

Geschwindigkeit / Kapazitäten

Eigenschaften und Funktionen

R&S®Trusted Objects Manager

Kobra Client VS



VS-Datenträger

Sichere Speichermedien für geheimhaltungsbetonte Unternehmen und Behörden

Kobra Drive VS
Externe verschlüsselte USB-C HDD / SSD

Kobra Stick VS
Verschlüsselter USB-C Speicher Stick



Die **Kobra VS-Datenträger** entsprechen dem aktuellen Stand der Technik und ermöglichen die DSGVO-, BDSG- und VSA-konforme Speicherung, Aufbewahrung, Weitergabe sowie den sicheren Transport sensibler, personenbezogener und VS-ingestufte Informationen bis zum Geheimhaltungsgrad VS-NfD (Verschlussache - NUR FÜR DEN DIENSTGEBRAUCH), RESTREINT UE/EU RESTRICTED und NATO RESTRICTED.

Für die Authentisierung können neben den Kobra Smartcards auch PKI-basierte Werks-, Dienst- und Truppenausweise verwendet werden. Im Hinblick auf die Vertraulichkeit sind somit alle auf den Kobra VS-Datenträgern gespeicherten Daten vor unbefugten Zugriffen, bei Verlust oder Entwendung, geschützt.

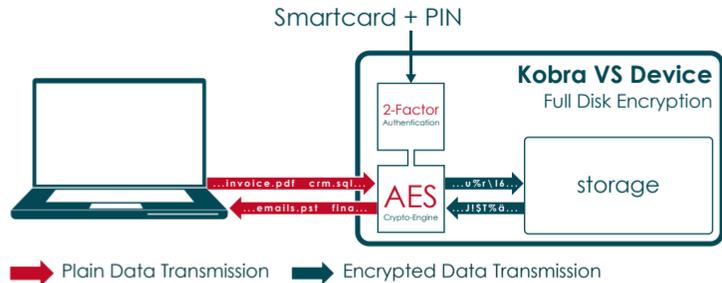
Kobra Stick VS

- Lese-/Schreibgeschwindigkeit: bis zu 120 MB/s
- Kapazitäten: 16GB, 32GB, 64GB, 128GB, 256GB, 512GB, 1TB

Kobra Drive VS

- Lese-/Schreibgeschwindigkeit:
 - SSD: bis zu 300 MB/s
 - HDD: bis zu 130 MB/s
- Kapazitäten:
 - HDD: 1TB, 2TB
 - SSD: TB, 2TB, 4TB, 8TB, 16TB

Für die Kobra VS-Datenträger werden ausschließlich hochwertige Industriespeicher verwendet.



- Nutzer können Verschlüsselung nicht umgehen
- Einfach und sicher
- Transparent und betriebssystemunabhängig

Sicherheitsfunktionen und technische Informationen:

- Stabiles, vor Spritzwasser geschütztes Metallgehäuse
- Rollenaufteilung zwischen Administrator & Benutzer
- Automatische Formatierung nach Schlüsselwechsel
- Bis zu 8 Smartcards (PKI-Karten) integrierbar
- Betriebssystemunabhängig und bootfähig
- Verwaltungssoftware Kobra Client VS
- Verwendung als Smartcard-Reader & Boot-Devices
- Lock-Out- & Quick-Out-Funktionen
- Time-Out-Funktion (1 bis 30 min)
- Schreibschutz-Mechanismus
- Integrierte Stromversorgung

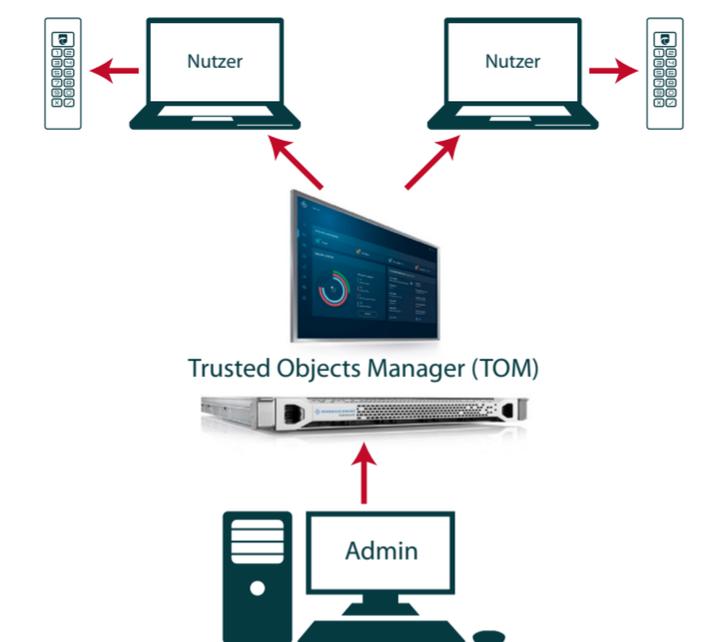
Optionale Konfigurationen:

- pSLC-Speicher (Kobra Stick VS)
- Lasergravur von Logo, Inventarnummern, scannbaren QR-Codes, Bezeichnungen o.Ä. nach Wunsch
- Kundenspezifische USB-VID, -PID und Seriennummer
- Integration PKI-basierter Ausweise & Smartcards

Sicherheitszertifikat:

- Zulassung durch das BSI bis VS-NfD RESTREINT UE / EU RESTRICTED und NATO RESTRICTED - BSI-VSA-10737

Fernverwaltung von VS-Datenträgern mit TOM-System



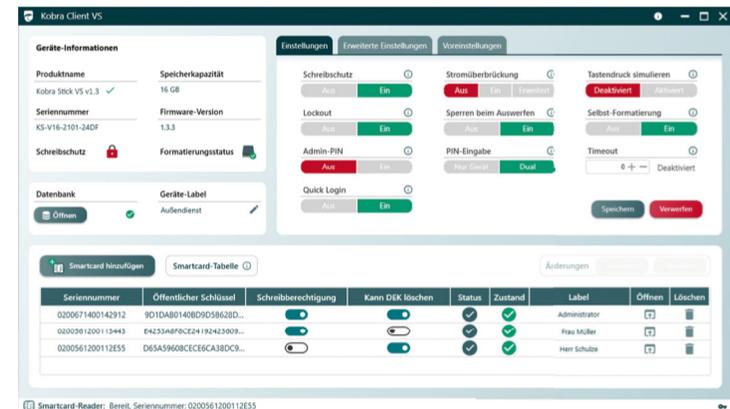
- Ergänzende Lösung für Kobra Client VS
- Ermöglicht VS-NfD-Zugelassene Verwaltung von Kobra VS-Datenträgern bei Militär, Behörden und Unternehmen aus der Ferne
- Fernverwaltung VS-Datenträger über Web-Interface des TOM-Systems & örtlich verteilte Endpoints
- Administrator kann Kobra VS-Datenträger aus der Ferne einfach und zentral für jeweilige Verwendung bereitstellen
- Zentrales Managementsystem mit einer BSI-Empfehlung zur Datenverarbeitung bis VS-NfD, EU & NATO RESTRICTED

Software Kobra Connect

- Ermöglicht den Aufbau einer Data Defence Zone
- Authentisierung des Host-Systems am Datenträger mit HAK
- Datenträger-Authentisierung am Host-System mit DAK
- Automatische Versetzung des VS-Datenträgers in den schreibgeschützten Zustand bei Verbindung mit einem höher eingestuftem System
- Nutzung des VS-Datenträgers als Boot-Device im Windows-Read-Only-Modus
- Nutzung des VS-Datenträgers als Smartcard-Reader

Zentrale Verwaltungssoftware für Kobra VS-Datenträger

- Schnelle & einsatzbezogene Konfiguration der Kobra VS-Datenträger
- Speicherung vorgenommener Konfigurationen als Voreinstellung für spezifische Einsatzszenarien
- Auslesen öffentlicher Schlüssel & Seriennummern der Smartcard (PKI-Karte)
- Auslesen Smartcard-Tabelle & Schreibberechtigung der jeweiligen Smartcard-Besitzer
- Konfiguration von Time-Out, Lock-Out, Admin-PIN, Update-Schlüssel
- Direkter Zugriff auf Smartcard-Parameter durch integrierte Datenbank



+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

Externe verschlüsselte Festplatten und USB-Sticks mit BSI-Zulassung für staatliche Verschlussachen bis

- VS-NfD
- EU RESTRICTED
- NATO RESTRICTED

Erhältlich im Kaufhaus des Bundes
RV-Nr. 21413



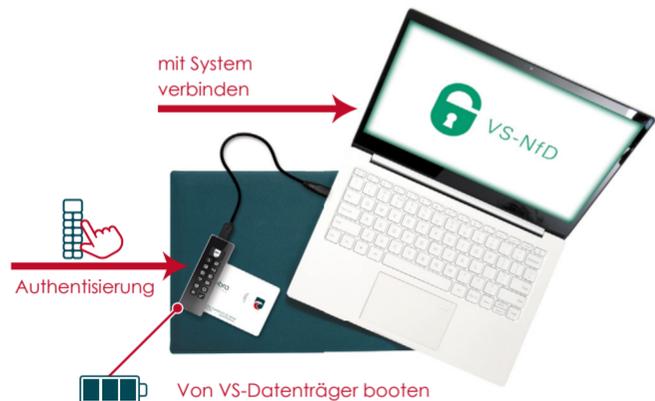
- **Verschlüsselung:** 256 Bit AES Full-Disk Hardware-Verschlüsselung im XTS-Modus mittels zweier 256 Bit Krypto-Schlüssel
- **Zugriffskontrolle:** Zwei-Faktor-Authentifizierung mittels Smartcard und PIN nach dem Prinzip „Besitzen und Wissen“
- **Verwaltung der kryptografischen Schlüssel:** Die kryptografischen Schlüssel können vom Benutzer mit der Smartcard erstellt, geändert und zerstört werden

Vereinfachter Datentransport

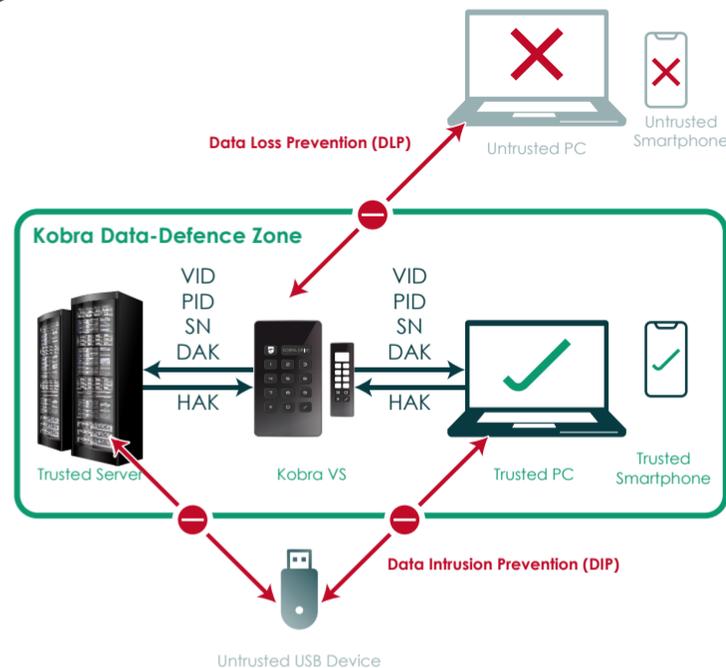
- Absender und Empfänger besitzen / erhalten je eine Smartcard
- Administrator integriert beide Smartcards in VS-Datenträger
- Versand ohne Smartcard nach Datenaufnahme



**Sicherer mobiler VS-Arbeitsplatz
(z.B. Linux, Mac OS und Windows)**



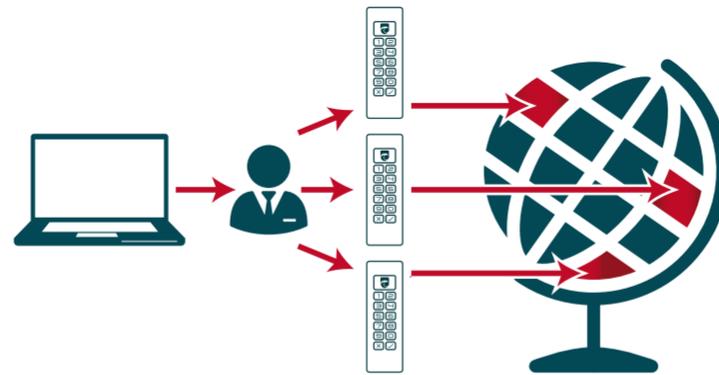
- Betriebssysteme, Anwendungen und Daten sind auf VS-Datenträger vor dem Booten & nach dem Ausschalten des PCs verschlüsselt gespeichert
- Interne Festplatte wird deaktiviert/entfernt
- Integrierte Stromversorgung zur Pre-Boot-Authentisierung
- Stromüberbrückung im Boot-Vorgang
- Ausschalten der Funktion "Sperrern beim Auswerfen"
- Konfiguration als lokaler-/Wechseldatenträger
- Erhöhung der Lebensdauer durch pSLC-Speicher



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

- Verarbeitung eingestufter Informationen unterwegs und im Homeoffice
- Sicherer Datenaustausch zwischen geschützten stationären und mobilen Systemen
- Daten können Data-Defence-Zone nicht verlassen
- Gegenseitige Authentisierung: Host-System / VS-Datenträger
- Datenträger-Authentisierung am Host-System mit VID, PID, SN und DAK
- Datenträger ohne erlaubte kryptografische Identität können an Host-Systeme nicht angeschlossen werden
- Authentisierung des Host-Systems am Datenträger mit HAK
- Datenträger können nur an die Host-Systeme mit erlaubter kryptografischer Identität angeschlossen werden

Geo-Redundante Backups und Instant Recovery



- Schützt Backup-Daten vor unberechtigtem Zugriff
- Sichere Backups von projektbezogenen Laptops
- Freischaltung mit eigener Smartcard oder Ausweis
- VS-Datenträger können geo-redundant an verschiedenen Standorten und Objekten verteilt werden
- Im Notfall können Daten oder VMs sofort bereitgestellt werden
- HW-Schreibschutz sichert die Datenintegrität des Backups
- Somit erfolgt der Anschluss an Live-Systeme risikofrei

Migration von Serversystemen



- Kobra Drive VS: Bis zu 16 TB Speicherplatz
- Hardware-Schreibschutz verhindert Datenabfluss vom Zielsystem
- Bedienung mehrerer VS-Datenträger mit einer Smartcard

Secure Software Deployment



- Software wird vom Quell-System auf VS-Datenträger kopiert und zum Einsatzort / Fahrzeug transportiert
- Anschließend erfolgt Übertragung, Installation und Aktualisierung auf ein Zielsystem
- Schutz der Integrität und Vertraulichkeit von Software-Systemen und Konfigurationen während des Transports

Log-Daten aus Fahrzeugen



- Log-Daten von Einsatzfahrzeugen (Flugzeuge, Schiffe, Hubschrauber, Nutzfahrzeuge) werden nach Einsatz verschlüsselt auf dem Kobra VS Datenträger gespeichert und zur Auswertungsstelle transportiert

Quellcode Hinterlegung



- Quellcode wird auf Kobra VS-Datenträger gespeichert und Auftraggeber übergeben
- Hinterlegung der Zugriffs-Smartcard bei Notar
- Im Bedarfsfall erhält Auftraggeber Smartcard und somit Zugriff auf Daten

Kartenleser und Zwei-Faktor-Authentifizierung



- Kartenleser und Datenträger in einem Gerät
- Digitale Signierung von Dokumenten und Dateien
- Anmeldung unter Windows, Linux oder macOS
- E-Mail-Verschlüsselung
- VPN- und Cloud-Zugriff

Read-Only Windows / OS



- Aktivierter Schreibschutz: Kein unerwünschtes Abfließen von Informationen
- Benutzer kann Systemdaten nicht ändern
- Verarbeitete Informationen werden nie dauerhaft auf Kobra VS-Datenträger gespeichert
- Einfaches Update der Softwaresysteme durch Austausch der Datenträger per normalem Postversand
- Schnelles Booten durch Flash-Speicher

Verwendung als Datendiode



- Aktivierter Schreibschutz, um das unerwünschte Abfließen von Informationen aus höher eingestuft Systemen in niedriger eingestufte Systeme zu verhindern
- Administrator konfiguriert zwei Smartcards mit folgenden Zugriffsrechten: Smartcard 1 für die Arbeit im VS-NfD-Bereich (Lesen und Schreiben), Smartcard 2 für den geheimen Bereich (nur Lesen)