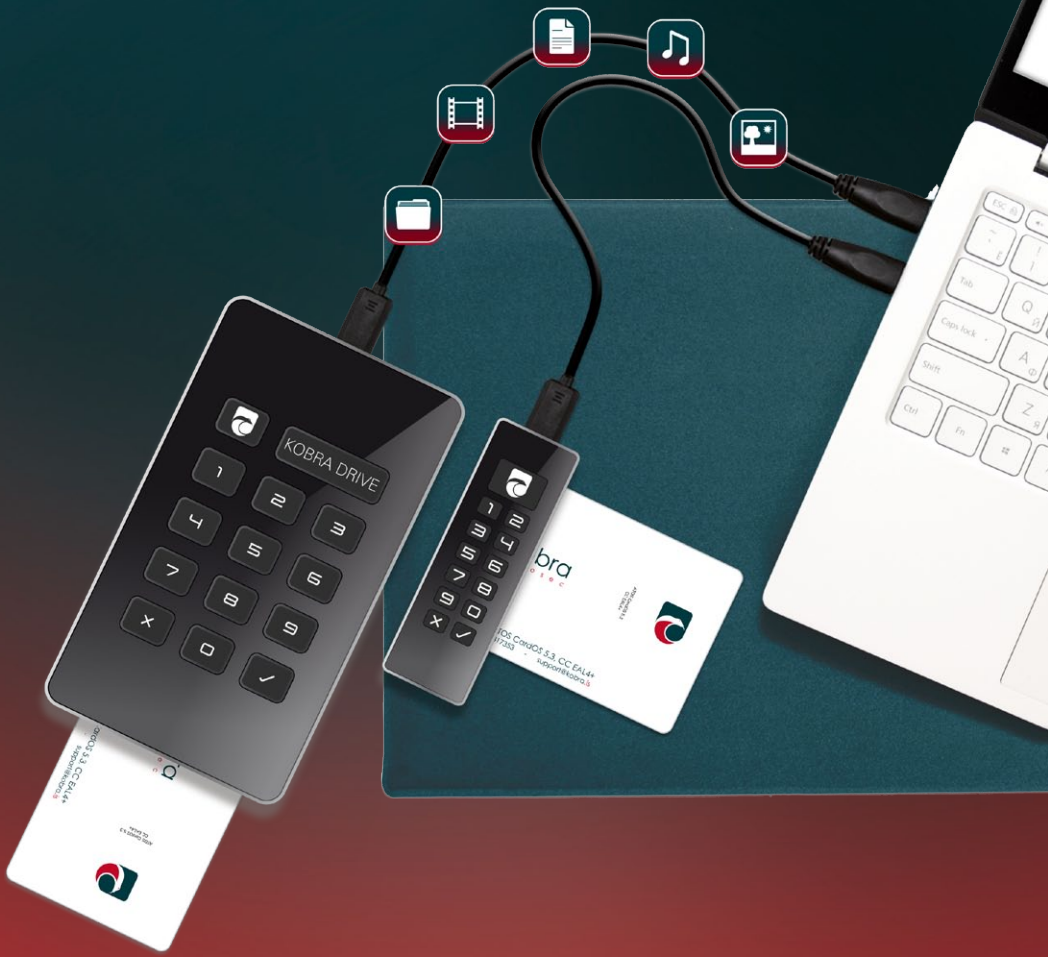
Administratorhandbuch
Administrator's Guide

Kobra VS-Datenträger

Externe verschlüsselte USBC-Festplatte und USBC-Stick



Version 1.3
22.12.2023

for business and governmental use

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 DIGITTRADE GmbH heruntergeladen werden:
www.digittrade.de/download

Produktversion:	Kobra Drive VS, Kobra Stick VS (1FF) und Kobra Stick VS (2FF) - (Kobra VS-Datenträger) Version 1.0
Administratorhandbuch:	Version 1.3 (Stand 22.12.2023)

Inhaltsverzeichnis

Präambel

Das Administratorhandbuch dient zur Unterstützung der Administration von VS-Datenträgern. Es werden die Einstellungsmöglichkeiten und erforderliche Schritte detaillierter als im Benutzerhandbuch beschrieben. Für eine bessere Nachvollziehbarkeit sind zudem alle Abschnitte aus dem Benutzerhandbuch enthalten und durch die Administrator-Funktionen ergänzt.

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 Speichersticks 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 sie 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 entwickelt und verfügen über das Qualitätszeichen „IT-Security made in Germany“. Sie entsprechen dem aktuellen Stand der Technik und sind auf Grund ihrer Sicherheitsfunktionen aktuell eine der sichersten Möglichkeiten Daten mobil zu speichern.

Die auf dem Kobra VS-Datenträger gespeicherten Daten sind in Hinblick auf die Vertraulichkeit der Informationen vor unbefugten Zugriffen geschützt, etwa wenn der Kobra VS-Datenträger verloren, verlegt oder entwendet wird. Dabei hält er gegen logische und physikalische Angriffe stand.

Dank des eingebauten Datenträgers im 2,5”-Format ist die Kobra Drive VS bereits als HDD/SSD klein und handlich. Die optionale Verwendung von SSD-Datenträgern bei dem 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 nur Kobra VS-Datenträger zur Verfügung gestellt. Die Einrichtung dieser erfolgt durch die Administratoren des Nutzers. Daher werden auch die PKI bezogenen Eigenschaften des 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 (PUK)-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 DIGITTRADE 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)
- Überprüfen Sie über das Host-System, dass die USB-Eigenschaften des Datenträgers mit der Modellbezeichnung und der Seriennummer auf der Rückseite des Kobra VS-Datenträgers übereinstimmen
  (Kapitel 4)
- Ändern Sie die Benutzer- und SO-PIN (PUK) auf beiden DIGITTRADE Smartcards
  (Kapitel 9.3, 9.5)
- Ändern Sie die Admin-PIN, falls Sie über Administrator-Rechte verfügen
  (Kapitel 9.6)
- Bei der Wahl der Admin-, Benutzer- und SO-PIN (PUK) sollen Trivial-PINs vermieden und die Standard-PINs ausgeschlossen werden
- Erzeugen Sie einen neuen Krypto-Schlüssel auf dem Kobra VS-Datenträger
  (Kapitel 9.7)
- Überprüfen Sie, ob die Anmeldung mit allen freigeschalteten DIGITTRADE 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 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 Software Kobra Client VS und über den 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

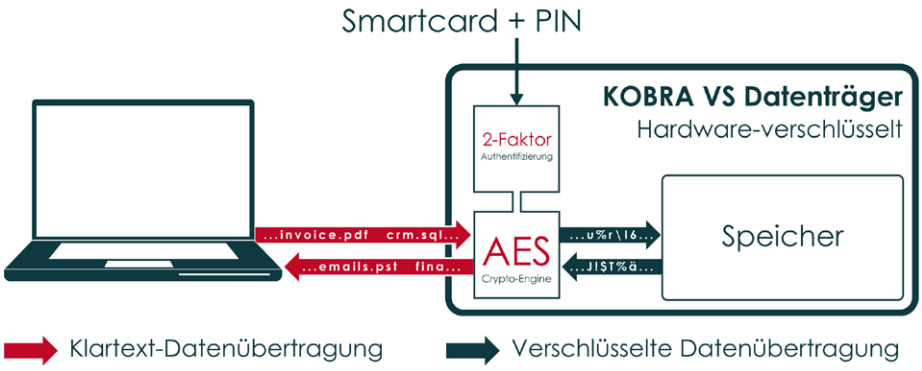
2.1 Verschlüsselung

- 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 DIGITTRADE Smartcard wird automatisch gesperrt, sobald die zulässige Anzahl der fehlerhaften PIN-Eingaben überschritten wurde. Die Freischaltung gesperrter DIGITTRADE Smartcards kann durch die Eingabe der SO-PIN (PUK) erfolgen. Die unwiderrufliche Sperre der DIGITTRADE 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 interne 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 DIGITTRADE 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 DIGITTRADE Smartcard (bzw. PKI-Karte) und der Benutzer-PIN kann der Benutzer jederzeit den Krypto-Schlüssel auf dem Kobra VS-Datenträger erzeugen, ändern und zerstören (Kapitel 9.7, 9.8).

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

Die Benutzerverwaltung führt der Administrator grundsätzlich mithilfe der Software Kobra Client VS und der Admin-PIN durch. Überdies ist eine für den jeweiligen VS-Datenträger freigegebene DIGITTRADE Smartcard oder PKI-Karte einschließlich der jeweiligen Benutzer-PIN erforderlich, um zusätzliche DIGITTRADE Smartcards oder PKI-Karten für jeweilige Kobra VS-Datenträger frei zu geben.

Für einen VS-Datenträger kann der Administrator bis zu 10 Benutzer freigeben. Er kann ebenfalls festlegen, welche Benutzer nur zum lesenden Zugriff auf die Daten auf dem Kobra VS-Datenträger berechtigt sind und welche Nutzer zudem über Schreibrechte verfügen. Für diese Zwecke steht ihm eine Smartcard-Tabelle in der Software Kobra Client VS zur Verfügung.

Mithilfe der Software „Kobra Client VS“ kann der Administrator die für einen Kobra VS-Datenträger bereits freigegebenen Benutzer überprüfen. Er kann einen oder mehrere Benutzer gleichzeitig sowohl löschen als auch hinzufügen. (Kapitel 9.14)

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-Authentifizierung mittels DIGITTRADE 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, welche 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 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 DIGITTRADE 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 DIGITTRADE 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 basieren, so ist eine Rücksprache mit dem BSI erforderlich, ob diese Smartcards eine ausreichende Schutzleistung für VS-NfD erbringen.

Die DIGITTRADE Smartcards werden für die VS-Datenträger Kobra Drive VS und Kobra Stick VS (1FF) im EC-Karten-Format geliefert. Der Kobra Stick VS (2FF) wird mit den DIGITTRADE Smartcards im Mini-SIM-Karten-Format ausgestattet. Sie werden in den folgenden Kapiteln als **„DIGITTRADE Smartcard“** bezeichnet. Die DIGITTRADE 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 dieses. Die Verwaltung des Krypto-Schlüssels erfolgt auf dem Kobra VS-Datenträger mithilfe der DIGITTRADE Smartcard (bzw. PKI-Karte) und der Benutzer-PIN völlig unabhängig von einem PC.

Für die Anmeldung am Kobra VS-Datenträger verfügen beide DIGITTRADE Smartcards bei der Auslieferung über eine Benutzer- und SO-PIN (PUK) mit Standard-Werten (Kapitel 13). Alle DIGITTRADE Smartcards verfügen über unterschiedliche Seriennummern sowie gespeicherte Schlüsselpaare, die aus öffentlichem und privatem Schlüssel bestehen. Auf der Vorderseite der DIGITTRADE Smartcard sind die Modellbezeichnung und die Seriennummer der jeweiligen Smartcard aufgetragen. Mithilfe der Software Kobra Client VS kann der Administrator bis zu 10 DIGITTRADE Smartcards oder PKI-Karten für einen Kobra VS-Datenträger freigeben und die Berechtigungen der jeweiligen Nutzer unterschiedlich definieren. Dies geschieht durch die Eintragung der DIGITTRADE Smartcards (bzw. PKI-Karten) in die Smartcard-Tabelle des Kobra VS-Datenträgers. (Kapitel 9.14)

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 DIGITTRADE 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 erzeugen sowie die Benutzer-PIN ändern. Zudem kann er den Schreibschutz aktivieren und deaktivieren, falls er über Schreibrechte verfügt.

Die SO-PIN (PUK) wird sowohl für die Änderung der SO-PIN (PUK) als auch für die Freischaltung der DIGITTRADE 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 DIGITTRADE Smartcard wird endgültig gesperrt, sobald die Anzahl der erlaubten Fehlversuche (10 Fehlversuche) für die Eingabe der SO-PIN (PUK) ebenfalls überschritten ist.

Die DIGITTRADE 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 eine Länge ebenfalls 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 DIGITTRADE Smartcard nach Sperrung der Benutzer-PIN nicht freigeschaltet oder die SO-PIN geändert werden.

3.5 Admin-PIN

Die Admin-PIN steht dem Administrator zur Verfügung und kann von ihm jederzeit geändert werden. Der Zugriff auf die gespeicherten Daten ist mit der Admin-PIN nicht möglich.

Der Administrator benötigt die Admin-PIN, um diese PIN zu ändern, Time-Out- und Lock-Out-Einstellungen vorzunehmen sowie die Liste der berechtigten Smartcards bei einem Kobra VS-Datenträger zu ergänzen, zu löschen oder neu zu erstellen. Des Weiteren kann er festlegen welche Nutzer ausschließlich über Leserechte und welche zudem über Schreibrechte verfügen.

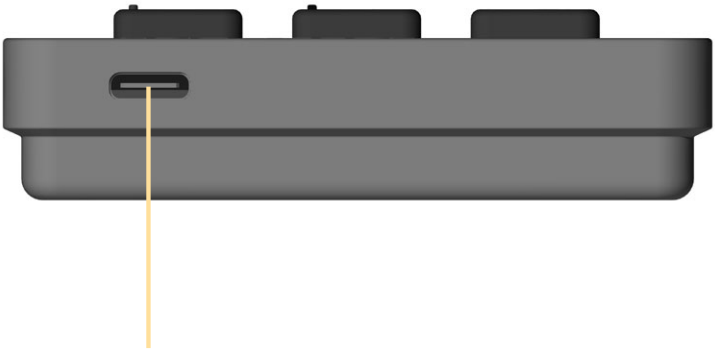
Der Kobra VS-Datenträger wird mit der Admin-PIN 8-7-6-5-4-3-2-1 ausgeliefert. Die Werkseinstellungen ermöglichen für die Admin-PIN 16 Eingabeversuche und eine Länge von 4 bis 16 Stellen. Nach Überschreitung der erlaubten Fehlversuche ist die Admin-PIN dauerhaft gesperrt. Der Administrator kann anschließend die oben beschriebenen Einstellungen am Kobra VS-Datenträger nicht mehr vornehmen.

Mit Unterstützung der Software Kobra Client VS kann der Administrator die Eingabe der Admin-PIN über die Tastatur des Kobra VS-Datenträgers deaktivieren, um fehlerhafte Eingaben durch den Nutzer zu vermeiden. Die Eingabe der Admin-PIN über die Software Kobra Client VS ist in diesem Fall weiterhin möglich. Bei Bedarf kann der Administrator die Eingabe der Admin-PIN über die Tastatur des Kobra VS-Datenträgers erneut aktivieren.

3.6 USB-Anschluss, Smartcard-Slot und Eingabeoberfläche

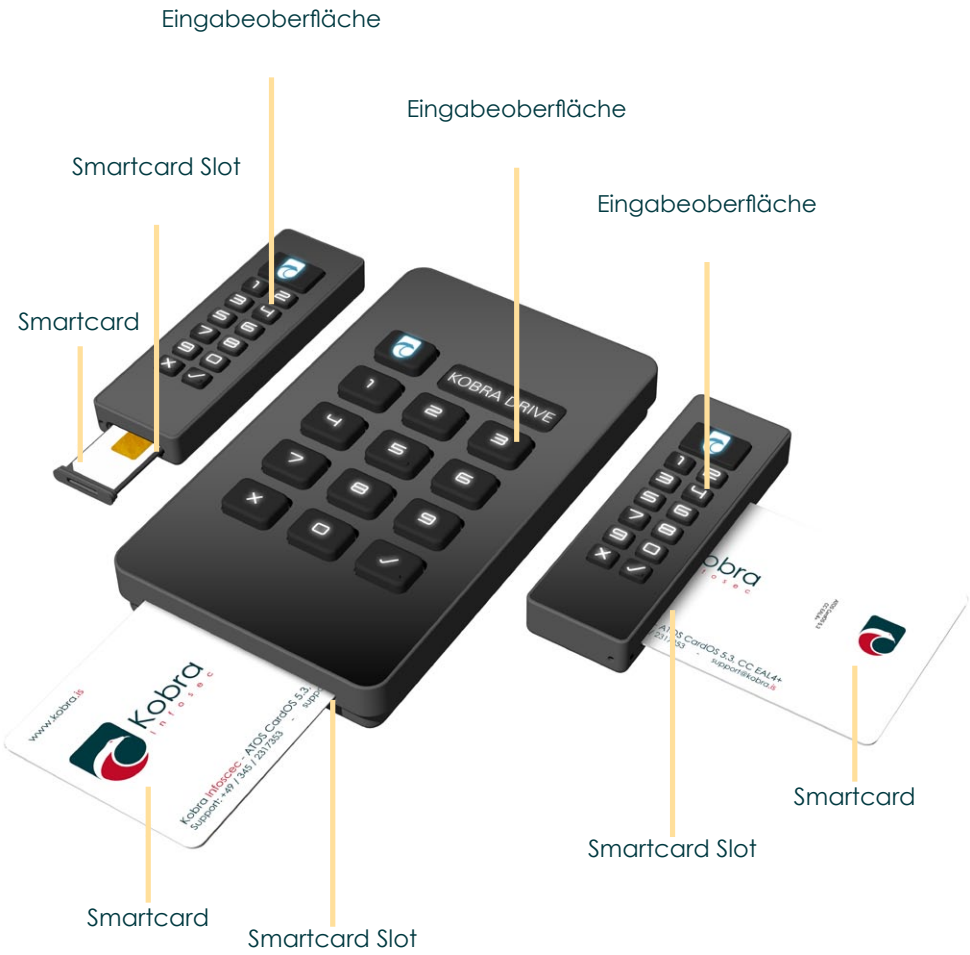
USB-C 3.0 Anschluss
Kobra Stick VS (2FF)

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 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 To Go oder andere Betriebssystemen)
- Änderung der Benutzer-PIN ohne Anschluss an einen PC
- Zerstören eines gültigen Krypto-Schlüssels 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 einen anderen externen Stromversorger (z.B. USB-Netzteil oder Hub) aufgeladen.

4. Echtheitsprüfung

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

Zur ergänzenden Authentizitätsprüfung im Betrieb empfiehlt sich die Verwendung einer s.g. Authentizitätsdatei. Diese kann beliebig so gewählt werden, dass sie einmalig ist und durch den Besitzer leicht verifiziert werden kann, sobald dieser auf den Datenträger zugreift.

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

5. Firmware Update

Im Rahmen einer sicheren Update-Strategie sind Firmware-Updates über die USB-Schnittstelle durch technische Maßnahmen verhindert. Die Durchführung eines Updates erfordert die Einhaltung folgender Bedingungen:

a) Zum Installieren der Firmware benötigt der Administrator ein separates Firmware-Update-Gerät und die vom Hersteller bereitgestellte Firmware-Datei.
b) Ein Update ist nur auf eine neuere Version der Firmware möglich.
c) Zum Ausführen eines Updates muss auf dem Kobra VS-Datenträger zuvor ein 256 Bit Update-Schlüssel hinterlegt werden.

Der 256 Bit Update-Schlüssel kann in den Kobra VS-Datenträger sowohl manuell hexadezimal als auch durch das Auslesen einer Binärdatei mit Unterstützung der Software Kobra Client VS eingetragen werden. Dieser Schlüssel ist anschließend zur Authentisierung mit dem Firmware-Update-Gerät erforderlich. (Kapitel 9.12)

Die detaillierte Anleitung zur Update-Durchführung ist im Handbuch des Firmware-Update-Geräts enthalten. Weitere Informationen hierzu erhalten Sie auf www.digittrade.de

6. Inbetriebnahme des 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 schaltet nach dem Anschluss an einen PC oder einen externen Stromversorger sofort in den Authentisierungsmodus, falls eine für diesen Kobra VS-Datenträger bestimmte DIGITTRADE 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 falsch, so blinkt die Haupttaste ununterbrochen rot oder gelb bis eine für diesen Datenträger bestimmte DIGITTRADE 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 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. DIGITTRADE 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 VS-Datenträgers eingetragene Smartcard, so leuchtet die Haupttaste gleich nach der Betätigung der Taste „1“ kurz rot und anschließend dauerhaft weiß. Der VS-

Datenträger wechselt in den Warte-Modus. Die Authentisierung ist auch in diesem Fall nicht möglich.

Alle Kommandos werden mit der „√“-Taste 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 schaltet sich 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 DIGITTRADE 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 nicht gezählt (Kapitel 9.4).
Die fehlerhafte Eingabe der SO-PIN (PUK) führt nach Überschreitung der Fehlversuche zu der endgültigen Sperre der DIGITTRADE Smartcard. Der Zugriff auf die Daten ist anschließend nur mit einer anderen für diesen Kobra VS-Datenträger freigeschalteten DIGITTRADE Smartcard und korrekter Eingabe der Benutzer-PIN möglich. In diesem Fall muss mithilfe der Software Kobra Client VS die bestehende Smartcard-Tabelle auf dem Kobra VS-Datenträger gelöscht und eine neue Smartcard-Tabelle erstellt werden. Dabei erfolgt die automatische Löschung und anschließend Generierung eines neuen Krypto-Schlüssels. Damit einhergehend werden alle zuvor gespeicherten Daten irreversibel vernichtet. (Kapitel 9.14)

Liegen keine weiteren für diesen Kobra VS-Datenträger berechtigten DIGITTRADE Smartcards vor, verbleibt nur die Möglichkeit eine neue DIGITTRADE 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. In Fällen 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)

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, 9.5). Verändern Sie zudem die Benutzer-PIN auch zukünftig in regelmäßigen Abständen. Zusätzlich empfiehlt es sich, unterschiedliche Benutzer-PIN für verschiedene DIGITTRADE Smart-cards zu verwenden. Die Benutzer- und SO-PIN (PUK) müssen vertraulich behandelt werden.

Hinweis:
Bitte beachten Sie, dass die "Kobra Client-Software" (Kapitel 8) ausgeschaltet sein muss, sobald sie den 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 erzeugen sowie die DIGITTRADE Smartcard nach der Sperre durch die fehlerhafte Benutzer-PIN-Eingabe freischalten. Zudem kann er den Schreibschutz aktivieren und deaktivieren, falls er über Schreibrechte verfügt.

Der Administrator kennt die Admin-PIN. Er kann die Admin-PIN ändern sowie die Time-Out- und Lock-Out-Einstellungen vornehmen. Ebenfalls kann er die Liste der berechtigten DIGITTRADE Smartcards des Kobra VS-Datenträgers (auch Smartcard-Tabelle genannt) ergänzen, löschen oder neu erstellen. Zudem kann er festlegen, ob der Benutzer ausschließlich zum Lesen oder zum Lesen und Schreiben der Daten auf dem Kobra VS-Datenträger autorisiert ist.

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 DIGITTRADE 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 Software Kobra Client VS 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 Software Kobra Client VS 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.

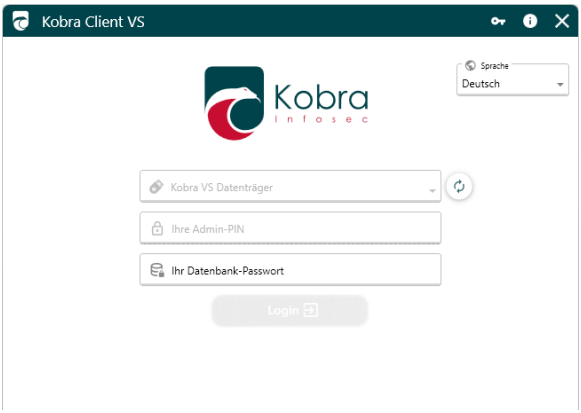
8. Kobra Client VS

Der Kobra Client VS ist eine Verwaltungssoftware für Kobra VS-Datenträger. Er 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 vorgenommen, exportiert und importiert werden:

a) Die Änderung der Admin-PIN
b) Verwendung der Admin-PIN über die Tastatur des Kobra VS-Datenträgers
c) Erzeugung und Änderung des Update-Schlüssels
d) Das Konfigurieren von Lock-Out- und Time-Out-Funktionen
e) Löschen und Erstellen einer Smartcard-Tabelle
f) Eintragen zusätzlicher Smartcards (PKI-Karten) in die Smartcard-Tabelle
g) Setzen der Schreib- und Leserechte individuell für jeden Nutzer

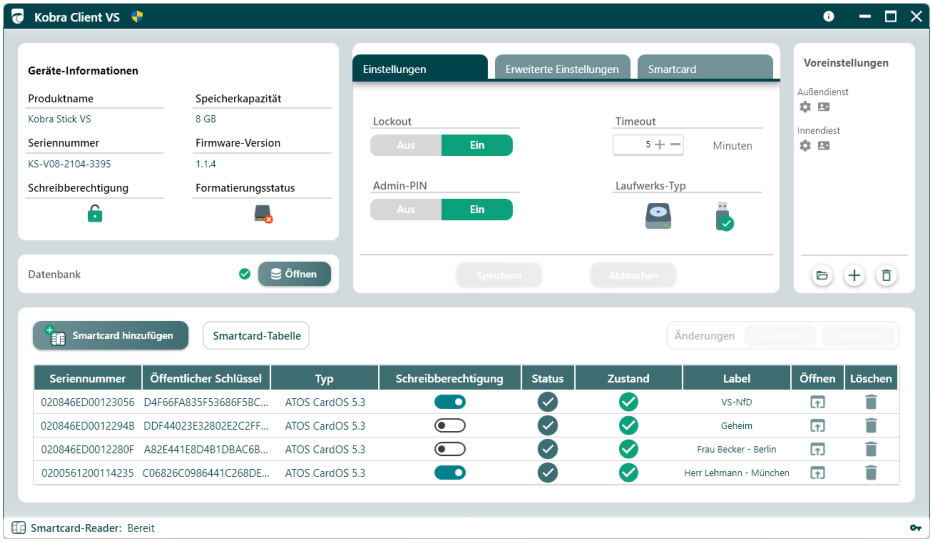
Mit Hilfe dieser Software kann der Administrator die Seriennummer und den öffentlichen Schlüssel direkt aus der in den Kobra VS-Datenträger hineingesteckten DIGITTRADE Smartcard (PKI-Karte) auslesen. Ebenfalls kann er diese Informationen aus der Smartcard-Tabelle des Kobra VS-Datenträgers entnehmen. In diesem Fall kann er zusätzlich erfahren, ob der jeweiligen Smartcard-Besitzer nur zum Lesen oder auch zum Schreiben auf dem Kobra VS-Datenträger berechtigt ist.

Nach dem Start der Software Kobra Client VS erscheint zuerst das Login-Fenster. In diesem Fenster kann der Administrator die Sprache auswählen sowie nach einem angeschlossenen Kobra VS-Datenträger suchen. An dieser Stelle können ein oder mehrere Kobra VS-Datenträger an das Host-System angeschlossen werden, falls dies noch nicht erfolgt ist. Nach der Aktualisierung kann der Administrator das Listenfeld der verfügbaren Kobra VS-Datenträger erneut durchsuchen. Zum ausgewählten Kobra VS-Datenträger wird im Login-Fenster auch die Seriennummer angezeigt.



Login-Fenster

Zur Anmeldung gibt der Administrator die Admin-PIN des ausgewählten Kobra VS-Datenträgers ein und klickt auf den Login-Button. Bei erfolgreicher Authentisierung öffnet sich das Hauptmenü. Gleichzeitig werden in dieses Menü die aktuellen Einstellungen des Kobra VS-Datenträgers sowie die Smartcard-Tabelle mit den freigegebenen DIGITTRADE Smartcards (PKI-Karten) geladen.



Login-Fenster

Weitere Angabe sind in Kapitel 9 zu finden.

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.

9.1 Benutzer-Authentisierung

Die Benutzer-Authentisierung ist erforderlich um den Zugriff auf den Datenträger freizuschalten.

Für die Authentisierung:

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

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.

Hinweis: *Hat der Benutzer eine gültige Smartcard in den VS-Datenträger bereits während des Schlaf-Modus (alle Tasten waren ausgeschaltet) eingeführt, so wechselt der VS-Datenträger nach dem langen Betätigen der Haupttaste oder nach dem Anschluss an einen PC sofort in den Authentisierungs-Modus. Die Benutzer-PIN kann in diesem Fall direkt eingegeben werden.*

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 schaltet zurück in den Warte-Modus.

Der Administrator kann mithilfe der Software Kobra Client VS festlegen ob der Benutzer nur zum Lesen oder zusätzlich auch zum Schreiben berechtigt ist.

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 kurz grün und der Kobra VS-Datenträger schaltet wieder in den Warte-Modus.

9.4 Freischalten/Zurücksetzen der Benutzer-PIN

Nach der Überschreitung der zulässigen Fehlversuche sperrt sich die DIGITTRADE 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 DIGITTRADE Smartcard blinkt die Haupttaste kurz grün und der Datenträger schaltet in den Warte-Modus.

Die fehlerhafte Eingabe der SO-PIN (PUK) führt nach Überschreitung der erlaubten Fehlversuche zu der endgültigen Sperrung der DIGITTRADE 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)

Der Anwender kann für die SO-PIN (PUK) eine Kombination von 4 bis 12 Ziffern wählen.

Für die Änderung der SO-PIN (PUK):

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 „5“ und anschließend „√“. Die Haupttaste blinkt hellblau und alle anderen Tasten bleiben aktiv.
3) Geben Sie die aktuelle SO-PIN (PUK) ein und bestätigen Sie mit „√“.
4) Geben Sie die neue SO-PIN (PUK) ein und bestätigen Sie mit „√“.
5) Wiederholen Sie die neue SO-PIN (PUK) und bestätigen Sie ebenfalls mit „√“.

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

9.6 Ändern oder Ausschalten der Admin-PIN

Der Administrator kann für die Admin-PIN eine Kombination von 4 bis 16 Ziffern wählen. Er kann die Admin-PIN direkt am Kobra VS-Datenträger ändern. Mithilfe der Software Kobra Client VS kann er neben der Änderung der Admin-PIN noch die Eingabe der Admin-PIN über die Tastatur des Kobra VS-Datenträgers ausschalten oder wieder einschalten.

A. Ändern der Admin-PIN 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 „9“ und anschließend „√“. Die Haupttaste blinkt dauerhaft violett und alle anderen Tasten bleiben aktiv.
3) Geben Sie die aktuelle Admin-PIN ein und bestätigen Sie mit „√“.
4) Geben Sie die neue Admin-PIN ein und bestätigen Sie mit „√“.
5) Wiederholen Sie die neue Admin-PIN und bestätigen Sie mit „√“.

Nach einer erfolgreichen PIN-Änderung blinkt die Haupttaste kurz grün und der Datenträger schaltet wieder in den Warte-Modus.

B. Ändern der Admin-PIN über die Software Kobra Client VS

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus.
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Klicken Sie auf „Admin-PIN bearbeiten“.
5) Geben Sie die aktuelle Admin-PIN ein.
6) Geben Sie die neue Admin-PIN zweimal ein und klicken Sie auf „Änderung speichern“.
7) Nach erfolgreicher PIN-Änderung erscheint die Meldung „Die Änderung war erfolgreich“. Bei fehlerhaften Eingaben erscheint eine entsprechende Fehlermeldung.

C. Aus- und Einschalten der Admin-PIN

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus.
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Klicken Sie auf „Admin-PIN bearbeiten“.
5) Setzen Sie den Haken für die Option „Admin-PIN ausschalten“ und klicken Sie auf „Änderung speichern“.
6) Nach erfolgreicher Änderung erscheint die Meldung „Die Änderung war erfolgreich“. Bei fehlerhaften Eingaben erscheint eine entsprechende Fehlermeldung

9.7 Erzeugen eines neuen Krypto-Schlüssel

Der Anwender kann mithilfe einer initialisierten DIGITTRADE Smartcard (bzw. PKI-Karte) und Benutzer-PIN jederzeit den Krypto-Schlüssel auf dem zugehörigen Kobra VS-Datenträger erzeugen, 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 verzichtet werden, da dies die Lebensdauer des Datenträgers wesentlich beeinträchtig. Sicher und effizient erfolgt die Löschung der Daten durch das Generieren eines neuen Krypto-Schlüssels oder das Löschen der Smartcard-Tabelle. (Kapitel 9.8)

Zum Erzeugen oder Ändern des Krypto-Schlüssels:

1) Stellen Sie sicher, dass der VS-Datenträger an ein Host-System angeschlossen ist und 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 „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) Drücken Sie die Taste „√“, falls Sie diese Funktion tatsächlich durchführen möchten. Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
4) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“.

Nach der erfolgreichen Erzeugung oder Änderung des Krypto-Schlüssels leuchtet die Haupttaste vorerst gelb und anschließend dauerhaft weiß. Der Kobra VS-Datenträger schaltet zurück 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 grün oder violett, je nachdem ob der Schreibschutz aktiviert (violett) oder deaktiviert (grün) 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 und/oder Vernichten des Krypto-Schlüssels kann auf drei Wegen erfolgen.

A: Zerstörung ohne Erzeugung eines neuen Krypto-Schlüssels (erfolgt ohne Anschluss an ein Host-System)

Diese Methode kann der Anwender mithilfe der Benutzer-PIN durchführen. Während dieses Vorgangs wird der alte Krypto-Schlüssel unwiderruflich gelöscht. Der Zugriff auf alle zuvor gespeicherten Daten ist ab diesem Zeitpunkt nicht mehr möglich. Diese Methode ermöglicht eine schnelle Vernichtung der auf dem Kobra VS-Datenträger gespeicherten Daten, ohne den Datenträger an einen PC anzuschließen.

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 „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) Drücken Sie die Taste „√“, falls Sie diese Funktion tatsächlich durchführen möchten. Die Haupttaste blinkt grün und alle anderen Tasten bleiben aktiv.
4) Geben Sie die Benutzer-PIN ein und bestätigen Sie mit „√“. Die Haupttaste leuchtet vorerst grün, danach blinkt sie gelb-rot-rot und leuchtet anschließend weiß.

Durch diesen Vorgang wird der aktuelle Krypto-Schlüssel gelöscht. Für die weitere Nutzung des VS-Datenträgers muss anschließend ein neuer Krypto-Schlüssel nach dem Anschluss an ein Host-System erzeugt werden. (Kapitel 9.7)

B: Zerstörung durch Erzeugung eines neuen Krypto-Schlüssels (erfolgt mit Anschluss an ein Host-System)

Diese Methode kann der Anwender nur nach dem Anschluss an ein Host-System mithilfe der Benutzer-PIN durchführen. Während dieses Vorgangs wird der alte Krypto-Schlüssel unwiderruflich überschrieben. Der Zugriff auf alle zuvor gespeicherten Daten ist ab diesem Zeitpunkt ebenfalls nicht mehr möglich. (Kapitel 9.7)

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 Software Kobra Client VS 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. Infolgedessen sind ebenfalls alle auf dem Kobra VS-Datenträger zuvor gespeicherten Daten unwiderruflich vernichtet. (Kapitel 9.14)

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 kurz 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 Auswahl für die Sperre liegt zwischen 1 und 30 Minuten. Zur Aufhebung der Sperre ist „0“ auszuwählen. (Kapitel 13)

A. Festlegen eines Time-Out 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 „8“ und anschließend „√“ Die Haupttaste blinkt violett und alle anderen Tasten bleiben aktiv.
3) Geben Sie die Admin-PIN ein und bestätigen Sie mit „√“.
4) Geben Sie eine Zahl von 0 bis 30 ein und bestätigen Sie mit „√“.

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

B. Festlegen eines Time-Out über die Software Kobra Client VS

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus.
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Geben Sie in das Eingabefeld „Time-Out“ eine Zahl von 0 bis 30 ein. Sie können dazu auch die Zeichen „+“ und „-“ verwenden.
5) Klicken Sie anschließend auf „Speichern“, damit die vorgenommenen Änderungen in den Kobra VS-Datenträger übertragen werden.

Hinweis: *Sollten Programme oder das Betriebssystem in regelmäßigen Abständen automatisch lesend oder schreibend auf den Kobra VS-Datenträger zugreifen, so verliert die Time-Out Funktion möglicherweise ihre Wirkung.*

9.10 Quick-Out Funktion

Die Quick-Out-Funktion ermöglicht eine schnelle Sperrung des Kobra VS-Datenträgers. Sie wird durch das doppelte Klicken auf die „×“-Taste innerhalb von 2 Sekunden ausgeführt.

9.11 Lock-Out Funktion

Mittels der Lock-Out Funktion kann der Administrator festlegen, ob die DIGITTRADE Smartcard (PKI-Karte) im Kobra VS-Datenträger nach der Authentisierung verbleiben soll oder sie entfernt werden kann. Im eingeschalteten Lock-Out Modus wird der Zugriff auf die Daten nach dem Entfernen der DIGITTRADE Smartcard (PKI-Karte) aus dem Gehäuse des Kobra VS-Datenträgers sofort unterbrochen. Den Lock-Out Modus kann der Administrator ein- oder ausschalten. Dazu gehen Sie wie folgt vor:

A. Ein- oder Ausschalten des Lock-out über die Tastatur des Kobra VS-Datenträgers:

1) Verbinden Sie den Kobra VS-Datenträger mit einem PC oder USB-Hub und stecken Sie eine zugelassene Smartcard (auch wenn diese gesperrt ist) ein. Stellen Sie sicher, dass der VS-Datenträger sich im Warte-Modus befindet. (Die Haupttaste leuchtet weiß und alle anderen Tasten sind ausgeblendet).
2) Drücken Sie nachfolgend die Haupttaste, die Taste „6“ und anschließend „√“ Die Haupttaste blinkt 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 kurz grün und der Kobra VS-Datenträger wechselt zurück in den Warte-Modus.

B. Ein- oder Ausschalten des Lock-out über die Software Kobra Client VS

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus.
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Klicken Sie im Eingabebereich „Lock-Out“ auf das Feld „ein“ oder „aus“. Das aktive Feld „ein“ leuchtet grün und das aktive Feld „aus“ leuchtet rot. Das inaktive Feld ist immer grau.
5) Klicken Sie anschließend auf „Speichern“, damit die vorgenommenen Änderungen in den Kobra VS-Datenträger übertragen werden.

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. Dazu gehen Sie wie folgt vor:

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Klicken Sie auf das Feld „Update-Schlüssel bearbeiten“.
5) Im Fenster „Update-Schlüssel bearbeiten“ können Sie einen 256 Bit Update-Schlüssel entweder manuell hexadezimal eintragen oder aus einer Binär-Datei mit dem Klicken auf den Button „Update-Schlüssel importieren“ laden.
6) Klicken Sie anschließend auf „Speichern“, damit die vorgenommenen Änderungen in den Kobra VS-Datenträger übertragen werden.

Hinweis: *Der Update-Schlüssel sorgt dafür, dass nur Sie in der Lage sind eine neue Firmware auf den Kobra VS Datenträger zu installieren. Sollten Sie den Update-Schlüssel vergessen oder verlegen, können Sie jederzeit, wie oben beschrieben, einen neuen vergeben.*

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. Dazu gehen Sie wie folgt vor:

1) Starten Sie die Software Kobra Client VS und verbinden Sie den Kobra VS-Datenträger mit dem PC.
2) Wählen Sie den Kobra VS-Datenträger im Login-Fenster aus.
3) Geben Sie die gültige Admin-PIN ein und klicken Sie auf „Login“. Die Software wechselt dabei zum Hauptmenü.
4) Setzen Sie den Haken für die Option „Mit Smartcard-Tabelle“, falls die Smartcard-Tabelle ebenfalls exportiert oder importiert werden soll.
5) Klicken Sie im Bereich „Alle Einstellungen“ auf das Feld „exportieren“ oder „importieren“.
6) Beim Exportieren speichern Sie die Einstellungen an einem sicheren Speicherort. Beim Importieren suchen Sie eine Datei mit dem zuvor erstellten gewünschten Einstellungsprofil und importieren diese.

7) Die neuen Einstellungen (außer der Smartcard-Tabelle) werden sofort in den Kobra VS-Datenträger übernommen.
8) Die importierte Smartcard-Tabelle ist vorerst nur visuell in der Software Kobra Client VS vorhanden. Für die Übernahme in den Kobra VS-Datenträger klicken Sie auf „Änderung speichern“. (im Bereich Smartcard-Tabelle)
9) Nach erfolgreicher Übertragung der Smartcard-Tabelle erscheint die Meldung „Änderung war erfolgreich“.
10) War im Kobra VS-Datenträger mindestens eine Smartcard bereits eingetragen, erscheint die Aufforderung zum Einlegen einer bereits berechtigten Smartcard und zur Eingabe der Benutzer-PIN.
11) Erst nach der Erfüllung dieser Bedingungen wird die neue Smartcard-Tabelle in den Kobra VS-Datenträger integriert.

9.14 Smartcard-Tabelle

Die Smartcard-Tabelle beinhaltet Informationen über die DIGITTRADE Smartcards oder PKI-Karten, welche für den Zugriff auf den Kobra VS-Datenträger freigegeben sind. Der Administrator kann bis zu 10 DIGITTRADE Smartcards in eine Smartcard-Tabelle mittels der Software Kobra Client VS eintragen. Zudem kann der Administrator festlegen ob der jeweiligen Benutzer nur zum Lesen oder auch zum Schreiben berechtigt ist.

Die Smartcard-Tabelle wird nach der erfolgreichen Authentisierung des Administrators aus dem Kobra VS-Datenträger in das Hauptmenü der Software Kobra Client VS geladen. Alle bereits integrierten Smartcards bekommen im Feld „Status“ die Bezeichnung „aktiv“. Die neu eingetragenen oder die aus einer externen Smartcard-Tabelle importierten Smartcards erhalten vorerst die Bezeichnung „neu“.

Zur Eintragung einer einzelnen DIGITTRADE Smartcard (PKI-Karte) klicken Sie auf den Button „Smartcard hinzufügen“. Es erscheint das Fenster „Smartcard“. Tragen Sie in dieses Fenster die Seriennummer und den öffentlichen Schlüssel manuell ein oder legen Sie die zu erfassende Smartcard in den Kobra VS-Datenträger ein und klicken Sie anschließend auf den Button „Smartcard auslesen“. Die erforderlichen Informationen erscheinen folglich automatisch im Fenster „Smartcard“. Zur Übertragung dieser Informationen in die Smartcard-Tabelle klicken Sie auf „Speichern“. Im nächsten Schritt können weitere DIGITTRADE Smartcards (PKI-Karten) in die Smartcard-Tabelle aufgenommen werden. Zudem kann der Administrator für jede einzelne Smartcard die Rechte zum Schreiben und Lesen vergeben sowie die nicht benötigten Smartcards einzeln aus der Smartcard-Tabelle entfernen (löschen).

Des Weiteren verfügt der Administrator über die Möglichkeit, die Smartcard-Tabelle mit einer oder mehrerer DIGITTRADE Smartcards (PKI-Karten) gleichzeitig zu importieren, zu exportieren oder zu löschen. Entsprechende Buttons befinden sich im Bereich „Smartcard-Tabelle“.

Nach dem Klicken auf den Button „Exportieren“ erzeugt die Software Kobra Client VS eine Datei mit ID, Seriennummer, öffentlichen Schlüssel und Lese-/Schreibrechten aller in der Smartcard-Tabelle eingetragenen Smartcards. Die exportierte Datei kann bearbeitet und gespeichert werden. Anschließend können die gespeicherten Smartcard-Tabellen zum Importieren auf andere Kobra VS-Datenträger verwendet werden.

Beim Klicken auf den Button „Löschen“ erscheint die Mitteilung, dass die gesamte Smartcard-Tabelle gelöscht wird und folglich alle gespeicherten Daten unwiderruflich vernichtet werden. An dieser Stelle kann der Vorgang durch das Klicken auf „Abbrechen“ unterbrochen werden. Klickt der Administrator statt dessen auf das auf „OK“, werden alle Einträge aus der Smartcard-Tabelle entfernt.

Alle Änderungen in der Smartcard-Tabelle sind vorerst nur als visuelle Änderungen in der Software Kobra Client VS zu betrachten und können durch das Klicken auf den Button „Änderungen stornieren“ immer noch zurückgesetzt werden. In diesem Fall werden in der Smartcard-Tabelle nur die bereits im Kobra VS-Datenträger integrierten Einträge angezeigt. Alle diese Einträge haben entsprechend den Status „Aktiv“. An dieser Stelle können die Änderung von vorne vorgenommen werden.

Zur Übernahme der vorbereiteten Smartcard-Einträge klicken Sie auf den Button „Änderungen speichern“. Die Änderungen werden sofort übernommen, falls die eigentliche Smartcard-Tabelle des Kobra VS-Datenträgers noch über keine Smartcard-Einträge verfügt oder die zu übermittelnde Änderung das Löschen der gesamten Smartcard-Tabelle beinhaltet.

In anderen Fällen erscheint die Aufforderung zum Einlegen einer bereits berechtigten Smartcard und zur Eingabe der entsprechenden Benutzer-PIN. Nach erfolgreicher Erfüllung dieser Aufforderung werden die Änderung in den Kobra VS-Datenträger übertragen und es erscheint die Meldung, dass die Änderung erfolgreich war. Bei einer Fehlermeldung kann der Vorgang „Änderungen speichern“ wiederholt werden.

Nach dem Löschen einer vorhandenen Smartcard-Tabelle und dem anschließenden Erstellen einer neuen Smartcard-Tabelle ist es erforderlich, einen neuen Krypto-Schlüssel zu erzeugen. Beim Drücken auf die Taste “1” im Menümodus blinkt die Haupttaste einmal rot und leuchtet anschließend weiß. Bitte erzeugen Sie in diesem Fall einen neuen Krypto-Schlüssel wie in Kapitel 9.7 beschrieben ist.

10. Formatierung

Der Kobra VS-Datenträger verfügt im Auslieferungszustand bereits über das Dateisystem FAT32. Dieses Format kann von fast allen Betriebssystemen (Windows, Mac OS und Linux) gelesen und beschrieben werden. Die maximale Dateigröße beträgt in diesem Format bis zu 4GB und reicht somit für die meisten Inhalte aus.

Der Benutzer kann den Kobra VS-Datenträger je nach Anwendungsszenarien wunschgemäß umformatieren. Für Windowsnutzer wird empfohlen, beispielsweise NTFS zu verwenden. Für Mac OS X ist APFS das leistungsstärkste Dateisystem und bei Linux kann EXT4 eingesetzt werden.

Mit Erweiterungsprogrammen können ggf. auch Daten auf Dateisysteme geschrieben werden, bei denen dies sonst nicht möglich ist. Selbstverständlich ist es auch möglich, den Kobra VS-Datenträger mit jedem anderen Dateisystem zu formatieren. Dies beeinflusst die Verschlüsselung der Daten und die Schutzleistung des Kobra VS-Datenträgers nicht.
Aus der nachstehenden Tabelle können Sie die Kompatibilität zwischen den 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) ausgeschaltet sein muss, sobald sie den VS-Datenträger formatieren.

11. Anwendungsmöglichkeiten

Die Eigenschaften des Kobra VS-Datenträgers bieten umfangreiche Möglichkeiten für die sichere Speicherung, Archivierung und Übermittlung sensibler, personenbezogener und vertraulicher Informationen bis zur Geheimhaltungsstufe VS-NfD. Die nachfolgenden Einsatz-Szenarien liegen ebenfalls im Geltungsbereich der VS-NfD Zulassung. Abweichungen von den beschriebenen Prozeduren sind mit dem BSI abzustimmen.

11.1 Verschärfung des Schutz-Niveaus für VS-Datenträger im Unternehmen

Der Administrator im Unternehmen oder einer Behörde kann festlegen, wie restriktiv sich der Kobra VS-Datenträger eines 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 ob der Anwender nur lesenden oder auch schreibenden Zugriff auf die gespeicherten Daten erhält. Des Weiteren kann er festlegen welche andere Nutzer und mit welchen Schreib-/Leserechten auf den Kobra VS-Datenträger zugreifen dürfen. Mithilfe der Lock-Out-Funktion legt der Administrator fest, ob die DIGITTRADE 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.

11.2 Sicherer und kosteneffizienter Datentransport

Der Kobra VS-Datenträger kann für den Transport vertraulicher Daten verwendet werden. Dazu werden die DIGITTRADE Smartcards des Senders und Empfängers in die Smartcard-Tabelle des Kobra VS-Datenträgers eingetragen. Der Absender versendet ausschließlich den Kobra VS-Datenträger. Auf diese Weise kann ein regelmäßiger Datenaustausch zwischen zwei Stellen organisiert werden.

In der Stand-Alone Ausführung verfügt der Nutzer über zwei DIGITTRADE Smartcards, die in der Smartcard-Tabelle bereits eingetragen sind. In diesem Fall kann er seine zweite DIGITTRADE Smartcard dem Empfänger zur Entschlüsselung der Daten zur Verfügung stellen. Ebenso kann der Administrator für den Empfänger eine zusätzliche DIGITTRADE Smartcard in die Smartcard-Tabelle des Kobra VS-Datenträgers eintragen. Der Kobra VS-Datenträger und die DIGITTRADE Smartcard werden an den Empfänger auf getrennten Wegen versendet. Die Übermittlung der Benutzer- und ggfl. SO-PIN (PUK) erfolgt ebenfalls separat und erst nach Erhalt der DIGITTRADE Smartcard.

Bei der Nutzung von PKI-Karten trägt der Administrator die Seriennummer und den öffentlichen Schlüssel der PKI-Karten des Senders und des Empfängers in die Smartcard-Tabelle des Kobra VS-Datenträgers mittels der Kobra Client VS Software ein. Hierzu ist es notwendig, dass dem Administrator der Kobra VS-Datenträger physisch vorliegt, die Smartcards hingegen können bei den Anwendern verbleiben.

Während des Transport des Kobra VS-Datenträgers muss, durch eine geeignete Verpackung, die Erkennung von Manipulationsversuchen sichergestellt werden. Hierzu empfiehlt sich beispielsweise die Verwendung der versiegelten DIGITTRADE Sicherheitstaschen. (Informationen zu den zu prüfenden Sicherheitsmerkmalen am Kobra VS-Datenträger finden Sie in Kapitel 4 und zu den Sicherheitstaschen in Kapitel 12.2)

Bei Erhalt des Datenträgers ist dessen Authentizität zu prüfen. Hierzu wird über einen separaten sicheren Weg die Seriennummer des Datenträgers mitgeilt sowie eine Datei mit einer bestimmten Kennung innerhalb des Datenträgers gespeichert. Die Seriennummer ist sowohl auf dem Gehäuse als auch bei der USB-Anmeldung des Geräts zu finden. Der Kobra Client VS zeigt die Modelbezeichnung und Seriennummer des Kobra VS-Datenträgers sofort nach dem Anschließen an einen PC komfortabel an.

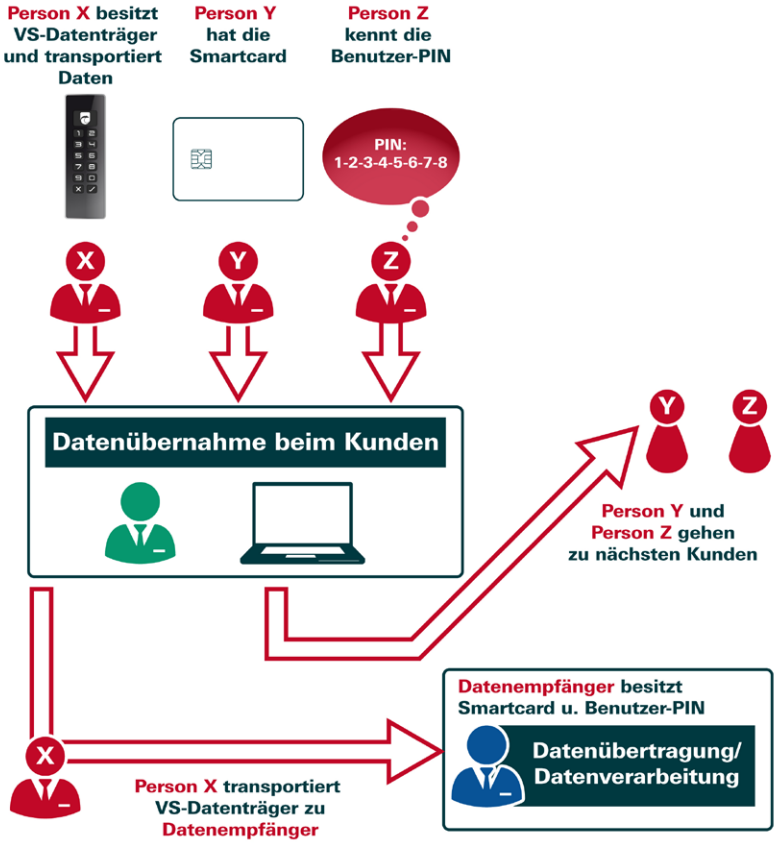
Diese Methode ermöglicht es den Kobra VS-Datenträger mit vertraulichen Daten dem Empfänger kostengünstig und versichert durch einen Paketdienstleister oder Kurier zuzustellen.

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

11.3 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 DIGITTRADE 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.



11.4 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 öffentlichen 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 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. Dieser 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)

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 DIGITTRADE Smartcards (bzw. PKI-Karten) in der Smartcard-Tabelle des Kobra VS-Datenträgers eingetragen werden.

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

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

11.5 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.

11.6 Betreiben mehrerer Datenträger mit nur einer Smartcard

Zum Betreiber 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 Software Kobra Client VS 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 11.2 beschrieben werden.

11.7 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-To-Go, 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-To-Go 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.

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

Hinweis:
Die Windows-To-Go Kompatibilität kann durch den Administrator per Kobra Client VS konfiguriert werden.

11.8 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 erfolgen.

11.9 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.

11.10 Verwendung als Authentisierungs-Medium

Der Kobra VS-Datenträger ermöglicht eine sichere Speicherung von Authentisierungs-Merkmalen wie beispielsweise Benutzernamen, sehr komplexe Passwörter, digitale Zertifikate, Schlüsselpaare und andere. 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 Authentisierungs-Komponente nur Leserechte zur Verfügung stehen. Diese Datenträger können anschließend vom Administrator für die Nutzung an der Unternehmens-IT freigegeben werden. Jeder Mitarbeiter kann auf dieser Weise ein sicheres Authentisierungs-Medium erhalten, ohne die IT-Sicherheit des Unternehmens zu gefährden.

11.11 Nutzung als Smartcard-Reader mit PIN-Pad

Der Kobra VS-Datenträger kann außerdem als Smartcard-Reader mit Tastatur für die PIN-Eingabe bzw. als Authentisierungs-Token mit PIN-Pad verwendet werden. Diese Funktion ermöglicht dem Nutzer seine Smartcard mit digitalen Zertifikaten zum Unterzeichnen digitaler Dokumente zu verwenden, ohne für diese Zwecke einen anderen Kartenleser anschaffen zu müssen.

Die Smartcard kann beispielsweise für die E-Mail-Verschlüsselung, VPN-Zugang, Windows- oder Linux-Anmeldung und für allgemeine 2-Faktor-Authentifizierung mit digitalem Zertifikat durch den Hersteller eingerichtet werden . Weitere Informationen hierzu erhalten Sie bei Ihrem Lieferanten.

11.12 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 Zutrittsmanagement, Nutzerauthentisierung etc.) oder andere Smartcards, 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.

11.13 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.

11.14 Nutzung der VID und PID für den Schutz von Unternehmensdaten

Optional können die USB Vendor-ID (VID) und Produkt-ID (PID) kundenspezifisch implementiert werden. Durch diese Informationen können die Kobra VS-Datenträger verschiedenen Abteilungen und Nutzergruppen 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.

12. Optionales Zubehör

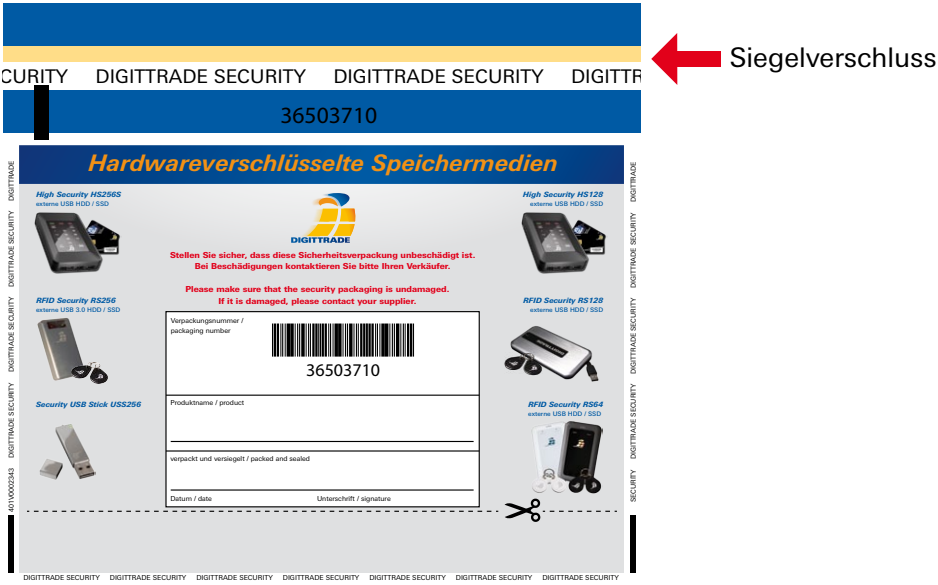
Zur Umsetzung der nutzerspezifischen Aufgaben werden zusätzliche Smartcards und Sicherheitsverpackungen als optionales Zubehör angeboten.

12.1 Zusätzliche Smartcards

Bei Bedarf können die zugelassenen DIGITTRADE Smartcards bei DIGITTRADE zusätzlich bestellt werden. Diese werden mit generierten Schlüsselpaaren ausgeliefert und verfügen über voreingestellte Benutzer- und SO-PIN (PUK) mit Standard-Werten. Zur Inbetriebnahme beachten Sie bitte Kapitel 6.

12.2 Sicherheitsverpackung

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



Der Inhalt der Sicherheitsverpackung wird auf der Verpackung beschrieben. Der Empfänger überprüft nach Erhalt die Unversehrtheit des Sicherheitsschriftzugs „DIGITTRADE 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. Menü-Übersicht, Kommandos und Werkseinstellungen

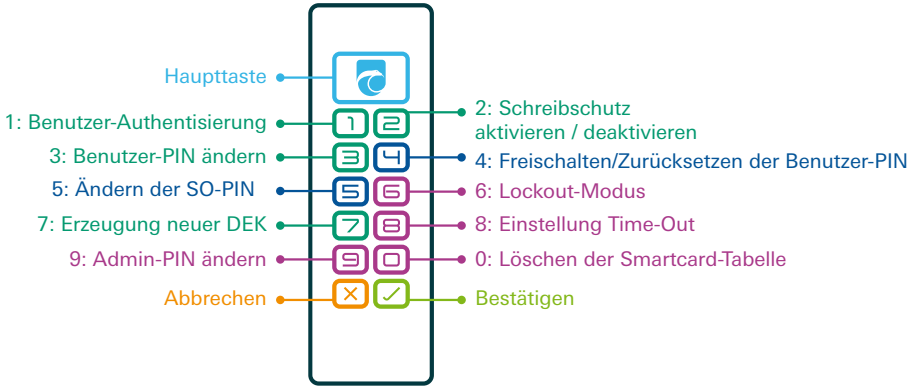
Benutzer	Taste 1 - Login Taste 2 - Schreibschutz * Taste 3 - Ändern der Benutzer-PIN Taste 4 - Freischalten der Benutzer-PIN Taste 5 - Ändern der SO-PIN (PUK) Taste 7 - Erzeugung neues Krypto-Schlüssels
Administrator	Taste 6 - Einstellung Lock-Out Taste 8 - Einstellung Time-Out Taste 9 - Ändern der Admin-PIN 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

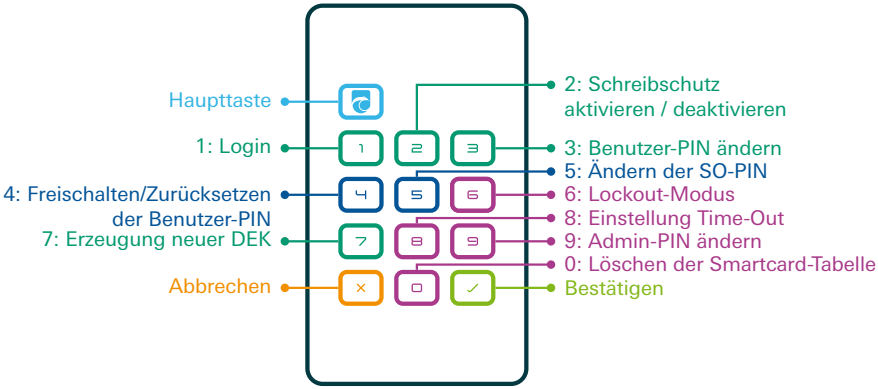
* – Der Administrator kann diese Einstellungen vor der Auslieferung an den Nutzer blockieren.

Benutzer-Kommandos

SO-PIN-Kommandos

Administrator-Kommandos





14. 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:	4 GB, 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Speicherarten:	3D TLC, MLC und pSLC

Kobra Drive VS

Speichergrößen:	250 GB, 500 GB, 1 TB, 2 TB, 4 TB, 8 TB
Speicherarten:	HDD, SSD

15. Lieferumfang

- Kobra VS-Datenträger Version 1.0
- 3 USB-Kabel (USB-C zu USB-C, USB-C zu USB-A, USB-C zu USB Micro-B)
- zwei DIGITTRADE Smartcards (optional)
- Verpackung

16. Datensicherheit, Datenverfügbarkeit und Haftungsausschluss

Die Kobra VS-Datenträger bieten Ihnen eine hohe Datensicherheit nach dem aktuellen Stand der Technik. Sie gewährleisten die datenschutzgerechte 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 DIGITTRADE GmbH haftet nicht für den Verlust von Daten sowie für dadurch entstehende Kosten und Schäden. Zudem trägt das genannte Unternehmen keine datenschutzrechtliche Verantwortlichkeit der gespeicherten Daten.

17. Sicheres Beenden nach Benutzung des VS-Datenträgers

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 bedeutende Unterstützung zum effektiven Datenschutz.

Die schnelle Abmeldung kann durch das doppelte Klicken auf die X-Taste innerhalb von 2 Sekunden erfolgen. (Quick-Out-Funktion)

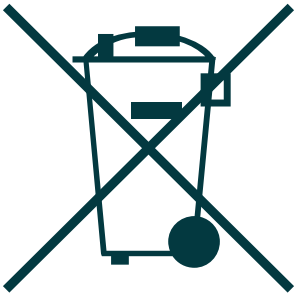
Für die sichere physikalische Trennung muss das USB-Kabel vom Kobra VS-Datenträger vollständig entfernt werden.

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.

18. Hinweis zum Schutz und Erhalt der Umwelt

Gemäß der EG-Richtlinie dürfen Elektro- und Elektronik-Altgeräte nicht als kommunale Abfälle entsorgt werden. Um die Verbreitung der enthaltenen Bausubstanzen in Ihrer Umgebung zu vermeiden und natürliche Ressourcen zu sparen, bitten wir Sie, dieses Produkt nach Ablauf seiner Lebensdauer ausschließlich an einer lokalen Altgerätesammelstelle in Ihrer Nähe abzugeben.

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



19. Umgang mit Sicherheitsfehlern

Für eine geregelte Erfassung, Klassifizierung und Behebung eventueller Fehler stellt der Hersteller ein Fehlermanagement den Administratoren von Kobra VS-Datenträgern zur Verfügung. In diesem Kapitel finden Sie die Hinweise, 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://www.digittrade.de/vs oder über die E-Mail Adresse vs@kobra-infosec.de durchführen.

19.1 Registrierung

Für automatische Benachrichtigungen zu eventuellen Sicherheitsproblemen Ihres Kobra VS-Datenträgers empfehlen wir eine Registrierung unter https://www.digittrade.de/vs. Obligatorisch ist die Eintragung einer E-Mail Adresse und die Auswahl des Produktes, 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, welche 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 der automatischen Benachrichtigungen zu eventuellen Sicherheitsproblemen erhalten Sie per E-Mail 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 wünschen, so können Sie sich jederzeit per E-Mail an vs@kobra-infosec.de aus dem Verteiler löschen lassen.

19.2 Fehler melden

Im Rahmen der kontinuierlichen Produktverbesserung und -wartung prüfen wir regelmäßig, ob die durch das 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 entdeckt haben, 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 geheim gehalten wird,

bis durch uns ein Firmware-Updates bereitgestellt werden kann und der Großteil der Anwender dieses in seine Geräte eingespielt hat. In diesem Zusammenhang soll die Mitteilung über eine eventuelle Schwachstelle ausschließlich verschlüsselt erfolgen. Hierzu dient entweder das Formular auf https://www.digittrade.de/vs oder eine verschlüsselte E-Mail an vs@kobra-infosec.de. Das S/MIME-Zertifikat und den PGP-Key hierzu finden Sie ebenfalls auf https://www.digittrade.de/vs.

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 kundendienst@digittrade.de, telefonisch an +49/345/2317353 oder per Web-Formular auf der Website https://www.digittrade.de/store/kontaktformular.

20. FAQ

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

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

Nach Drücken der Haupttaste blinkt die Haupttaste 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 VS-Datenträger.

B: Eine unbekannte Smartcard ist richtig eingelegt, aber sie wird nicht als eine Smartcard erkannt.

C: 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 für den VS-Datenträger unbekannt. 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 VS-Datenträger bekannt. Jedoch sind die SO- und / odern Benutzer-PIN gesperrt oder es wurde die Smartcard-Tabelle gelöscht.

Verhalten nach Eingabe und Bestätigung der Benutzer-PIN

Die Haupttaste blinkt blau und alle anderen Tasten sind ausgeblendet

Sie haben den VS-Datenträger das erste Mal mit dem Host-System verbunden. Der VS-Datenträger formatiert sich deshalb automatisch, damit Sie diesen verwenden können. Die Erstformatierung findet auch statt, wenn der Schreibschutz vorher aktiviert wurde.

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

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

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.

Die Haupttaste blinkt einmal rot (oder mehrmals hintereinander) und der 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.

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

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

Weitere Fragen und Lösungen

Die Sicherheitsabfrage ist fehlgeschlagen

Die Haupttaste blinkt rot.
Eine falsche Benutzer-PIN wurde eingegeben. Drücken Sie die “Haupttaste” + “1” + “V” um die Sicherheitsabfrage 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 VS-Datenträger nicht mit einem USB-Hub oder einem Verlängerungskabel angeschlossen ist.

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 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 VS-Datenträger wurde über einen USB-Hub angeschlossen:
Stellen Sie sicher, dass der 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 VS-Datenträger anschließend schneller arbeitet.

Ich kann keine Dateien auf die Festplatte schreiben

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 USB-Sticks KOBRA Stick Basic 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**.

Ihre Notizen / Your Notes

Ihre Notizen / Your Notes

DIGITTRADE 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