Speed / Capacities

Kobra Drive VS
External encrypted
USB-C HDD / SSD

Kobra Stick VS
Encrypted
USB-C flash drive

The **Kobra VS storage** devices comply with the current state of technology, as regulated by the German Federal Office for Information Security (BSI), and enable GDPR-compliant data storage, retention, forwarding, and secure transport of sensitive, personal, and classified information up to the classification level VS-NfD (German public sector classification), RESTREINT UE/EU RESTRICTED and NATO RESTRICTED.

In addition to the Kobra Infosec Smartcards existing PKI-based company ID-, Service- and Troop ID Cards can be used for authentication. In terms of confidentiality, all data stored on the Kobra VS storage devices is protected against unauthorized access in case of loss or theft of the device.

Kobra Stick VS

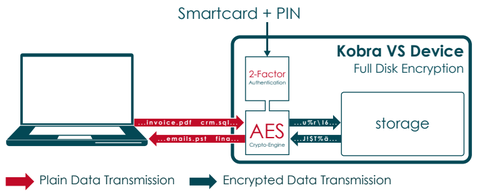
- Read/Write speed: up to 120 MB/s
- Capacities: 16GB, 32GB, 64GB, 128GB, 256GB, 512GB, 1TB

Kobra Drive VS

- Read/Write speeds:
  SSD: up to 300 MB/s
  HDD: up to 130 MB/s
- Capacities:
  HDD: 1TB, 2TB
  SSD: TB, 2TB, 4TB, 8TB, 16TB

Only industrial grade storage is built into the Kobra VS storage devices.

Features / Functions



- Users cannot bypass encryption
- Simple and secure
- Transparent and operating system-independent

Security features and technical information:

- Sturdy metal casing, resistant to splashes
- Distribution of roles between administrator and user
- Automatic formatting after key change
- Support for up to 8 smartcards (PKI cards)
- Operating system independent and bootable
- Management software Kobra Client VS
- Can be used as a smartcard-reader and boot device
- Lock-Out and Quick-Out functions
- Time out function (1 to 30 min)
- Read-Only Mode mechanism
- Integrated power supply

Optional configurations:

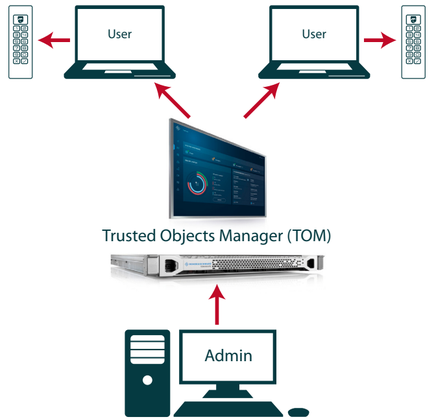
- pSLC memory (Kobra Stick VS)
- Custom laser engraving of logos, inventory numbers, scannable QR codes, labels, or other customer-specific markings
- Custom USB VID, PID & Serial Number
- Integration of PKI-based badges or smartcards

Security certificates:

- Approved by BSI for German VS-NfD, RESTREINT UE/EU RESTRICTED and NATO RESTRICTED - BSI-VSA-10737

R&S®Trusted Objects Manager

Remote management of VS storage devices with TOM



- Supplementary solution for Kobra Client VS
- Enables VS-NfD-approved remote management of Kobra VS storage devices for the military, public sector and corporations
- Remote management of VS storage devices via the TOM system's web interface and locally distributed endpoints
- Administrators can centrally and easily provide Kobra VS storage devices for specific use
- Central management system recommended by the BSI for data processing up to VS-NfD, EU & NATO RESTRICTED

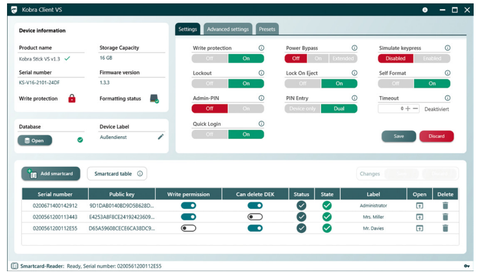
Software Kobra Connect

- Enables the creation of a Data Defence Zone
- Host system authentication on the storage device via HAK
- Storage device authentication on the host system via DAK
- The VS storage device automatically switches to read-only mode when connected to a system with a higher security classification
- Use of the VS storage device as a boot device in Windows read-only mode
- Use of the VS storage device as a smartcard-reader

Kobra Client VS

Central management software for Kobra VS storage devices

- Quick & application-specific configuration of Kobra VS storage devices
- Saving configurations as presets for specific use cases
- Read public keys and serial numbers of the smartcard (PKI card)
- Read smartcard table and write permissions of the respective smartcard owners
- Configure timeout, lock-out, admin PIN, and update key
- Access smartcard parameters directly via integrated database



+49 / 345 / 2317350
info@kobra-infosec.de
www.kobra-infosec.de

Kobra Infosec GmbH
Ernst-Thälmann-Str.39
D-06179 Teutschenthal
www.kobra-infosec.de

Kobra VS

Secure storage media for classified companies and governments

External encrypted hard disks and USB-C flash drives with approval by the German Federal Office for Information Security (BSI) for classified data up to

- VS-NfD
- EU RESTRICTED
- NATO RESTRICTED

Trust Seal
www.teletrust.de/itsmig

Encryption:
256-bit AES full-disk hardware encryption in XTS mode using two 256-bit cryptographic keys

Access Control:
Two-factor authentication using smartcard and PIN, based on the principle of "possession and knowledge"

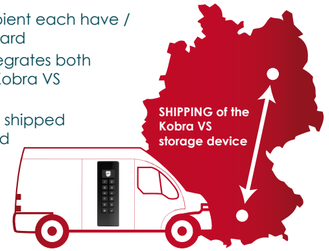
Cryptographic Keys Management:
Cryptographic keys can be created, modified, and deleted by the user using the smartcard.

Kobra VS

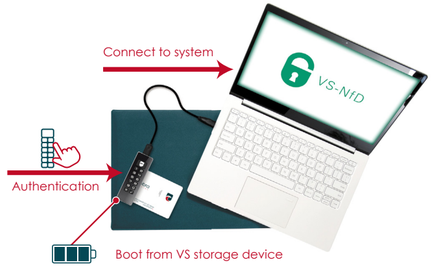
Encrypted storage devices
manufactured in germany

Simplified data transport

- Sender and recipient each have / receive a smartcard
- Administrator integrates both smartcards into Kobra VS storage device
- Kobra VS can be shipped without smartcard

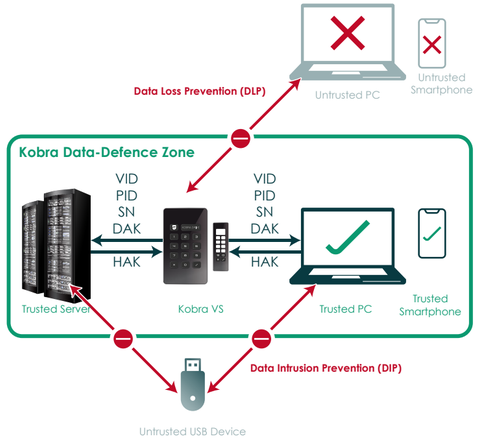


Secure mobile VS workstation (e.g., Linux, Mac OS, and Windows)



- Operating systems, applications and data are stored encrypted on the VS storage device before booting and after shutting down the PC
- Internal storage device is disabled/removed
- Integrated power supply for pre-boot authentication
- Power bypass during the boot process
- Deactivation of the "Lock on ejection" function
- Configuration as local/removable disk
- Extended service life due to pSLC memory (optional)

Data Defence Zone

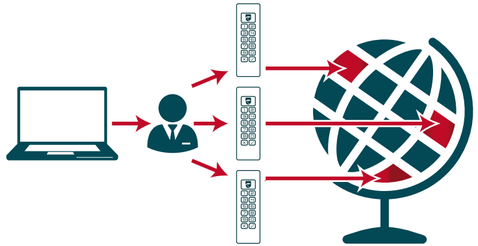


1. **Interface control:** VID (USB Vendor-ID), PID (Produkt-ID), SN (Serial number), DAK (Device Authentication Key)
2. **Host authentication:** HAK (Host authentication key)

- Processing of classified information on the go and in the home office
- Secure data exchange between protected stationary and mobile systems
- Data cannot leave the Data Defence Zone
- Mutual authentication: host system / VS storage device
- Storage device authentication on the host system via VID, PID, SN, and DAK
- Storage devices without an authorized cryptographic identity cannot be connected to host systems
- Authentication of the host system on the storage device with HAK
- Storage devices can only be connected to host systems with an authorized cryptographic identity

Possible Use Cases

Geo-redundant backups and instant recovery



- Protects backup data from unauthorized access
- Secure backups from project-related laptops
- Unlocking with personal smartcard or ID card
- Kobra VS storage devices can be distributed geo-redundantly across different sites and facilities
- In emergencies, data or VMs can be made available immediately
- Hardware write protection ensures the data integrity of backups
- Safe connection to live systems is ensured

Migration of server systems

- Kobra VS storage devices: Up to 16 TB of storage space
- Hardware write protection prevents data leakage from the target system
- Operation of multiple Kobra VS storage devices with a single smartcard

Secure Software Deployment

- Software is copied and transported to the deployment site / vehicle on an Kobra VS storage device
- Subsequently transferred, installed and updated on a target system
- Integrity and confidentiality of software systems and configurations are protected during transport

Log data from vehicles

- Log data from operational vehicles (aircraft, ships, helicopters, commercial vehicles) is encrypted on the Kobra VS storage device after the mission and transported to the analysis center.

Source Code Escrow

- Source code is stored on the Kobra VS storage device and handed over to the client
- Access smartcard is deposited with a notary
- Should the need arise, the client is given the smartcard to access the data.

Card reader and two-factor authentication

- Card reader and storage device in one device
- Digital signing of documents and files
- Login on Windows, Linux or macOS
- E-mail encryption
- VPN and cloud access

Read-Only Windows / OS

- Enabled write protection: No unwanted leakage of information
- Users cannot modify system data
- Processed information is never permanently stored on the Kobra VS storage device
- Simple software system updates by exchanging storage devices via regular mail
- Fast booting through flash memory

Use as data diode

- Enabled write protection to prevent unwanted leakage of information from higher-classified systems into lower-classified systems
- Administrator configures two smartcards with the following access rights:
  Smartcard 1 for work in the restricted system (read and write)
  Smartcard 2 for the secret classified system (read-only)