Kobra Infosec

Benutzerhandbuch

Kobra VS-Datenträger

Externe verschlüsselte USB-C-Festplatte und USB-C-Stick

für Behörden, Konzerne und
geheimschutzbetreute Unternehmen

Version 1.3
07.08.2026

BITTE LESEN SIE DIE ANLEITUNG SORGFÄLTIG UND FOLGEN SIE DEN ANWEISUNGEN.

EINE FEHLERHAFTE BEDIENUNG KANN ZU SCHÄDEN AN DEM KOBRA VS-DATENTRÄGER SOWIE ZU DATENVERLUSTEN FÜHREN.

Die digitale Fassung des Handbuchs kann im Download-Center der Kobra Infosec GmbH heruntergeladen werden:
https://kobra-infosec.de/de/all-support-sites/support.html

Produktversion:	Kobra Drive VS, Kobra Stick VS (1FF) und Kobra Stick VS (2FF) - (Kobra VS-Datenträger) Version 1.0
Benutzerhandbuch:	Version 1.3 (Stand 07.08.2026)

Inhaltsverzeichnis

1. Über die Kobra VS-Datenträger: Kobra Drive VS und Kobra Stick VS

Die externen verschlüsselten Datenträger Kobra Drive VS sowie Kobra Stick VS (1FF) und Kobra Stick VS (2FF) sind eine externe USB-C-Festplatte (HDD/SSD) und USB-C-Speicherstick mit hardwarebasierter Verschlüsselung in stabilen, eleganten Metallgehäusen mit integrierter Eingabetastatur. Die Geräte erbringen die gleichen Sicherheitsleistungen und unterscheiden sich ausschließlich in der Bauform und den möglichen Speicherkapazitäten. Daher werden diese im vorliegenden Administratorhandbuch als Kobra VS-Datenträger bezeichnet.

Die Kobra VS-Datenträger ermöglichen die datenschutzgerechte Speicherung und Aufbewahrung sowie den sicheren Transport sensibler, personenbezogener und vertraulicher Informationen bis zur Geheimhaltungsstufe NATO Restricted, EU Restricted und VS-NfD (Verschlusssache - Nur für den Dienstgebrauch). Diese Datenträger wurden unter Berücksichtigung der „Technischen Richtlinien" des BSI in Deutschland entwickelt und hergestellt. Sie verfügen über das Vertrauenszeichen „IT-Security made in Germany" und entsprechen dem aktuellen Stand der Technik. Aufgrund ihrer Sicherheitsfunktionen sind die Kobra VS-Datenträger aktuell eine der sichersten Möglichkeiten, Daten mobil zu speichern.

Die auf dem Kobra VS-Datenträger gespeicherten Daten sind im Hinblick auf die Vertraulichkeit der Informationen vor unbefugten Zugriffen geschützt, etwa wenn der Kobra VS-Datenträger verloren, verlegt oder entwendet wird. Dabei hält er logischen und physikalischen Angriffen stand.

Die Kobra Drive VS werden sowohl als HDD- als auch als SSD-Varianten angeboten. Die optionale Verwendung als SSD-Datenträgern bei der Kobra Drive VS bietet zusätzlichen Schutz vor Stößen und Erschütterungen. Die Datenübertragung und Stromversorgung erfolgen über den USB-C-Anschluss. Der Kobra Stick VS (1FF) und der Kobra Stick VS (2FF) bieten die gleichen Sicherheitsleistungen wie die Kobra Drive VS in einem noch kompakteren Format.

Die Auslieferung der Kobra VS-Datenträger kann in einer PKI-basierten- oder in einer Stand-Alone-Umgebung erfolgen. Darin unterscheiden sich grundlegend zwei Anwendungsszenarien:

In der PKI-basierten Variante werden einzig Kobra VS-Datenträger zur Verfügung gestellt. Die Einrichtung dieser erfolgt durch die Administratoren des Nutzers. Daher werden auch die PKI-bezogenen Eigenschaften des Kobra VS-Datenträgers durch die IT-Sicherheitskonzepte des Administrators geregelt.

Dabei handelt es sich vor allem um die Generierung und Speicherung des Schlüsselpaares (bestehend aus einem öffentlichen und einem privaten Schlüssel), die Benutzer- und SO-PIN (PUK), SO-PIN-Vorgaben (Länge und Anzahl der Fehlversuche) sowie die sonstigen organisatorischen Maßnahmen. Deshalb werden im Folgenden die Eigenschaften des Kobra VS-Datenträgers, überwiegend bezüglich der Stand-Alone-Umgebung, detailliert beschrieben.

Das Stand-Alone-Szenario (auch eigenständiges Szenario genannt) beinhaltet dagegen die Lieferung des Kobra VS-Datenträgers zusammen mit zwei Kobra Infosec-Smartcards (Atos CardOS 5.3, CC EAL 4+) im komplett voreingestellten Zustand. Dieser Kobra VS-Datenträger kann grundsätzlich bei dringendem Bedarf sofort verwendet werden. In der VS-NfD-zugelassenen Konfiguration darf der Nutzer den Kobra VS-Datenträger jedoch erst in Betrieb nehmen, nachdem er zuvor die Benutzer- und SO-PIN (PUK) geändert und einen neuen Krypto-Schlüssel auf dem Kobra VS-Datenträger selbst generiert hat.

Um die Sicherheitseigenschaften des Kobra VS-Datenträgers im vollen Umfang und innerhalb des Geltungsbereichs der VS-NfD-Zulassung zu nutzen, sind folgende Schritte erforderlich:

- Gewährleisten Sie, dass an Ihrem Host-System ein angemessener Schutz für alle aus dem geschützten Speicherbereich des Kobra VS-Datenträgers aufgerufenen Daten besteht
- Überprüfen Sie nach Erhalt des Kobra VS-Datenträgers die Vollständigkeit und die Richtigkeit der Lieferung (Kapitel 15. Lieferumfang)
- Überprüfen Sie über das Host-System, ob die USB-Eigenschaften des Datenträgers mit der Modellbezeichnung und der Seriennummer auf der Rückseite des Kobra VS-Datenträgers übereinstimmen (Kapitel 4. Echtheitsprüfung)
- Ändern Sie die Benutzer- und SO-PIN (PUK) auf beiden Kobra Infosec-Smartcards (Kapitel 9.3 Ändern der Benutzer-PIN , Kapitel 4.3.3 SO-PIN/PUK ändern im Kobra Client VS Handbuch)
- Ändern Sie die Admin-PIN, falls Sie über Administrator-Rechte verfügen (Kapitel 9.6 Ändern oder Ausschalten der Admin-PIN)
- Bei der Wahl der Admin-, Benutzer- und SO-PIN (PUK) sollen Trivial-PINs vermieden und die Standard-PINs ausgeschlossen werden.
- Generieren Sie einen neuen Krypto-Schlüssel auf dem Kobra VS-Datenträger (Kapitel 9.7 Generieren eines neuen Krypto-Schlüssels)
- Überprüfen Sie, ob die Anmeldung mit allen freigeschalteten Kobra Infosec-Smartcards (bzw. Ihrer PKI-Karte) möglich ist
- Behandeln Sie Ihre Authentifizierungsmerkmale (Smartcard und PIN) vertraulich

Eine ausführliche Beschreibung der oben genannten Schritte finden Sie in diesem Benutzerhandbuch und im Administratorhandbuch in den entsprechenden Kapiteln. Die Modellbezeichnung sowie die Seriennummer befinden sich auf der Rückseite des jeweiligen Kobra VS-Datenträgers. Diese Informationen sind mithilfe der mitgelieferten Kobra Client VS Software und über die USB-Geräte-Informationen am Host-System abrufbar.

2. Sicherheitsmechanismen

Der Kobra VS-Datenträger gewährleistet die Vertraulichkeit der Daten durch folgende Sicherheitsmechanismen:

- Verschlüsselung
- Zugriffskontrolle
- Schlüsselverwaltung
- Benutzerverwaltung

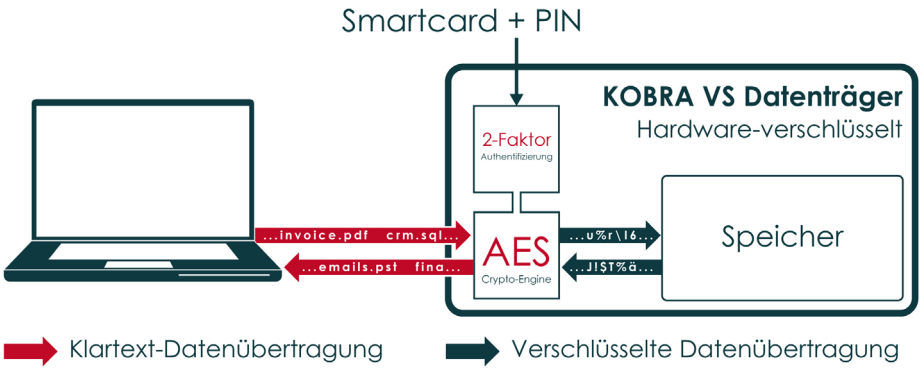
2.1 Verschlüsselung

- 256 Bit AES Full-Disk-Verschlüsselung im XTS-Modus

Das im Sicherheitsgehäuse integrierte Verschlüsselungsmodul führt eine komplette Verschlüsselung des Kobra VS-Datenträgers durch. Jedes gespeicherte Byte und jeder beschriebene Sektor auf dem Kobra VS-Datenträger wird nach 256 Bit AES (Advanced Encryption Standard) im XTS-Modus mittels zweier kryptografischer Schlüssel mit jeweils 256 Bit verschlüsselt.

Der Kobra VS-Datenträger verschlüsselt außerdem die gesamte Partition. Dies umfasst ebenfalls auf der Partition geschriebene temporäre Dateien und Boot-Sektoren, welche von Verschlüsselungssoftware oft unbeachtet bleiben.

Die Hardwareverschlüsselung ermöglicht die Verwendung des Kobra VS-Datenträgers unabhängig vom Anwenderbetriebssystem und erfolgt transparent. Der Zugriff auf die Daten findet ohne Einschränkungen der Lese- und Schreibgeschwindigkeit statt.



2.2 Zugriffskontrolle

Die Zugriffskontrolle erfolgt nach dem Prinzip „Besitzen und Wissen": Für den Zugriff auf die Daten muss der Benutzer eine passende Smartcard besitzen und die richtige Benutzer-PIN kennen.

Die Kobra Infosec-Smartcard wird automatisch gesperrt, sobald die zulässige Anzahl der fehlerhaften PIN-Eingaben überschritten wurde. Die Freischaltung gesperrter Kobra Infosec-Smartcards kann durch die Eingabe der SO-PIN (PUK) erfolgen. Die unwiderrufliche Sperre der Kobra Infosec-Smartcard tritt ein, sobald die zulässige Anzahl der fehlerhaften Eingaben der SO-PIN (PUK) ebenfalls überschritten wurde. Anschließend ist der Zugriff auf die Daten nur mit einer anderen für diesen Kobra VS-Datenträger freigeschalteten Smartcard und der korrekten PIN-Eingabe möglich.

Für die PKI-Karten werden diese Eigenschaften durch die IT-Sicherheitskonzepte und internen Richtlinien der Administratoren geregelt.

2.3 Schlüsselverwaltung

Die beiden für die Ver- und Entschlüsselung der Daten zuständigen 256-Bit-Verschlüsselungsschlüssel stehen in unmittelbarer Beziehung zum Krypto-Schlüssel. Daher fokussiert sich die Schlüsselverwaltung auf die Erzeugung, Speicherung sowie auf die Änderung und Vernichtung des Krypto-Schlüssels. Er wird auf dem Kobra VS-Datenträger mittels Verwendung einer auf der Kobra Infosec-Smartcard generierten Zufallszahl erzeugt und in einem sicheren Bereich so verschlüsselt gespeichert, dass er nur durch die zugelassenen Smartcards entschlüsselt werden kann.

Zur Ver- und Entschlüsselung der Daten wird der verschlüsselte Krypto-Schlüssel nach der korrekten Eingabe der Benutzer-PIN mithilfe der Smartcard entschlüsselt und dem Verschlüsselungsmodul des Kobra VS-Datenträgers zur Verfügung gestellt. Mit der Kobra Infosec-Smartcard (bzw. PKI-Karte) und der Benutzer-PIN kann der Benutzer jederzeit den Krypto-Schlüssel auf dem Kobra VS-Datenträger generieren, ändern und zerstören (Kapitel 9.7 Generieren eines neuen Krypto-Schlüssels, Kapitel 9.8 Löschen eines Krypto-Schlüssel).

Diese Vorgänge sind irreversibel. Nach der Erzeugung eines neuen Krypto-Schlüssels werden der alte Krypto-Schlüssel und somit alle auf dem Kobra VS-Datenträger gespeicherten Daten endgültig vernichtet. Daher müssen die gespeicherten Informationen unter Umständen zuvor auf einem anderen VS-NfD- und/oder **Nato-Restricted-/EU-Restricted-**zugelassenen Datenträger gesichert werden.

2.4 Benutzerverwaltung

Für einen VS-Datenträger können mehrere Benutzer freigegeben werden. Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

3. Eigenschaften und Besonderheiten

Die Kobra VS-Datenträger verfügen über zahlreiche Alleinstellungsmerkmale.

3.1. Eigenschaften im Überblick

Verschlüsselung

- 256-Bit-AES-Full-Disk-Hardwareverschlüsselung im XTS-Modus mit zwei kryptografischen Schlüsseln
- 2-Faktor-Authentisierung mittels Kobra Infosec-Smartcard (bzw. PKI-Karte) und PIN-Eingabe
- Externe Speicherung des Schlüssels zur Entschlüsselung des Krypto-Schlüssels
- Erstellen, Ändern und Zerstören des Krypto-Schlüssels durch den Nutzer
- Hardwarebasiertes Verschlüsselungsmodul (Datenverschlüsselung aller gespeicherten Bytes und beschriebenen Sektoren)

Sicherheit ergänzende Funktionen

- Integrierter Schreibschutz-Mechanismus
- Time-Out-Funktion
- Quick-Out-Funktion
- Lock-Out-Funktion

Interoperabilität

- Pre-Boot-Authentisierung und Boot-Fähigkeit
- Unabhängig von Betriebssystemen (Unterstützung aller Betriebssysteme, Multimediageräte und Maschinen mit USB-Datenträger-Unterstützung)
- Kompatibel mit USB 3.0 und USB 2.0
- Keine Einschränkungen der Lese- und Schreibgeschwindigkeit
- Interne Stromversorgung, die eine Authentisierung ohne Anschluss an einen PC oder USB-Hub ermöglicht

PKI Kompatibilität

- Unterstützung von verschiedenen PKI-Karten
- Verwendbar als Smartcard-Reader mit PIN-Pad (CCID)

Mechanischer Schutz

- Robustes Metallgehäuse

Personalisierung

- USB VID, PID & Seriennummer nach Kundenvorgaben definierbar
- Hochwertige Lasergravur auf der Rückseite des Kobra VS-Datenträgers

3.2 Vorteile des Kobra VS-Datenträgers

Einfache und sichere Handhabung

Anschließen, Anmelden, Verwenden

Sichere Speicherung von Verschlusssachen

Vertrauliche Informationen von Behörden und Unternehmen bis zur Geheimhaltungsstufe VS-NfD können auf den Kobra VS-Datenträgern VSA-konform gespeichert werden.

Transparenter Einsatz

Durch die Hardwareverschlüsselung werden alle Daten automatisch und ohne Performanceverluste sofort verschlüsselt gespeichert.

EU-DSGVO Konform

Personenbezogene Daten können dem Stand der Technik entsprechend gemäß den Forderungen von EU-DSGVO und BDSG gespeichert werden.

PKI-Integration

Integrationsmöglichkeit in bereits bestehende PKI-Infrastrukturen bei Behörden und Unternehmen.

3.3 Smartcard

Serienmäßig wird der Kobra VS-Datenträger mit zwei nach Common Criteria EAL4+ zertifizierten Kobra Infosec-Smartcards (Atos CardOS 5.3, CC EAL 4+) ausgeliefert. In der Stand-Alone-Umgebung sind für die Benutzung gemäß VS-NfD-Zulassung vorerst nur diese Kobra Infosec-Smartcards genehmigt. Außerdem können eigene PKI-Karten des Nutzers verwendet werden. Auf diesem Wege besteht die Möglichkeit, die Kobra VS-Datenträger als Bestandteil in die PKI-Infrastruktur des Nutzers zu integrieren. In speziellen Fällen kann geprüft werden, ob auch andere kundenspezifische Smartcards bzw. PKI-Karten integrierbar sind. Sollten die PKI-Karten weder auf Atos CardOS 5.0 noch CardOS 5.3 oder höher basieren, so ist eine Rücksprache mit dem BSI erforderlich, ob diese Smartcards eine ausreichende Schutzleistung für VS-NfD erbringen.

Die Kobra Infosec-Smartcards werden für die Kobra VS-Datenträger Kobra Drive VS und Kobra Stick VS (1FF) im EC-Karten-Format geliefert. Der Kobra Stick VS (2FF) wird mit den Kobra Infosec-Smartcards im Mini-SIM-Karten-Format ausgestattet. Sie werden in den folgenden Kapiteln als „Kobra Infosec-Smartcard“ bezeichnet. Die Kobra Infosec-Smartcard ermöglicht sowohl den Zugang zu den Daten auf dem Kobra VS-Datenträger als auch das Erstellen, Ändern und Zerstören des Krypto-Schlüssels sowie die Ver- und Entschlüsselung des Kobra VS-Datenträgers. Die Verwaltung des Krypto-Schlüssels erfolgt auf dem Kobra VS-Datenträger mithilfe der Kobra Infosec-Smartcard (bzw. PKI-Karte) und der Benutzer-PIN völlig unabhängig von einem PC.

Für die Anmeldung am Kobra VS-Datenträger verfügen die Kobra Infosec-Smartcards bei der Auslieferung über eine Benutzer- und SO-PIN (PUK) mit Standard-Werten (Kapitel 3.7 Menü-Übersicht, Kommandos und Werkseinstellungen). Alle Kobra

Infosec-Smartcards verfügen über unterschiedliche Seriennummern sowie gespeicherte Schlüsselpaare, die aus öffentlichem und privatem Schlüssel bestehen. Auf der Vorderseite der Kobra Infosec-Smartcard sind die Modellbezeichnung und die Seriennummer der jeweiligen Smartcard aufgetragen.

Mithilfe der Kobra Client VS Software kann der Administrator bis zu 8 Kobra Infosec-Smartcards oder PKI-Karten für einen Kobra VS-Datenträger freigeben und die Berechtigungen der jeweiligen Nutzer unterschiedlich definieren. Dies geschieht durch die Eintragung der Kobra Infosec-Smartcards (bzw. PKI-Karten) in die Smartcard-Tabelle des Kobra VS-Datenträgers. (9.14 Smartcard-Tabelle)

3.4 Benutzer- und SO-PIN (PUK)

Die Benutzer-PIN und SO-PIN (PUK) stehen dem Nutzer zur Verfügung und können von ihm jederzeit verändert werden. Sie ermöglichen in Verbindung mit einer gültigen Kobra Infosec-Smartcard die Authentisierung am Kobra VS-Datenträger und folglich den Zugriff auf die gespeicherten Daten.

Mithilfe der Benutzer-PIN kann der Nutzer sich an dem Kobra VS-Datenträger authentisieren (anmelden), einen neuen Krypto-Schlüssel generieren sowie die Benutzer-PIN ändern. Zudem kann er den Schreibschutz aktivieren und deaktivieren, falls er über die entsprechenden Schreibrechte verfügt.

Die SO-PIN (PUK) wird sowohl für die Änderung der SO-PIN (PUK) als auch für die Freischaltung der Kobra Infosec-Smartcard nach der Sperre der Benutzer-PIN benötigt. Dies kann vorkommen, wenn die Anzahl der erlaubten Fehlversuche für die Eingabe der Benutzer-PIN überschritten ist. Die Kobra Infosec-Smartcard wird endgültig gesperrt, sobald die Anzahl der erlaubten Fehlversuche (10 Fehlversuche) für die Eingabe der SO-PIN (PUK) ebenfalls überschritten ist.

Die Kobra Infosec-Smartcard wird mit der Benutzer-PIN 1-2-3-4 und der SO-PIN (PUK) 1-2-3-4-5-6-7-8-9-0 ausgeliefert. Die Werkseinstellungen ermöglichen für die Benutzer-PIN eine Länge von 4 bis 12 Stellen und drei Eingabeversuche. Für die SO-PIN (PUK) sind zehn Eingabeversuche und ebenfalls eine Länge von 4 bis 12 Stellen erlaubt. Im PKI-Szenario werden diese Einstellungen durch die PKI-Administratoren geregelt.

Hinweis:

Die Weitergabe der SO-PIN (PUK) an den Nutzer kann durch die internen Richtlinien des jeweiligen Unternehmens unterschiedlich geregelt werden.

Warnhinweis:

Merken Sie sich Ihre SO-PIN: Ohne diese kann eine Kobra Infosec-Smartcard nach Sperrung der Benutzer-PIN nicht freigeschaltet oder die SO-PIN geändert werden.

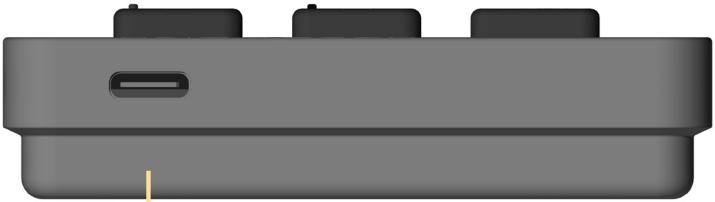
3.5 Admin-PIN

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

3.6 USB-Anschluss, Smartcard-Slot und Eingabeoberfläche

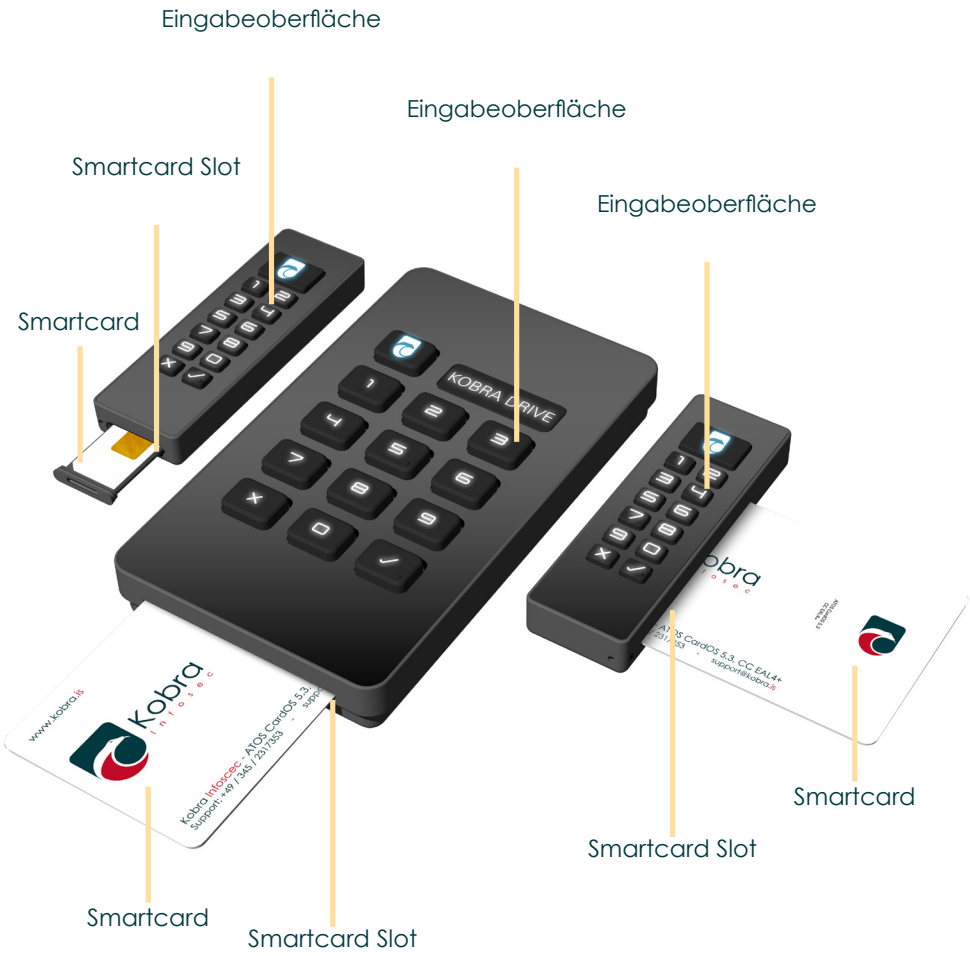
USB-C 3.0 Anschluss
Kobra Stick VS (2FF)

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



USB-C 3.0 Anschluss
Kobra Drive VS

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



3.7 Menü-Übersicht, Kommandos und Werkseinstellungen

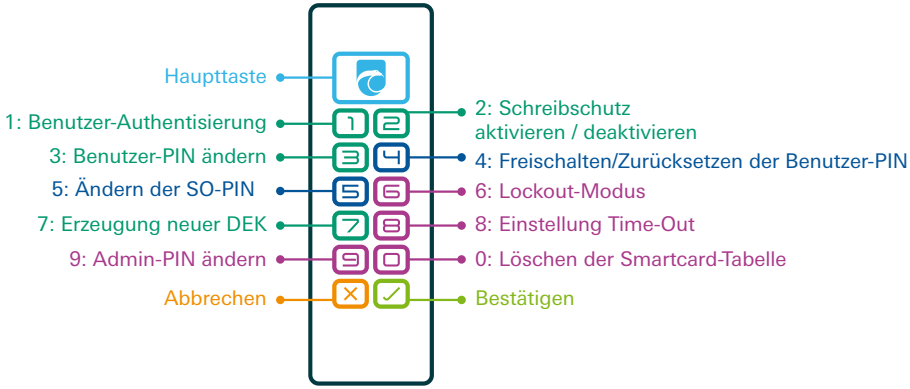
Benutzer	Taste 1 - Login Taste 2 - Schreibschutz * Taste 3 - Ändern der Benutzer-PIN Taste 4 - Freischalten der Benutzer-PIN Taste 7 - Erzeugung neues Krypto-Schlüssels
Administrator	Taste 6 - Einstellung Lock-Out Taste 8 - Einstellung Time-Out Taste 9 - Ändern der Admin-PIN Taste 0 - Löschen der Smartcard-Tabelle
Bestätigung der Eingaben	Taste √ oder Haupttaste
Abbrechen	Taste X
Schnelles Abmelden	2 x Taste X innerhalb von 2 Sekunden drücken
Benutzer-PIN (Standard)	1-2-3-4
Fehlversuche Benutzer-PIN	3
Stellenanzahl Benutzer-PIN)	4 bis 12
SO-PIN (PUK) (Standard)	1-2-3-4-5-6-7-8-9-0
Fehlversuche SO-PIN (PUK)	10
Stellenanzahl SO-PIN (PUK)	4 bis 12
Admin-PIN (Standard)	8-7-6-5-4-3-2-1
Fehlversuche Admin-PIN	16
Stellenanzahl Admin-PIN	4 bis 16
Time-Out	Einstellbar: 0 bis 30
Time-Out (Standard)	ausgeschaltet*
Lock-Out (Standard)	eingeschaltet*
Schreibschutz (Standard)	deaktiviert*
Admin-PIN-Eingabe	eingeschaltet*
Laufwerk-Typ	Wechseldatenträger

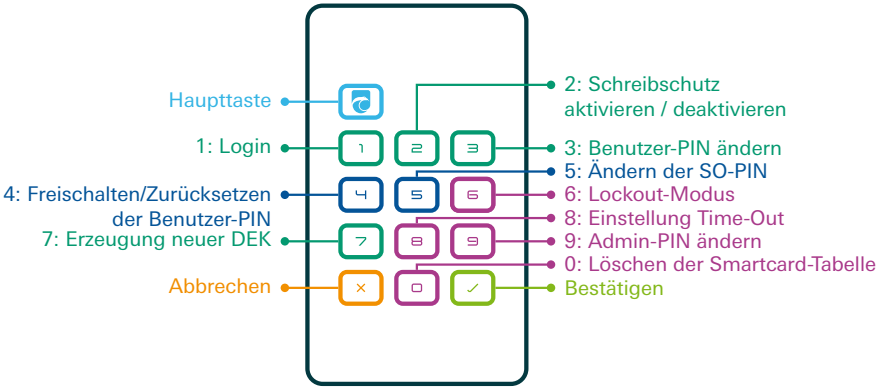
* – Der Administrator kann diese Einstellungen vor der Auslieferung an den Nutzer blockieren.

Benutzer-Kommandos

SO-PIN-Kommandos

Administrator-Kommandos





3.8 Integrierte Batterie als interne Stromversorgung

Der Kobra VS-Datenträger verfügt über eine integrierte Batterie. Diese gewährleistet die interne Stromversorgung und Ausführung folgender Funktionen ohne Anschluss des Kobra VS-Datenträgers an einen PC oder eine andere externe Stromversorgung (z.B. USB-Netzteil oder Hub):

- Überprüfen, Aktivieren und Deaktivieren des Schreibschutzes
- Sowohl die Authentisierung vor dem Anschluss an einen PC (z.B. als Pre-Boot Authentisierung) als auch das Booten vom Kobra VS-Datenträger nach dem Anschluss an einen PC (z.B. Windows oder andere Betriebssysteme)
- Änderung der Benutzer-PIN ohne Anschluss an einen PC
- Zerstören eines gültigen Krypto-Schlüssels oder Löschen der Smartcard-Tabelle und infolgedessen Löschen aller Daten auf dem Kobra VS-Datenträger ohne Anschluss an einen PC

Der Kobra VS-Datenträger befindet sich im Schlaf-Modus, solange er nicht mit dem PC oder einem anderen Stromversorger verbunden ist. Zum Einschalten muss die Menü-Taste etwa 3 Sekunden gedrückt gehalten werden.

Falls alle Tasten unbeleuchtet bleiben, kann dies an einer leeren Batterie liegen. Diese wird über den USB-C-Anschluss nach dem Verbinden des Kobra VS-Datenträgers mit einem PC oder einem anderen externen Stromversorger (z.B. USB-Netzteil oder Hub) aufgeladen.

4. Echtheitsprüfung

Nach jedem Erhalt eines Kobra VS-Datenträgers muss dieser auf Echtheit geprüft werden. Wesentlich hierbei ist der Vergleich der Seriennummer und Modellbezeichnung im Lieferschein mit den eingravierten Angaben auf dem Gehäuse des Kobra VS-Datenträgers sowie mit den digitalen Informationen, welche mithilfe der unterstützenden Kobra Client VS Software ausgelesen werden können.

Zur ergänzenden Authentizitätsprüfung im Betrieb empfiehlt sich die Verwendung einer s.g. Authentizitätsdatei. Sie dient dazu, die Echtheit und Unverfälschtheit der Daten nachzuweisen. Die Authentizitätsdatei kann beliebig so gewählt werden, dass sie einmalig ist und durch den Besitzer leicht verifiziert werden kann, sobald dieser auf den Datenträger zugreift.

Je nach Einsatzgebiet lässt sich eine Authentizitätsdatei auf unterschiedliche Art erzeugen und nutzen. In der einfachsten Variante enthält sie Prüfsummen – beispielsweise mittels SHA256 oder SHA512 – der ursprünglichen Dateien. Für ein höheres Maß an Sicherheit können diese Hash-Werte oder auch die kompletten Dateien mithilfe eines privaten Schlüssels, etwa über GPG, digital signiert werden.

Bei Abweichungen setzen Sie sich mit dem Lieferanten oder Ihrem Administrator in Verbindung.

5. Firmware-Updates

Die Beschreibung dieser Funktion finden Sie im Administratorhandbuch.

6. Inbetriebnahme des Kobra VS-Datenträgers

Für die korrekte Inbetriebnahme des Kobra VS-Datenträgers sind nur drei Schritte erforderlich:

1) Smartcard (bzw. PKI-Karte) einlegen
2) Verbinden mit Host-System (z.B. PC)
3) Benutzer-PIN eingeben

Die notwendige Stromversorgung erfolgt bei einem Kobra VS-Datenträger grundsätzlich über den USB-C-Anschluss. Daher soll dieser für die Inbetriebnahme an einem PC oder einem USB-Hub mit Stromversorgung angeschlossen werden. Außerdem verfügt der Kobra VS-Datenträger über eine integrierte Batterie. Diese ermöglicht das Ausführen bestimmter Funktionen, ohne den Kobra VS-Datenträger an eine externe Stromversorgung anzuschließen.

Solange der Kobra VS-Datenträger weder mit einem PC noch mit einem externen Stromversorger (z.B. USB-Netzteil oder Hub) verbunden ist, befindet sich dieser im Schlaf-Modus. Alle Tasten sind dabei ausgeschaltet.

Der Kobra VS-Datenträger wechselt nach dem Anschluss an einen PC oder einen externen Stromversorger sofort in den Authentisierungsmodus, falls eine für diesen Kobra VS-Datenträger bestimmte Kobra Infosec-Smartcard (bzw. PKI-Karte) korrekt eingelegt ist. Die Haupttaste blinkt grün und die Benutzer-PIN kann eingegeben werden. Befindet sich im Kobra VS-Datenträger noch keine Smartcard oder ist diese unzulässig beziehungsweise nicht integriert, so blinkt die Haupttaste ununterbrochen rot oder gelb bis eine für diesen Datenträger bestimmte Kobra Infosec-Smartcard (bzw. PKI-Karte) korrekt eingeführt wird. Werden innerhalb von 20 Sekunden keine weiteren Kommandos oder Eingaben getätigt, so wechselt der Kobra VS-Datenträger automatisch in den Warte-Modus.

Durch die Betätigung der Haupttaste erfolgt der Wechsel aus dem Warte-Modus in den Menü-Modus. In diesem Zustand leuchtet die Haupttaste blau und alle anderen Eingabe-Tasten weiß. Die leuchtenden Eingabe-Tasten signalisieren, dass diese aktiv sind und die entsprechenden Kommandos eingegeben werden können. Nach dem Drücken auf die Taste „1“ und anschließend auf „√“ wechselt der Benutzer erneut in den Authentisierungsmodus. Die Haupttaste blinkt grün und alle anderen Tasten sind weiterhin aktiv. An dieser Stelle kann die Benutzer-PIN eingegeben werden. Sind die Benutzer- oder SO-PIN (PUK) bereits gesperrt, so blinkt die Haupttaste nach der PIN-Eingabe und Bestätigung durch die „√”-Taste abwechselnd gelb-rot-gelb-rot und leuchtet anschließend weiß. Der Kobra VS-Datenträger wechselt dabei in den Warte-Modus. Die Authentisierung ist in diesem Fall nicht möglich. Die gesperrte

Benutzer-PIN kann mit der gültigen SO-PIN (PUK) zurückgesetzt werden. Kobra Infosec-Smartcards mit gesperrten Benutzer- und SO-PIN (PUK) können nicht mehr verwendet werden.

Befindet sich im Smartcard-Slot eine noch nicht in die Smartcard-Tabelle des Kobra VS-Datenträgers eingetragene Smartcard, so leuchtet die Haupttaste gleich nach der Betätigung der Taste „1" kurz rot und anschließend dauerhaft weiß: Der Kobra VS-Datenträger ist in den Warte-Modus gewechselt. Die Authentisierung ist auch in diesem Fall nicht möglich.

Alle Kommandos werden mit der „√"-Taste oder der Haupttaste bestätigt oder mit der „X"-Taste abgebrochen. Nach jeder Betätigung der „X"-Taste wechselt der Benutzer in den Warte-Modus und kann von diesem Zustand des Kobra VS-Datenträgers seine geplanten Schritte erneut beginnen. Die Haupttaste blinkt dabei einmal orange und leuchtet anschließend weiß.

Nach der erfolgreichen Authentisierung leuchtet die Haupttaste dauerhaft grün bei deaktiviertem und violett bei aktiviertem Schreibschutz. Die anderen Tasten sind unbeleuchtet und der Zugriff auf die Daten ist freigeschaltet.

War die PIN-Eingabe fehlerhaft, blinkt die Haupttaste entsprechend der Anzahl der erfolgten Fehlversuche einmal oder mehrfach rot (jedoch maximal entsprechend der Anzahl der zulässigen Fehlversuche) und der Kobra VS-Datenträger wechselt erneut in den Warte-Modus. Der Authentisierungsvorgang kann von dieser Stelle, wie oben beschrieben, wiederholt werden. Nach Überschreitung der zulässigen Fehlversuche blinkt die Haupttaste gelb-rot-gelb-rot und leuchtet anschließend weiß. Die Kobra Infosec-Smartcard sperrt sich dabei automatisch und kann danach nur durch die Eingabe der SO-PIN (PUK) freigeschaltet werden. Die PIN-Eingabeversuche unter 4 Stellen werden generell nicht als Fehlversuche gezählt (Kapitel 9.4 Freischalten/ Zurücksetzen der Benutzer-PIN).

Die fehlerhafte Eingabe der SO-PIN (PUK) führt nach Überschreitung der Fehlversuche zu der endgültigen Sperre der Kobra Infosec-Smartcard. Der Zugriff auf die Daten ist anschließend nur mit einer anderen für diesen Kobra VS-Datenträger freigeschalteten Kobra Infosec-Smartcard und korrekter Eingabe der Benutzer-PIN möglich. In diesem Fall kann mithilfe der Kobra Client VS Software die gesperrte Smartcard aus der-Smartcard-Tabelle auf dem Kobra VS-Datenträger gelöscht und eine andere kompatible Smartcard eingetragen werden.

Liegen keine weiteren für diesen Kobra VS-Datenträger berechtigten Kobra Infosec-Smartcards vor, verbleibt nur die Möglichkeit eine neue Kobra Infosec-Smartcard für diesen Kobra VS-Datenträger zu initialisieren. Diese Aufgabe erledigt der Administrator durch das Löschen der aktuellen und das Erstellen einer neuen Smartcard-Tabelle. Alle zuvor gespeicherten Daten werden bei diesem Vorgang unwiderruflich zerstört.

Die Authentisierung kann auch ohne Anschluss an einen PC oder einen anderen externen Stromversorger (z.B. USB-Netzteil oder Hub) erfolgen. Die Stromversorgung wird in diesem Fall durch die integrierte Batterie gewährleistet. Nach langem Drücken (ca. 3 Sekunden) auf die Haupttaste wechselt der Kobra VS-Datenträger in den

Authentisierungsmodus. Anschließend legt der Benutzer seine Smartcard ein und gibt die dazugehörige Benutzer-PIN ein. Nach erfolgreicher Authentisierung kann der Kobra VS-Datenträger innerhalb von 20 Sekunden an einen PC angeschlossen werden.

Wenn innerhalb von 20 Sekunden keine weiteren Kommandos oder Eingaben getätigt werden, wechselt der Kobra VS-Datenträger automatisch in den Warte-Modus, falls dieser an einem PC oder einem anderen externen Stromversorger (z.B. USB-Netzteil oder Hub) angeschlossen ist. Ohne externe Stromversorgung kehrt der Kobra VS-Datenträger nach 20 Sekunden in den Schlaf-Modus zurück. Für den authentisierten Kobra VS-Datenträger trifft diese Regelung jedoch nicht zu, falls dieser bereits an einem PC angeschlossen ist.

Aus Sicherheitsgründen ist eine logische oder physikalische Trennung des Kobra VS-Datenträgers nach der Benutzung vom Wirtssystem durchzuführen. Dies empfiehlt sich vor allem bei Beendigung, kurzfristiger Unterbrechung sowie beim Verlassen des Arbeitsplatzes.

In diesem Zusammenhang bietet die aktivierte Time-Out-Funktion eine gute Unterstützung zum effektiven Datenschutz. Mittels dieser Einstellung kann auch für den angeschlossenen Datenträger eine automatische zeitliche Sperre bei Inaktivität konfiguriert werden (Kapitel 9.9 Time-Out Funktionen).

Zudem verfügt der Kobra VS-Datenträger neben den klassischen „Abmelde"-Mechanismen wie das „sichere Entfernen" über die Taskleiste des PC und das physische Trennen der USB-Verbindung noch über die Quick-Out-Funktion zur schnellen Abmeldung. Diese Funktion wird durch das doppelte Klicken auf die „×"-Taste innerhalb von 2 Sekunden ausgeführt.
Für die sichere physikalische Trennung muss das USB-Kabel vom Kobra VS-Datenträger vollständig entfernt werden.

Hinweis:

Um einen Datenverlust zu vermeiden, vergewissern Sie sich vor Trennung der Verbindungen, dass die Datenübertragung sowie die Zugriffe auf den Kobra VS-Datenträger vollständig abgeschlossen sind.

Hinweis:

Um die Sicherheit Ihrer Daten zu gewährleisten, ist es zwingend erforderlich, die voreingestellte Benutzer- und SO-PIN (PUK) zu ändern (Kapitel 9.3 Ändern der Benutzer-PIN , Kapitel 4.3.3 SO-PIN/PUK ändern im Kobra Client VS Handbuch). Verändern Sie zudem die Benutzer-PIN auch zukünftig in regelmäßigen Abständen. Zusätzlich empfiehlt es sich, unterschiedliche Benutzer-PINs für verschiedene Kobra Infosec-Smartcards zu verwenden. Die Benutzer- und SO-PIN (PUK) müssen vertraulich behandelt werden.

Hinweis:

Bitte beachten Sie, dass die "Kobra Client-Software" (Kapitel 8. Kobra Client VS) ausgeschaltet sein muss, sobald Sie den Kobra VS-Datenträger formatieren.

7. Rolle und Berechtigungen

Die Kobra VS-Datenträger ermöglichen die Aufteilung der Rollen und Berechtigungen bezüglich der Verwaltung und Benutzung des Datenträgers.

Der Benutzer verfügt über die Smartcard und kennt die Benutzer- und SO-PIN (PUK). Er kann die Benutzer- und SO-PIN (PUK) ändern, sich an dem Kobra VS-Datenträger authentisieren (anmelden), einen neuen Krypto-Schlüssel generieren sowie die Kobra Infosec-Smartcard nach der Sperre durch die fehlerhafte Benutzer-PIN-Eingabe wieder freischalten oder zurücksetzen. Zudem kann er den Schreibschutz aktivieren und deaktivieren, falls er über Schreibrechte verfügt.

Der Administrator kennt die Admin-PIN. Er kann den Kobra VS-Datenträger verwalten und entsprechend dem Sicherheitskonzept des Unternehmens sowie den beabsichtigten Anwendungsszenarien gestalten. Er kann u.a. die Admin-PIN ändern, Time-Out- und Lock-Out-Einstellungen vornehmen sowie die Liste der berechtigten Smartcards bei einem Kobra VS-Datenträger ergänzen, löschen oder neu erstellen. Überdies kann er festlegen, welche Nutzer ausschließlich über Leserechte und welche zudem über Schreibrechte verfügen, sowie ob jeweiliger Benutzer den Kryptoschlüssel zerstören oder erzeugen darf. Weitere Informationen sind in Kapitel 8 sowie in den Anleitungen für den Kobra Client VS und Kobra Connect zu entnehmen.

Der Administrator hat auf der Basis seiner Berechtigungen keine Möglichkeit, auf die gespeicherten Daten eines Kobra VS-Datenträgers zuzugreifen. Jedoch kann er eventuell während der Freischaltung einer zusätzlichen Kobra Infosec-Smartcard für einen Kobra VS-Datenträger in Kenntnis von einer Benutzer-PIN gelangen, da diese beim Hinzufügen einzugeben ist. Daher ist es dringend erforderlich, dass der Benutzer nach diesem Vorgang die Benutzer-PIN neu definiert.

Mithilfe der Kobra Client VS Software kann der Administrator die oben genannten Einstellungen schnell auf andere Kobra VS-Datenträger übertragen. Weiterhin kann er die Eingabe der Admin-PIN über die Tastatur des Kobra VS-Datenträgers deaktivieren oder aktivieren. Die Eingabe der Admin-PIN über die Kobra Client VS Software ist in jedem Fall weiterhin möglich. Auf diesem Wege kann die fehlerhafte Eingabe der Admin-PIN durch den Benutzer und somit die unwiderrufliche Sperre der Admin-PIN vermieden werden. Nach der Sperre der Admin-PIN ist es nicht mehr möglich, die vom Administrator vorgenommenen Einstellungen zu ändern.

Die Konzeptionierung der PKI-Karten und die Weitergabe der SO-PIN (PUK) an den Benutzer kann durch interne Richtlinien und Sicherheitskonzepte der jeweiligen Unternehmen oder Behörden individuell geregelt werden.

Warnhinweis:

Es muss davon ausgegangen werden, dass der Administrator möglicherweise Zugriff auf die im Kobra VS-Datenträger gespeicherten Daten hat. Daher muss der Administrator vertrauenswürdig sein. Bei Zweifeln am Vertrauen zum Administrator muss der Benutzer selbst zum Administrator werden und die Smartcard-Tabelle selbstständig verwalten.

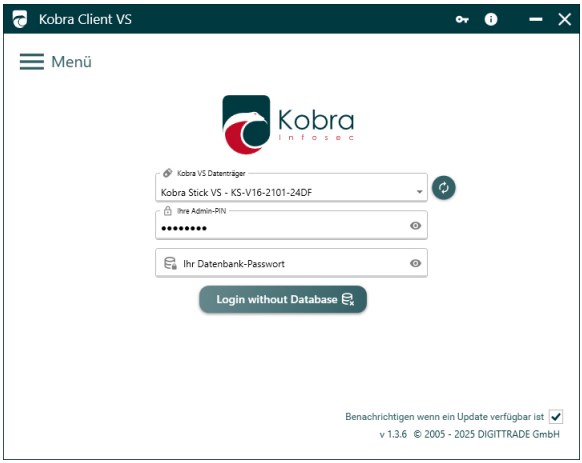
8. Kobra Client VS

Der Kobra Client VS ist eine Verwaltungssoftware für Kobra VS-Datenträger. Sie ermöglicht dem Administrator, die Kobra VS-Datenträger für jeden einzelnen Nutzer schnell und aufgabenorientiert zu konfigurieren. Die vorgenommenen Einstellungen können exportiert und als Einstellungsprofile für bestimmte Nutzer-Gruppen gespeichert werden. Anschließend können diese Einstellungen auf beliebige Kobra VS-Datenträger schnell angewendet werden. Folgende Einstellungen können unter anderem vorgenommen, exportiert und importiert werden:

- Änderung der Admin-PIN, Benutzer-PIN und SO-PIN (mit optionalem Passwort Generator)
- Verwendung der Admin-PIN über die Tastatur des Kobra VS-Datenträgers
- Erzeugung und Änderung des Update-Schlüssels
- Das Konfigurieren von Lock-Out- und Time-Out-Funktionen
- Löschen und Erstellen von Smartcard-Tabellen
- Eintragen zusätzlicher Smartcards (PKI-Karten) in die Smartcard-Tabelle
- Individuelles Setzen der Schreib- und Leserechte für jeden Nutzer
- Selbst-Formatierung ein- und ausschalten
- Stromüberbrückung
- Datenbank-Funktionen, Smartcard Assistent, uvm.

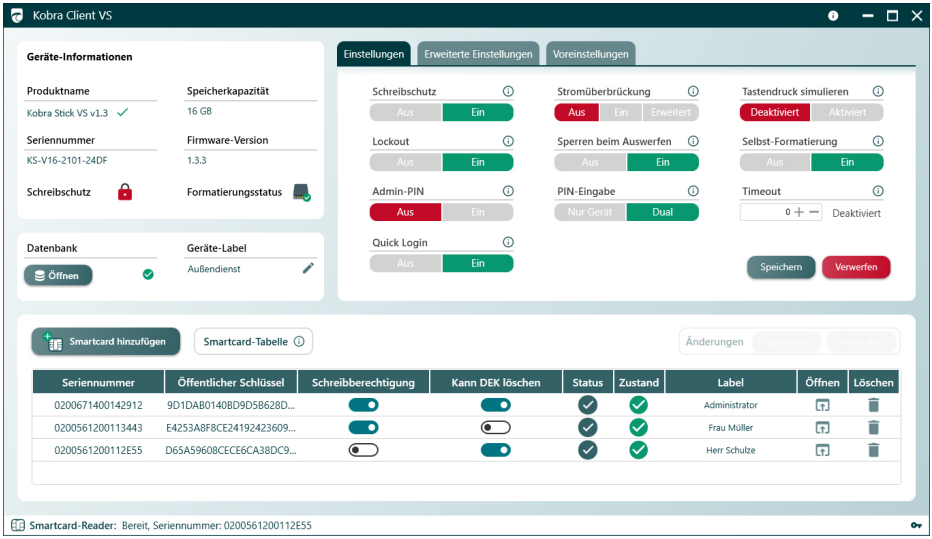
Mithilfe dieser Software kann der Administrator die Seriennummer und den öffentlichen Schlüssel direkt aus der in den Kobra VS-Datenträger hineingesteckten Kobra Infosec-Smartcard (PKI-Karte) auslesen. Er kann diese Informationen sowohl aus der Datenbank als auch aus der Smartcard-Tabelle des VS-Datenträgers entnehmen. Dabei kann er zusätzlich festlegen, ob der jeweilige Smartcard-Besitzer über Schreibrechte verfügt und den DEK löschen darf.

Nach dem Start der Kobra Client VS Software erscheint zuerst das Login-Fenster:



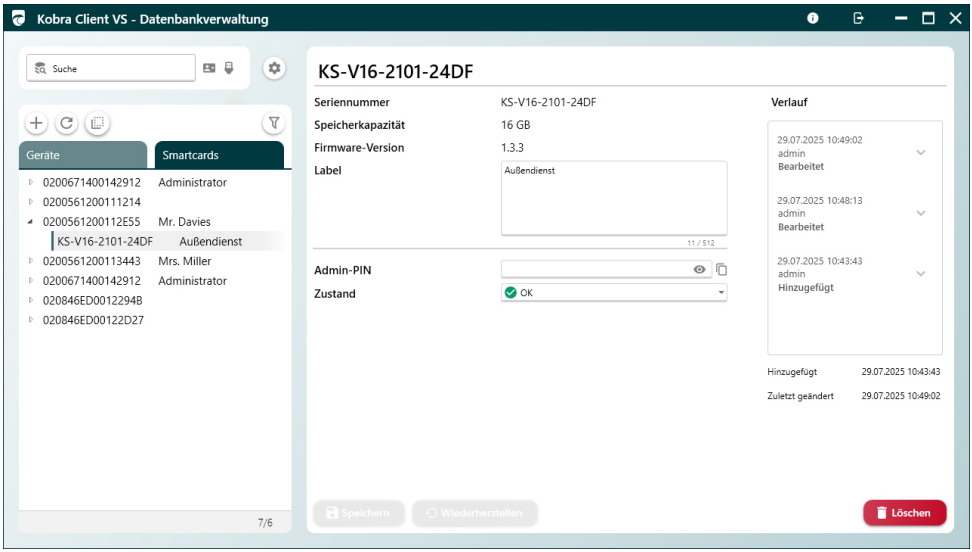
Login-Fenster

Im Login-Fenster kann der Administrator die Sprache auswählen und nach einem angeschlossenen VS-Datenträger suchen. Nach erfolgreicher Authentisierung mit der Admin-PIN öffnet sich das Hauptmenü. In dieses Menü werden die aktuellen Einstellungen des Kobra VS-Datenträgers sowie die Smartcard-Tabelle mit den freigegebenen Kobra Infosec-Smartcards (PKI-Karten) geladen.



Hauptmenü

Gleichzeitig wird die Datenbankanmeldung vorgenommen, sodass alle Änderungen am Datenträger und an den Smartcards in der Datenbank erfasst werden.



Datenbank Ansicht

Eine detaillierte Beschreibung dazu befindet sich in der Bedienungsanleitung Kobra Client VS auf der Webseite www.kobra-infosec.de.

9. Menü-Modus: Authentisierung und Verwaltung

Die Authentisierung und Verwaltung des Kobra VS-Datenträgers erfolgt über den Menü-Modus mittels Eingabe von Ziffern und Kommandos. Die Umschaltung in den Menü-Modus geschieht generell aus dem Warte-Modus durch die Betätigung der Haupttaste. Im Menü-Modus leuchtet die Haupttaste blau und alle anderen Eingabe-Tasten weiß.

Zum Ausführen der Kommandos benötigt der Kobra VS-Datenträger meist den Anschluss an einen PC oder einen anderen externen Stromversorger (z.B. USB-Netzteil oder USB-Hub). Ausnahmen bilden die Authentisierung am Kobra VS-Datenträger, die Aktivierung oder Deaktivierung des Schreibschutzes sowie die Erzeugung eines neuen Krypto-Schlüssels. Diese Funktionen können auch im Batteriebetrieb ausgeführt werden.

Im Menü-Modus werden alle Eingaben und Kommandos mit der „√"-Taste bestätigt oder mit der „X"-Taste abgebrochen. Nach jeder Betätigung der „X"-Taste wechselt der Kobra VS-Datenträger in den Warte-Modus. Der Vorgang kann von dieser Stelle aus wiederholt werden.

Nach dem Start einer Menü-Funktion beginnt die Haupttaste grün zu blinken, wenn die Benutzer-PIN einzugeben ist. Für die Eingabe der Admin-PIN blinkt die Haupttaste dagegen dauerhaft violett und für die SO-PIN (PUK) hellblau. Alle anderen Tasten sind in diesem Moment aktiv. Wird die Eingabe mit der „√"-Taste bestätigt, leuchtet die Haupttaste bei korrekter PIN grün auf.

Beim Auftreten eines Fehlers blinkt die Haupttaste kurz rot und leuchtet anschließend weiß. Der Kobra VS-Datenträger wechselt in den Warte-Modus. Der Vorgang kann von dieser Stelle aus wiederholt werden.

War bei einem der Vorgänge die PIN-Eingabe fehlerhaft, blinkt die Haupttaste entsprechend der Anzahl der erfolgten Fehlversuche einmal oder mehrfach rot (jedoch maximal entsprechend der Anzahl der erlaubten Fehlversuche) und der Kobra VS-Datenträger wechselt in den Warte-Modus. Der geplante Vorgang kann von dieser Stelle aus erneut gestartet werden.

Zudem wechselt der Kobra VS-Datenträger nach jeder erfolgreichen Ausführung eines Kommandos (ausgenommen Benutzer-Authentisierung) in den Warte-Modus.

Ist eine gültige Smartcard hineingesteckt und wird der Kobra VS-Datenträger per USB-Kabel an einen PC angeschlossen oder im Batteriemodus die Haupttaste länger gedrückt, blinkt die Hauptaste grün. Der Kobra VS-Datenträger befindet sich im Authentisierungs-Modus:

- Nach Eingabe der Benutzer-PIN ist der Zugriff auf die Daten freigeschaltet
- Nach Drücken der X-Taste-Taste oder der Haupttaste wechselt der Kobra VS-Datenträger in den Warte-Modus.

9.1 Benutzer-Authentisierung

Die Benutzer-Authentisierung ist erforderlich, um den Zugriff auf den Datenträger freizuschalten. Diese kann auf zwei unterschiedlichen Wegen erfolgen: Entweder mit Anschluss an einem externen Stromversorger (z. B. Host-System) oder als Pre-Boot-Authentisierung im Batteriebetrieb.

A. Authentisierung am Host-System:

1) Stecken Sie eine für den Kobra VS-Datenträger zugelassene Smartcard in den dafür vorhergesehenen Steckplatz
2) Schließen Sie den Kobra VS-Datenträger an ein Host-System an. Die Haupttaste blinkt nun grün und alle anderen Tasten bleiben aktiv.
3) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“.

Falls der Kobra VS-Datenträger ohne eingesteckte Smartcard mit Host-System verbunden wird, beginnt die Haupttaste dauerhaft rot zu blinken:

1) Stecken Sie eine für den Kobra VS-Datenträger zugelassene Smartcard in den dafür vorhergesehenen Steckplatz. Die Haupttaste beginnt grün zu blinken und alle anderen Tasten bleiben aktiv.
2) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“

B. Authentisierung im Batteriebetrieb:

1) Stecken Sie eine für den Kobra VS-Datenträger zugelassene Smartcard in den dafür vorhergesehenen Steckplatz
2) Drücken Sie die Haupttaste, bis diese grün blinkt.
3) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“.

Falls der Kobra VS-Datenträger mit eingesteckter Smartcard sich im Wartemodus befindet (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet), führen Sie folgende Schritte durch:

1) Drücken Sie nachfolgend die Haupttaste, die Taste „1“ und anschließend „√“. Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
2) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“.

Hinweis:

Nach der erfolgreichen Authentisierung leuchtet die Haupttaste dauerhaft grün, wenn der Schreibschutz deaktiviert ist, oder violett, wenn dieser aktiviert ist. Die anderen Tasten sind deaktiviert und der Zugriff auf die Daten ist freigeschaltet.

9.2 Schreibschutz-Mechanismus

Der aktivierte Schreibschutz bietet Ihnen einen zusätzlichen Schutz vor Viren und Trojanern während der Verwendung des Kobra VS-Datenträgers an einem fremden PC. Zudem kann dadurch eine versehentliche Speicherung sensibler Informationen von einem PC oder Server auf den Kobra VS-Datenträger verhindert werden.

Bereits vor der Authentisierung kann der Nutzer durch das Drücken auf die Taste „2“ prüfen, ob der Schreibschutz aktiviert ist. Dabei zeigt die dauerhaft violett leuchtende Haupttaste an, dass der Schreibschutz aktiviert ist. Ist der Schreibschutz deaktiviert, leuchtet die Haupttaste grün.

Für die Aktivierung oder Deaktivierung des Schreibschutzes:

1) Stellen Sie sicher, dass Sie sich im Warte-Modus befinden. (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet)
2) Drücken Sie nachfolgend die Haupttaste und die Taste „2“. Bei aktiviertem Schreibschutz leuchtet die Haupttaste violett, bei deaktiviertem Schreibschutz grün
3) Drücken Sie anschließend die „√“-Taste, falls Sie den Zustand ändern möchten. Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
4) Geben Sie anschließend die Benutzer-PIN ein und bestätigen Sie mit „√“.

Nach einer erfolgreichen Umschaltung blinkt die Haupttaste zweimal grün oder violett und der Kobra VS-Datenträger wechselt zurück in den Warte-Modus.

Mithilfe der Kobra Client VS Software kann der Administrator die Schreibberechtigung einzelner Benutzer sperren. In diesem Fall ist es für den Benutzer nicht möglich, den Schreibschutz zu deaktivieren.

9.3 Ändern der Benutzer-PIN

Der Nutzer kann für die Benutzer-PIN eine Kombination von 4 bis 12 Ziffern wählen.

Für die Änderung der Benutzer-PIN:

1) Stellen Sie sicher, dass Sie sich im Warte-Modus befinden. (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet)
2) Drücken Sie nachfolgend die Haupttaste, die Taste „3“ und anschließend „√“. Die Haupttaste blinkt dauerhaft grün und alle anderen Tasten bleiben aktiv.
3) Geben Sie die aktuelle Benutzer-PIN ein und bestätigen Sie mit „√“.
4) Geben Sie die neue Benutzer-PIN ein und bestätigen Sie mit „√“.
5) Wiederholen Sie die neue Benutzer-PIN und bestätigen Sie mit „√“.

Nach einer erfolgreichen PIN-Änderung blinkt die Haupttaste zweimal grün und der Kobra VS-Datenträger wechselt wieder in den Warte-Modus.

9.4 Freischalten/Zurücksetzen der Benutzer-PIN

Nach der Überschreitung der zulässigen Fehlversuche sperrt sich die Kobra Infosec-Smartcard automatisch und kann danach nur durch die Eingabe der SO-PIN (PUK) wieder freigeschaltet werden. Diese Funktion ermöglicht dem Anwender die gesperrte Benutzer-PIN durch eine neue zu ersetzen.

1) Stellen Sie sicher, dass Sie sich im Warte-Modus befinden. (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet)
2) Drücken Sie nachfolgend die Haupttaste, die Taste „4“ und anschließend „√“. Die Haupttaste blinkt hellblau und alle anderen Tasten bleiben aktiv.
3) Geben Sie die SO-PIN (PUK) ein und bestätigen Sie mit „√“.
4) Geben Sie die neue Benutzer-PIN ein und bestätigen Sie mit „√“.
5) Wiederholen Sie die neue Benutzer-PIN und bestätigen Sie ebenfalls mit „√“.

Nach einer erfolgreichen Freischaltung der Kobra Infosec-Smartcard blinkt die Haupttaste zweimal grün und der Datenträger wechselt in den Warte-Modus.

Die fehlerhafte Eingabe der SO-PIN (PUK) führt nach Überschreitung der erlaubten Fehlversuche zu der endgültigen Sperrung der Kobra Infosec-Smartcard. Der Zugriff auf die Daten ist anschließend nur mit einer anderen für diesen Kobra VS-Datenträger freigeschalteten Smartcard und korrekter PIN-Eingabe möglich.

9.5 Ändern der SO-PIN (PUK)

Die SO-PIN (PUK) kann nur mithilfe der Software Kobra Client VS geändert werden. Eine Beschreibung dazu befindet sich in der Bedienungsanleitung zum Kobra Client VS auf der Webseite www.kobra-infosec.de.

9.6 Ändern oder Ausschalten der Admin-PIN

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

9.7 Generieren eines neuen Krypto-Schlüssels

Der Anwender kann mithilfe einer initialisierten Kobra Infosec-Smartcard (bzw. PKI-Karte) und Benutzer-PIN jederzeit den Krypto-Schlüssel auf dem zugehörigen Kobra VS-Datenträger generieren, ändern und zerstören. Diese Vorgänge sind irreversibel. Nach der Erzeugung eines neuen Krypto-Schlüssels werden der alte Krypto-Schlüssel und somit alle auf dem Kobra VS-Datenträger gespeicherten Daten endgültig vernichtet. Daher sollen die gespeicherten Informationen unter Umständen zuvor auf einem anderen VS-NfD/EU RESTRICTED/NATO RESTRICTED-zugelassenen Datenträger gesichert werden.

Beim Löschen der Daten sollte auf das mehrmalige Überschreiben durch z.B. Formatierungen verzichtet werden, da dies die Lebensdauer des Datenträgers beeinträchtigen kann. Sicher und effizient erfolgt die Löschung der Daten durch das Generieren eines neuen Krypto-Schlüssels. Zudem können Daten durch das Löschen des Krypto-Schlüssels vernichtet werden (Kapitel 9.8 Löschen eines Krypto-Schlüssel) oder der Smartcard-Tabelle (Kapitel 9.14 Smartcard-Tabelle).

Zum Generieren oder Ändern des Krypto-Schlüssels:

1) Stecken Sie eine für den Kobra VS-Datenträger zugelassene Smartcard in den dafür vorhergesehenen Steckplatz
2) Stellen Sie sicher, dass der Kobra VS-Datenträger an ein Host-System angeschlossen ist und sich im Wartemodus befindet (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet).
3) Drücken Sie nachfolgend die Haupttaste und die Taste „7“. Die Haupttaste leuchtet dauerhaft rot und signalisiert damit, dass alle auf dem Kobra VS-Datenträger gespeicherten Daten nach der Ausführung dieser Funktion endgültig vernichtet sind.
4) Falls Sie diese Funktion tatsächlich durchführen möchten, drücken Sie die Taste „√“. Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
5) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“.

Nach der Eingabe und Bestätigung der Benutzer-PIN leuchtet die Haupttaste während der Erzeugung oder Änderung des Krypto-Schlüssels gelb. War der Vorgang erfolgreich blinkt die Haupttaste zweimal grün und leuchtet anschließend dauerhaft weiß. Der Kobra VS-Datenträger wechselt in den Warte-Modus. Dieser Vorgang kann

mehrere Sekunden dauern. Besonders wenn mehrere Smartcards in der Smartcard-Tabelle eingetragen sind.

Bei der nächsten Authentisierung blinkt die Haupttaste solange blau bis die Formatierung abgeschlossen ist. Dieser Vorgang kann je nach Speichergröße einige Minuten dauern. Im Anschluss leuchtet die Haupttaste violett, wenn der Schreibschutz aktiviert oder grün, wenn dieser deaktiviert ist. Der Zugriff auf die zuvor auf dem Kobra VS-Datenträger gespeicherten Daten ist ab diesem Zeitpunkt nicht mehr möglich.

9.8 Löschen eines Krypto-Schlüssel

Das Löschen (Vernichten) des Krypto-Schlüssels kann auf drei Wegen erfolgen.

A: Zerstörung ohne Generierung eines neuen Krypto-Schlüssels

Mit dieser Methode können die auf dem Kobra VS-Datenträger gespeicherten Daten schnell vernichtet werden, ohne dass der Datenträger an einen PC angeschlossen werden muss. Ab diesem Zeitpunkt können alle zuvor gespeicherten Daten nicht mehr abgerufen werden.

1) Stecken Sie eine Smartcard in den Kobra VS-Datenträger ein und drücken Sie die Haupttaste, bis diese grün blinkt. Drücken Sie danach auf die Taste "X", um in den Warte-Modus zu wechseln. (Die Haupttaste leuchtet weiß und andere Tasten sind ausgeblendet).
2) Drücken Sie nachfolgend die Haupttaste und anschließend die Taste „7". Die Haupttaste leuchtet dauerhaft rot und signalisiert damit, dass alle auf dem Kobra VS-Datenträger gespeicherten Daten nach der Ausführung dieser Funktion endgültig vernichtet sind.
3) Falls Sie diese Funktion tatsächlich durchführen möchten, drücken Sie die Taste „√", Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
4) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√". Die Haupttaste leuchtet während der Erzeugung oder Änderung des Krypto-Schlüssels gelb. War der Vorgang erfolgreich blinkt die Haupttaste zweimal grün und leuchtet anschließend dauerhaft weiß.

B: Zerstörung durch Generierung eines neuen Krypto-Schlüssels

Die Beschreibung dieses Vorgangs befindet sich im Kapitel 9.7 Generieren eines neuen Krypto-Schlüssels.

C: Zerstörung des Krypto-Schlüssels durch Löschung der Smartcard-Tabelle

Diese Methode kann der Administrator entweder durch die Eingabe über die Tastatur oder mithilfe der Kobra Client VS Software und der Admin-PIN durchführen. Während der Löschung der Smartcard-Tabelle erfolgt auch die endgültige Vernichtung des Krypto-Schlüssels. Ab diesem Zeitpunkt verfügt der Kobra VS-Datenträger über keinen Krypto-Schlüssel mehr. Infolgedessen sind ebenfalls alle auf dem Kobra VS-Datenträger zuvor gespeicherten Daten unwiderruflich vernichtet (*Kapitel 9.14 Smartcard-Tabelle)*.

Löschen der Smartcard-Tabelle über die Tastatur des Kobra VS-Datenträgers

1) Stellen Sie sicher, dass Sie sich im Warte-Modus befinden. (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet)
2) Drücken Sie nachfolgend die Haupttaste, die Taste „0“ und anschließend „√“. Die Haupttaste blinkt dauerhaft violett und alle anderen Tasten bleiben aktiv.
3) Geben Sie die Admin-PIN ein und bestätigen Sie mit „√“.

Nach einem erfolgreichen Vorgang blinkt die Haupttaste zweimal grün und der Kobra VS-Datenträger wechselt zurück in den Warte-Modus.

9.9 Time-Out Funktionen

Der Administrator kann festlegen, nach wie viel Minuten der freigeschaltete Kobra VS-Datenträger sich automatisch sperrt, wenn innerhalb der angegebenen Zeit weder lesender noch schreibender Zugriff auf den Kobra VS-Datenträger erfolgt. Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

9.10 Quick-Out Funktion

Die Quick-Out Funktion ermöglicht eine schnelle Sperrung des Kobra VS-Datenträgers, indem innerhalb von 2 Sekunden doppelt auf die „X“-Taste geklickt wird.

9.11 Lock-Out Funktion

Mittels der Lock-Out Funktion kann der Administrator festlegen, ob die Kobra-Infosec-Smartcard (PKI-Karte) nach der Authentisierung im Kobra-VS-Datenträger verbleiben soll oder ob sie entfernt werden kann. Im eingeschalteten Lock-Out Modus wird der Zugriff auf die Daten unterbrochen, sobald die Kobra-Infosec-Smartcard (PKI-Karte) aus dem Gehäuse des Kobra-VS-Datenträgers entfernt wird (bei einem an ein Host-System angeschlossenen Kobra-VS-Datenträger nach ca. 3 Sekunden und im Batterie-Modus nach ca. 30 Sekunden).

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

9.12 Hinterlegung eines Update-Schlüssels

Vor dem Ausführen eines Updates muss der Administrator auf dem Kobra VS-Datenträger einen 256 Bit (32 Bytes) Update-Schlüssel hinterlegen. Diese Aufgabe kann er auch im Vorfeld bereits bei der ersten Einrichtung des Kobra VS-Datenträgers erledigen.

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

9.13 Export und Import der Einstellungen

Die Einstellungen des Kobra VS-Datenträgers können jederzeit exportiert, extern gespeichert und auf jeden beliebigen Kobra VS-Datenträger angewendet (importiert) werden.

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

9.14 Smartcard-Tabelle

Die Smartcard-Tabelle beinhaltet Informationen über die Kobra Infosec-Smartcards oder PKI-Karten, welche für den Zugriff auf den Kobra VS-Datenträger freigegeben sind. Der Administrator kann bis zu 8 Kobra Infosec-Smartcards in eine Smartcard-Tabelle mittels der Kobra Client VS Software eintragen. Zudem kann der Administrator festlegen, ob der jeweiligen Benutzer nur zum Lesen oder auch zum Schreiben berechtigt ist und ob der Benutzer den DEK löschen kann.

Die Beschreibung dieser Funktion befindet sich im Administratorhandbuch.

10. Formatierung

Der Kobra VS-Datenträger wird bereits im Auslieferungszustand mit dem Dateisystem FAT32 formatiert. Dieses Format wird von nahezu allen Betriebssystemen (Windows, macOS und Linux) unterstützt und ermöglicht sowohl das Lesen als auch das Schreiben von Daten. Die maximale Dateigröße in diesem Format beträgt bis zu 4 GB, was für die meisten Inhalte ausreichend ist.

Der Benutzer hat jedoch die Möglichkeit, den Kobra VS-Datenträger je nach Anwendungsbedarf umzuformatieren. Für Windows-Nutzer wird empfohlen, beispielsweise NTFS zu verwenden. Für macOS bietet das APFS-Dateisystem die beste Leistung, während bei Linux das EXT4-Dateisystem eine gängige Wahl darstellt.

Mit speziellen Erweiterungsprogrammen kann es unter Umständen auch möglich sein, Daten auf Dateisysteme zu schreiben, auf denen dies normalerweise nicht unterstützt wird. Selbstverständlich kann der Kobra VS-Datenträger auch in jedes andere Dateisystem formatiert werden. Dies hat jedoch keine Auswirkungen auf die Verschlüsselung der Daten oder den Schutz des Kobra VS-Datenträgers.

Aus der folgenden Tabelle können Sie die Kompatibilität zwischen den verschiedenen Betriebs- und Dateisystemen entnehmen.

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

Bezeichnung: L - Lesen, S - Schreiben, X - Keine Kompatibilität

Hinweis:

Bitte beachten Sie, dass die "Kobra Client-Software" (Kapitel 8. Kobra Client VS) ausgeschaltet sein muss, sobald Sie den Kobra VS-Datenträger formatieren.

11. Anwendungsmöglichkeiten

Die technischen Eigenschaften und Sicherheitsfunktionen der Kobra VS-Datenträger bieten umfangreiche Möglichkeiten für die sichere Speicherung, Archivierung und Übermittlung sensibler, personenbezogener sowie vertraulicher Informationen bis zur Geheimhaltungsstufe VS-NfD.

Die nachfolgenden Einsatzszenarien fallen ebenfalls unter dem Geltungsbereich der VS-NfD-Zulassung. Abweichungen von den beschriebenen Abläufen müssen mit dem BSI (Bundesamt für Sicherheit in der Informationstechnik) abgestimmt werden.

11.1 Kobra Connect

Mit der Software Kobra Connect können Kobra VS-Datenträger auch als Smartcard-Reader mit integrierter Tastatur für die PIN-Eingabe oder als Authentisierungs-Token mit PIN-Pad genutzt werden. Dies ermöglicht eine sichere und komfortable Identitätsprüfung für geschützte Anmeldevorgänge und Zugangskontrollen.

Zudem unterstützt Kobra Connect sowohl die Host- als auch die Geräte-Authentisierung, sodass der Kobra VS-Datenträger mittels dieser gegenseitigen Authentisierung nur auf autorisierten Systemen genutzt werden kann. Sensible Daten bleiben so ausschließlich innerhalb eines kontrollierten und geschützten IT-Umfelds zugänglich.

Gleichzeitig kann der VS-Datenträger bei Verbindung mit einem höher eingestuften System automatisch in einen schreibgeschützten Zustand versetzt werden.

Zusätzlich ermöglicht Kobra Connect Nutzung des VS-Datenträgers als Boot-Device im Windows-Read-Only-Modus. Dadurch kann ein vollständig portables Windows-Betriebssystem genutzt werden, ohne dass Veränderungen am Speichermedium vorgenommen werden. Dies ist besonders vorteilhaft für hochsichere IT-Umgebungen, in denen eine unveränderliche und manipulationssichere Systemumgebung erforderlich ist.

11.2 Host-Authentisierung

Mithilfe von Kobra Connect kann der Administrator festlegen, an welche Host-Systeme der Kobra VS-Datenträger angeschlossen werden darf. Hierzu wird sowohl im VS-Datenträger als auch im Host-System ein HAK (Host Authentication Key) hinterlegt. Im VS-Datenträger erfolgt dies über den Kobra Client VS, im Host-System über Kobra Connect.

Beim Anschließen überprüft der VS-Datenträger automatisch, ob der Computer zu den freigegebenen Hosts gehört. Diese Authentisierung erfolgt über ein starkes kryptografisches Verfahren, sodass der VS-Datenträger nur nach Verbindung mit einem berechtigten Host-System freigeschaltet werden kann.

An nicht autorisierten Host-Systemen bleibt der Datenträger gesperrt. Der Benutzer kann diese Funktion nicht beeinflussen. Somit ist gewährleistet, dass die eingestuften Informationen ausschließlich in einer geschützten VS-NfD-Umgebung („Verschlusssache – Nur für den Dienstgebrauch“) bearbeitet werden.

Selbst bei Verlust oder Diebstahl des VS-Datenträgers bietet diese Funktion zusätzlichen Schutz für sensible Daten.

11.3 Kobra Defence Zone

Um einen unbefugten Datenabfluss zu vermeiden, werden die USB-Schnittstellen an Host-Systemen in vielen Behörden und Unternehmen grundsätzlich gesperrt. Zu diesem Zweck können die Einstellungen im Betriebssystem oder spezialisierte USB-Blocker-Software verwendet werden. Mit Kobra VS-Datenträgern besteht erstmals die Möglichkeit, VS-NfD-eingestufte Daten in einer sicheren Umgebung auch außerhalb des Host-Systems zu speichern und zu transportieren.

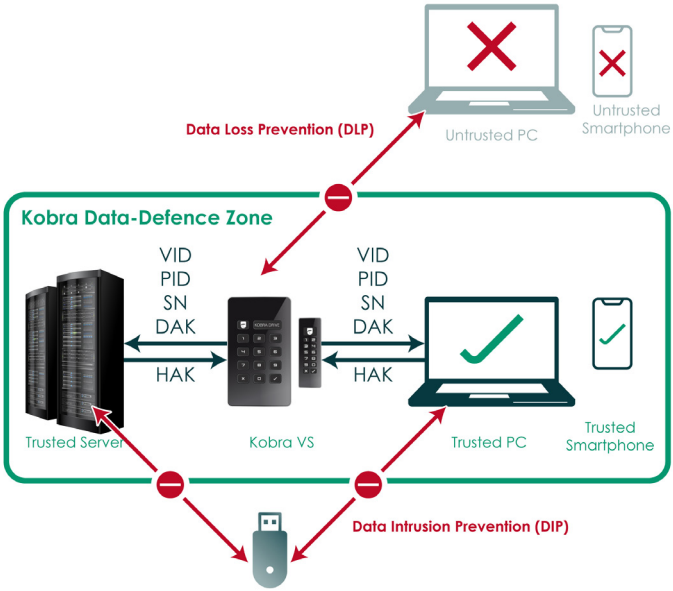
Neben den klassischen Erkennungsmerkmalen wie Vendor-ID (VID), Produkt-ID (PID) und Seriennummer (SN) bietet die Software Kobra Connect zusätzlich eine kryptographische Device-Authentisierung mittels DAK (Device Authentication Key). Der DAK wird ähnlich wie der HAK im VS-Datenträger und in Kobra Connect auf dem Host-System durch den Administrator gespeichert. Nach dem Anschluss des VS-Datenträgers an das Host-System erfolgt die Überprüfung und Freigabe des Datenträgers auf Basis eines kryptographischen Verfahrens. Dies ermöglicht eine eindeutige Identifizierung des angeschlossenen Datenträgers und dessen Freigabe für den jeweiligen Nutzer eines bestimmten Bereichs im internen Netzwerk.

Die Kombination aus gegenseitiger kryptographischer Host- und Device-Authentisierung bildet eine sichere Umgebung für sensible Daten – eine Kobra Defence Zone. Dies ist ein neues Konzept, bei dem USB-Datenträger erstmals Bestandteil der aktiven Schutzmaßnahmen für ein Netzwerk sind, statt als Einfallstor für Schadsoftware oder als Risiko für Datenverluste zu gelten.

Die Kobra Defence Zone stellt somit einen sicheren Bereich dar, in dem Daten durch Kobra VS-Datenträger geschützt und sicher zwischen air-gapped Systemen ausgetauscht werden können.

Ein typisches Beispiel hierfür ist die Übertragung von VS-NfD-eingestuften Daten von einem stationären Host-System (z. B. einem internen Netzwerk oder Server) auf einen VS-Datenträger zur weiteren Bearbeitung an einem mobilen Host-System (z. B. einem geschützten Laptop). Die Kobra Defence Zone gewährleistet, dass weder VS-Datenträger an ein nicht freigegebenes Host-System, noch andere Datenträger an die geschützten Host-Systeme innerhalb der Kobra Defence Zone angeschlossen werden können.

Somit wird sichergestellt, dass sämtliche Daten in der Kobra Defence Zone verbleiben und nicht abfließen können. Gleichzeitig wird verhindert, dass die Kobra-VS-Datenträger durch den Anschluss an unberechtigte Geräte mit Schadsoftware infiziert werden.



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 Erhöhen des Schutz-Niveaus für Kobra VS-Datenträger im Unternehmen

Der Administrator im Unternehmen oder einer Behörde kann festlegen, wie restriktiv sich der Kobra VS-Datenträger jedes Nutzers verhalten soll. Für diese Zwecke kann er für den Anwender die Anzahl der erlaubten Fehlversuche (beim Einsatz von PKI-Karten) und die Time-Out-Zeit festlegen. Zudem kann er festlegen, welcher Benutzer nur zum Lesen der Daten berechtigt ist und keinen DEK löschen darf. Mithilfe der Lock-Out-Funktion legt der Administrator fest, ob die Kobra Infosec-Smartcard (bzw. PKI-Karte) nach der Authentisierung im Kobra VS-Datenträger für die Sitzung verbleiben muss oder entfernt werden darf.

Der Benutzer kann diese Einstellungen auf der Basis seiner Berechtigungen nicht ändern.

11.5 Sicherer und kosteneffizienter Datentransport

Der Kobra VS-Datenträger kann für den sicheren Transport vertraulicher Daten verwendet werden. Dazu müssen die Kobra Infosec-Smartcards des Senders und des Empfängers in die Smartcard-Tabelle des Kobra VS-Datenträgers eingetragen

werden. Der Absender versendet ausschließlich den Kobra VS-Datenträger, denn auf diese Weise lässt sich ein regelmäßiger und sicherer Datenaustausch zwischen zwei Stellen organisieren.

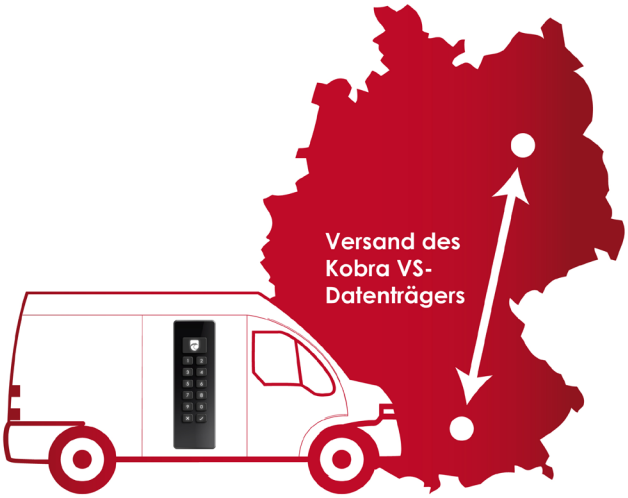
In der Stand-Alone-Ausführung verfügt der Nutzer über zwei Kobra Infosec-Smartcards, die bereits in der Smartcard-Tabelle des Kobra VS-Datenträgers eingetragen sind. In diesem Fall kann der Nutzer die zweite Kobra Infosec-Smartcard dem Empfänger zur Entschlüsselung der Daten zur Verfügung stellen. Alternativ kann der Administrator eine zusätzliche Kobra Infosec-Smartcard für den Empfänger in die Smartcard-Tabelle des Kobra VS-Datenträgers eintragen. Der Kobra VS-Datenträger und die Kobra Infosec-Smartcard werden dann separat an den Empfänger versendet. Auch die Benutzer-PIN und gegebenenfalls die SO-PIN (PUK) werden separat übermittelt, jedoch erst nach Erhalt der Kobra Infosec-Smartcard.

Bei der Nutzung von PKI-Karten trägt der Administrator die Seriennummer und den öffentlichen Schlüssel der PKI-Karten des Senders und Empfängers in die Smartcard-Tabelle des Kobra VS-Datenträgers ein. Dies erfolgt mit der Kobra Client VS Software. Der Kobra VS-Datenträger muss sich dabei physisch in Besitz des Administrators befinden, während die PKI-Karten bei den Anwendern verbleiben können.

Während des Transports des Kobra VS-Datenträgers muss durch eine geeignete Verpackung die Manipulationssicherheit gewährleistet werden. Empfohlen wird beispielsweise die Verwendung der versiegelten Kobra Infosec Sicherheitstaschen. Weitere Informationen zu den Sicherheitsmerkmalen des Kobra VS-Datenträgers finden Sie in *Kapitel 4. Echtheitsprüfung* und zu den Sicherheitstaschen in *Kapitel 12.2 Sicherheitsverpackung*.

Beim Erhalt des Kobra VS-Datenträgers ist dessen Authentizität zu prüfen. Dies erfolgt durch den Vergleich der Seriennummer des Datenträgers, die über einen separaten sicheren Weg mitgeteilt wird, sowie durch eine Datei mit einer spezifischen Kennung, die innerhalb des Datenträgers gespeichert ist. Die Seriennummer ist sowohl auf dem Gehäuse des Kobra VS-Datenträgers als auch bei der USB-Anmeldung des Geräts zu finden. Der Kobra Client VS zeigt die Modellbezeichnung und Seriennummer des Kobra VS-Datenträgers unmittelbar nach dem Anschließen an einen PC an.

Diese Methode ermöglicht es, den Kobra VS-Datenträger mit vertraulichen Daten kostengünstig und sicher über einen Paketdienstleister oder Kurier zu versenden.

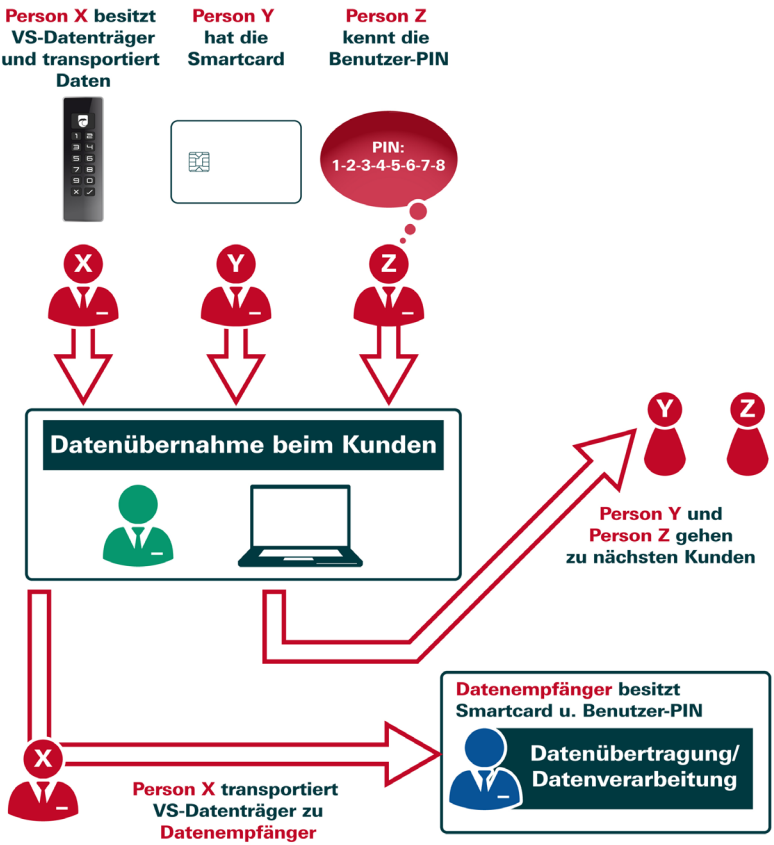


Warnhinweis:
Sollte es beim Transport zu Manipulationsversuchen gekommen sein, darf der Datenträger im Rahmen der VS-NfD Zulassung nicht mehr eingesetzt werden.

11.6 Trennung von Datenträger und Authentifizierungsmerkmalen

Der Zugriff auf die Daten kann so reglementiert sein, dass er nur durch das Zusammenführen von drei Personen möglich ist. Person X (z.B. Kurier) besitzt den Kobra VS-Datenträger, die Person Y verfügt über die freigegebene Kobra Infosec-Smartcard und die Person Z kennt die Benutzer-PIN. Die drei Personen kommen nur zur Datenübernahme an der Empfängerstelle zusammen und trennen sich anschließend wieder. Die Personen X, Y und Z haben dabei einzeln nicht die Möglichkeit auf die Daten zuzugreifen.

Warnhinweis:
Sollte es beim Transport zu Manipulationsversuchen gekommen sein, darf der Datenträger im Rahmen der VS-NfD Zulassung nicht mehr eingesetzt werden.



11.7 Verwendung weniger Datenträger bei großem Kundenkreis

Steht ein Unternehmen (z.B. ein Datenverarbeitungsunternehmen oder eine Datenzentrale von Großunternehmen/Behörden) im regelmäßigen Datenaustausch mit mehreren verschieden Anwendern, so können die Daten mit wenigen Kobra VS-Datenträgern kostengünstig und sicher transportiert werden.

Jeder Anwender erhält eine individuelle Smartcard. Die Seriennummer und der öffentliche Schlüssel aller Smartcards werden bei der Datenzentrale angelegt. Für jeden Datenaustausch mit einem anderen Anwender wird die Smartcard-Tabelle des Kobra VS-Datenträgers zuerst gelöscht. Im nächsten Schritt wird eine neue Tabelle mit den Smartcard-Informationen des Senders und Empfängers erstellt (Admin-PIN erforderlich). Anschließend können die Daten auf dem Kobra VS-Datenträger gespeichert und versendet werden.

Der Administrator löscht, nach Erhalt des Kobra VS-Datenträgers von einem Mitarbeiter, die alte Smartcard-Tabelle und erstellt eine neue mit den Smartcard-Informationen des nachfolgenden Nutzers. Aufwendige Datenlöschung und mehrmaliges Überschreiben des Datenträgers entfallen, da die verbliebenen Daten mit den vorherigen Krypto-Schlüsseln verschlüsselt wurden. Der Krypto-Schlüssel kann nach dem Löschen der Smartcard-Tabelle nicht rekonstruiert werden und somit besteht auch keine Möglichkeit auf die vorherigen Daten zuzugreifen.

Sollen mehrfach Daten in kurzen zeitlichen Abständen an den gleichen Empfänger verschickt werden, ist es nicht erforderlich, auf die Rücksendung eines personalisierten Kobra VS-Datenträgers zu warten. Es kann jeder im Unternehmen verfügbare Kobra VS-Datenträger verwendet werden. Hierzu kann die Smartcard-Tabelle des ersten Kobra VS-Datenträgers in die nächsten Kobra VS-Datenträger importiert werden *(Kapitel 9.14 Smartcard-Tabelle)*.

Die Anzahl der erforderlichen Datenträger kann dank dieser Eigenschaft wesentlich reduziert werden, da nicht für jeden Anwender ein personalisierter Kobra VS-Datenträger benötigt wird. Dabei ist es irrelevant, welche der im Unternehmen verfügbaren Kobra VS-Datenträger für den Datentransport verwendet werden. Entscheidend ist, welche Kobra Infosec-Smartcards (bzw. PKI-Karten) in der Smartcard-Tabelle des Kobra VS-Datenträgers eingetragen werden.

Hinweis:

Beim Löschen von Daten sollte auf das mehrmalige Überschreiben verzichtet werden, da dies die Lebensdauer des Datenträgers reduzieren kann. Sicher und effizient erfolgt die Löschung der Daten durch das Generieren eines neuen Krypto-Schlüssels (Kapitel 9.8 Löschen eines Krypto-Schlüssel) oder das Löschen der Smartcard-Tabelle (Kapitel 9.14 Smartcard-Tabelle).

Warnhinweis:

Sollte es beim Transport zu Manipulationsversuchen gekommen sein, darf der Datenträger im Rahmen der VS-NfD Zulassung nicht mehr eingesetzt werden.

11.8 Verwendung weniger Datenträger im Außendienst und bei Behörden

In einem Unternehmen verfügt jeder Außendienstmitarbeiter über seine personalisierte Smartcard (bzw. PKI-Karte) mit seinen eigenen kryptografischen Merkmalen. Für die Tätigkeit außerhalb des Unternehmens erhält der Mitarbeiter einen beliebigen Kobra VS-Datenträger, der zuvor für die Verwendung durch diesen Mitarbeiter vorbereitet wurde. Der Administrator löscht dazu die alte Smartcard-Tabelle und erstellt eine neue mit den Smartcard-Informationen dieses Mitarbeiters. Der Außendienstmitarbeiter speichert anschließend die Daten mit seinen eigenen kryptografischen Schlüsseln.

Nach der Benutzung gibt der Mitarbeiter den Kobra VS-Datenträger zurück. Dieser wird anschließend auf gleiche Weise innerhalb weniger Minuten für den nächsten Kollegen einsatzbereit gemacht. Dabei werden die Daten des Vornutzers

automatisch unwiderruflich gelöscht. Daher wird nicht für jeden Mitarbeiter ein eigener Kobra VS-Datenträger benötigt und die Anzahl der erforderlichen Datenträger im Unternehmen kann reduziert werden.

Hinweis:
Zusätzlich wird empfohlen vor der Rückgabe des Kobra VS-Datenträgers den aktuellen Krypto-Schlüssel zu löschen. Dadurch werden die Daten auf dem Kobra VS-Datenträger bereits vor der Rückgabe an den Administrator zerstört.

11.9 Betreiben mehrerer Datenträger mit nur einer Smartcard

Zum Betreiben mehrerer Datenträger mit nur einer Smartcard wird die Smartcard-Tabelle mit den gleichen Smartcard-Informationen (Seriennummer und öffentlicher Schlüssel) auf mehreren Kobra VS-Datenträgern mit Unterstützung der Kobra Client VS Software hinterlegt.

Von besonderem Interesse ist dieses Szenario für die Arbeit mit Datenvolumen, die die Kapazität eines Kobra VS-Datenträgers übersteigen. Hier können die Daten auf mehrere Kobra VS-Datenträger verteilt werden.

Auch wenn Daten sehr häufig, z.B. täglich verschickt werden, bietet es sich an, mehrere Speichermedien auf diese Weise zu verwenden. Es kann täglich ein neuer Kobra VS-Datenträger mit der gleichen Smartcard-Tabelle versendet werden, ohne dass auf einen personalisierten Kobra VS-Datenträger gewartet werden muss. Der Versender und der Empfänger können stets mit der gleichen Smartcard auf den Kobra VS-Datenträger zugreifen.

Hinweis:
Beim Versand des Kobra VS-Datenträgers sind weitere Maßnahmen erforderlich, die unter Kapitel 11.5 Sicherer und kosteneffizienter Datentransport beschrieben werden.

11.10 Verwendung als verschlüsseltes Boot-Device

Die integrierte autonome Stromversorgung ermöglicht die Authentisierung des Kobra VS-Datenträgers vor dem Start eines PCs (Pre-Boot-Authentisierung). Diese Eigenschaft bietet die Möglichkeit, Betriebssysteme verschlüsselt auf dem Kobra VS-Datenträger zu speichern und anschließend direkt vom Kobra VS-Datenträger zu starten.

In diesem Zusammenhang können Betriebssysteme, wie beispielsweise Windows, Linux, ECOS-OS und andere, sowie Benutzerdaten gespeichert werden. Dieses Anwendungsszenario ist sowohl für stationäre als auch mobile Computer geeignet. Zu beachten sind dabei die minimalen erforderlichen Speicherkapazitäten. Das Betriebssystem Windows kann erst auf Kobra VS-Datenträgern mit Speicherkapazitäten von mindestens 32 GB verwendet werden. Außerdem sind für diese Zwecke Kobra VS-Datenträger mit pSLC-Speicher zu empfehlen, um eine möglichst lange Lebensdauer zu gewährleisten.

Zudem ermöglichen die Funktionen „Stromüberbrückung“ und „Sperren beim Auswerfen ausschalten“, dass die Kobra VS-Datenträger auch an Host-Systemen mit verschiedenen Verhaltensweisen im Boot-Vorgang als Boot-Device verwendet werden können. Je nach Anforderung kann der Kobra VS-Datenträger sowohl als lokaler Datenträger als auch als Wechseldatenträger konfiguriert sein.

Beim Trennen des Datenträgers vom PC bleiben Daten, Programme und Betriebssysteme inklusive temporärer Dateien ausschließlich auf dem VS-Datenträger verschlüsselt gespeichert und sind für Unbefugte unzugänglich.

Bei der Verwendung des VS-Datenträgers als verschlüsseltes Boot-Device für den VS-Arbeitsplatz sollten zusätzlich noch folgende Maßnahmen berücksichtigt werden:

- Deaktivierung der internen Datenträger des Hosts über Gruppenrichtlinien bzw. Konfigurationen der Betriebssysteme.
- Einführung einer Schnittstellenkontrolle über zusätzliche Software oder Gruppenrichtlinien bzw. Konfigurationen der Betriebssysteme.
- Sofern der VS-Arbeitsplatz mit einem Netzwerk verbunden wird, sind in der Regel zusätzliche Software für VPN-Verbindungen und eine geeignete Firewall erforderlich.

Hinweis:

Die Windows Kompatibilität kann durch den Administrator per Kobra Client VS konfiguriert werden.

11.11 Verwendung an verschiedenen Betriebssystemen und Smartphones

Der Kobra VS-Datenträger funktioniert durch seine Hardware-Verschlüsselung und Hardware-Authentisierung unabhängig vom Betriebssystem und kann an nahezu jedem Gerät verwendet werden, das USB-Datenträger unterstützt.

Der optimierte Stromverbrauch ermöglicht es, den Kobra VS-Datenträger zum Datenaustausch mit einem Smartphone oder Tablet zu verwenden.

Hinweis:

Sofern sich VS-NfD eingestufte Informationen auf dem Datenträger befinden, ist die Verwendung ausschließlich an den zur Verarbeitung von VS-NfD Informationen zugelassenen Geräten im Rahmen der Zulassung erlaubt. Das Löschen von VS-NfD Informationen auf dem Datenträger muss entsprechend der Verfahren in Kapitel 9.8 Löschen eines Krypto-Schlüssel.

11.12 Verwendung als Datendiode

Der aktivierte Schreibschutz des Kobra VS-Datenträgers bietet einen sicheren Schutz für das ungewünschte Abfließen von Informationen aus höher eingestuften Systemen auf niedriger eingestufte Systeme.

Hierzu werden die Daten aus dem Quell-System (z.B. VS-NfD) auf den Kobra VS-Datenträger geschrieben und anschließend der Schreibschutz auf dem Kobra VS-Datenträger aktiviert. Im Folgenden wird der Kobra VS-Datenträger an das höher eingestufte System (z.B. Geheim) angeschlossen und die benötigten Daten von dem Kobra VS-Datenträger auf das Hostsystem übertragen. Im Nachgang kann der Datenträger wieder normal im Ursprungssystem eingesetzt werden.

Eventuelle weitere Sicherheitsmaßnahmen wie z.B. Virenscan sind weiterhin erforderlich. Optional kann vorher und hinterher ein schnelles, sicheres Löschen des Kobra VS-Datenträgers mittels Neugenerierung des Krypto-Schlüssels durchgeführt werden.

Für die Umsetzung der Datendiode-Funktion kann zudem der Administrator zwei Smartcards wie folgt definieren: Eine Smartcard ist für die Arbeit im VS-NfD-Bereich und die zweite Smartcard ist für den Bereich Geheim. Die Smartcard für den VS-NfD-Bereich ermöglicht das Lesen und Schreiben. Die Smartcard für den Bereich Geheim ermöglicht nur das Lesen.

Anschließend verbleibt die Smartcard „VS-NfD“ ausschließlich in dem IT-Bereich für VS-NfD. Die Smartcard „Geheim“ befindet sich ausschließlich im IT-Bereich Geheim. Werden nun Daten aus dem VS-NfD-Bereich in den Geheim-Bereich mittels Kobra VS-Datenträger übertragen, wird automatisch sichergestellt, dass der Kobra VS-Datenträger bei der Verwendung an dem Geheim-System ausschließlich lesend funktioniert. Weder bewusst noch unbewusst können sensible und als Geheim klassifizierte Informationen auf den Kobra VS-Datenträger gelangen.

11.12 Verwendung als Authentisierungs-Medium

Der Kobra VS-Datenträger ermöglicht eine sichere Speicherung von Authentisierungsmerkmalen, wie beispielsweise Benutzernamen, sehr komplexe Passwörter, digitale Zertifikate, Schlüsselpaare und anderen. Jedoch ist die Verwendung von USB-Speichermedien in einigen Unternehmen und Organisationen grundsätzlich verboten, um ungewollten Datenabfluss zu vermeiden.

Ähnlich wie bei der Verwendung als Datendiode kann der Kobra VS-Datenträger so konfiguriert werden, dass dem Nutzer nach der Speicherung der Authentisierungskomponenten nur Leserechte zur Verfügung stehen. Diese Datenträger können anschließend vom Administrator für die Nutzung an der Unternehmens-IT freigegeben werden. Jeder Mitarbeiter kann auf diese Weise ein sicheres Authentisierungsmedium erhalten, ohne die IT-Sicherheit des Unternehmens zu gefährden.

11.13 Nutzung als Smartcard-Reader mit PIN-Pad

Der VS-Datenträger kann außerdem als Smartcard-Reader mit der Tastatur für die PIN-Eingabe bzw. als Authentisierungs-Token mit PIN-Pad verwendet werden. Mithilfe dieser Funktion kann der Nutzer sowohl die Kobra Smartcard als auch seine eigene Smartcard zum Unterzeichnen digitaler Dokumente verwenden, ohne dafür einen anderen Kartenleser anschaffen zu müssen. Dadurch können sowohl die Anzahl der erforderlichen Geräte auf einem Arbeitsplatz als auch die Beschaffungskosten reduziert werden.

Die Kobra Infosec Smartcard kann beispielsweise für die E-Mail-Verschlüsselung, den VPN-Zugang, die Windows- oder Linux-Anmeldung und die allgemeine 2-Faktor-Authentifizierung mit digitalem Zertifikat eingerichtet werden.

Zur Verwendung als Smartcard-Reader mit PIN-Pad wird die Software „Kobra Connect" auf den Host-Systemen benötigt.

11.14 Integration in bereits vorhandene Smartcard- und PKI-Infrastrukturen

Wird in einem Unternehmen bereits die Smartcard Atos CardOS 5.0 oder 5.3, CC EAL 4+ verwendet (z. B. für das Zutrittsmanagement, die Nutzerauthentisierung etc.) oder werden andere Smartcards genutzt, die den Anforderungen an die Sicherheit für VS-NfD erfüllen, ist eine Integration des Kobra VS-Datenträgers möglich. Außerdem können die Kobra VS-Datenträger in die PKI-Infrastrukturen bei Behörden oder Unternehmen integriert werden. In diesem Fall können die Anwender beispielsweise ihren Mitarbeiterausweis zur Freischaltung des Datenträgers verwenden.

11.15 Integration von bestehenden Softwarelösungen

Alle bereits im Unternehmen existierenden Softwarelösungen für externe Datenträger können weiterhin ergänzend verwendet werden, um die Sicherheitseigenschaften und Verwendungsmethoden zu erweitern.

11.16 Nutzung der VID, PID, SN und DAK zum Schutz von Unternehmensdaten

Optional können die USB Vendor ID (VID) und Product ID (PID) kundenspezifisch implementiert werden. Die Kobra VS-Datenträger können anhand dieser Informationen sowie der Seriennummer und des DAK (Device Authentication Key) verschiedenen Abteilungen und Nutzergruppen eindeutig zugeordnet werden. Diese verfügen gegebenenfalls zusätzlich über unterschiedliche Berechtigungen für USB-Verbindungen im firmeninternen Netzwerk. Auf diesem Wege kann festgelegt werden, welche Kobra VS-Datenträger an welchen USB-Schnittstellen im Unternehmen angeschlossen werden dürfen. Das Anschließen von anderen „unberechtigten" USB-Datenträgern kann dadurch verhindert werden. Zur Steuerung der USB-Anschlüsse an den Host-Systemen kann zusätzliche Software erforderlich sein.

11.17 Sicherer Arbeitsplatz mit Read-Only Betriebssystemen (z.B. Windows)

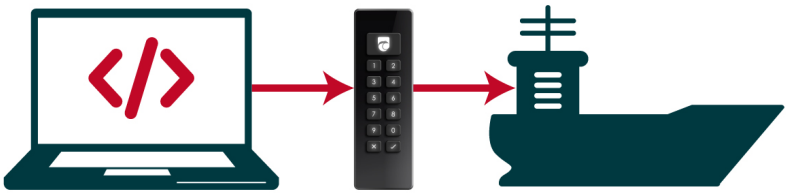
Auch nach der Installation eines Betriebssystems kann der Kobra VS-Datenträger in den schreibgeschützten Modus versetzt und anschließend gebootet werden. Dadurch verbleibt das Betriebssystem immer im Originalzustand und die verarbeiteten Daten werden niemals auf diesem Datenträger gespeichert. Dies ist insbesondere sinnvoll für Fernwartung, Remote-Access oder wenn Inhalte, die höher als VS-NfD eingestuft sind, verarbeitet werden sollen.

Für Updates oder zusätzliche Software kann der Schreibschutz wieder deaktiviert werden. Speziell für Windows empfiehlt sich die Verwendung der Software „Kobra Connect", um zur Laufzeit einen beschreibbaren Datenträger zu simulieren.

11.18 Secure Software Deployment

Ein großer Vorteil der Kobra VS-Datenträger ist die hardware- und softwareunabhängige Interoperabilität. Dadurch kann der Datenträger an sämtlichen informationstechnischen Anlagen, Maschinen und Systemen angeschlossen werden, welche USB-Datenträger unterstützen. „Secure Software Deployment" dient dazu, gezielt abgesicherte Offline-Systeme mit Software-Updates oder initialen Installationen auszustatten.

Hervorzuheben ist, dass Informationen nicht auf einem unverschlüsselten Datenträger zwischengespeichert werden, sondern direkt vom Kobra VS-Datenträger in das System übertragen werden können. Somit können diese Datenträger in unmittelbarer Nähe zu den betreffenden Systemen hinterlegt werden, um sie im Notfall zur schnellen Wiederherstellung des Systems zu nutzen.



Typische Fälle sind:

- Update von PKI-Root-Systemen,
- Installation und Wiederherstellung von Systemen im Feld,
- Ersteinrichtung von Maschinen und Anlagen.

11.19 Data-Logging

Aufgrund der hardware- und softwareunabhängigen Interoperabilität kann der VS-Datenträger ebenfalls an sämtlichen informationsverarbeitenden Anlagen, Maschinen und Systemen angeschlossen werden, um Log-Daten dieser Hosts direkt auf den Kobra VS-Datenträger zu schreiben, ohne dass die Informationen vorher unverschlüsselt zwischengespeichert werden.

Typische Anwendungsfälle sind:

- Log-Daten von Fahrzeugen
- Aufzeichnung von Kameras
- Beweissicherung aus unbekannten Systemen

11.20 Zwei-Faktor-Authentisierung für weitere Anwendungen

Generisch ist der Smartcard Reader der Kobra VS Datenträger mit allen Softwarelösungen kompatibel, die CCID Smartcard Reader unterstützen. Die mitgelieferte Kobra Smartcard kann über geeignete PKI-Lösungen mit zusätzlichen Zertifikaten und Schlüsseln beschrieben werden. In diesen Fällen übernimmt der Kobra VS-Datenträger die Funktion eines Smartcard-Readers mit PIN-Pad und stellt den sicheren Zugriff auf die Smartcard bereit. Die Smartcard enthält zusätzliche Zertifikate, die dem jeweiligen Anwendungsfall entsprechen und dessen Spezifikationen erfüllen. Dadurch wird die Anzahl der benötigten Hardware-Komponenten bei den Endanwendern reduziert.

Beispielhafte Einsätze sind:

- UEFI Preboot-Authentisierung für softwarebasierte Festplattenverschlüsselungslösungen wie R&S® Trusted Disk oder Utimaco DiskEncrypt VS-NfD.
- Sichere E-Mail-Verschlüsselung mit Softwareprodukten wie Cryptovision GreenShield oder GnuPG VS-Desktop.
- Sichere VPN-Verbindungen mit Softwareprodukten wie R&S® Trusted VPN Client, GenuConnect, NCP VS GovNet Connector oder TheGreenBow.

Auf den Host-Systemen wird die ergänzende Software Kobra Connect benötigt.

11.21 Kombinierter Einsatz mit Datenschleusen

Datenschleusen wie PROVAIA, itWash, OPSWAT MetaDefender Kiosk oder das Hunna USB Sanitation System werden immer beliebter. Sie prüfen Daten von mobilen Datenträgern, bevor diese in geschützte Netze übertragen werden können. In diesem Kontext ist die Kombination mit Kobra VS-Datenträgern sehr sinnvoll. So können die internen Netze so konfiguriert werden, dass nur bestimmte Kobra VS-Datenträger angeschlossen werden können.

Auf diese Weise wird sichergestellt, dass weder bewusst noch unbewusst ungeprüfte Medien an die geschützten Netze angeschlossen werden. Des Weiteren kann der Kobra VS-Datenträger in den Read-Only-Modus versetzt werden, nachdem er mit den geprüften Daten von der Datenschleuse beschrieben wurde. Dadurch kann nach der Prüfung keine Schadsoftware mehr auf diesen Datenträger gelangen.

In Kombination mit der Kobra Defence Zone wird sichergestellt, dass „gewaschene" Datenträger ausschließlich innerhalb der vertrauenswürdigen Netze angeschlossen werden. Gleichzeitig wird verhindert, dass unberechtigte Datenträger mit den vertrauenswürdigen Netzen verbunden werden.

11.22 Passwortspeicher

Die Kombination aus dem Kobra VS-Datenträger und einer etablierten Passwort-Manager-Software wie KeePass erhöht das Schutzniveau für sensible Passwörter.

Einerseits wird die Passwort-Datenbank sicher im verschlüsselten Speicher des Kobra VS-Datenträgers abgelegt. Zum anderen ist der Zugriff auf die Passwort-Datenbank nur nach vorheriger 2-Faktor-Authentisierung durch die Smartcard im Kobra VS-Datenträger und die PIN-Eingabe möglich.

11.23 Schutz sensibler Daten vor versehentlicher oder unbefugter Löschung

In einigen Situationen – beispielsweise nach der Aufnahme besonders sensibler Informationen – muss gewährleistet sein, dass der Nutzer die gespeicherten Daten weder zerstören noch verändern kann.

Zu diesem Zweck integriert der Administrator mithilfe der Software Kobra Client VS in den VS-Datenträger einen Benutzer mit Schreibberechtigung, damit dieser die Daten aufnehmen kann, sowie einen zweiten Benutzer ohne Schreibberechtigung, damit dieser die Daten transportieren und auswerten kann. Bei beiden Benutzern wird die Funktion „Kann DEK löschen" deaktiviert.

11.24 Geo-Redundante Backups und Instant Recovery

In die Smartcard-Tabelle eines Kobra VS-Datenträgers können bis zu 8 Smartcards integriert werden. Zudem kann der Administrator einrichten, dass bestimmte Benutzer weder über eine Schreibberechtigung verfügen, noch DEK löschen können. Somit werden die Integrität und die Verfügbarkeit der gespeicherten Daten gleichzeitig gewährleistet. In der Kombination mit sicherem Schutz gegen unbefugte Zugriffe machen diese Funktionen den Kobra VS-Datenträger zu einer Top-Lösung für Geo-redundante Backups und Instant Recovery.

Zu diesem Zweck werden neben der Smartcard einer global verantwortlichen Person noch die Smartcards einer oder mehrerer lokaler Benutzer aus verschiedenen Rechenzentren oder Standorten in den Kobra VS-Datenträger erfasst.

Die Datenkopien werden auf mehreren Kobra VS-Datenträgern gespeichert und geo-redundant an geografisch weit voneinander entfernte Rechenzentren und Standorte verteilt. So ist die Datensicherheit im Falle eines lokalen Ausfalls, einer Naturkatastrophe oder eines anderen Ereignisses am primären Standort gewährleistet.

Diese Methode eignet sich ebenfalls sehr gut für Instant Recovery: Nach einem Systemausfall sind virtuelle Maschinen oder Anwendungen so in kürzester Zeit (oft in Minuten statt Stunden) wieder einsatzbereit. Anstatt die gesamte Backup-Datenmenge wiederherzustellen, wird die Anwendung direkt vom Kobra VS-

Datenträger gestartet. Dabei werden nur die tatsächlich benötigten Daten in Echtzeit bereitgestellt. Dies reduziert Ausfallzeiten (RTO) drastisch und sorgt für Kontinuität im Geschäftsbetrieb.

Zusammenfassung:

- 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

11.25 Quellcode Hinterlegung

Bei einer auftragsbezogenen Softwareentwicklung verlangt der Auftraggeber oft eine Hinterlegung des Quellcodes, um sich vor Ausfällen des Softwareherstellers (z. B. Insolvenz) zu schützen. Unter bestimmten Bedingungen soll dabei der Zugang zum Quellcode ermöglicht werden, um die Software nach Wartung oder Weiterentwicklung durch den ursprünglichen Anbieter absichern zu können.

Mit Unterstützung der Kobra VS-Datenträger kann diese Aufgabe leicht gelöst werden. Der Quellcode wird auf einem VS-Datenträger gespeichert und dem Auftraggeber übergeben. Die Smartcard, die zum Zugriff auf diesen Datenträger berechtigt, wird bei einem Notar hinterlegt. Im Bedarfsfall erhält der Auftraggeber die Smartcard und kann somit auf die gespeicherten Daten zugreifen.

Diese Methode sichert die Investitionen des Kunden, gewährleistet die Kontinuität des Betriebs und schützt gleichzeitig das geistige Eigentum des Herstellers.

11.25 Fernverwaltung von VS-Datenträgern mit TOM-System

Das System R&S®Trusted Objects Manager (TOM-System) ist ein zentrales Managementsystem mit einer BSI-Empfehlung zur Datenverarbeitung bis VS-NfD, EU & NATO RESTRICTED. Es ermöglicht die VS-NfD-zugelassene Verwaltung von Kobra VS-Datenträgern bei Militär, Behörden und Unternehmen aus der Ferne und kann als ergänzende Lösung für die Software „Kobra Client VS" eingesetzt werden.

Der Administrator kann den Kobra VS-Datenträger über das Web-Interface des TOM-Systems und die örtlich verteilten Endpoints einfach und zentral für die jeweilige Verwendung bereitstellen.

12. Optionales Zubehör

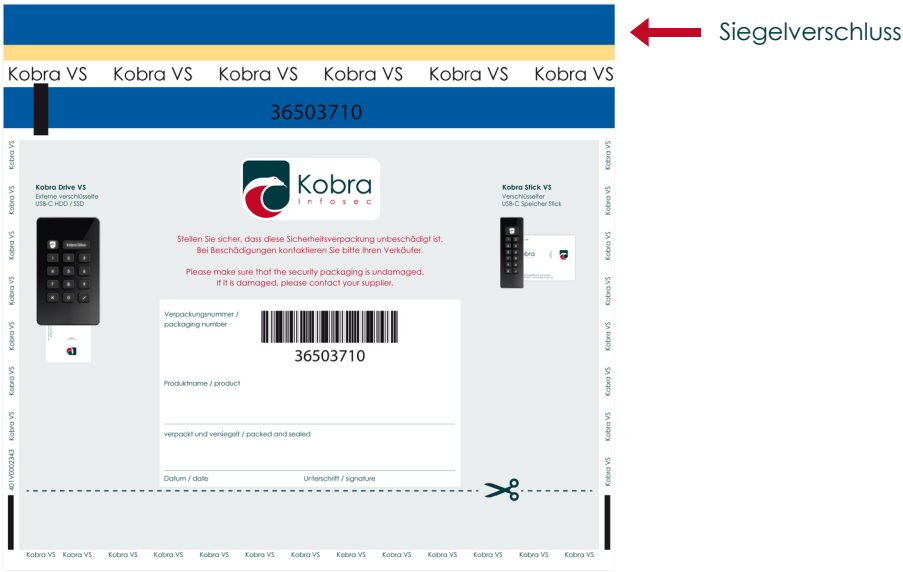
Zur Umsetzung der nutzerspezifischen Aufgaben werden zusätzliche Smartcards und Sicherheitsverpackungen als optionales Zubehör angeboten.

12.1 Zusätzliche Smartcards

Bei Bedarf können die zugelassenen Kobra Infosec-Smartcards zusätzlich bei der Kobra Infosec GmbH bestellt werden. Diese werden mit vorgenerierten Schlüsselpaaren ausgeliefert und verfügen über voreingestellte Benutzer- und SO-PIN (PUK) mit Standardwerten. Zur Inbetriebnahme beachten Sie bitte *Kapitel 6. Inbetriebnahme des Kobra VS-Datenträgers*.

12.2 Sicherheitsverpackung

Um Manipulationen zu erkennen, wird für den Versand des Kobra VS-Datenträgers und der Kobra Infosec-Smartcards (bzw. PKI-Karten) eine spezielle Kobra VS Sicherheitsverpackung empfohlen. Diese Verpackung kann ebenfalls als optionales Zubehör bei autorisierten Lieferanten bestellt werden.



Der Inhalt der Sicherheitsverpackung wird auf der Verpackung beschrieben. Der Empfänger überprüft nach Erhalt die Unversehrtheit des Sicherheitsschriftzugs „KOBRA VS SECURITY " an den Seiten. Zusätzlich befindet sich am oberen Ende ein spezieller Siegelverschluss, der jegliche Manipulationsversuche anzeigt.
Mögliche Indikatoren:

Der blaue Streifen unter dem oberen Bereich des Siegelverschlusses und der blassgelbe Thermostreifen deuten darauf hin, dass die Sicherheitsverpackung korrekt verschlossen ist und nicht wieder geöffnet wurde.

Bei extremer Kälte (z.B. Einsatz von Kältespray) trennen sich Bereiche des blauen Verschlussbandes vom Trägermaterial. Die Warnung "STOP" wird lesbar.

Durch starke Wärmeeinwirkung (z.B. durch Föhn) färbt sich der blassgelbe Thermostreifen rot.

Beim Einsatz von Lösungsmitteln löst sich die blaue Farbe des Siegelverschlusses auf. Die Manipulation ist sofort sichtbar.

Stellen Sie nach Erhalt sicher, dass diese Indikatoren nicht ausgelöst wurden.

13. Technische Spezifikationen

Transferrate:	USB 3.0 max. 5 GBit/s USB 2.0 max. 480 MBit/s Die tatsächlich zu erreichende Schreib- und Leserate hängt von der gewählten Speichergröße, Speicherart, dem USB-Anschluss und dem Host-System ab.
Verschlüsselung:	256 Bit AES Hardwareverschlüsselung, XTS-Modus, mit 2 x 256-Bit Krypto-Schlüssel

Kobra Stick VS

Speichergrößen:	16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB, 1 TB
Speicherarten:	3D TLC, MLC und pSLC

Kobra Drive VS

Speichergrößen:	500 GB, 1 TB, 2 TB, 4 TB, 8 TB, 16 TB
Speicherarten:	HDD, SSD

14. Lieferumfang

- Kobra VS-Datenträger Version 1.0
- 2 USB-Kabel (USB-C zu USB-C, USB-C zu USB-A)
- zwei Kobra Infosec-Smartcards (optional)
- Quick Start Guide

15. Datensicherheit, Datenverfügbarkeit und Haftungsausschluss

Die Kobra VS-Datenträger bieten Ihnen eine hohe Datensicherheit nach dem aktuellen Stand der Technik. Sie gewährleisten die datenschutzkonforme Speicherung und Aufbewahrung sowie den sicheren Transport sensibler, personenbezogener und vertraulicher Informationen bis zur Geheimhaltungsstufe VS-NfD.

Um ebenso hohe Datenverfügbarkeit zu erreichen, empfehlen wir Ihnen, die auf dem Kobra VS-Datenträger befindlichen Daten regelmäßig auf anderen Kobra VS-Datenträgern zusätzlich zu sichern. Dies schützt Sie in unvorhergesehenen Situationen vor einem vollständigen Datenverlust.

Die Kobra Infosec GmbH haftet nicht für den Verlust von Daten sowie für dadurch entstehende Kosten und Schäden. Zudem trägt das genannte Unternehmen keine datenschutzrechtliche Verantwortung für die gespeicherten Daten.

16. Sicheres Beenden nach Benutzung des Kobra VS-Datenträgers

Aus Sicherheitsgründen ist eine logische oder physische Trennung des Kobra VS-Datenträgers nach der Benutzung vom Wirtssystem durchzuführen. Dies empfiehlt sich vor allem bei der Beendigung einer Sitzung, kurzfristigen Unterbrechungen sowie beim Verlassen des Arbeitsplatzes. In diesem Zusammenhang bietet die aktivierte Time-Out-Funktion bedeutende Unterstützung zum effektiven Datenschutz.

Die schnelle Abmeldung kann durch doppeltes Drücken der X-Taste innerhalb von 2 Sekunden erfolgen (Quick-Out-Funktion).

Für die sichere physische Trennung muss das USB-Kabel vom Kobra VS-Datenträger vollständig entfernt werden.

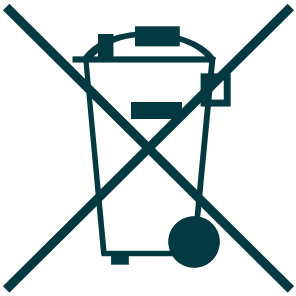
Hinweis:

Um einen Datenverlust zu vermeiden, vergewissern Sie sich vor Trennung der Verbindungen, dass die Datenübertragung sowie die Zugriffe auf den Kobra VS-Datenträger vollständig abgeschlossen sind.

17. Hinweis zum Schutz und Erhalt der Umwelt

Gemäß der EG-Richtlinie dürfen Elektro- und Elektronik-Altgeräte nicht als kommunaler Abfall entsorgt werden. Um die Freisetzung der enthaltenen Schadstoffe in Ihrer Umgebung zu vermeiden und natürliche Ressourcen zu schonen, bitten wir Sie, dieses Produkt nach Ablauf seiner Lebensdauer ausschließlich an einer lokalen Sammelstelle für Elektro-Altgeräte in Ihrer Nähe abzugeben.

Dank dieser Maßnahmen können die Materialien Ihres Produkts umweltfreundlich wiederverwendet werden.



18. Umgang mit Sicherheitsfehlern

Für eine geregelte Erfassung, Klassifizierung und Behebung eventueller Fehler stellt der Hersteller ein Fehlermanagement für die Administratoren von Kobra VS-Datenträgern zur Verfügung. In diesem Kapitel finden Sie Hinweise dazu, wie Sie sich beim Hersteller registrieren können, sowie die genauen Schritte zum Melden von vermuteten Fehlern. Sämtliche Vorgänge zum Fehlermanagement können Sie über die Webseite https://kobra-infosec.de/de/all-support-sites/analysis.html oder über die E-Mail-Adresse vs@kobra-infosec.de durchführen.

18.1 Registrierung

Für automatische Benachrichtigungen zu eventuellen Sicherheitsproblemen Ihres Kobra VS-Datenträgers empfehlen wir eine Registrierung unter https://kobra-infosec.de/de/contact.html. Obligatorisch ist die Angabe einer E-Mail-Adresse und die Auswahl des Produkts, alle weiteren Angaben sind freiwillig. Hilfreich ist zudem die Angabe der Seriennummern, um konkretere Handlungsempfehlungen im Falle von auftretenden Sicherheitsrisiken geben zu können.

Nach der erfolgreichen Registrierung erhalten Sie von uns eine Geheimhaltungsvereinbarung, die Sie per E-Mail unterschrieben und eingescannt an vs@kobra-infosec.de zusenden können. Nach einer durch uns erfolgten Prüfung werden Sie auf die Verteilerliste aufgenommen und erhalten hierzu eine separate Bestätigungs-E-Mail.

Neben den automatischen Benachrichtigungen zu eventuellen Sicherheitsproblemen erhalten Sie per E-Mail auch die Hinweise zur Vermeidung dieser Probleme. Auf Wunsch können Sie zusätzlich Benachrichtigungen zu Firmware-Updates und neuen Modellen erhalten.

Sollten Sie keine weiteren Informationen zu Sicherheitsproblemen mit Ihrem Kobra VS-Datenträger mehr wünschen, können Sie sich jederzeit per E-Mail an vs@kobra-infosec.de aus dem Verteiler löschen lassen.

18.2 Fehler melden

Im Rahmen der kontinuierlichen Produktverbesserung und -wartung prüfen wir regelmäßig, ob die durch das BSI zugelassene Sicherheitsleistung im Rahmen von VS-NfD trotz neuer Angriffsstrategien weiterhin erbracht wird. Sollten Sie oder ein von Ihnen beauftragter Dienstleister vor uns eine mögliche Schwachstelle entdecken, sind wir über entsprechende Hinweise dankbar, um die Sicherheit für alle Nutzer zu verbessern.

Da eine mögliche Zero-Day-Attacke die Sicherheit einer großen Anzahl von Nutzern maßgeblich einschränken könnte, ist es wesentlich, dass diese Information geheim gehalten wird, bis durch uns ein Firmware-Update bereitgestellt werden kann und der Großteil der Anwender dieses in seine Geräte integriert hat. In diesem Zusammenhang soll die Mitteilung über eine eventuelle Schwachstelle ausschließlich

verschlüsselt erfolgen. Hierzu dient entweder das Formular auf https://kobra-infosec.de/de/contact.html oder eine verschlüsselte E-Mail an vs@kobra-infosec.de. Das S/MIME-Zertifikat und den PGP-Key hierzu finden Sie ebenfalls auf https://kobra-infosec.de/de/contact.html.

Für die korrekte Einordnung und schnelle Behebung des möglichen Fehlers benötigen wir folgende Informationen:

1) Betreffendes Modell und Version
2) Seriennummer des Gerätes bei dem der Fehler aufgetreten ist
3) Eine Beschreibung des Vorgehens zur Reproduktion des Fehlers
4) Welche Vorteile kann ein Angreifer durch diesen Fehler erhalten (optional)
5) Empfehlungen zur Behebung des Fehlers (optional)

Auch nicht sicherheitskritische Fehler und benutzerspezifische Verbesserungshinweise können uns über den oben beschriebenen Kontaktweg mitgeteilt werden. Allgemeine Fragen zur Verwendung und Funktionsweise des Kobra VS-Datenträgers richten Sie an uns bitte per E-Mail an info@kobra-infosec.de, telefonisch an +49/345/2317353 oder per Web-Formular auf der Website https://kobra-infosec.de/de/contact.

19. FAQ

Hier finden Sie die wichtigsten FAQ der Kobra VS-Datenträger. Weitere FAQ, Anleitungen und Videos finden Sie auf www.kobra-infosec.de

Allgemein

Der Kobra VS-Datenträger bleibt nach Drücken der Haupttaste im Schlafmodus (Alle Tasten sind unbeleuchtet)

Der Kobra VS-Datenträger muss per USB-Kabel für ein paar Minuten aufgeladen werden.

Die Haupttaste blinkt rot und andere Tasten sind aus

Prüfen Sie, ob eine gültige Smartcard eingelegt wurde und die Ausrichtung korrekt ist. Die Smartcard muss mit den Kontakten nach oben eingeschoben werden.

Smartcard eingelegt / nicht eingelegt

Die Haupttaste blinkt rot, während alle anderen Tasten aus sind.

Es gibt 3 mögliche Indikatoren, warum die Haupttaste rot blinkt:

A: Es befindet sich keine Smartcard im Kobra VS-Datenträger.

B: Eine Smartcard ist seitenverkehrt eingelegt (es besteht kein Kontakt mit dem Kartenleser) oder es ist kein Chip vorhanden.

Die Haupttaste blinkt gelb, während alle anderen Tasten aus sind.

Eine Smartcard ist richtig eingelegt, jedoch ist diese nicht mit dem Kobra VS-Datenträger kompatibel (EC-Karte, fremde Chip-Karten). Es ist kein Login möglich. Wenn Sie die Haupttaste und Taste 1 drücken, leuchtet die Haupttaste blau.

Die Haupttaste leuchtet weiß, während alle anderen Tasten aus sind.

Eine Smartcard ist richtig eingelegt und dem Kobra VS-Datenträger bekannt. Jedoch sind die SO- und / oder Benutzer-PIN gesperrt. Diese Smartcard befindet sich nicht in der Smartcard-Tabelle, oder die Smartcard-Tabelle wurde gelöscht. *(Siehe Kapitel 9.14 Smartcard-Tabelle)*.

Verhalten nach Eingabe und Bestätigung der Benutzer-PIN

Die Haupttaste blinkt blau und alle anderen Tasten sind ausgeblendet

Der Kobra VS-Datenträger formatiert sich automatisch, damit Sie diesen verwenden können. Die Erstformatierung findet auch statt, wenn der Schreibschutz vorher aktiviert oder ein neuer Krypto-Schlüssel generiert wurde.
Die Formatierung erfolgt, wenn der Kobra VS-Datenträger das erste Mal mit dem Host-System verbunden wurde, der Krypto-Schlüssel geändert oder eine neue Smartcard-Tabelle erstellt wurde.

Die Haupttaste blinkt einmal rot und der Kobra VS-Datenträger wechselt in den Wartemodus

Es ist kein Krypto-Schlüssel vorhanden. Dieser sollte nach dem Anschließen der Kobra VS-Datenträger an einen Rechner erzeugt werden *(Siehe Kapitel 9.7 Generieren eines neuen Krypto-Schlüssels)*.

Diese Reaktion kann vorkommen, wenn der Krypto-Schlüssel gelöscht wurde und noch nicht erzeugt ist, oder eine neue Smartcard-Tabelle mit mehreren neuen Smartcards erstellt wurde und der automatische Vorgang der Krypto-Schlüssels-Erzeugung somit unterbrochen wurde.

Hinweis:

Bitte beachten Sie, dass ein Zugriff auf die alten Daten nicht mehr möglich ist, sobald ein neuer Krypto-Schlüssel erzeugt wurde.

Die Haupttaste blinkt einmal rot (oder mehrmals hintereinander) und der Kobra VS-Datenträger wechselt in den Wartemodus

Die Benutzer-PIN wurde falsch eingegeben. Die Haupttaste blinkt nach jeder Falscheingabe der Benutzer-PIN entsprechend der Anzahl der Fehlversuche kurz rot.

Hinweis:

Bitte beachten Sie, dass die Benutzer-PIN gesperrt wird, wenn diese zu oft falsch eingegeben wurde. Die gesperrte Benutzer-PIN kann mit der gültigen SO-PIN (PUK) zurückgesetzt werden.

Die Haupttaste blinkt gelb-rot-gelb-rot und der Kobra VS-Datenträger wechselt in den Wartemodus

Die Benutzer-PIN ist gesperrt, weil diese zu oft falsch eingegeben wurde.

Hinweis:

Die gesperrte Benutzer-PIN kann mit der gültigen SO-PIN (PUK) zurückgesetzt werden. Beachten Sie jedoch, dass die Kobra Infosec-Smartcard endgültig gesperrt wird, sobald die Anzahl der erlaubten Fehlversuche (10 Fehlversuche) für die Eingabe der SO-PIN (PUK) ebenfalls überschritten ist.

Weitere Fragen und Lösungen

Die Authentisierung ist fehlgeschlagen

Die Haupttaste blinkt rot.
Eine falsche Benutzer-PIN wurde eingegeben. Drücken Sie die “Haupttaste” + “1” + “V” um die Authentisierung erneut zu starten. (Sie haben maximal so viele Versuche, wie der Administrator für Sie eingestellt hat).

Der Datenträger wird nicht erkannt

Laufwerkssymbol wird nicht angezeigt:
Stellen Sie sicher, dass der Kobra VS-Datenträger über einen funktionierenden USB-Hub oder ein funktionierendes Verlängerungskabel mit dem Host-System verbunden ist. Versuchen Sie es gegebenenfalls mit einem anderen USB-Kabel oder einem anderen USB-Port am Host-System.

Fehlende Formatierung / Partition oder nicht lesbares Dateisystem:
Lesen Sie dazu im Administrator- oder Benutzerhandbuch das *Kapitel 10. Formatierung* für weitere Informationen.

Es wird ein minderwertiges Kabel verwendet:
Verwenden Sie bitte die im Lieferumfang enthaltenen USB-Kabel und verbinden Sie den USB-Stecker mit Ihrem Host-System.

Der Datenträger arbeitet langsam

Bitte prüfen Sie, ob der Kobra VS-Datenträger mit einer USB-Schnittstelle richtig verbunden ist.

Ein anderes USB-Kabel wird verwendet:
Verwenden Sie bitte die im Lieferumfang enthaltenen USB-Kabel und verbinden Sie den USB-Stecker mit Ihrem Host-System.

Inkorrekter Anschluss:
Prüfen Sie, ob der USB-Anschluss fest mit dem USB-Anschluss Ihres Host-Systems verbunden ist.

Der Kobra VS-Datenträger wurde über ein USB-Hub angeschlossen:
Stellen Sie sicher, dass der Kobra VS-Datenträger nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist.

Es sind andere Geräte mit gleichem Anschluss verbunden:
Entfernen Sie bitte alle anderen USB-Geräte und beobachten Sie, ob der Kobra VS-Datenträger anschließend schneller arbeitet.

Ich kann keine Dateien auf die Festplatte schreiben

Überprüfen Sie, ob der Schreibschutz aktiviert ist (Die Haupttaste leuchtet nach der Authentisierung in diesem Fall violett).

Ist der Schreibschutz nicht aktiviert (Die Haupttaste leuchtet nach der Authentisierung grün) - überprüfen Sie, ob die Festplatte mit dem richtigen Dateisystem für Ihr Betriebssystem formatiert ist. Das NFTS-Dateisystem kann nur von Windows- Nutzern verwendet werden.

Eventuelle Schreibfehler bei MacOS

Die verschlüsselten Kobra VS-Datenträger Kobra Drive VS und KOBRA Stick VS werden derzeit serienmäßig mit dem Dateisystem Fat32 ausgeliefert. Ebenfalls erhalten diese Datenträger während der automatischen Formatierung nach dem Schlüsselwechsel das Dateisystem Fat32. Dieses Dateisystem ermöglicht Datenaustausch sowohl mit meisten Windows-Systemen als auch mit Nicht-Windows-Systemen wie beispielsweise macOS und Linux.

Es kann vorkommen, dass bei einigen Anwendungen von MacOS (z.B. TextEditor-Software) im Dateisystem Fat32 Fehler auftreten. Dieses Problem kann wie folgt behoben werden:

- Verwendung einer anderen Textverarbeitungssoftware. Bei anderen Texteditoren von MacOS tritt dieser Fehler nicht auf.
- Formatierung des Datenträgers in ExFAT. Dieses Dateisystem hat bessere Kompatibilität sowohl mit Windows als auch mit verschiedenen Versionen von MacOS und Linux.

Zur Formatierung unter MacOS verwenden Sie das Festplattendienstprogramm:

1. Schließen Sie das USB-Laufwerk an den Mac an und starten Sie das Festplattendienstprogramm über Anwendungen, Sie können es auch z. B. über die Spotlight-Suche und unter **Programme > Dienstprogramme** finden.
2. Auf der linken Seite sehen Sie den Namen des USB-Laufwerks.
3. Klicken Sie auf den Namen des USB-Laufwerks und wechseln Sie auf die Registerkarte **Löschen**.
4. Dort sehen Sie die Option **Format**, wo Sie das Format **ExFAT** und das Schema **Master Boot** Record auswählen können.
5. Bestätigen Sie mit einem Klick auf **Löschen**.

Glossar

Admin-PIN
Der Administrator benötigt die Admin-PIN, um einen Kobra VS-Datenträger zu verwalten und diesen entsprechend dem Sicherheitskonzept des Unternehmens sowie den beabsichtigten Anwendungsszenarien zu gestalten.

AES (Advaned Encryption Standard)
AES ist ein sicheres und weltweit genutztes symmetrisches Verschlüsselungsverfahren, bei dem derselbe Schlüssel zum Ver- und Entschlüsseln von Daten verwendet wird. Es verschlüsselt Daten blockweise mit Schlüssellängen von 128, 192 oder 256 Bit und gilt als sehr sicher.

BDSG (Bundesdatenschutzgesetz)
Das Bundesdatenschutzgesetz ergänzt die Datenschutz-Grundverordnung (DSGVO) und regelt den Umgang mit personenbezogenen Daten in Deutschland. Es enthält unter anderem Vorschriften für öffentliche Stellen des Bundes sowie besondere Regelungen für Unternehmen. Ziel ist es, die Rechte betroffener Personen zu schützen und eine rechtmäßige Datenverarbeitung sicherzustellen.

BSI (Bundesamt für Sicherheit in der Informationstechnik)
Das Bundesamt für Sicherheit in der Informationstechnik ist die zentrale Cybersicherheitsbehörde des Bundes. Es entwickelt Standards und Empfehlungen für die Informationssicherheit und unterstützt Behörden, Unternehmen sowie Bürgerinnen und Bürger beim Schutz ihrer IT-Systeme. Außerdem warnt das BSI vor aktuellen Cyberbedrohungen und koordiniert Maßnahmen zur Erhöhung der IT-Sicherheit.

DSGVO (Datenschutz-Grundverordnung)
Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union zum Schutz personenbezogener Daten. Sie legt einheitliche Regeln für die Verarbeitung personenbezogener Daten fest und stärkt die Rechte betroffener Personen, beispielsweise auf Auskunft, Berichtigung und Löschung. Ziel der DSGVO ist es, ein hohes Datenschutzniveau innerhalb der EU zu gewährleisten und den freien Datenverkehr zu ermöglichen.

EU RESTRICTED / RESTREINT UE
EU RESTRICTED (französisch: RESTREINT UE) ist die erste Geheimhaltungsstufe der Europäischen Union. Informationen dieser Einstufung müssen vor unbefugtem Zugriff geschützt werden, da ihre Offenlegung den Interessen der EU oder eines Mitgliedstaates schaden könnte. Der Zugang ist ausschließlich Personen gestattet, die ihn für ihre dienstlichen Aufgaben benötigen.

Benutzer-PIN
Mithilfe der Benutzer-PIN kann der Nutzer sich an dem Kobra VS-Datenträger authentisieren (anmelden), einen neuen Krypto-Schlüssel generieren sowie die Benutzer-PIN ändern. Zudem kann er den Schreibschutz aktivieren und deaktivieren, falls er über die entsprechenden Schreibrechte verfügt.

Krypto-Schlüssel (Kryptografischer Schlüssel)
Ein kryptografischer Schlüssel ist eine Zeichenfolge aus Zahlen, Buchstaben oder Bits, die in der Kryptografie zum Ver- und Entschlüsseln von Daten verwendet wird. Er sorgt dafür, dass nur berechtigte Personen auf geschützte Informationen zugreifen oder diese lesen können. Die Sicherheit eines Verschlüsselungsverfahrens hängt wesentlich davon ab, dass der Schlüssel geheim und ausreichend komplex ist.

MLC (Multi-Level Cell):
MLC ist eine Flash-Speichertechnologie, bei der pro Speicherzelle zwei oder mehr Bits gespeichert werden. Dadurch können Speichermedien mit höherer Kapazität zu geringeren Kosten hergestellt werden. Im Vergleich zu SLC ist MLC jedoch langsamer, weniger langlebig und anfälliger für Schreib- und Lesefehler.

NATO RESTRICTED
NATO RESTRICTED ist die erste Sicherheitsklassifizierung der NATO. Sie kennzeichnet Informationen, deren unbefugte Offenlegung den Interessen der NATO oder ihrer Mitgliedstaaten nachteilig sein könnte. Der Zugriff erfolgt nur für autorisierte Personen im Rahmen des dienstlichen Bedarfs.

PKI-Smartcard
Eine PKI-Smartcard ist eine Chipkarte, die digitale Zertifikate und kryptografische Schlüssel sicher speichert. Sie wird zur sicheren Authentifizierung von Benutzern sowie zum Verschlüsseln und digitalen Signieren von Daten eingesetzt. Durch die geschützte Speicherung der Schlüssel erhöht sie die Sicherheit gegenüber rein softwarebasierten Lösungen.

pSLC (Pseudo Single-Level Cell):
pSLC ist ein Betriebsmodus, bei dem MLC- oder TLC-Flash so genutzt wird, dass pro Speicherzelle nur ein Bit gespeichert wird. Dadurch werden die Schreibgeschwindigkeit, Zuverlässigkeit und Lebensdauer des Speichers deutlich verbessert. pSLC wird häufig in industriellen Anwendungen eingesetzt, bei denen hohe Datensicherheit und eine lange Haltbarkeit wichtig sind.

SO-PIN (PUK)
Die SO-PIN (PUK) wird sowohl für die Änderung der SO-PIN (PUK) als auch für die Freischaltung der Kobra Infosec-Smartcard nach der Sperre der Benutzer-PIN benötigt.

VSA (Verschlusssachenanweisung)
Die Verschlusssachenanweisung regelt den Umgang mit Verschlusssachen in Behörden und anderen berechtigten Stellen des Bundes. Sie legt fest, wie Informationen eingestuft, gekennzeichnet, aufbewahrt, transportiert und vernichtet werden müssen. Ziel der VSA ist der Schutz sicherheitsrelevanter Informationen vor unbefugter Kenntnisnahme.

VS-NfD
VS-NfD steht für „Verschlusssache – Nur für den Dienstgebrauch“ und ist die erste Geheimhaltungsstufe für schutzbedürftige Informationen in Deutschland. Dokumente mit dieser Einstufung dürfen nur von berechtigten Personen eingesehen

und verarbeitet werden, da ihre unbefugte Offenlegung den Interessen der Bundesrepublik Deutschland oder einer Behörde schaden kann. Für den Umgang mit VS-NfD-Datenträgern und Unterlagen gelten besondere Sicherheits- und Schutzmaßnahmen.

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