Version 1.05
04.04.2019

KOBRA STICK

encrypted USB-C secure flash drive

für Unternehmen und Behörden
for business and governmental use

Benutzerhandbuch
User Manual

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

EINE FEHLERHAFTE BEDIENUNG KANN ZU SCHÄDEN AM KOBRA STICK SOWIE ZU DATENVERLUSTEN FÜHREN.

Die digitale Fassung des Handbuchs kann auf www.digittrade.de im Download-Center heruntergeladen werden.

Produktversion:	Kobra Stick (Encrypted USB-C Stick) Version 1.0
Benutzerhandbuch Version:	1.05 (04.04.2019)

Inhaltsverzeichnis

1. Über den Kobra Stick

Der KOBRA Stick ist ein verschlüsselter USB-C Speicherstick in einem stabilen, eleganten Metallgehäuse. Er ermöglicht die datenschutzgerechte Speicherung und Aufbewahrung sowie den sicheren Transport sensibler Geschäfts- und Privatdaten von Behörden und Unternehmen. Er wurde unter Berücksichtigung der „Technischen Richtlinien" des BSI entwickelt, verfügt über das Qualitätszeichen „IT-Security made in Germany" und ist aufgrund seiner Sicherheitsfunktionen eine gute Option, um Daten mobil sicher zu speichern.

Die auf dem KOBRA Stick gespeicherten Daten sind in Hinblick auf die Vertraulichkeit der Informationen vor unbefugten Zugriffen geschützt, etwa wenn der Datenträger verloren oder entwendet wird sowie auch bei logischen oder physikalischen Angriffen.

Um die Sicherheitseigenschaften des KOBRA Stick in vollem Umfang zu nutzen, sind folgende Schritte erforderlich:

- Gewährleisten Sie, dass an Ihrem Host-System ein angemessener Schutz für alle aus dem geschützten Speicherbereich des KOBRA Stick aufgerufenen Daten besteht
- Sorgen Sie dafür, dass keine Malware auf den KOBRA Stick übertragen werden kann
- Überprüfen Sie nach Erhalt des KOBRA Stick die Vollständigkeit und die Richtigkeit der Lieferung
- Überprüfen Sie nach der Erstanmeldung die Funktionen des KOBRA Stick (Kapitel 5)
- Ändern Sie die Benutzer-PIN (Kapitel 5.2)
- Ändern Sie die Admin-PIN, falls Sie als Administrator für die Verwaltung des KOBRA Stick zuständig sind (Kapitel 5.3)
- Erzeugen Sie neue Verschlüsselungsschlüssel (auch Kryptoschlüssel oder KS genannt) auf dem KOBRA Stick (Kapitel 5.5)
- Behandeln Sie Ihre Authentifizierungsdaten (Benutzer-PIN und Admin-PIN) vertraulich

Eine ausführliche Beschreibung der oben genannten Schritte finden Sie in diesem Benutzerhandbuch in den referenzierten Kapiteln.

Auf der Rückseite des KOBRA Stick befinden sich die Seriennummer und der entsprechende QR-Code. Diese Informationen sowie die Vendor-ID (VID) und Produkt-ID (PID) sind über die USB-C-Schnittstelle auslesbar.

Der KOBRA Stick gewährleistet die Vertraulichkeit der Daten durch folgende Sicherheitsmechanismen:

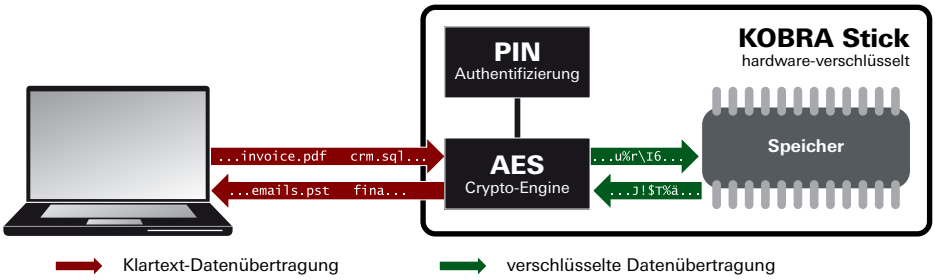
- Verschlüsselung
- Zugriffskontrolle
- Verwaltung der kryptografischen Schlüssel

1.1 Verschlüsselung

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

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

Der KOBRA Stick verschlüsselt außerdem temporäre Dateien und Bereiche, die von der Verschlüsselungssoftware oft unbeachtet bleiben.



1.2 Zugriffskontrolle

- Der Zugriff erfolgt über die Eingabe einer Benutzer-PIN.

Der KOBRA Stick erzeugt automatisch die neuen Verschlüsselungsschlüssel und setzt die Benutzer-PIN auf die Werkseinstellungen zurück, sobald die zulässige Anzahl der fehlerhaften PIN-Eingaben überschritten wurde. Der Zugriff auf die zuvor auf dem Stick gespeicherten Daten ist danach nicht mehr möglich.

1.3 Verwaltung der kryptografischen Schlüssel

Der Benutzer kann die kryptografischen Schlüssel jederzeit erstellen, ändern und zerstören. Diese Vorgänge sind irreversibel. Nach der Erzeugung neuer Kryptoschlüssel werden die alten Kryptoschlüssel und somit alle auf dem Datenträger gespeicherten Daten endgültig vernichtet. Daher sollen die gespeicherten Informationen unter Umständen zuvor auf einem anderen verschlüsselten Datenträger gesichert werden.

Die beiden für die Ver- und Entschlüsselung der Daten zuständigen 256-Bit Verschlüsselungsschlüssel werden mit Hilfe eines Hardware-Zufallszahlengenerators erzeugt und innerhalb des Sticks sicher gespeichert. Sie werden nach korrekter Eingabe der Benutzer-PIN für die Ver- und Entschlüsselung der Daten an das Verschlüsselungsmodul des KOBRA Stick übertragen.

1.4 Die wichtigsten Eigenschaften im Überblick

- AES-Full-Disk-Hardwareverschlüsselung im XTS-Modus mit zwei 256-Bit kryptografischen Schlüsseln
- Authentifizierung mittels Benutzer-PIN
- Hardwarebasiertes Verschlüsselungsmodul
- Datenverschlüsselung aller gespeicherten Bytes und beschriebenen Sektoren
- Unabhängig von Betriebssystemen (Unterstützung aller Betriebssysteme, Multimediageräte, Smartphones und Maschinen mit USB-Datenträger-Unterstützung)
- Integrierter Schreibschutz
- Einstellbare Anzahl der erlaubten Fehlversuche
- Kompatibel mit USB 3.0 und USB 2.0
- Keine Einschränkungen der Lese- und Schreibgeschwindigkeit
- Robustes Metallgehäuse
- Time-Out & Quick-Out Funktionen
- Pre-Boot-Authentisierung und Boot-Fähigkeit
- Interne Stromversorgung, welche eine Authentisierung ohne Anschluss an einen PC oder USB-Hub ermöglicht.

Optional:

- USB VID, PID & Seriennummer nach Kundenvorgaben definierbar
- Lasergravur kundenspezifischer Informationen auf der Rückseite des KOBRA Stick

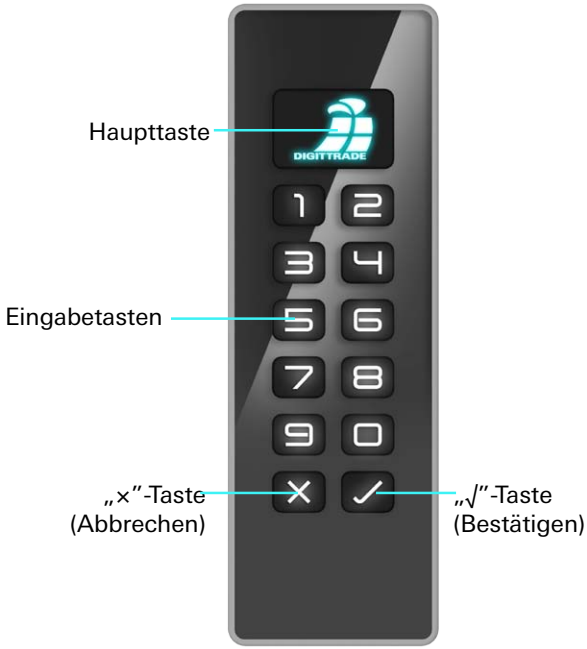
1.5 Vorteile des KOBRA Stick

- Privat- und Geschäftsdaten sind sicher vor dem Zugriff Unbefugter geschützt
- Einfache und sichere Handhabung durch Hardwareverschlüsselung: Anschließen, Anmelden, Verwenden
- Alle Daten sind sofort verschlüsselt gespeichert
- Keine Performanceverluste

2. USB-Anschluss und Eingabeoberfläche

Der KOBRA Stick kann per USB-Schnittstelle mit einem Computer verbunden werden.

USB-C 3.0 Anschluss



Auf der Vorderseite verfügt der KOBRA Stick über eine Eingabetastatur mit einer Haupttaste, zwei Kommandotasten („×"-Abbruchtaste und „√"-Bestätigungstaste) und zehn Eingabetasten (0 bis 9). Die Verbindung mit einem PC erfolgt über die USB-C 3.0 Schnittstelle.

3. Inbetriebnahme des KOBRA Stick

Für die korrekte Inbetriebnahme des KOBRA Stick sind nur zwei Schritte erforderlich:

1) KOBRA Stick mit dem PC verbinden
2) PIN-Eingabe auf dem KOBRA Stick durchführen

Es ist ebenso ein Vertauschen der Reihenfolge möglich.

Die notwendige Stromversorgung erfolgt bei dem KOBRA Stick generell über den USB-Anschluss. Zudem verfügt dieser USB-Stick über eine integrierte autonome Stromversorgung, die eine Freischaltung vor dem Anschluss an einen PC sowie eine Pre-Boot-Authentisierung und einen anschließenden Computerstart vom KOBRA Stick ermöglicht.

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

Der KOBRA Stick geht sowohl nach langem Drücken (ca. 3 Sekunden) auf die Haupttaste als auch nach dem Anschluss an einen PC sofort in den Authentisierungsmodus. Die Haupttaste blinkt grün und alle anderen Tasten sind aktiv. An dieser Stelle kann die Benutzer-PIN zur Freischaltung des KOBRA Stick eingegeben werden.

Alle Eingaben und Kommandos werden immer mit der „√"-Taste bestätigt oder mit der „×"-Taste abgelehnt. Nach jeder Betätigung der „×"-Taste wechselt der Benutzer in den Warte-Modus und kann von dort aus erneut beginnen. Zur Bestätigung kann anstatt der „√"-Taste auch die Haupttaste verwendet werden.

Durch die Betätigung der Hauptaste im Warte-Modus wechselt der Stick in den Menü-Modus. In diesem Zustand leuchten 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 die „√"-Taste wechselt der Benutzer erneut in den Authentisierungsmodus und kann auch auf diesem Wege durch die Eingabe der Benutzer-PIN den Stick freischalten. Nach der erfolgreichen Authentisierung leuchtet die Haupttaste dauerhaft grün. Die anderen Tasten sind deaktiviert 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 maximal zulässigen Fehlversuche). Der KOBRA Stick schaltet anschließend erneut in den Warte-Modus um. Der Authentisierungsvorgang kann von dieser Stelle wie oben beschrieben wiederholt werden. PIN-Eingabeversuche unter 4 Stellen werden nicht als Fehlversuche angesehen und demzufolge nicht gezählt.

Nach der Überschreitung der zulässigen Anzahl an Fehlversuchen blinkt die Haupttaste abwechselnd jeweils dreimal rot und gelb. Der KOBRA Stick schaltet danach in den Authentisierungsmodus um. Dabei löscht der KOBRA Stick automatisch die alten Kryptoschlüssel, erzeugt zwei neue Kryptoschlüssel und setzt die Benutzer-PIN auf die Werkseinstellungen zurück.

Nach erfolgreicher Authentisierung mit der neuen Benutzer-PIN formatiert der KOBRA Stick den Speicher. Die Haupttaste blinkt während der Formatierung dauerhaft blau. Anschließend leuchtet die Haupttaste ununterbrochen grün oder violett entsprechend der zuvor vorgenommenen Schreibschutzeinstellungen. Die anderen Tasten sind deaktiviert und der Zugriff auf den KOBRA Stick ist freigeschaltet. Die Stick-Partition erscheint auf dem Desktop und kann bedient werden.

Alle zuvor gespeicherten Daten werden bei diesem Vorgang endgültig gelöscht!

Werden in einem begonnenen Kommando innerhalb von 20 Sekunden keine weiteren Eingaben getätigt, so wechselt der an einen PC angeschlossene KOBRA Stick automatisch in den Warte-Modus. Im Batteriebetrieb kehrt der Stick nach 20 Sekunden in den Schlaf-Modus zurück.

Für den authentisierten KOBRA Stick trifft diese Regelung nicht zu, falls dieser bereits an einem PC angeschlossen ist oder spätestens innerhalb von 20 Sekunden nach der erfolgreichen Authentisierung angeschlossen wird. Die Zeit für eine eventuelle automatische Sperre des authentisierten und an einen PC angeschlossenen KOBRA Stick wird gegebenen falls durch die Time-Out-Einstellungen geregelt. (Kapitel 5.7)

Zudem verfügt der KOBRA Stick neben den klassischen „Abmelde"-Mechanismen wie das „sichere Entfernen" über die Taskleiste des PCs 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.

Hinweis:
Um die Sicherheit Ihrer Daten zu gewährleisten, ist es zwingend erforderlich, die voreingestellte Benutzer-PIN zu ändern. Verändern Sie zudem die Benutzer-PIN auch zukünftig in regelmäßigen Abständen. Die Benutzer-PIN muss vertraulich behandelt werden.

4. Rolle und Berechtigungen

Der KOBRA Stick ermöglicht eine Aufteilung der Rollen und Berechtigungen bezüglich der Verwaltung und Bedienung des Datenträgers.

Der Benutzer kennt die Benutzer-PIN. Er kann diese PIN ändern, sich an dem Stick authentisieren (anmelden), den Schreibschutz aktivieren und deaktivieren sowie die gültigen Verschlüsselungsschlüssel vernichten und neue erzeugen. Die Benutzer-PIN ermöglicht die Authentisierung am KOBRA Stick und folglich den Zugriff auf die gespeicherten Daten.

Der Administrator kennt die Admin-PIN. Er kann die Admin-PIN ändern, Time-Out-Einstellungen vornehmen sowie die Anzahl der erlaubten Fehlversuche festlegen. Der Administrator hat auf der Basis seiner Berechtigungen keine Möglichkeit, auf die gespeicherten Daten eines KOBRA Stick zu zuzugreifen.

5. Menü-Modus: Authentisierung und Verwaltung

Die Authentisierung und Verwaltung des KOBRA Stick erfolgt über den Menü-Modus mittels Eingabe von Zahlen und Kommandos. Die Umschaltung in den Menü-Modus geschieht generell aus dem Warte-Modus durch die Betätigung der Haupttaste. Im Menü-Modus leuchten die Haupttaste blau und alle anderen Eingabe-Tasten weiß.

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

Im Menü-Modus sollen alle Eingaben und Kommandos mit der „√"-Taste bestätigt werden. Alternativ können diese auch mit der „×"-Taste abgebrochen werden. Nach jeder Betätigung der „×"-Taste leuchtet die Hauptaste kurz orange und danach weiß. Der KOBRA Stick wechselt dabei 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. Sofern die Admin-PIN gefordert ist, blinkt die Haupttaste violett. 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 Stick schaltet dabei in den Warte-Modus um. 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 Fehlversuche einmal oder mehrfach rot (jedoch maximal entsprechend der Anzahl der eingestellten Fehlversuche) und der KOBRA Stick schaltet in den Warte-Modus um. Der geplante Vorgang kann von dieser Stelle aus erneut gestartet werden.

Der KOBRA Stick gelangt nach jeder erfolgreichen Ausführung eines Kommandos wieder in den Warte-Modus. Eine Ausnahme bildet nur die erfolgreiche Authentisierung.

Hinweis:
Bei allen Funktionen und Einstellungen, welche die Eingabe der Benutzer-PIN erfordern, blinkt die Haupttaste dauerhaft grün und alle anderen Tasten bleiben aktiv. Für die Eingabe der Admin-PIN blinkt die Haupttaste dagegen dauerhaft violett.

5.1 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 Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie die Tasten „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, die anderen Tasten sind deaktiviert und der Zugriff auf die Daten ist freigeschaltet.

5.2 Ändern der Benutzer-PIN

Die Benutzer-PIN wird benötigt, um sich an dem KOBRA Stick zu authentisieren (anmelden), den Schreibschutz zu aktivieren und zu deaktivieren sowie die Verschlüsselungsschlüssel zu vernichten oder zu erzeugen.

Im Auslieferungszustand verfügt der KOBRA Stick über die Benutzer-PIN „1-2-3-4-5-6-7-8“. Diese PIN erhält der Stick außerdem nach der Überschreitung der erlaubten Fehlversuche und anschließender Zurücksetzung der Benutzer-PIN auf die Werkseinstellungen. Der Benutzer kann für die Gestaltung der Benutzer-PIN eine Kombination von 4 bis 16 Ziffern wählen.

1) Stellen Sie sicher, dass Sie sich im Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie die Taste „3“ und anschließend „√“. Die Haupttaste blinkt dauerhaft grün und alle anderen Tasten bleiben aktiv.
3) Geben Sie die alte 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 Datenträger schaltet wieder in den Warte-Modus.

5.3 Ändern der Admin-PIN

Die Admin-PIN (auch Geräte-PIN genannt) wird für die Time-Out-Einstellung und die Festlegung der erlaubten Fehlversuche benötigt. Sie kann eine Länge von 4 bis 16 Stellen besitzen, hat eine reine Verwaltungsfunktion und bietet keine Möglichkeit, auf die Daten zu zugreifen.

Im Auslieferungszustand verfügt der KOBRA Stick über die Admin-PIN „8-7-6-5-4-3-2-1“. Für die Eingabe der Admin-PIN stehen 16 Fehlversuche zur Verfügung. Nach der Überschreitung der erlaubten Fehlversuche wird die Admin-PIN unwiderruflich blockiert. Anschließend können die oben genannten Admin-Funktionen nicht mehr geändert werden. Die Benutzer-Funktionen können unabhängig davon weiterhin bedient werden.

Für die Änderung der Admin-PIN:

1) Stellen Sie sicher, dass Sie sich im Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie die Taste „9“ und anschließend die „√“. Die Haupttaste blinkt dauerhaft violett und alle anderen Tasten bleiben aktiv.
3) Geben Sie die alte 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.

5.4 Schreibschutz-Mechanismus

Der aktivierte Schreibschutz bietet Ihnen einen zusätzlichen Schutz vor Viren und Trojanern während der Verwendung des Sticks an einem fremden PC. Zudem kann dadurch eine versehentliche Speicherung sensibler Informationen von einem PC oder Server auf den Stick 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 Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie die Taste „2". Bei aktiviertem Schreibschutz leuchtet die Haupttaste violett, bei deaktiviertem Schreibschutz grün.
3) Drücken Sie anschließend die „√"-Taste. 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 Datenträger schaltet zurück in den Warte-Modus.

5.5 Erzeugen neuer Kryptoschlüssel

Bei dem Erzeugen neuer Kryptoschlüssel werden die alten Kryptoschlüssel und somit alle auf dem Datenträger gespeicherten Daten endgültig vernichtet. Daher sollten die gespeicherten Informationen gegebenenfalls zuvor auf einem anderen zugelassenen Datenträger gesichert werden.

Zum Erzeugen oder Ändern der Verschlüsselungsschlüssel:

1) Stellen Sie sicher, dass Sie sich im Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie die Taste „7". Die Haupttaste leuchtet dauerhaft rot und signalisiert damit, dass alle auf dem Stick gespeicherten Daten nach der Ausführung dieser Funktion endgültig vernichtet werden.
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 mit „√".

Nach der erfolgreichen Erzeugung oder Änderung der Verschlüsselungsschlüssel blinkt die Haupttaste kurz grün und der KOBRA Stick schaltet zurück in den Warte-Modus.

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 Stick gespeicherten Daten ist ab diesem Zeitpunkt nicht mehr möglich.

5.6 Löschen der Kryptoschlüssel

Das Löschen und/oder Vernichten der Kryptoschlüssel kann auf zwei Wegen erfolgen.

a) Zerstörung durch Erzeugung neuer kryptografischer Schlüssel

Während dieses Vorgangs werden die alten Verschlüsselungsschlüssel unwiderruflich überschrieben. Der Zugriff auf alle zuvor gespeicherten Daten ist ab diesem Zeitpunkt nicht mehr möglich.

Diese Methode ermöglicht eine schnelle Vernichtung der auf dem KOBRA Stick gespeicherten Daten, ohne den Stick an einen PC anzuschließen.

b) Zerstörung der kryptografischen Schlüssel durch Überschreitung der erlaubten Anzahl an Fehlversuchen für die Eingabe der Benutzer-PIN

Während dieses Vorgangs werden neben der Zurücksetzung auf die Werkseinstellungen der Benutzer-PIN auch die alten Kryptoschlüssel unwiderruflich zerstört und neue erzeugt. Der Zugriff auf alle zuvor gespeicherten Daten ist auch in diesem Fall nicht mehr möglich.

5.7 Time-Out und Quick-Out Funktionen

Der Administrator kann festlegen, nach wie viel Minuten der freigeschaltete KOBRA Stick sich automatisch sperrt, wenn innerhalb der angegebenen Zeit weder lesender noch schreibender Zugriff auf den Stick erfolgt. Die Auswahl für die Sperre liegt zwischen 1 und 30 Minuten. Zur Aufhebung der Sperre ist „0“ auszuwählen.

Für das Festlegen eines Time-Out:

1) Stellen Sie sicher, dass Sie sich im Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie 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 Stick wechselt zurück in den Warte-Modus.

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

5.8 Erlaubte Fehlversuche für die Eingabe der Benutzer-PIN

Im Auslieferungszustand stehen dem Benutzer 8 erlaubte Fehlversuche zur Verfügung. Der Administrator kann diese Anzahl auf 1 bis 16 Fehlversuche anpassen. Nach der Überschreitung der festgelegten Anzahl löscht der KOBRA Stick automatisch die alten Kryptoschlüssel, erzeugt die neuen und setzt die Benutzer-PIN auf die Werkseinstellungen zurück. Alle verfügbaren Daten werden dabei endgültig vernichtet.

Für die Einstellung der erlaubten Fehlversuche:

1) Stellen Sie sicher, dass Sie sich im Menü-Modus befinden. (Die Haupttaste leuchtet blau und die anderen Tasten leuchten weiß.)
2) Drücken Sie 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 zwischen 1 und 16 ein und bestätigen Sie mit „√“

Nach einer erfolgreichen Ausführung blinkt die Haupttaste kurz grün und der KOBRA Stick schaltet zurück in den Warte-Modus.

Hinweis:
Die Reduzierung der erlaubten Fehlversuche ist sofort gültig. Die Erhöhung dieser Anzahl wird erst nach einer erfolgreichen Eingabe der Benutzer-PIN wirksam, auch wenn diese Eingabe erstmalig nach der Zurücksetzung des Sticks auf die Werkseinstellungen erfolgt.

6. Formatierung

Der KOBRA Stick 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 Stick je nach Anwendungsszenarien wunschgemäß umformatieren. Für Windowsnutzer wird empfohlen, beispielsweise NTFS zu verwenden. Für Mac OS X ist HFS+ 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 Stick mit jedem anderen Dateisystem zu formatieren. Dies beeinflusst die Verschlüsselung der Daten und die bereits vorgenommenen Einstellungen nicht.

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

	NTFS	FAT32	HFS+	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

7. Anwendungsmöglichkeiten

Die Eigenschaften des KOBRA Stick bieten umfangreiche Möglichkeiten für die sichere Speicherung, Archivierung und Übermittlung persönlicher und sensibler Daten. Im Folgenden finden Sie zudem einige spezifische Szenarien.

7.1 Verschärfung des Schutz-Niveaus für KOBRA Stick im Unternehmen

Der Administrator im Unternehmen oder einer Behörde kann festlegen, wie restriktiv sich der KOBRA Stick eines Nutzers verhalten soll. Für diese Zwecke kann er für den Nutzer die Anzahl der erlaubten Fehlversuche und die Time-Out-Zeit festlegen.

Mit Hilfe der Time-Out-Einstellung kann der Administrator festlegen, nach wie viel Minuten der freigeschaltete KOBRA Stick sich automatisch sperrt, wenn innerhalb der angegebenen Zeit weder lesender noch schreibender Zugriff auf den Stick erfolgt.

Der Benutzer kann diese Einstellungen auf der Basis seiner Berechtigungen nicht ändern. Dies ist selbst dann nicht möglich, wenn die Anzahl der erlaubten Fehlversuche überschritten ist und die Benutzer-PIN auf die Werkseinstellungen zurückgesetzt wurde.

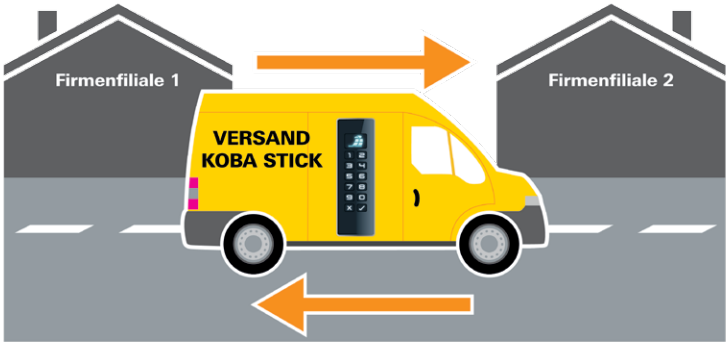
7.2 Sicherer und kosteneffizienter Datentransport

Der KOBRA Stick kann für den Transport sensibler Daten verwendet werden. Dazu werden im Vorfeld neue Verschlüsselungsschlüssel erzeugt und die Benutzer-PIN geändert. Die Anzahl der erlaubten Fehlversuche kann für diese Zwecke auf die minimalen Werte, zum Beispiel auf 1 bis 3 Versuche, reduziert werden. Zusätzlich kann auch der Schreibschutz nach der Speicherung der zu versendenden Daten aktiviert werden. Der Absender versendet in diesem Fall nur den KOBRA Stick per Post oder per Kurier.

Des Weiteren müssen der Sender und der Empfänger bei jedem Datentransport sicherstellen, dass sie eine Manipulation an dem KOBRA Stick erkennen können. Hierzu empfiehlt sich die Verwendung von versiegelten Sicherheitstaschen. Dies gilt auch für alle anderen Datentransportmöglichkeiten mittels des KOBRA Stick.

Bei Erhalt des Datenträgers ist dessen Authentizität zu prüfen. Hierzu wird über einen separaten sicheren Weg die Seriennummer des Datenträgers mittgeilt. Die Seriennummer befindet sich sowohl auf dem Gehäuse als auch in den Geräteinformationen des Sticks, welche über den USB-Anschluss auszulesen sind. Erst nach der Übereinstimmung dieser Angaben erfolgt die Übermittlung der Benutzer-PIN an den Empfänger.

Diese Methode ermöglicht es den KOBRA Stick mit sensiblen Daten dem Empfänger kostengünstig und versichert durch einen Paketdienstleister oder Kurier zuzustellen.



7.3 Verwendung weniger Datenträger bei großem Kundenkreis

Für beispielsweise Datenverarbeitungsunternehmen, Datenzentralen von Großunternehmen oder Behörden, die im ständigen Datenaustausch mit vielen Datenempfängern stehen, bietet der KOBRA Stick die Möglichkeit Daten mit wenigen Speichermedien kostengünstig sicher zu transportieren.

Für jeden Datenversand an einen anderen Empfänger werden die Kryptoschlüssel des KOBRA Stick neu erzeugt und die Benutzer-PIN neu festgelegt. Die Anzahl der erlaubten Fehlversuche kann für diese Zwecke ebenfalls auf die minimalen Werte, zum Beispiel auf 1 bis 3, reduziert werden. Anschließend können die Daten auf dem KOBRA Stick gespeichert und per Post oder per Kurier versendet werden. (siehe Kapitel 7.2)

Aufwendige Datenlöschungen und mehrmaliges Überschreiben des Datenträgers entfallen, da die verbliebenen Daten mit den vorherigen Kryptoschlüsseln verschlüsselt sind. Jedoch existieren die alten Kryptoschlüssel nach dem Erzeugen der neuen nicht mehr. Der Speicher ist mit den neu erzeugten Kryptoschlüssel formatiert.

Die Stückzahl der erforderlichen Datenträger kann dank dieser Eigenschaft reduziert werden, da nicht für jeden Datenempfänger ein personalisierter KOBRA Stick benötigt wird.

Hinweis:
Das Löschen des Datenträgers durch das Erzeugen neuer Kryptoschlüssel ist zu empfehlen, da dies die Lebensdauer des Speichers wesentlich weniger beansprucht als ein vollständiges mehrmaliges Überschreiben des gesamten Speichers.

7.4 Verwendung weniger Datenträger im Außendienst und bei Behörden

Für die Tätigkeit außerhalb des Unternehmens erhält der Mitarbeiter einen beliebigen KOBRA Stick, der zuvor beispielweise bei einem anderen Mitarbeiter in der Verwendung war und anschließend mittels der Überschreitung der erlaubten Fehlversuche aufbereitet wurde.

Durch diesen Vorgang setzt der Administrator oder auch der neue Mitarbeiter die Benutzer-PIN auf die Werkseinstellungen zurück, löscht die beiden alten Kryptoschlüssel, erzeugt die neuen Verschlüsselungsschlüssel und formatiert den Datenträger. Alle diese Prozesse verlaufen im Hintergrund nachdem der Mitarbeiter oder der Administrator die Anzahl der erlaubten Fehlversuche überschritten hat.

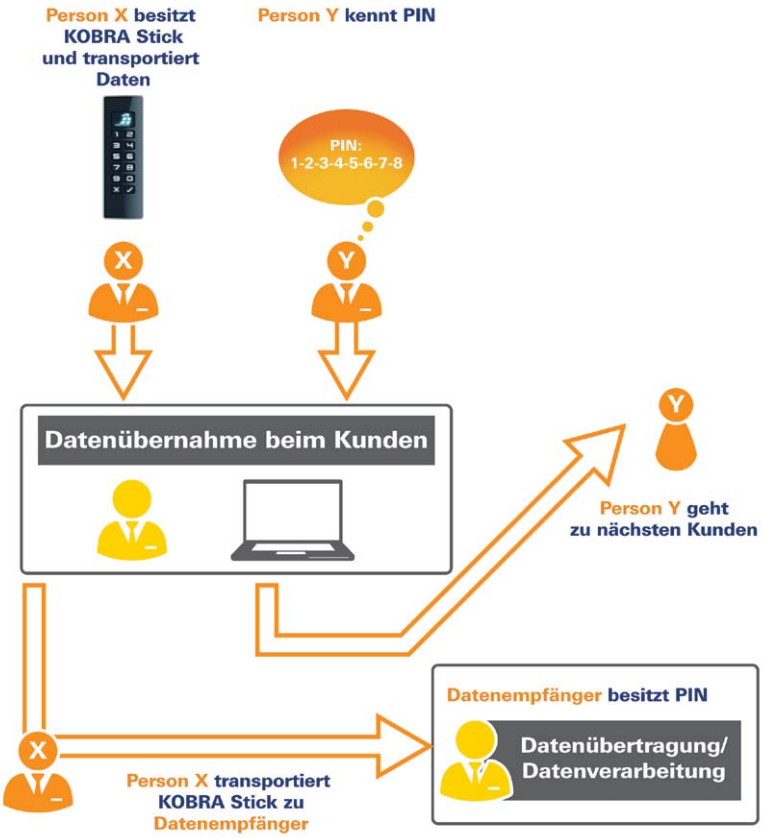
Anschließend ändert der neue Mitarbeiter die Benutzer-PIN und kann den KOBRA Stick für die sichere Speicherung seiner Daten verwenden. Falls Präsentationen an fremden PCs anstehen oder aus anderen Gründen die gespeicherten Dateien unverändert bleiben sollen, kann der Schreibschutz aktiviert werden.

Nach der Benutzung gibt der Mitarbeiter den KOBRA Stick zurück. Vor der Rückgabe vernichtet er die aktuellen Verschlüsselungsschlüssel und die auf dem KOBRA Stick gespeicherten Daten mittels Erzeugung neuer Kryptoschlüssel (Kapitel 5.5).

Der KOBRA Stick wird anschließend auf gleicher Weise innerhalb weniger Minuten für den nächsten Kollegen wie oben beschrieben einsatzbereit gemacht. Es wird daher nicht für jeden Mitarbeiter ein eigener KOBRA Stick benötigt und die Anzahl der erforderlichen Datenträger im Unternehmen kann dadurch reduziert werden.

7.5 Trennung von Datenträger und Authentifizierungen

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



7.6 Verwendung als verschlüsseltes Boot-Device

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

In diesem Zusammenhang können Betriebssysteme, wie beispielsweise Windows To Go, Linux, ECOS Secure Linux und andere, sowie die erforderlichen Daten auf dem Stick gespeichert werden. Diese Anwendung ist sowohl für stationäre als auch mobile Computer geeignet. Zu beachten sind dabei die minimalen erforderlichen Speicherkapazitäten. Das Betriebssystem Windows To Go kann erst mit dem KOBRA Stick mit einer Speicherkapazität ab 32 GB verwendet werden und benötigt eine spezielle Konfiguration des Sticks, die bereits vor der Auslieferung durchgeführt werden muss.

7.7 Verwendung an verschiedenen Betriebssystemen und Smartphones

Der KOBRA Stick funktioniert durch seine Hardwareverschlüsselung unabhängig vom Betriebssystem und kann an fast jedem Gerät verwendet werden, das USB-Datenträger unterstützt.

Der optimierte Stromverbrauch ermöglichen es, den KOBRA Stick zum Datenaustausch mit einem Smartphone oder Tablet zu verwenden.

7.8 Integration von bestehenden Softwarelösungen

Alle im Unternehmen bereits existierenden Softwarelösungen können weiterhin ergänzend verwendet werden, um die Sicherheitseigenschaften und Verwendungsmethoden zu erweitern. Durch die integrierte Batterie kann die Authentisierung auch im Vorfeld ohne Anschluss an einen PC oder einen anderen externen Stromversorger (z.B. USB-Netzteil oder USB-Hub) erfolgen. Diese Eigenschaft des Datenträgers wird als Pre-Boot-Authentisierung bezeichnet. (Kapitel 3)

Zudem kann der KOBRA Stick als Boot-Medium mit installiertem Betriebssystem verwendet werden. Beim Anschließen an einem beliebigen PC startet das auf dem Stick installierte Betriebssystem. Mit dem Trennen des KOBRA Stick vom PC bleiben die Daten, Programme und temporären Dateien ausschließlich auf dem KOBRA Stick verschlüsselt gespeichert und sind für Unbefugte unzugänglich.

7.9 Nutzung der VID und PID für den Schutz von Unternehmensdaten

Optional können die Vendor-ID (VID) und Produkt-ID (PID) kundenspezifisch implementiert werden. Durch diese Informationen können die KOBRA Stick verschiedenen Abteilungen und Nutzergruppen zugeordnet werden. Diese verfügen ggf. ebenfalls über unterschiedliche Berechtigungen für USB-Verbindungen im firmeninternen Netzwerk.

Auf diesem Wege kann festgelegt werden, welche KOBRA Stick an welche 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 ist ggf. zusätzliche Software erforderlich.

7.10 Verwendung als Datendiode

Der aktivierte Schreibschutz der KOBRA Stick Datenträger bieten 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 auf den Datenträger geschrieben und anschließend der Schreibschutz auf dem Stick aktiviert. Im Folgenden wird der Datenträger an das höher eingestufte System angeschlossen und die benötigten Daten von dem KOBRA Stick auf das Hostsystem übertragen. Im Nachgang kann der Datenträger wieder normal im Ursprungssystem eingesetzt werden.

Eventuelle weitere Sicherheitsmaßnahmen wie z.B. Vierenscan sind weiterhin erforderlich. Optional kann vorher und hinterher ein schnelles sicheres Löschen des Datenträgers mittels Neugenerierung der Verschlüsselungsschlüssel durchgeführt werden.

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

9. Datensicherheit und Haftungsausschluss

Wir empfehlen, die auf den KOBRA Stick befindlichen Daten regelmäßig auf anderen Speichermedien zusätzlich zu sichern. Dies schützt Sie vor einem vollständigen Datenverlust. Die DIGITTRADE GmbH haftet nicht für den Verlust von Daten sowie dadurch entstehende Kosten und Schäden. Zudem trägt das genannte Unternehmen keine datenschutzrechtliche Verantwortlichkeit der gespeicherten Daten.

10. Sicheres Beenden nach Benutzung des KOBRA Sticks

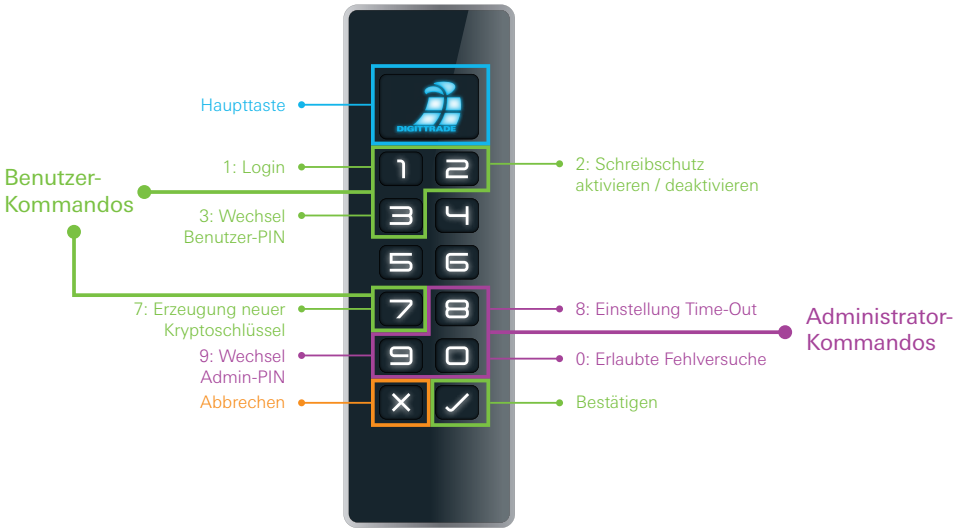
Aus Sicherheitsgründen ist eine logische oder physikalische Trennung des Sticks nach der Benutzung vom Wirtssystem durchzuführen. Dies empfiehlt sich vor allem bei Beendigung, kurzfristiger Unterbrechung sowie beim Verlassen des Arbeitsplatzes. In diesem Zusammenhang bietet die aktivierte Time-Out-Funktion bedeutende Unterstützung zum effektiven Datenschutz.

Zudem kann die schnelle Abmeldung 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 Stick 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 Stick vollständig abgeschlossen sind.

11. Menü-Übersicht, Kommandos und Werkseinstellungen



Benutzer	Taste 1 - Login Taste 2 - Schreibschutz Taste 3 - Wechsel Benutzer-PIN Taste 7 - Erzeugung neuer Kryptoschlüssel
Administrator	Taste 8 - Einstellung Time-Out Taste 9 - Wechsel Admin-PIN Taste 0 - Erlaubte Fehlversuche
Benutzer-PIN	1-2-3-4-5-6-7-8
Admin-PIN	8-7-6-5-4-3-2-1
PIN-Länge	8 Stellen (Einstellbar: 4 bis 16)
Fehlversuche Benutzer-PIN	8 Mal (Einstellbar: 1 bis 16)
Fehlversuche Admin-PIN	16 Mal (nicht veränderbar)
Time-Out	0 Minuten (Einstellbar: 0 bis 30)

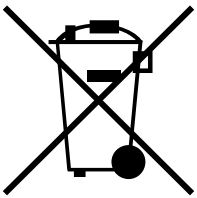
12. Lieferumfang

- KOBRA Stick (external encrypted USB-C Stick) Version 1.0
- 3 USB-Kabel (USB-C zu USB-C, USB-C zu USB-A, USB-C zu USB Micro-B)
- Verpackung

13. 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.



Ihre Notizen / Your Notes

DIGITTRADE GmbH
Ernst-Thälmann-Strasse 39
06179 Holleben Germany

Fon +49 / 3 45 / 2 31 73 53
Fax +49 / 3 45 / 6 13 86 97
Web www.digittrade.de
E-Mail beratung@digittrade.de