to the user can be individually regulated by the internal policies and security concepts of the respective companies or government agencies.

Warning:

It must be assumed that the administrator may have access to the data stored on the Kobra VS storage device. Therefore, the administrator must be trustworthy. If there are any doubts about the administrator's trustworthiness, the user must become the administrator and manage the Smartcard table independently.

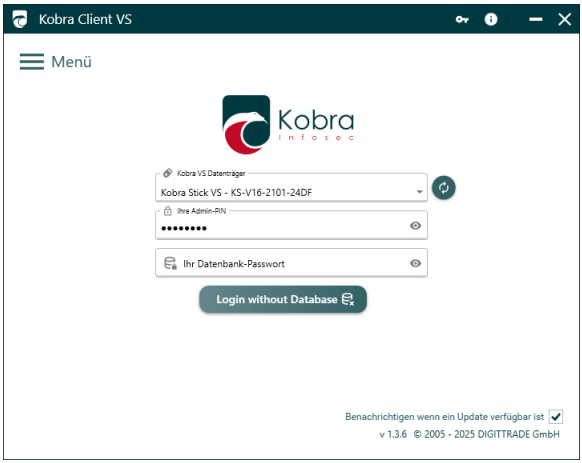
8. Kobra Client VS

The Kobra Client VS is management software for Kobra VS storage devices. It enables the administrator to configure Kobra VS storage devices for each individual user quickly and in a task-oriented manner. The settings can be exported and saved as configuration profiles for specific user groups. These settings can then be quickly applied to any Kobra VS storage device. The following settings, among others, can be configured, exported, and imported:

- Changing the Admin PIN, User PIN, and SO PIN
  (with optional password generator)
- Using the Admin PIN via the Kobra VS storage device's keypad
- Generating and changing the update key
- Configuring lockout and timeout functions
- Deleting and creating Smartcard tables
- Adding Additional Smartcards (PKI Cards) to the Smartcard Table
- Setting Individual Read and Write Permissions for Each User
- Enabling and Disabling Self-Formatting
- Power Bypass
- Database Functions, Smartcard Wizard, and Much More

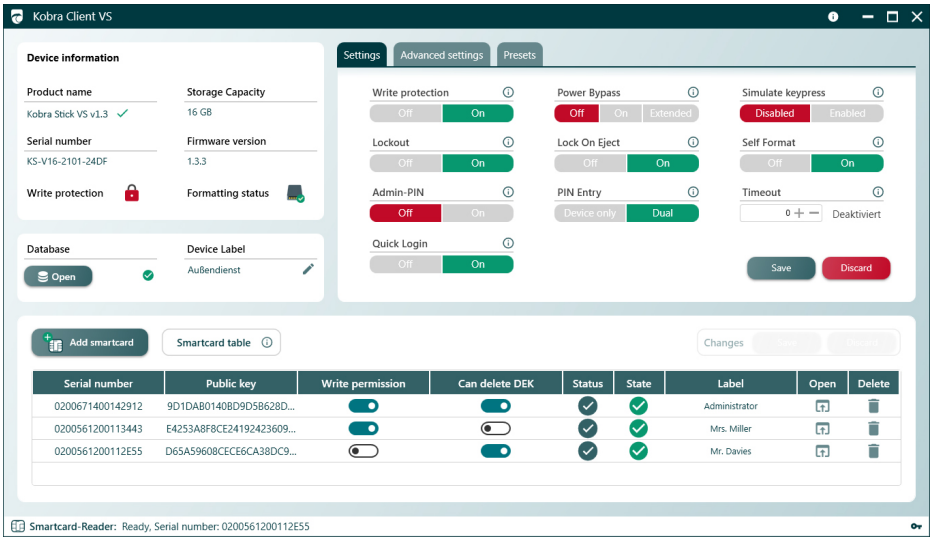
Using this software, the administrator can read the serial number and public key directly from the Kobra Infosec Smartcard (PKI card) inserted into the Kobra VS storage device. The administrator can retrieve this information from both the database and the Smartcard table on the VS storage device. In addition, the administrator can specify whether the respective Smartcard owner has write permissions and is allowed to delete the DEK.

After launching the Kobra Client VS software, the login window appears first:



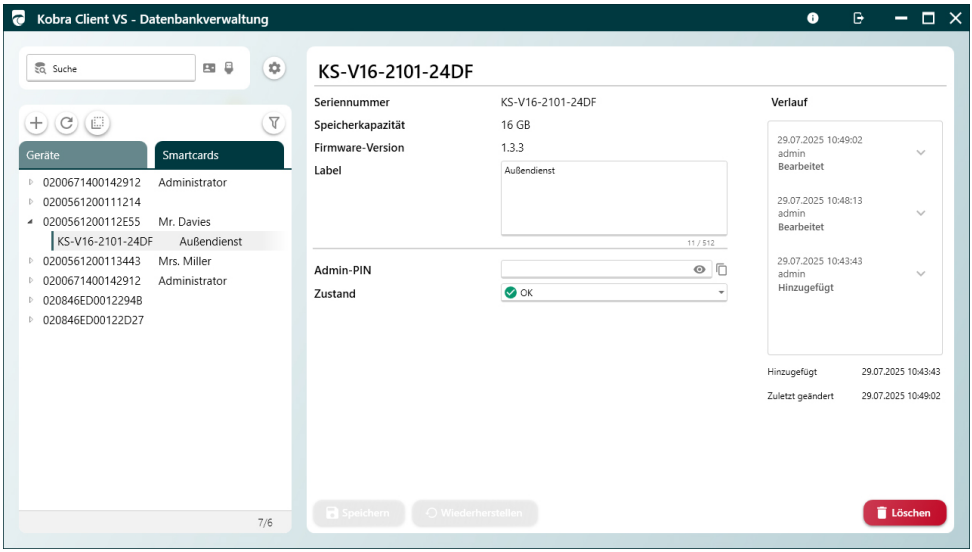
Login-Fenster

In the login window, the administrator can select the language and search for a connected VS storage device. After successful authentication with the Admin PIN, the main menu opens. The current settings of the Kobra VS storage device, as well as the Smartcard table containing the authorized Kobra Infosec Smartcards (PKI cards), are loaded into this menu.



Hauptmenü

At the same time, the database is updated so that all changes to the storage device and the Smartcards are recorded in the database.



Database View

A detailed description can be found in the Kobra Client VS user manual on the website www.kobra-infosec.de.

9. Menu Mode: Authentication and Management

Authentication and management of the Kobra VS storage device are performed in menu mode by entering numbers and commands. To switch to menu mode from standby mode, press the main button. In menu mode, the main button lights up blue and all other input buttons light up white.

To execute commands, the Kobra VS storage device usually requires a connection to a PC or another external power source (e.g., a USB power adapter or USB hub). Exceptions include authentication on the Kobra VS storage device, enabling or disabling write protection, and generating a new cryptographic key. These functions can also be performed while the device is running on battery power.

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

After launching a menu function, the main button begins to flash green when the User PIN must be entered. In contrast, the main button flashes continuously in purple for entering the Admin PIN and in light blue for the SO PIN (PUK). All other buttons are active at this time. If the entry is confirmed with the "√" button, the main button lights up green if the PIN is correct.

If an error occurs, the main button flashes red briefly and then lights up white. The Kobra VS storage device switches to standby mode. The process can be repeated from this point.

If the PIN entry was incorrect during any of the operations, the main button flashes red once or multiple times depending on the number of failed attempts (up to the maximum number of allowed failed attempts), and the Kobra VS storage device switches to standby mode. The intended operation can be restarted from this point.

In addition, the Kobra VS storage device enters standby mode after every successful execution of a command (except for user authentication).

If a valid Smartcard is inserted and the Kobra VS storage device is connected to a PC via a USB cable, or if the main button is held down for an extended period while in battery mode, the main button flashes green. The Kobra VS storage device is in authentication mode:

- Once the User PIN has been entered, access to the data is enabled
- After pressing the X button or the main button, the Kobra VS storage device enters standby mode.

9.1 User Authentication

User authentication is required to enable access to the storage device. This can be done in two different ways: either by connecting to an external power source (e.g., a host system) or as pre-boot authentication when running on battery power.

A. Authentication on the host system:

1) Insert a Smartcard approved for use with the Kobra VS storage device into the designated slot.
2) Connect the Kobra VS storage device to a host system. The Main button will now flash green, and all other buttons will remain active.
3) Enter the User PIN and confirm with "√".

If the Kobra VS storage device is connected to the host system without a Smartcard inserted, the main button will begin to flash red continuously:

1) Insert a Smartcard approved for use with the Kobra VS storage device into the designated slot. The main button will begin to flash green, and all other buttons will remain active.
2) Enter the User PIN and confirm with "√"

B. Authentication in battery mode:

1) Insert a Smartcard approved for use with the Kobra VS storage device into the designated slot.
2) Press the Main button until it flashes green.
3) Enter the User PIN and confirm with "√"

If the Kobra VS storage device with a Smartcard inserted is in standby mode (the main button is lit white and all other buttons are dimmed), follow these steps:

1) Next, press the main button, the "1" button, and then "√." The Main button will flash green, and all other buttons will remain active.
2) Enter the User PIN and confirm with "√"

Note:

After successful authentication, the main button glows green continuously if write protection is disabled, or purple if it is enabled. The other buttons are disabled, and access to the data is enabled.

9.2 Write-protection mechanism

When write protection is enabled, it provides you with additional protection against viruses and Trojans when using the Kobra VS storage device on a third-party PC. It also prevents sensitive information from being accidentally saved from a PC or server to the Kobra VS storage device.

Even before authentication, the user can press the "2" button to check whether write protection is enabled. The main button, which glows purple continuously, indicates that write protection is enabled. If write protection is disabled, the main button glows green.

To enable or disable write protection:

1) Make sure you are in wait mode. (The main button is lighting up white, and all other buttons are dimmed.)
2) Next, press the main button and the "2" button. When write protection is enabled, the Main button lights up purple; when write protection is disabled, it lights up green.
3) Then press the "√" button if you want to change the status. The main button will flash green, and all other buttons will remain active.
4) Next, enter your User PIN and confirm by pressing "√".

After a successful switch, the main button flashes green or purple twice, and the Kobra VS storage device returns to standby mode.

Using the Kobra Client VS software, the administrator can disable write permissions for individual users. In this case, the user cannot disable write protection.

9.3 Changing the User PIN

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

To change your User PIN:

1) Make sure you are in wait mode. (The main button is lighting up white, and all other buttons are dimmed.)
2) Next, press the main button, the "3" button, and then "√." The main button will flash green continuously, and all other buttons will remain active.
3) Enter the current User PIN and confirm by pressing "√".
4) Enter the new User PIN and confirm by pressing "√".
5) Re-enter the new User PIN and confirm by pressing "√"."

After successfully changing the PIN, the main button flashes green twice, and the Kobra VS storage device returns to wait mode.

9.4 Unlocking/resetting the User PIN

Once the maximum number of failed attempts has been exceeded, the Kobra Infosec Smartcard automatically locks itself and can only be unlocked by entering the SO PIN (PUK). This feature allows the user to replace the locked User PIN with a new one.

1) Make sure you are in wait mode. (The main button is lighting up white, and all other buttons are dimmed.)
2) Next, press the Main button, the "4" button, and then "√". The Main button will flash light blue, and all other buttons will remain active.
3) Enter the SO PIN (PUK) and confirm by pressing "√".
4) Enter the new User PIN and confirm by pressing "√"
5) Re-enter the new User PIN and confirm by pressing "√"."

After the Kobra Infosec Smartcard has been successfully activated, the main button flashes green twice and the Smartcard enters standby mode.

If the SO PIN (PUK) is entered incorrectly more times than the allowed number of attempts, the Kobra Infosec Smartcard will be permanently locked. Afterward, access to the data is only possible with another Smartcard that has been activated for this Kobra VS storage device and by entering the correct PIN.

9.5 Changing the SO PIN (PUK)

The SO PIN (PUK) can only be changed using the Kobra Client VS software. Instructions for doing so can be found in the Kobra Client VS user manual on the website www.kobra-infosec.de.

9.6 Changing or Disabling the Admin PIN

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

9.7 Generating a new DEK (Data Encryption Key)

Using an initialized Kobra Infosec Smartcard (or PKI card) and the User PIN, the user can generate, change, and destroy the cryptographic key on the associated Kobra VS storage device at any time. These operations are irreversible. After a new cryptographic key is generated, the old cryptographic key- and thus all data stored on the Kobra VS storage medium- is permanently destroyed. Therefore, under certain circumstances, the stored information should first be backed up onto another storage device approved for VS-NfD/EU RESTRICTED/NATO RESTRICTED.

When deleting data, you should avoid overwriting it multiple times—for example, by formatting—as this can shorten the lifespan of the storage device. Data can be deleted securely and efficiently by generating a new cryptographic key. In addition, data can be destroyed by deleting the cryptographic key (Chapter 9.8 Deleting a Cryptographic Key) or the Smartcard table (Chapter 9.14 Smartcard Table).

To generate or modify the DEK:

1) Insert a Smartcard approved for use with the Kobra VS storage device into the designated slot.
2) Make sure the Kobra VS strorade device is connected to a host system and that you are in wait mode. (The main button is lighting up white, and all other buttons are dimmed.)
3) Next, press the main button and the “7” button. The main button lights up red permanently, indicating that all data stored on the Kobra VS storage device will be permanently destroyed after this function has been executed.
4) Press the “√” button if you want to perform this function. he main key flashes green and all other keys remain active.
5) Enter the User PIN (PUK) and confirm by pressing “√”.

After entering and confirming the User PIN, the main button lights up yellow while the cryptographic key is being generated or changed. If the process is successful, the main button flashes green twice and then remains white. The Kobra VS storage device switches to wait mode. This process may take several seconds. This is especially true if multiple Smartcards are listed 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 storage device is no longer possible from this point on.

9.8 Deleting a DEK (Data Encryption Key)

There are three ways to delete (destroy) the DEK.

A: Destruction of the DEK without generating a new cryptographic key

This method allows you to quickly destroy the data stored on the Kobra VS storage device without having to connect it to a PC. From that point on, any previously stored data can no longer be retrieved.

1) Insert a Smartcard into the Kobra VS storage device and press the main button until it flashes green. Then press the "X" button to enter wait mode. (The main button lights up white, and the other buttons are dimmed.)
2) Next, press the main button and the "7" button. The main key lights up red permanently, indicating that all data stored on the Kobra VS storage device will be permanently destroyed after this function has been executed.
3) Press the "√" button if you want to perform this function. he main key flashes green and all other keys remain active.
4) Enter the User PIN (PUK) and confirm by pressing "√". After entering and confirming the User PIN, the main button lights up yellow while the cryptographic key is being generated or changed. f the process is successful, the main button flashes green twice and then remains white.

B: Destruction by generating a new DEK

A description of this process can be found in Chapter 9.7, „Generating a new DEK (Data Encryption Key)"

C: Destruction of the DEK by deleting the Smartcard table

This method can be performed by the administrator either by entering commands via the keyboard or by using the Kobra Client VS software and the Admin PIN. During the deletion of the Smartcard table, the final destruction of the DEK also takes place. From this point on, the Kobra VS storage device no longer contains a cryptographic key. As a result, all data previously stored on the Kobra VS storage device is also irrevocably destroyed. (Chapter 9.14 Smartcard table)

Deleting the Smartcard table using the keypad of the Kobra VS:

1) Make sure you are in wait mode. (The main button is lighting up white, and all other buttons are dimmed.)
2) Next, press the main button and the "0" button. The main button flashes purple continuously, and all other buttons remain active.
3) Enter the Admin PIN and confirm by pressing "√".

After a successful operation, the main button flashes green twice, and the Kobra VS storage device returns to wait mode.

9.9 Time-Out functions

The administrator can specify the number of minutes after which the unlocked Kobra VS storage device will automatically lock if there is no read or write access to the Kobra VS storage device within the specified time. A description of this feature can be found in the Administrator's Manual.

9.10 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.

9.11 Lock-Out Function

Using the lockout function, the administrator can specify whether the Kobra-Infosec Smartcard (PKI card) should remain in the Kobra-VS storage device after authentication or whether it can be removed. When Lock-Out mode is enabled, access to the data is interrupted as soon as the Kobra-Infosec Smartcard (PKI card) is removed from the Kobra-VS storage device's housing. (approximately 3 seconds when a Kobra VS storage device is connected to a host system, and approximately 30 seconds in battery mode).

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

9.12 Depositing an Update-Key

Before performing an update, the administrator must store a 256-Bit (32 bytes) update-key on the Kobra VS. This task can also be done in advance during the first setup of the Kobra VS.

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

9.13 Export and Import of Settings

The settings for the Kobra VS storage device can be exported at any time, saved externally, and applied (imported) to any Kobra VS storage devic.

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

9.14 Smartcard Table

The Smartcard table contains information about the Kobra Infosec Smartcards or PKI cards that have been authorized to access the Kobra VS storage device. The administrator can add up to 8 Kobra Infosec Smartcards to a Smartcard table using the Kobra Client VS software. In addition, the administrator can specify whether the respective user has read-only or read-write access and whether the user can delete the DEK.

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

10. 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	R, W	R, W	X	X
Mac OS X	R	R, W	R, W	X
Linux	R	R, W	X	R, W

Title: R - Read, W - Write, X - No compatibility

Important:

Please note that the "Kobra Client software" (chapter 8) must be switched off as soon as you format the VS storage device.

11. Possible Applications

The technical characteristics and security features of Kobra VS storage devices offer extensive possibilities for the secure storage, archiving, and transmission of sensitive, personal, and confidential information up to the VS-NfD classification level.

The following usage scenarios also fall within the scope of the VS-NfD certification. Any deviations from the described procedures must be coordinated with the BSI (Federal Office for Information Security).

11.1 Kobra Connect

With the Kobra Connect software, Kobra VS storage devices can also be used as Smartcard readers with an integrated keyboard for PIN entry or as authentication tokens with a PIN pad. This enables secure and convenient identity verification for protected login processes and access controls.

In addition, Kobra Connect supports both host and device authentication, ensuring that the Kobra VS storage device can only be used on authorized systems through this mutual authentication. Sensitive data thus remains accessible exclusively within a controlled and protected IT environment.

At the same time, when connected to a higher-level system, the Kobra VS storage device can automatically be set to a read-only state.

Furthermore, Kobra Connect enables the use of the Kobra VS storage device as a boot device in Windows Read-Only mode. This allows for the use of a fully portable Windows operating system without making any changes to the Kobra VS storage device. This is particularly advantageous for high-security IT environments where an immutable and tamper-proof system environment is required.

11.2 Host Authentication

Using Kobra Connect, the administrator can specify which host systems the Kobra VS storage device is permitted to connect to. To do this, a HAK (Host Authentication Key) is stored on both the Kobra VS storage device and the host system. On the Kobra VS storage device, this is done via the Kobra Client VS; on the host system, via Kobra Connect.

Upon connection, the Kobra VS storage device automatically verifies whether the computer is one of the authorized hosts. This authentication is performed using a strong cryptographic method, ensuring that the Kobra VS storage device can only be unlocked after connecting to an authorized host system.

On unauthorized host systems, the storage device remains locked. The user cannot override this function. This ensures that classified information is processed exclusively in a protected VS-NfD environment (“Classified – For Official Use Only”).

Even if the classified data storage device is lost or stolen, this feature provides additional protection for sensitive data.

11.3 Kobra Defence Zone

To prevent unauthorized data leakage, USB ports on host systems are generally blocked in many government agencies and companies. To this end, settings in the operating system or specialized USB blocker software can be used. With Kobra VS data storage devices, it is now possible for the first time to store and transport VS-NfD-classified data in a secure environment even outside the host system.

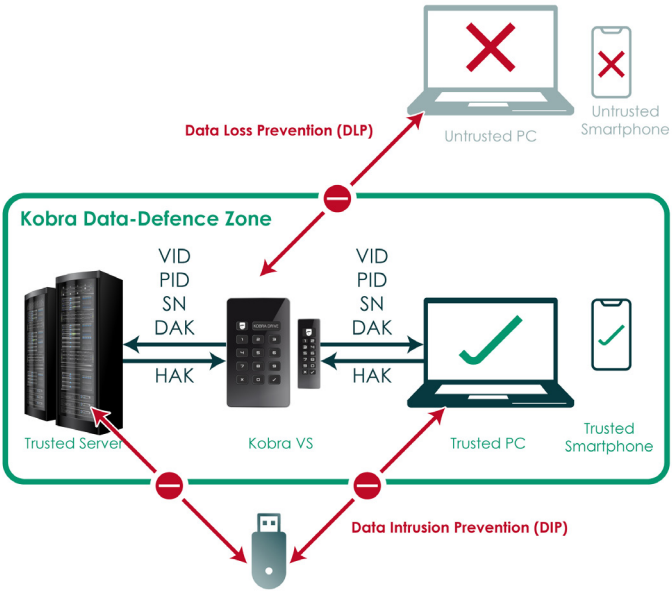
In addition to standard identification features such as Vendor ID (VID), Product ID (PID), and serial number (SN), the Kobra Connect software also offers cryptographic device authentication using a DAK (Device Authentication Key). Similar to the HAK, the DAK is stored by the administrator on the Kobra VS storage device and in Kobra Connect on the host system. After the Kobra VS storage device is connected to the host system, the device is verified and authorized using a cryptographic procedure. This enables the unambiguous identification of the connected storage device and its authorization for the respective user in a specific area of the internal network.

The combination of mutual cryptographic host and device authentication creates a secure environment for sensitive data—a Kobra Defence Zone. This is a new concept in which USB storage devices are, for the first time, an integral part of active network protection measures, rather than being considered a gateway for malware or a risk for data loss.

The Kobra Defence Zone thus represents a secure area in which data can be protected by Kobra VS storage devices and exchanged securely between air-gapped systems.

A typical example of this is the transfer of VS-NfD-classified data from a stationary host system (e.g., an internal network or server) to a VS storage device for further processing on a mobile host system (e.g., a protected laptop). The Kobra Defence Zone ensures that neither VS data storage devices can be connected to an unauthorized host system nor can other data storage devices be connected to the protected host systems within the Kobra Defence Zone.

This ensures that all data remains within the Kobra Defence Zone and cannot be leaked. At the same time, it prevents Kobra classified data storage devices from being infected with malware when connected to unauthorized devices.



1) **Interface control:** VID (USB Vendor-ID), PID (Produkt-ID), SN (Serial number), DAK (Device Authentication Key)
2) **Host authentication:** HAK (Host authentication key)

11.4 Increasing the Level of Protection for Kobra VS in the Organization

The administrator in a company or government agency can specify how restrictive each user's Kobra VS storage device should be. For this purpose, the administrator can set the number of allowed failed attempts (when using PKI cards) and the timeout period for the user. In addition, they can specify which users are authorized only to read data and are not permitted to delete a DEK. Using the lockout function, the administrator determines whether the Kobra Infosec Smartcard (or PKI card) must remain in the Kobra VS storage device for the session after authentication or may be removed.

The user cannot change these settings based on their permissions.

11.5 Secure and Cost-Effective Data Transport

The Kobra VS storage device can be used for the secure transport of confidential data. To do this, the Kobra Infosec Smartcards of the sender and recipient must be entered into the Smartcard table of the Kobra VS storage device. The sender sends only the Kobra VS storage device, as this allows for the organization of a regular and secure data exchange between two offices.

In the stand-alone version, the user has two Kobra Infosec Smartcards that are already entered in the Smartcard table on the Kobra VS storage device. In this case, the user can provide the second Kobra Infosec Smartcard to the recipient for decrypting the data. Alternatively, the administrator can add an additional Kobra Infosec Smartcard for the recipient to the Smartcard table on the Kobra VS storage device. The Kobra VS storage device and the Kobra Infosec Smartcard are then sent separately to the recipient. The User PIN and, if applicable, the SO PIN (PUK) are also sent separately, but only after the Kobra Infosec Smartcard has been received.

When using PKI cards, the administrator enters the serial number and public key of the sender's and recipient's PKI cards into the Smartcard table on the Kobra VS storage device. This is done using the Kobra Client VS software. The Kobra VS storage device must be physically in the administrator's possession during this process, while the PKI cards may remain with the users.

During transport of the Kobra VS storage device, tamper-resistance must be ensured through appropriate packaging. For example, the use of sealed Kobra Infosec security pouches is recommended. For more information on the security features of the Kobra VS storage device, see Chapter 4, "Authentication," and for information on the security pouches, see Chapter 12.2, "Security Packaging."

Upon receipt of the Kobra VS storage device, its authenticity must be verified. This is done by comparing the storage device's serial number—which is communicated via a separate secure channel—with a file containing a specific identifier stored within the storage device. The serial number can be found both on the casing of the Kobra VS storage device and when the device is connected via USB. The Kobra Client VS displays the model name and serial number of the Kobra VS storage device immediately after it is connected to a PC.

This method makes it possible to ship the Kobra VS storage device containing confidential data cost-effectively and securely via a parcel service or courier.

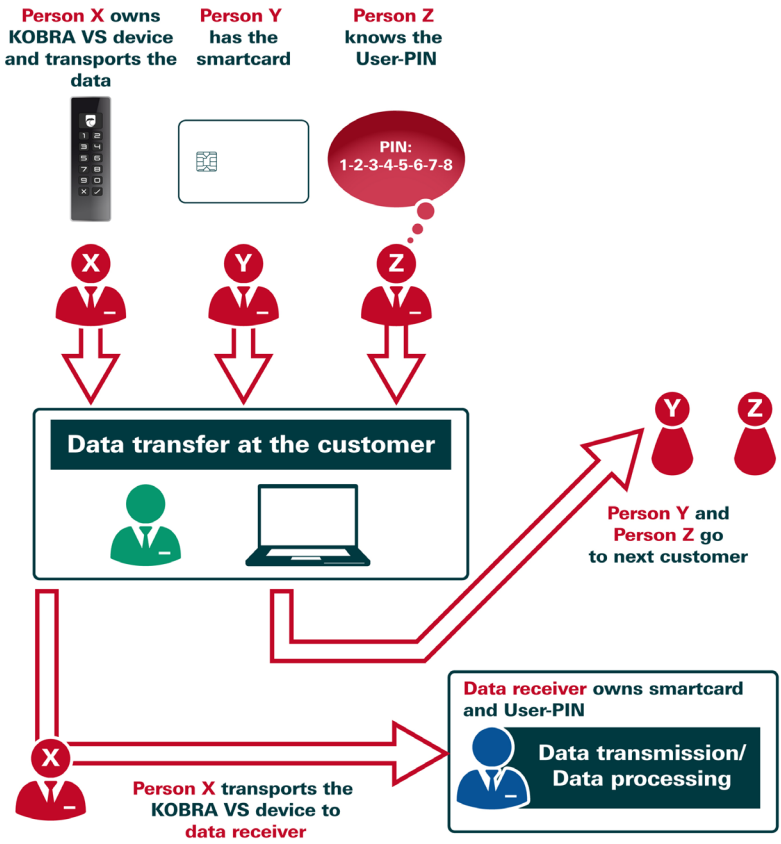
Warning:
If any attempts to tamper with the device occurred during transport, the storage device may no longer be used under the VS-NfD certification.

11.6 Separation of Data Storage Device and Authentication Features

Access to the data can be regulated so that it is only possible when three individuals come together. Person X (e.g., courier) possesses the Kobra VS storage device, Person Y has the authorized Kobra Infosec Smartcard, and Person Z knows the User PIN. The three individuals come together only at the recipient's location to transfer the data and then go their separate ways. Individually, persons X, Y, and Z do not have the ability to access the data.

Warning:

If any attempts at tampering occurred during transport, the Kobra VS storage device may no longer be used under the VS-NfD certification.



11.7 Use of fewer Storage devices for a Large Customer Base

If a company (e.g., a data processing company or a data center for large enterprises/government agencies) regularly exchanges data with multiple different users, the data can be transported cost-effectively and securely using just a few Kobra VS storage devices.

Each user receives an individual Smartcard. The serial number and public key of all Smartcards are registered at the data center. For each data exchange with another user, the Smartcard table on the Kobra VS storage device is first deleted. In the next step, a new table is created with the Smartcard information of the sender and recipient (Admin PIN required). The data can then be saved to the Kobra VS storage device and sent.

Upon receiving the Kobra VS storage device from an employee, the administrator deletes the old Smartcard table and creates a new one with the Smartcard information of the next user. There is no need for time-consuming data deletion or repeated overwriting of the storage device, since the remaining data was encrypted with the previous cryptographic keys. The cryptographic key cannot be reconstructed after the Smartcard table has been deleted, and therefore there is no way to access the previous data.

If data needs to be sent multiple times to the same recipient within a short period, it is not necessary to wait for a personalized Kobra VS storage device to be returned. Any Kobra VS storage device available within the company can be used. To do this, the Smartcard table from the first Kobra VS storage device can be imported into the subsequent Kobra VS storage devices (Chapter 9.14 Smartcard Table).

Thanks to this feature, the number of storage devices required can be significantly reduced, since a personalized Kobra VS storage device is not needed for every user. It does not matter which of the Kobra VS storage devices available within the company are used for data transfer. What matters is which Kobra Infosec Smartcards (or PKI cards) are entered in the Smartcard table of the Kobra VS storage device.

Note:

When deleting data, avoid overwriting it multiple times, as this can reduce the storage device's lifespan. Data can be deleted securely and efficiently by generating a new cryptographic key (Chapter 9.8 Deleting a DEK) or by deleting the Smartcard table (Chapter 9.14 Smartcard Table).

Warnhinweis:

If any attempts at tampering occurred during transport, the Kobra VS storage device may no longer be used under the VS-NfD certification.

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

In a company, each field employee has their own personalized Smartcard (or PKI card) with their own cryptographic characteristics. For work outside the company, the employee receives any Kobra VS storage device that has been previously prepared for use by that employee. To do this, the administrator deletes the old Smartcard table and creates a new one with that employee's Smartcard information. The field employee then stores the data using their own cryptographic keys.

After use, the employee returns the Kobra VS storage device. It is then prepared for the next employee in the same manner within a few minutes. In the process, the previous user's data is automatically and irrevocably deleted. Therefore, a separate Kobra VS storage device is not required for every employee, and the number of storage devices needed within the company can be reduced.

Note:
It is also recommended to delete the current cryptographic key before returning the Kobra VS storage device. This ensures that the data on the Kobra VS storage device is destroyed before it is returned to the administrator.

11.9 Operating multiple Kobra VS storage devices with a single Smartcard

To operate multiple storage devices with a single Smartcard, the Smartcard table containing the same Smartcard information (serial number and public key) is stored on multiple Kobra VS storage devices using the Kobra Client VS software.

This scenario is particularly useful when working with data volumes that exceed the capacity of a single Kobra VS storage device. In such cases, the data can be distributed across multiple Kobra VS storage devices.

Even if data is sent very frequently—for example, daily—it makes sense to use multiple storage devices in this way. A new Kobra VS storage device with the same Smartcard table can be sent daily without having to wait for a personalized Kobra VS storage device. The sender and the recipient can always access the Kobra VS storage device with the same Smartcard.

Note:
When sending the Kobra VS storage device, additional measures are required, which are described in Chapter 11.5, "Secure and Cost-Effective Data Transport".

11.10 Use as an Encrypted Boot Device

The integrated autonomous power supply enables authentication of the Kobra VS storage device before a PC starts up (pre-boot authentication). This feature makes it possible to store operating systems in encrypted form on the Kobra VS storage device and then boot them directly from the Kobra VS storage device.

In this context, operating systems such as Windows, Linux, ECOS-OS, and others, as well as user data, can be stored. This application scenario is suitable for both desktop and mobile computers. The minimum required storage capacities must be taken into account. The Windows operating system can only be used on Kobra VS storage devices with a storage capacity of at least 32 GB. In addition, Kobra VS storage devices with pSLC memory are recommended for this purpose to ensure the longest possible service life.

Furthermore, the "Power Bridge" and "Disable Lock on Ejection" features allow Kobra VS storage devices to be used as boot devices even on host systems with varying boot process behaviors. Depending on requirements, the Kobra VS storage device can be configured as either a local drive or a removable drive.

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

When using the Kobra VS storage device as an encrypted boot device for the VS workstation, the following additional measures should also be taken into account:

- Disabling the host's internal Kobra VS storage devices via Group Policy or operating system configurations.
- Implement interface control using additional software, Group Policy, or operating system configurations.
- If the VS workstation is connected to a network, additional software for VPN connections and a suitable firewall are generally required.

Note:

Windows compatibility can be configured by the administrator using the Kobra Client VS.

11.11 Use on Various Operating Systems and Smartphones

Thanks to its hardware encryption and hardware authentication, the Kobra VS storage device works independently of the operating system and can be used on virtually any device that supports USB storage devices.

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

Note:

If the storage device contains information classified as VS-NfD, its use is permitted exclusively on devices authorized to process VS-NfD information within the scope of that authorization. Deleting VS-NfD information from the storage device must be performed in accordance with the procedures outlined in Chapter 9.8, "Deleting a Crypto Key."

11.12 Use as a Data Diode

The activated write protection on the Kobra VS storage device provides secure protection against the unintended leakage of information from higher-classified systems to lower-classified systems.
To achieve this, the data from the source system (e.g., VS-NfD) is written to the Kobra VS storage device, and then the write protection on the Kobra VS storage device is activated. Next, the Kobra VS storage device is connected to the higher-classified system (e.g., Secret), and the required data is transferred from the Kobra VS storage device to the host system. Afterward, the storage device can be used normally again in the original system.

Any additional security measures, such as a virus scan, are still required. Optionally, the Kobra VS storage device can be quickly and securely erased before and after the transfer by regenerating the cryptographic key.

To implement the data diode function, the administrator can also define two Smartcards as follows: One Smartcard is for use in the VS-NfD area, and the second Smartcard is for the "Secret" area. The Smartcard for the VS-NfD area allows both reading and writing. The Smartcard for the "Secret" area allows only reading.

Subsequently, the "VS-NfD" Smartcard remains exclusively in the IT area designated for VS-NfD. The "Geheim" Smartcard is located exclusively in the "Geheim" IT area. If data is now transferred from the VS-NfD area to the "Geheim" area using a Kobra VS storage device, the system automatically ensures that the Kobra VS storage device operates in read-only mode when used on the "Geheim" system. Sensitive information classified as "Geheim" cannot be transferred to the Kobra VS storage device, either intentionally or unintentionally.

11.12 Use as an Authentication Medium

The Kobra VS storage device enables the secure storage of authentication credentials, such as usernames, highly complex passwords, digital certificates, key pairs, and others. However, the use of USB storage media is generally prohibited in some companies and organizations to prevent unintended data leakage.

Similar to its use as a data diode, the Kobra VS storage device can be configured so that, after the authentication components have been stored, the user has only read access. These storage devices can then be approved by the administrator for use on the company's IT network. In this way, every employee can receive a secure authentication medium without compromising the company's IT security.

11.13 Use as a Smartcard Reader with PIN Pad

The Kobra VS storage device can also be used as a Smartcard reader with a keypad for PIN entry or as an authentication token with a PIN pad. With this feature, users can use both the Kobra Infosec Smartcard and their own Smartcard to sign digital documents without having to purchase a separate card reader. This reduces both the number of devices required at a workstation and procurement costs.

The Kobra Infosec Smartcard can be configured, for example, for email encryption, VPN access, Windows or Linux login, and general two-factor authentication with a digital certificate.

To use it as a Smartcard reader with a PIN pad, the "Kobra Connect" software is required on the host systems.

11.14 Integration into Existing Smartcard and PKI Infrastructures

If a company is already using the Atos CardOS 5.0 or 5.3, CC EAL 4+ Smartcard (e.g., for access management, user authentication, etc.) or other Smartcards that meet the security requirements for VS-NfD, integration of the Kobra VS storage device is possible. In addition, the Kobra VS storage devices can be integrated into the PKI infrastructures of government agencies or companies. In this case, users can, for example, use their employee ID card to activate the storage device.

11.15 Integration of Existing Software Solutions

All software solutions for external storage devices already in use within the company can continue to be used as a supplement to expand security features and usage methods.

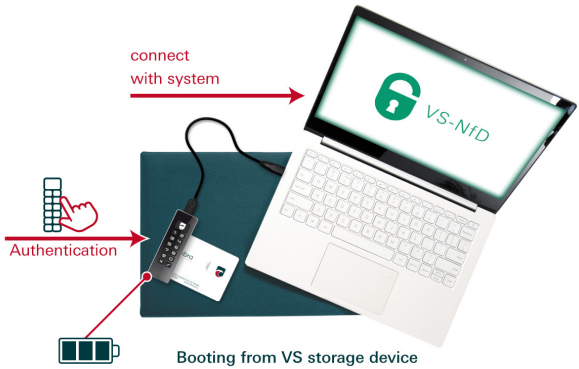
11.16 Use of VID, PID, SN, and DAK to Protect Corporate Data

Optionally, the USB Vendor ID (VID) and Product ID (PID) can be customized. Based on this information, as well as the serial number and the DAK (Device Authentication Key), Kobra VS storage devices can be uniquely assigned to different departments and user groups. These groups may also have different permissions for USB connections within the company's internal network. In this way, it is possible to specify which Kobra VS storage devices may be connected to which USB ports within the company. This prevents the connection of other "unauthorized" USB storage devices. Additional software may be required to control the USB ports on the host systems.

11.17 Secure Workstation with Read-Only Operating Systems (e.g. Windows)

Even after installing an operating system, the Kobra VS storage device can be set to read-only mode and then booted. This ensures that the operating system always remains in its original state and that processed data is never saved to this storage device. This is particularly useful for remote maintenance, remote access, or when processing content classified higher than VS-NfD.

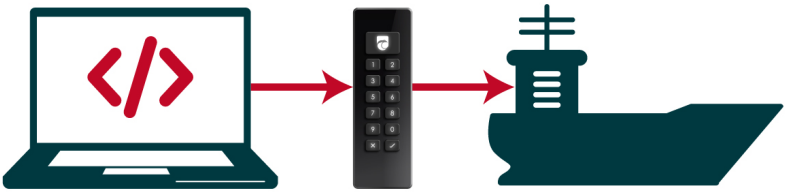
For updates or additional software, write protection can be disabled again. Specifically for Windows, we recommend using the "Kobra Connect" software to simulate a writable storage device at runtime.



11.18 Secure Software Deployment

A major advantage of Kobra VS storage devices is their hardware- and software-independent interoperability. This allows the storage media to be connected to all IT equipment, machines, and systems that support USB storage devices. "Secure Software Deployment" is used to provide specifically secured offline systems with software updates or initial installations.

It is important to note that information is not temporarily stored on an unencrypted storage device but can be transferred directly from the Kobra VS storage device to the system. Thus, these storage devices can be kept in close proximity to the relevant systems so they can be used for rapid system recovery in an emergency.



Typical use cases include:

- Updating PKI root systems,
- Installation and recovery of systems in the field,
- Initial setup of machines and equipment

11.19 Data-Logging

Due to its hardware- and software-independent interoperability, the Kobra VS storage device can also be connected to all information-processing equipment, machines, and systems to write log data from these hosts directly to the Kobra VS storage device without first temporarily storing the information in unencrypted form.

Typical use cases include:

- Log data from vehicles
- Camera recordings
- Evidence preservation from unknown systems

11.20 Two-Factor Authentication for Additional Applications

In general, the Kobra VS Smartcard reader is compatible with all software solutions that support CCID Smartcard readers. The included Kobra Smartcard can be programmed with additional certificates and keys using suitable PKI solutions. In these cases, the Kobra VS Smartcard reader functions as a Smartcard reader with a PIN pad and provides secure access to the Smartcard. The Smartcard contains additional certificates that correspond to the respective use case and meet its specifications. This reduces the number of hardware components required by end users.

Examples of applications include:

- UEFI preboot authentication for software-based hard disk encryption solutions such as R&S® Trusted Disk or Utimaco DiskEncrypt VS-NfD.
- Secure email encryption with software products such as Cryptovision GreenShield or GnuPG VS-Desktop.
- Secure VPN connections with software products such as R&S® Trusted VPN Client, GenuConnect, NCP VS GovNet Connector, or TheGreenBow.

The Kobra Connect software is required on the host systems.

11.21 Combined Use with Data Gateways

Data gateways such as PROVAIA, itWash, OPSWAT MetaDefender Kiosk, or the Hunna USB Sanitation System are becoming increasingly popular. They scan data from removable storage devices before it can be transferred to protected networks. , in this context, combining them with Kobra VS storage devices makes a lot of sense. This allows internal networks to be configured so that only specific Kobra VS storage devices can be connected.

This ensures that no unchecked media—whether intentionally or unintentionally—is connected to the protected networks. Furthermore, the Kobra VS storage device can be set to read-only mode after it has been written to with the verified data from the data gateway. This prevents any malware from reaching the storage device after the verification process.

In combination with the Kobra Defence Zone, this ensures that "cleaned" storage media are connected exclusively within the trusted networks. At the same time, it prevents unauthorized storage media from being connected to the trusted networks.

11.22 Password Manager

The combination of the Kobra VS storage device and established password manager software such as KeePass increases the level of protection for sensitive passwords.

On the one hand, the password database is securely stored in the encrypted memory of the Kobra VS storage device. On the other hand, access to the password database is only possible after prior two-factor authentication via the Smartcard in the Kobra VS storage device and the entry of a PIN.

11.23 Preventing Accidental or Unauthorized Deletion

In some situations—for example, after recording particularly sensitive information—it must be ensured that the user cannot destroy or modify the stored data.

To this end, the administrator uses the Kobra Client VS software to integrate a user with write permissions into the Kobra VS storage device so that this user can record the data, as well as a second user without write permissions so that this user can transport and analyze the data. For both users, the "Can delete DEK" function is disabled.

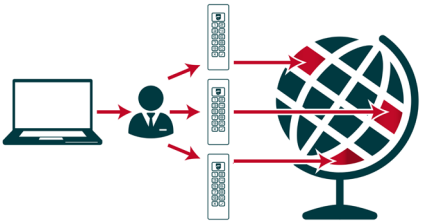
11.24 Geo-Redundant Backups and Instant Recovery

Up to 8 Smartcards can be integrated into the Smartcard table of a Kobra VS storage device. In addition, the administrator can configure the system so that certain users have neither write permissions nor the ability to delete DEK. This ensures both the integrity and availability of the stored data. Combined with robust protection against unauthorized access, these features make the Kobra VS storage device a top solution for geo-redundant backups and instant recovery.

To this end, in addition to the Smartcard of a globally responsible person, the Smartcards of one or more local users from different data centers or locations are also registered on the Kobra VS storage device.

The data copies are stored on multiple Kobra VS storage devices and distributed in a geo-redundant manner across data centers and locations that are geographically distant from one another. This ensures data security in the event of a local failure, a natural disaster, or any other incident at the primary location.

This method is also ideal for instant recovery: After a system failure, virtual machines or applications are back up and running in no time (often in minutes rather than hours). Instead of restoring the entire backup data set, the application is launched directly from the Kobra VS storage device. Onsly the data that is actually needed is made available in real time. This drastically reduces recovery time objectives (RTO) and ensures business continuity.



Summary:

- Protects backup data from unauthorized access
- Secure backups of project-related laptops
- Access granted via personal Smartcard or ID card
- Kobra VS storage devices can be distributed geographically across different locations and facilities
- In an emergency, data or VMs can be made available immediately
- Hardware write protection ensures the data integrity of the backup
- This ensures risk-free connection to live systems

11.25 Source Code Deposit

In custom software development, the client often requires the source code to be deposited to protect against failures on the part of the software vendor (e.g., bankruptcy). Under certain conditions, access to the source code must be provided to ensure the software can be maintained or further developed by the original vendor.

With the support of Kobra VS storage devices, this task can be easily accomplished. The source code is stored on a Kobra VS storage device and handed over to the client. The Smartcard, which grants access to this storage device, is deposited with a notary. If necessary, the client receives the Smartcard and can thus access the stored data.

This method safeguards the customer's investment, ensures operational continuity, and simultaneously protects the manufacturer's intellectual property.

11.25 Remote Management of Classified Kobra VS devices with TOM System

The R&S®Trusted Objects Manager (TOM) system is a centralized management system recommended by the BSI for data processing up to the VS-NfD, EU & NATO RESTRICTED classifications. It enables VS-NfD-approved remote management of Kobra VS storage devices for the military, government agencies, and companies, and can be used as a complementary solution to the "Kobra Client VS" software.

The administrator can easily and centrally provision the Kobra VS storage device for the respective use via the TOM system's web interface and the geographically distributed endpoints.

12. Optional accessories

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

12.1 Additional Smartcards

If required, additional approved Kobra Infosec Smartcards can be purchased. These are delivered with generated key pairs and have a pre-set User PIN and SO PIN with standard values. On how to get started, please refer to chapter 6.

12.2 Security Packaging

In order to detect unauthorized tampering, special Kobra VS security packaging is recommended for the dispatch of the Kobra VS devices and Kobra Infosec 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 "Kobra VS SECURITY" on the sides. In addition, there is a special seal at the top end to indicate any attempts at tampering.

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.

13. 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:	16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB, 1 TB
Memory types:	3D TLC, MLC and pSLC

Kobra Drive VS

Memory sizes:	500 GB, 1 TB, 2 TB, 4 TB, 8 TB, 16 TB
Memory types:	HDD, SSD

14. Scope of delivery

- Kobra VS storage device version 1.0
- 2 USB cables (USB-C to USB-C, USB-C to USB-A)
- 2 Kobra Infosec Smartcards (optional)
- Quick Start Guide

15. Data security, data availability and disclaimer

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.

Kobra Infosec 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.

16. 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.

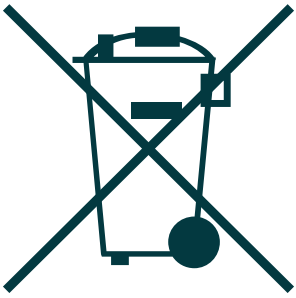
Note:

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

17. 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.



18. Handling Security Errors

The manufacturer provides an error management system for the administrators of Kobra VS storage devices for a controlled recording, classification and elimination of possible errors. In this chapter you will find instructions on how to register with the manufacturer and the exact steps for reporting suspected errors. All error management procedures can be accessed via the website https://kobra-infosec.de/de/all-support-sites/analysis.html or via the e-mail address vs@kobra-infosec.de.

18.1 Registration

For automatic notifications about possible security problems with your Kobra VS device, we recommend that you register at https://kobra-infosec.de/de/contact.html. Registering an e-mail address and selecting the product is mandatory, all other details are voluntary. It is also helpful to provide the serial numbers in order to be able to give more concrete recommendations for action in case of security risks.

After the successful registration you will receive a non-disclosure agreement, which you can sign and scan by e-mail to vs@kobra-infosec.de. After a check, you will be added to the distribution list and will receive a separate confirmation e-mail.

In addition to automatic notifications of potential security problems, you will receive email notifications of how to avoid these problems. If you wish, you can also receive notifications about firmware updates and new models.

If you do not wish to receive further information about security problems with your Kobra VS device, you can request to be removed from the distribution list at any time, just send an e-mail to
vs@kobra-infosec.de.

18.2 Reporting errors

As part of our continuous product improvement and maintenance, we regularly check whether the security services approved by the German Federal Office for Information Security (BSI) are still provided within the scope of VS-NfD despite new attack strategies. If you or a service provider had discovered a possible weakness, we would be grateful if you could inform us accordingly to improve security for all users.

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 communication about a possible vulnerability should be exclusively encrypted. This can be done either by using the form on https://kobra-infosec.de/de/contact.html or an encrypted email to vs@kobra-infosec.de. You can also find the S/MIME certificate and the PGP key at https://kobra-infosec.de/de/contact.html.

We require the following information for the correct classification and quick elimination of the possible error:

1) Model and version of the concerned device
2) Serial number of the device on which the error occurred
3) A description of the procedure to reproduce the type of error
4) What benefits can an attacker gain from this bug (optional)
5) Recommendations for remedying the error (optional)

Non-safety-critical errors and user-specific suggestions for improvement can also be reported to us using the contact method described above. Please direct general questions regarding the use and functionality of the Kobra VS storage medium to us via email at info@kobra-infosec.de, by phone at +49/345/2317353, or via the web form at https://kobra-infosec.de/de/contact.

19. FAQ

Here you'll find the most important FAQs about Kobra VS storage devices. For more FAQs, instructions, and videos, visit www.kobra-infosec.de

General

The Kobra VS data storage device remains in sleep mode after pressing the main button (all buttons are unlit).

The Kobra VS data storage device must be charged via a USB cable for a few minutes.

The main button is flashing red, and the other buttons are off

Check to see if a valid Smartcard has been inserted and if it is oriented correctly. The Smartcard must be inserted with the contacts facing up.

Smartcard inserted / not inserted

The main button flashes red while all the other buttons are off.

There are two possible reasons why the main button is flashing red:

A: There is no Smartcard inserted into the Kobra VS storage device.

B: A Smartcard is inserted the wrong way round (there is no contact with the card reader) or there is no chip present.

The main button flashes yellow while all other buttons are off.

A Smartcard is inserted correctly, but it is unknown for the Kobra VS storage device. A login is not possible. If you press the main button and the „1" button, the main button lights up blue.

The main button lights up white while all other buttons are off.

A Smartcard is inserted correctly and recognized by the Kobra VS storage device. However, the SO PIN and/or User PIN are locked. This Smartcard is not listed in the Smartcard table, or the Smartcard table has been deleted. (See Chapter 9.14, „Smartcard Table.")

Behavior After Entering and Confirming the User PIN

The main button flashes blue and all other buttons are unlit

The Kobra VS storage device formats itself automatically so that you can use it. Initial formatting also takes place if write protection was previously enabled or a new cryptographic key was generated. Formatting occurs when the Kobra VS storage device is connected to the host system for the first time, when the cryptographic key is changed, or when a new Smartcard table is created.

The main button flashes red once, and the Kobra VS storage device enters wait mode

There is no encryption key. This key should be generated after connecting the Kobra VS storage device to a computer (see Chapter 9.7, „9.7 Generating a new DEK (Data Encryption Key)“).

This response may occur if the cryptographic key has been deleted and has not yet been regenerated, or if a new Smartcard table containing multiple new Smartcards has been created, thereby interrupting the automatic cryptographic key generation process.

Note:

Please note that once a new cryptographic key has been generated, you will no longer be able to access the old data.

The main button flashes red once (or several times in a row), and the Kobra VS storage device enters wait mode

The User PIN was entered incorrectly. The main button flashes red briefly after each incorrect entry of the User PIN, corresponding to the number of failed attempts.

Note:

Please note that the User PIN will be locked if it is entered incorrectly too many times. A locked User PIN can be reset using the valid SO PIN (PUK).

The main button flashes yellow-red-yellow-red, and the Kobra VS storage deviceenters wait mode

The User PIN has been locked because it was entered incorrectly too many times.

Note:

A locked User PIN can be reset using the valid SO PIN (PUK). Please note, however, that the Kobra Infosec Smartcard will be permanently locked once the limit on the number of allowed failed attempts (10 attempts) to enter the SO PIN (PUK) has also been exceeded.

Further questions and solutions

The security enquiry has failed

The main button flashes red.
An incorrect User PIN was entered. Press the “Main Button”, next the “1” button and confirm by pressing the “√” button to restart the authentication process. (You have a maximum number of attempts, as set by the administrator.)

The storage device is not recognized

The drive icon is not displayed:
Make sure the Kobra VS storage device is connected to the host system via a working USB hub or extension cable. If necessary, try using a different USB cable or a different USB port on the host system.

Missing formatting / partition or unreadable file system:
For more information, see Chapter 10, „Formatting," in the Administrator's or User's guide.

A low-quality cable is being used:
Please use the USB cables included in the package and connect the USB plug to your host system.

The storage device is running slowly

Please check to make sure the Kobra VS storage device is properly connected to a USB port.

Ein anderes USB-Kabel wird verwendet:
Please use the USB cables included in the package and connect the USB plug to your host system.

Incorrect connection:
Check to see if the USB port is stable connected to the USB port on your host system.

The Kobra VS storage device was connected via a USB hub:
Make sure the Kobra VS storage device is not connected via a USB hub or extension cable.

Other devices are connected via the same port:
Please remove all other USB devices and see if the Kobra VS storage device runs faster afterward.

I can't write files to the Kobra VS storage device

Check to see if write protection is enabled (in this case, the main button will light up purple after authentication).

If write protection is not enabled (the main button lights up green after authentication), check to see if the hard drive is formatted with the correct file system for your operating system. The NTFS file system can only be used by Windows users.

Possible writing errors with MacOS
The encrypted Kobra VS storage device- Kobra Drive VS and KOBRA Stick VS- currently come standard with the FAT32 file system. These storage devices are also formatted with the FAT32 file system during the automatic formatting process that occurs after a key change. This file system enables data exchange with most Windows systems as well as with non-Windows systems such as macOS and Linux.

It may happen that some applications of MacOS (e.g. TextEditor software) encounter errors in the Fat32 file system. This problem can be solved as follows:

- Use another text editor software. This error does not occur with other MacOS text editors.

- Formatting the Kobra VS storage device in ExFAT. This file system has better compatibility with Windows as well as with different versions of MacOS and Linux.

To format a disk on macOS, use Disk Utility:

1. Connect the USB drive to the Mac and start Disk Utility from Applications, you can also find it e.g. via Spotlight search and under **Applications > Utilities**.
2. On the left side you will see the name of the USB drive.
3. Click on the name of the USB drive and switch to the **Delete tab**.
4. There you will see the Format option, where you can select the **ExFAT** format and the **Master Boot Record scheme**.
5. confirm with a click on **Delete**.

Glossary

Admin PIN

The administrator needs the Admin PIN to manage a Kobra VS storage medium and configure it in accordance with the company's security policy and the intended use cases.

AES (Advaned Encryption Standard)

AES is a secure, symmetric encryption algorithm used worldwide, in which the same key is used to both encrypt and decrypt data. It encrypts data in blocks with key lengths of 128, 192, or 256 bits and is considered very secure.

Crypto Key (Cryptographic Key)

A cryptographic key is a string of numbers, letters, or bits used in cryptography to encrypt and decrypt data. It ensures that only authorized individuals can access or read protected information. The security of an encryption method depends largely on the key being kept secret and sufficiently complex.

EU RESTRICTED / RESTREINT UE

EU RESTRICTED (French: RESTREINT UE) is the European Union's first classification level. Information classified at this level must be protected from unauthorized access, as its disclosure could harm the interests of the EU or a member state. Access is granted only to individuals who need it to perform their official duties.

German BDSG (Federal Data Protection Act)

The German Federal Data Protection Act supplements the General Data Protection Regulation and governs the handling of personal data in Germany. Among other things, it contains provisions for federal government agencies as well as specific regulations for businesses. Its purpose is to protect the rights of data subjects and ensure lawful data processing.

German BSI (Federal Office for Information Security)

The German Federal Office for Information Security (BSI) is the federal government's central cybersecurity authority. It develops standards and recommendations for information security and assists government agencies, businesses, and citizens in protecting their IT systems. In addition, the BSI issues warnings about current cyber threats and coordinates measures to enhance IT security.

German DSGVO (General Data Protection Regulation)

The German General Data Protection Regulation is a European Union regulation designed to protect personal data. It establishes uniform rules for the processing of personal data and strengthens the rights of data subjects, such as the right to access, rectification, and erasure. The goal of the German DSGVO is to ensure a high level of data protection within the EU and to facilitate the free flow of data.

German VSA (Classified Information Directive)
The Classification Directive governs the handling of classified information in federal agencies and other authorized federal entities. It specifies how information must be classified, marked, stored, transported, and destroyed. The purpose of the Classification Directive is to protect security-sensitive information from unauthorized access.

German VS-NfD
VS-NfD stands for "Classified – For Official Use Only" and is the first classification level for sensitive information in Germany. Documents with this classification may only be viewed and processed by authorized persons, as their unauthorized disclosure could harm the interests of the Federal Republic of Germany or a government agency. Special security and protection measures apply to the handling of VS-NfD data carriers and documents.

MLC (Multi-Level Cell):
MLC is a flash memory technology in which two or more bits are stored per memory cell. This allows for the production of higher-capacity storage media at a lower cost. Compared to SLC, however, MLC is slower, has a shorter lifespan, and is more prone to read and write errors.

NATO RESTRICTED
„NATO RESTRICTED" is NATO's first security classification. It designates information whose unauthorized disclosure could be detrimental to the interests of NATO or its member states. Access is restricted to authorized personnel on a need-to-know basis.

PKI Smartcard
A PKI Smartcard is a chip card that securely stores digital certificates and cryptographic keys. It is used for secure user authentication, as well as for encrypting and digitally signing data. By securely storing the keys, it provides greater security than purely software-based solutions.

pSLC (Pseudo Single-Level Cell):
pSLC is an operating mode in which MLC or TLC flash memory is used in such a way that only one bit is stored per memory cell. This significantly improves the memory's write speed, reliability, and lifespan. pSLC is frequently used in industrial applications where high data security and a long service life are important.

SO PIN (PUK)
The SO PIN (PUK) is required both to change the SO PIN (PUK) and to unlock the Kobra Infosec Smartcard after the User PIN has been locked.

User PIN
Using the User PIN, the user can authenticate (log in) to the Kobra VS storage device, generate a new cryptographic key, and change the User PIN. The user can also enable and disable write protection, provided they have the appropriate write permissions.

Ihre Notizen / Your Notes

Ihre Notizen / Your Notes

Ihre Notizen / Your Notes

Ihre Notizen / Your Notes

Kobra Infosec GmbH
Ernst-Thälmann-Straße 39
06179 Teutschenthal

Fon +49 / 3 45 / 2 31 73 53
Fax +49 / 3 45 / 6 13 86 97
Web: www.kobra-infosec.de
E-Mail: vs@kobra-infosec.de