Verze 1.05
04.04.2019

KOBRA STICK

šifrovaný zabezpečený USB-C flash disk

pro obchodní a vládní použití

Uživatelský manuál

PŘEČTĚTE SI PROSÍM POZORNĚ TENTO NÁVOD A ŘIĎTE SE DŮLEŽITÝMI POKYNY.

NESPRÁVNÉ ZACHÁZENÍ MŮŽE ZPŮSOBIT POŠKOZENÍ KOBRA STICK
A ZTRÁTU ÚDAJŮ.

Digitální verzi manuálu si můžete stáhnout z www.digittrade.de v Download Center.

Verze produktu:	Kobra Stick (Šifrovaný USB-C Stick) Verze 1.0
Uživatelský manuál Verze:	1.05 (04.04.2019)

Obsah

1. O produktu KOBRA Stick

KOBRA Stick je šifrovaný USB-C Stick v robustním kovovém krytu. Umožňuje ukládání, úschovu a bezpečný přenos citlivých obchodních a soukromých údajů pro veřejné orgány a společnosti v souladu s předpisy o ochraně údajů. Byl vyvinut v souladu s „Technickými směrnicemi“ BSI, má kvalitní značku „IT Security made in Germany“ a díky svým bezpečnostním funkcím je dobrou volbou pro bezpečné ukládání dat na cestách.

Důvěrné údaje uložené na kartě KOBRA Stick jsou chráněny před neoprávněným přístupem, například v případě ztráty nebo odcizení nosiče dat nebo v případě virtuálních nebo fyzických útoků.

Chcete-li plně využít bezpečnostních funkcí karty KOBRA Stick, postupujte podle následujících kroků:

- Ujistěte se, že ve vašem hostitelském systému existuje dostatečná ochrana pro všechna data přístupná z chráněného úložiště KOBRA Stick
- Ujistěte se, že na KOBRA Stick nelze přenést žádný malware
- Po obdržení KOBRA Stick zkontrolujte, zda je dodávka kompletní a správně sestavená
- Po prvním přihlášení zkontrolujte funkce KOBRA Stick (kapitola 5).
- Změňte PIN uživatele (kapitola 5.2)
- Změňte administrátorský PIN, pokud jste administrátor odpovědný za správu KOBRA Stick (kapitola 5.3).
- Na KOBRA Stick vytvořte nové šifrovací klíče (nazývané také krypto klíče nebo KS) (kapitola 5.5).
- Uchovávejte ověřovací data (PIN uživatele a PIN správce) v utajení

Podrobný popis výše uvedených kroků je uveden v odkazovaných kapitolách této uživatelské příručky.

Sériové číslo a odpovídající QR kód najdete na zadní straně KOBRA Stick. Tyto informace a ID dodavatele (VID) a ID produktu (PID) lze číst přes rozhraní USB-C:

KOBRA Stick zaručuje bezpečí a utajení dat pomocí následujících bezpečnostních mechanismů:

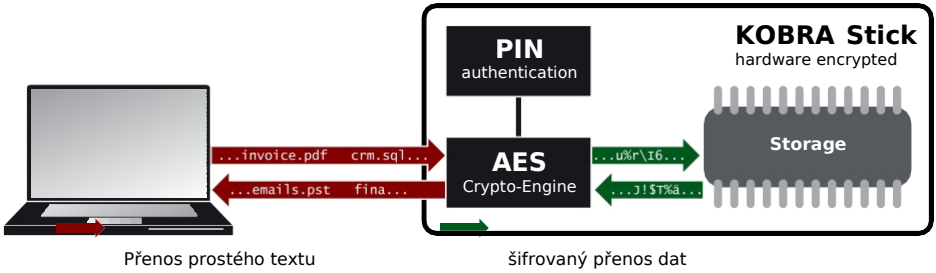
- Šifrování
- Kontrola přístupu
- Správa kryptografických klíčů

1.1 Šifrování

- 256bitové šifrování AES na plný disk v režimu XTS

Šifrovací modul integrovaný do bezpečnostního pouzdra provádí kompletní šifrování KOBRA Stick. Každý uložený bajt a každý zapsaný sektor na paměťovém zařízení je šifrován v režimu XTS pomocí dvou kryptografických klíčů podle 256bitového AES (Advanced Encryption Standard).

KOBRA Stick také šifruje dočasná data a oblasti, které jsou šifrovacím softwarem často ignorovány.



1.2 Kontrola přístupu

- Přístup je povolen zadáním uživatelského PIN.

KOBRA Stick automaticky vytvoří nový šifrovací klíč a resetuje PIN uživatele na výchozí nastavení, jakmile je překročen povolený počet nesprávných zadání PIN. Přístup k údajům na ní uloženým již potom není možný.

1.3 Správa kryptografických klíčů

Uživatel může kdykoli vygenerovat, změnit nebo zničit kryptografické klíče. Tento proces je nevratný. Po vygenerování nových kryptografických klíčů jsou staré kryptografické klíče, a tedy všechna data uložená na nosiči dat, nevratně zničeny. Proto by měly být jakékoli informace uložené na kartě nejprve uloženy na jiném šifrovaném datovém nosiči, pokud je to nutné.

Dva 256bitové šifrovací klíče pro šifrování a dešifrování dat jsou generovány hardwarovým generátorem náhodných čísel a uloženy v paměti. Pokud je PIN uživatele zadán správně, jsou přenášeny do šifrovacího modulu KOBRA Stick pro šifrování a dešifrování dat.

1.4 Přehled nejdůležitějších funkcí

- Hardwarové šifrování AES na celý disk v režimu XTS se dvěma 256bitovými kryptografickými klíči
- Ověření pomocí PIN uživatele
- Hardwarový šifrovací modul
- Šifrování dat všech uložených bajtů a psaných sektorů
- Nezávislá na operačním systému (podporuje všechny operační systémy, multimediální zařízení, smartphony a přístroje podporující datové nosiče USB)
- Integrovaná ochrana proti zápisu
- Nastavitelný počet nesprávných pokusů
- Kompatibilní s USB 3.0 a USB 2.0
- Žádné omezení rychlosti čtení a zápisu
- Robustní kovové pouzdro
- Funkce time-out a quick-out
- Ověřování před zavedením a bootovatelnost
- Interní zdroj napájení, který umožňuje ověření bez připojení k počítači nebo rozbočovači USB.

Fakultativní:

- USB VID, PID a sériová čísla lze definovat podle specifikace zákazníka
- Laserem vyryté informace o zákazníkovi na zadní straně KOBRA Stick

1.5 Výhody KOBRA Stick

- Soukromá a obchodní data jsou bezpečně chráněna před neoprávněným přístupem
- Snadná a bezpečná manipulace díky hardwarovému šifrování: připojení, přihlášení, použití
- Všechna data jsou okamžitě uložena jako šifrovaná
- Žádné ztráty výkonu

2. USB port a vstupní rozhraní

KOBRA Stick lze připojit k PC přes USB port.

Česky

Na přední straně KOBRA Stick je vstupní klávesnice s hlavním tlačítkem, dvě příkazové klávesy („×“ zrušit a „√“ potvrdit) a deset vstupních kláves (0 až 9). Připojení k PC je přes port USB-C 3.0.

3. Použití KOBRA Stick

Pro správné použití KOBRA Stick jsou nutné pouze dva kroky:

1) Připojte KOBRA Stick k PC
2) Zadejte PIN na KOBRA Stick

Tyto kroky je možné provést i v jiném pořadí.

Zdroj napájení potřebný pro fungování KOBRA Stick je obvykle poskytován přes USB port. Kromě toho má tato USB Stick integrovaný autonomní zdroj napájení, který umožňuje aktivaci před připojením k počítači a ověření před spuštěním s následným spuštěním počítače z KOBRA Stick.

Dokud není KOBRA Stick připojena k počítači nebo k externímu zdroji napájení (např. Napájení USB nebo rozbočovač USB), zůstane v režimu spánku a všechny klávesy jsou deaktivovány.

KOBRA Stick přechází do autentizačního režimu po stisknutí hlavního tlačítka na cca. 3 sekundy a ihned po připojení k počítači. Hlavní tlačítko bliká zeleně a ostatní tlačítka jsou aktivována. Nyní můžete zadat PIN uživatele pro odemčení KOBRA Stick.

Všechny vstupy a příkazy jsou potvrzeny klávesou „√“ nebo zrušeny klávesou „×“. Po každém stisknutí tlačítka „×“ se uživatel vrátí do čekacího režimu a může odtud začít znovu. Hlavní klávesu lze také použít k potvrzení vstupu namísto tlačítka „√“.

Stisknutím hlavního tlačítka v režimu čekání se KOBRA Stick přepne do režimu nabídky. V tomto režimu se hlavní tlačítko rozsvítí modře a všechny ostatní vstupní klávesy jsou bílé. Rozsvícené vstupní klávesy označují, že jsou aktivní a lze zadávat příslušné příkazy.

Po stisknutí klávesy „1“ následované klávesou „√“ se uživatel přepne zpět do režimu ověřování a může zařízení znovu odemknout zadáním uživatelského PIN. Po úspěšném ověření se hlavní tlačítko rozsvítí zeleně. Ostatní tlačítka jsou aktivována a přístup k datům je povolen.

Pokud je zadán nesprávný PIN, hlavní tlačítko bliká červeně podle toho, kolikrát byl zadán nesprávný PIN (ne ale vícekrát, než je maximální povolený počet neúspěšných pokusů). Poté se KOBRA Stick automaticky přepne zpět do režimu čekání. Proces ověřování lze od tohoto bodu opakovat, jak je popsáno výše. Pokusy o zadání PIN s menším počtem znaků, než jsou 4, se nepokládají za neúspěšné pokusy, a proto se nepočítají.

Po překročení povoleného počtu neúspěšných pokusů bliká hlavní tlačítko střídavě červeně a žlutě třikrát. KOBRA Stick se poté přepne do režimu ověřování. Současně KOBRA Stick automaticky odstraní staré krypto klíče, vygeneruje dva nové krypto klíče a nastaví PIN uživatele zpět na výchozí nastavení.

Po úspěšné autentizaci s novým uživatelským PINem, KOBRA Stick naformátuje úložiště dat. Během formátování hlavní tlačítko nepřetržitě bliká modře. Poté se hlavní tlačítko rozsvítí zeleně nebo fialově v závislosti na dříve vybraném nastavení ochrany proti zápisu. Ostatní tlačítka jsou deaktivována a je povolen přístup na KOBRA Stick. Oddíl Stick se zobrazí na ploše a lze jej použít.

Během tohoto procesu budou všechna dříve uložená data vymazána!

Pokud do 20 sekund od zahájení příkazového procesu nebudou provedeny žádné další vstupy, KOBRA Stick připojený k PC se automaticky přepne do režimu čekání. V režimu baterie se zařízení po 20 sekundách vrátí do režimu spánku.

Tato funkce se nevztahuje na ověřenou kartu KOBRA, pokud je již připojena k počítači nebo je připojena nejpozději do 20 sekund po úspěšné autentizaci. Čas možného automatického uzamčení ověřené karty KOBRA připojené k počítači se řídí nastavením časového limitu, pokud byl nastaven (kapitola 5.7).

Kromě klasických mechanismů „odhlášení“, jako je „bezpečné odstranění“ z hlavního panelu počítače a fyzické odpojení USB, má KOBRA Stick také funkci rychlého odhlášení pro rychlé odhlášení. Tato funkce se provádí dvojitým kliknutím na tlačítko „×“ během 2 sekund.

Poznámka:
Pro zajištění bezpečnosti vašich dat je nezbytné změnit výchozí PIN uživatele. V budoucnu byste měli PIN uživatele také pravidelně měnit. PIN uživatele musí být uchován v tajnosti.

4. Role a oprávnění

KOBRA Stick umožňuje správu rolí a oprávnění s ohledem na správu a provoz datového nosiče.

Uživatel zná uživatelský PIN. Tento PIN umožňuje uživateli změnit PIN, přihlásit se (autentizace), aktivovat nebo deaktivovat funkci ochrany proti zápisu nebo zničit aktuální šifrovací klíče a vygenerovat nové. PIN uživatele umožňuje autentizaci KOBRA Stick a umožňuje přístup k uloženým datům.

Správce zná administrátorský PIN. Může změnit PIN správce, definovat nastavení časového limitu a nastavit počet povolených neúspěšných pokusů. Správce není oprávněn nebo nemá přístup k datům uloženým na kartě KOBRA.

5. Režim nabídky: autentizace a správa

Ověřování a správa KOBRA Stick se provádí prostřednictvím režimu nabídky zadáním čísel a příkazů. Přepnutí do režimu nabídky se obvykle provádí z režimu čekání stisknutím hlavního tlačítka. V režimu nabídky se hlavní tlačítko rozsvítí modře a všechny ostatní vstupní klávesy bíle.

KOBRA Stick potřebuje ke spuštění příkazů připojení k počítači nebo jinému externímu zdroji napájení (např. Napájení USB nebo rozbočovač USB). Výjimky jsou během autentizace KOBRA Stick, aktivace nebo deaktivace ochrany proti zápisu a při generování nových krypto klíčů. Tyto procesy lze také provádět v režimu baterie.

V režimu nabídky by měly být všechny vstupy a příkazy potvrzovány klávesou „√“. Alternativně je lze také zrušit tlačítkem „×“. Po každém stisknutí tlačítka „×“ se hlavní tlačítko krátce rozsvítí oranžově a poté bíle. Poté se KOBRA Stick přepne do režimu čekání. Z této polohy lze postup opakovat.

Po spuštění funkce menu začne hlavní tlačítko blikat zeleně, když je třeba zadat uživatelský PIN. Pokud je vyžadován PIN správce, hlavní tlačítko bliká fialově. Všechny ostatní klávesy jsou v tuto chvíli aktivní. Pokud je zadání potvrzeno tlačítkem „√“, hlavní klíč se rozsvítí zeleně, pokud je PIN správný.

Pokud dojde k chybě, hlavní tlačítko krátce zabliká červeně a poté se rozsvítí bíle. Poté se KOBRA Stick přepne do režimu čekání. Z této polohy lze postup opakovat.

Pokud bylo při jedné z operací zadání PINu nesprávné, hlavní tlačítko jednou nebo několikrát blikne červeně podle počtu neúspěšných pokusů (ale ne vícekrát, než je maximální nastavený počet povolených neúspěšných pokusů). Poté se KOBRA Stick přepne do režimu čekání. Od tohoto bodu lze plánovaný proces restartovat.

Po každém úspěšném provedení příkazu se KOBRA Stick vrátí do čekacího režimu.

Jedinou výjimkou je úspěšná autentizace.

Poznámka:
U všech funkcí a nastavení, které vyžadují zadání PIN uživatele, hlavní tlačítko nepřetržitě bliká zeleně a všechna ostatní tlačítka zůstávají aktivní. Chcete-li však zadat PIN správce, hlavní tlačítko nepřetržitě bliká fialově.

5.1 Ověřování uživatelů

Pro povolení přístupu k datovému nosiči je vyžadováno ověření uživatele. Pro ověření:

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní tlačítka bíle).

2) Stiskněte tlačítka „1“ a poté „√“. Hlavní tlačítko bliká zeleně a všechna ostatní tlačítka zůstávají aktivní.

3) Zadejte PIN uživatele a potvrďte „√“. Po úspěšném ověření se hlavní klíč rozsvítí zeleně, ostatní tlačítka jsou deaktivována a přístup k datům je povolen.

5.2 Změna uživatelského PINu

Na KOBRA Stick je potřeba PIN uživatele pro provedení autentizace (přihlášení), aktivaci ochrany proti zápisu a deaktivaci, zničení nebo generování šifrovacích klíčů.

V továrním nastavení KOBRA Stick je PIN uživatele „1-2-3-4-5-6-7-8“. Stick bude mít také tento PIN v případě, že byl překročen maximální povolený počet neúspěšných pokusů o přihlášení a PIN uživatele byl resetován na tovární nastavení. PIN uživatele lze vytvořit kombinací 4–16 číslic.

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte „3“ a poté „√“. Hlavní tlačítko nepřetržitě bliká zeleně a ostatní tlačítka zůstávají aktivována.
3) Zadejte starý PIN uživatele a potvrďte „√“
4) Zadejte nový PIN uživatele a potvrďte „√“
5) Zadejte znovu nový PIN uživatele a potvrďte „√“

Pokud byla změna kódu PIN úspěšně dokončena, hlavní tlačítko krátce zabliká zeleně a nosič dat se přepne zpět do režimu čekání.

5.3 Změna kódu PIN správce

PIN správce (nazývaný také PIN zařízení) je potřebný pro nastavení funkce časového limitu a počtu neúspěšných pokusů o přihlášení, které jsou povoleny. Tento PIN může mít délku 4–16 znaků, je určen čistě pro správu a neumožňuje přístup k datům uloženým v zařízení.

V továrním nastavení KOBRA Stick je PIN správce „8-7-6-5-4-3-2-1“. Při zadávání PIN správce je povoleno 16 neúspěšných pokusů. Pokud je toto číslo překročeno, PIN správce je nevratně zablokován a výše uvedené funkce již nelze změnit. Uživatelské funkce lze však provozovat stále.

Změna kódu PIN správce:

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte „9“ a poté „√“. Hlavní tlačítko nepřetržitě bliká fialově a ostatní tlačítka zůstávají aktivována.
3) Zadejte starý PIN správce a potvrďte „√“
4) Zadejte nový PIN správce a potvrďte „√“
5) Zadejte znovu nový PIN správce a potvrďte „√“

Pokud byl PIN úspěšně změněn, hlavní tlačítko krátce zabliká zeleně a nosič dat se přepne zpět do režimu čekání.

5.4 Funkce ochrany proti zápisu

Aktivovaná ochrana proti zápisu vám nabízí další ochranu před viry a trojskými koni v momentě, kdy používáte KOBRA Stick na neznámém počítači. Zabraňuje také nechtěnému uložení citlivých informací z počítače nebo serveru na zařízení.

Už před autentizací může uživatel zkontrolovat, zda je ochrana proti zápisu aktivována stisknutím tlačítka „2“. Pokud se hlavní tlačítko rozsvítí fialově, je ochrana proti zápisu aktivována. Pokud se hlavní tlačítko rozsvítí zeleně, ochrana proti zápisu je deaktivována.

Aktivace nebo deaktivace ochrany proti zápisu:

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte tlačítko „2“. Pokud je aktivována ochrana proti zápisu, hlavní klíč se rozsvítí fialově, pokud je ochrana proti zápisu deaktivována, rozsvítí se zeleně.
3) Poté stiskněte klávesu „√“. Hlavní tlačítko bliká zeleně a všechna ostatní tlačítka zůstávají aktivní.
4) Poté zadejte uživatelský PIN a potvrďte „√“. Po úspěšném přepnutí hlavní tlačítko dvakrát zabliká zeleně nebo fialově a nosič dat se přepne zpět do režimu čekání.

5.5 Generování nových krypto klíčů

Když jsou generovány nové krypto klíče, staré krypto klíče jsou zničeny, a tak jsou všechna data uložená na nosiči dat nevratně vymazána. Proto by měla být všechna uložená data v případě potřeby dříve uložena na jiném schváleném nosiči dat.

Generování nebo změna šifrovacích klíčů:

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte klávesu „7“. Hlavní tlačítko se rozsvítí červeně, což znamená, že po provedení této funkce budou všechna data uložená na tyči nevratně vymazána.
3) Pokud chcete tuto funkci opravdu provést, stiskněte klávesu „√“. Hlavní tlačítko bliká zeleně a všechna ostatní tlačítka zůstávají aktivní.
4) Zadejte PIN uživatele a potvrďte „√“.

Po úspěšném vygenerování nebo změně krypto klíče hlavní tlačítko krátce zabliká zeleně a KOBRA Stick se přepne zpět do režimu čekání.

Během další autentizace bliká hlavní tlačítko modře, dokud není formátování dokončeno.

V závislosti na velikosti paměti může tento proces trvat několik minut. Hlavní tlačítko se poté rozsvítí zeleně nebo fialově v závislosti na tom, zda je ochrana proti zápisu aktivována (fialová) nebo deaktivována (zelená).

Přístup k dříve uloženým datům již není možný.

5.6 Odstranění krypto klíčů

Vymazání a / nebo zničení kryptografických klíčů lze provést dvěma způsoby.

a) Zničení generováním nových kryptografických klíčů.

Během tohoto procesu jsou staré šifrovací klíče nevratně přepsány. Přístup k dříve uloženým datům již není možný.

Tato metoda je rychlý způsob, jak zničit data uložená na jednotce, aniž byste je museli připojovat k počítači.

b) Zničení kryptografických klíčů překročením povoleného počtu neúspěšných pokusů o zadání uživatelského PIN.

Během tohoto procesu, kromě resetování uživatelského PIN zpět na tovární nastavení, jsou staré kryptografické klíče nevratně zničeny a generovány nové. V tomto případě již není možný přístup ke všem dříve uloženým datům.

5.7 Funkce time-out a quick-out

Správce může definovat, po kolika minutách se aktivovaná KOBRA Stick automaticky zamkne, pokud ve stanoveném čase neprobíhá čtení nebo zápis. Čas zámku lze zvolit mezi 1 a 30 minutami. Chcete-li zámek odstranit, stiskněte „0“.

Nastavení funkce časového limitu:

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte tlačítko „8“ a poté stiskněte „√“. Hlavní tlačítko bliká fialově a všechny ostatní klávesy zůstávají aktivní.
3) Zadejte PIN správce a potvrďte „√“.
4) Zadejte číslo od 0 do 30 a potvrďte „√“.

Pokud byl proces úspěšný, hlavní tlačítko krátce zabliká zeleně a KOBRA Stick se přepne zpět do režimu čekání.

Funkce quick-out umožňuje rychlé odhlášení. Provádí se dvojitým kliknutím na tlačítko „×“ během dvou sekund.

5.8 Povolený počet neúspěšných pokusů o zadání uživatelského PIN

Původní tovární nastavení umožňuje uživateli provést 8 neúspěšných pokusů o zadání uživatelského PIN. Správce může toto číslo změnit na 1 až 16 neúspěšných pokusů. Po překročení zadaného čísla KOBRA Stick automaticky odstraní staré krypto klíče, vygeneruje nové krypto klíče a resetuje PIN uživatele na tovární nastavení.

Všechna dostupná data jsou trvale zničena.

1) Ujistěte se, že jste v režimu nabídky. (Hlavní tlačítko se rozsvítí modře a ostatní klávesy bíle.)
2) Stiskněte tlačítko „8“ a poté stiskněte „√“. Hlavní tlačítko bliká fialově a všechny ostatní klávesy zůstávají aktivní.
3) Zadejte PIN správce a potvrďte „√“.
4) Zadejte číslo mezi 1 a 16 a potvrďte „√“.

Pokud byl proces úspěšný, hlavní tlačítko krátce bliká zeleně a KOBRA Stick se přepne zpět do režimu čekání.

Poznámka:
Snížení maximálního počtu povolených neúspěšných pokusů je okamžitě platné. Zvýšení počtu povolených pokusů vstoupí v platnost až po úspěšném zadání uživatelského PIN, a to i v případě, že je tento krok proveden poprvé po obnovení továrního nastavení.

6. Formátování

KOBRA Stick je standardně dodáván se systémem souborů FAT32. Tento formát lze číst a zapisovat téměř ve všech operačních systémech (Windows, Mac OS a Linux). Maximální velikost souboru v tomto formátu je až 4 GB, proto se hodí i pro větší objem dat.

Uživatel může KOBRA Stick přeformátovat podle scénáře aplikace. Pro uživatele Windows se doporučuje použít například NTFS. HFS+ je nejvýkonnější systém souborů pro Mac OS X a EXT4 lze použít pro Linux.

Programy rozšíření lze také použít k zápisu dat do souborových systémů, kde by to jinak nebylo možné. Samozřejmě je také možné KOBRA Stick naformátovat pomocí jakéhokoli jiného systému souborů. Toto neovlivní šifrování dat a již provedená nastavení.

Následující tabulka ukazuje kompatibilitu mezi operačními systémy a systémy souborů.

	NTFS	FAT32	HFS+	EXT4
Windows XP, Vista, 7, 8, 10	Č, Z	Č, Z	X	X
Mac OS X	Č	Č, Z	Č, Z	X
Linux	Č	Č, Z	X	Č, Z

Tlačítka: Č – čtení, Z – zápis, X – nekompatibilní

7. Aplikace

Funkce KOBRA Stick nabízejí širokou škálu možností pro bezpečné ukládání, archivaci a přenos osobních a citlivých dat. V následujícím textu najdete některé konkrétní scénáře.

7.1 Zvyšování stupně ochrany KOBRA Stick ve firemním prostředí

Firemní správce nebo správce veřejného úřadu může určit, jak restriktivní by měla KOBRA Stick být. Správce může definovat počet povolených neúspěšných pokusů a time-out uživatele.

Správce může pomocí nastavení časového limitu určit, po kolika minutách se aktivovaná KOBRA Stick automaticky zablokuje, pokud nedojde ke čtení ani zápisu.

Uživatel nemá povolení měnit tato nastavení. To není možné ani po překročení počtu povolených neúspěšných pokusů a obnovení uživatelského kódu PIN na tovární nastavení.

7.2 Bezpečný a nízkonákladový přenos dat

KOBRA Stick lze použít k přenosu citlivých dat. Za tímto účelem se nejprve vygenerují nové šifrovací klíče a změní se PIN uživatele. Počet povolených neúspěšných pokusů lze snížit na minimální hodnotu, např. 1 až 3 pokusy. Ochranu proti zápisu lze aktivovat také po uložení přenášených dat. Odesílatel pak pouze zašle KOBRA Stick poštou nebo kurýrem.

Odesílatel a příjemce musí také zajistit detekovatelnost jakéhokoli pokusu o manipulaci s KOBRA Stick, ke které mohlo dojít během převozu. Za tímto účelem se doporučuje použití zapečetěných bezpečnostních vaků. To platí také pro všechny ostatní možnosti přenosu dat pomocí KOBRA Stick.

Jakmile je datový nosič doručen, musí být zkontrolována jeho pravost. Za tímto účelem je sériové číslo datového nosiče také předáváno příjemci pomocí samostatné zabezpečené metody. Sériové číslo je umístěno jak na krytu, tak v informacích o zařízení, které lze přečíst pomocí připojení USB. Uživatelský PIN se nepředává příjemci, dokud se tyto informace neshodují.

Tento postup umožňuje zařízení KOBRA Stick doručit citlivá data příjemci bezpečně a nízkonákladově pomocí pojištěné zásilkové nebo kurýrní služby.

7.3 Použití menšího počtu datových nosičů s velkou zákaznickou základnou

Pro společnosti zpracovávající data, datová centra velkých společností nebo orgány veřejné správy, které si například neustále vyměňují data s mnoha příjemci dat, je KOBRA Stick ideální pro bezpečnou a nákladově efektivní přepravu dat, protože je vyžadováno pouze několik paměťových médií.

Je tomu tak proto, že pro každý přenos dat k jinému příjemci jsou znovu generovány krypto klíče KOBRA Stick a uživatelský PIN je znovu definován. Počet povolených neúspěšných pokusů lze pro tyto účely také snížit na

minimální hodnoty, např. 1 až 3. Data pak mohou být uložena na KOBRA Stick a zaslána poštou nebo kurýrem (viz kapitola 7.2).

Složité vymazání dat a opakované přepisování datového nosiče již není nutné, protože původní data jsou šifrována pomocí předchozích krypto klíčů a všechny staré krypto klíče jsou vymazány po vytvoření nových. Při vytváření nových krypto klíčů se paměť automaticky formátuje.

KOBRA Stick proto snižuje počet potřebných datových nosičů, protože personalizovaná KOBRA Stick není vyžadována pro každého příjemce dat.

Poznámka:
Je doporučeno odstranit data na datovém nosiči vytvořením nových krypto klíčů, protože to způsobuje menší zátěž na životnost paměti než opakované přepsání celé paměti.

7.4 Použití menšího počtu nosičů dat v terénu a u orgánů veřejné moci

Pro činnosti mimo společnost obdrží zaměstnanec KOBRA Stick, kterou dříve použil jiný zaměstnanec a která byla poté naformátována překročením povoleného počtu neúspěšných pokusů o zadání PIN.

Během tohoto procesu je PIN uživatele resetován na tovární nastavení, jsou odstraněny dva staré krypto klíče, generovány nové šifrovací klíče a formátován nosič dat. Všechny tyto procesy probíhají na pozadí poté, co zaměstnanec nebo správce překročil počet povolených neúspěšných pokusů.

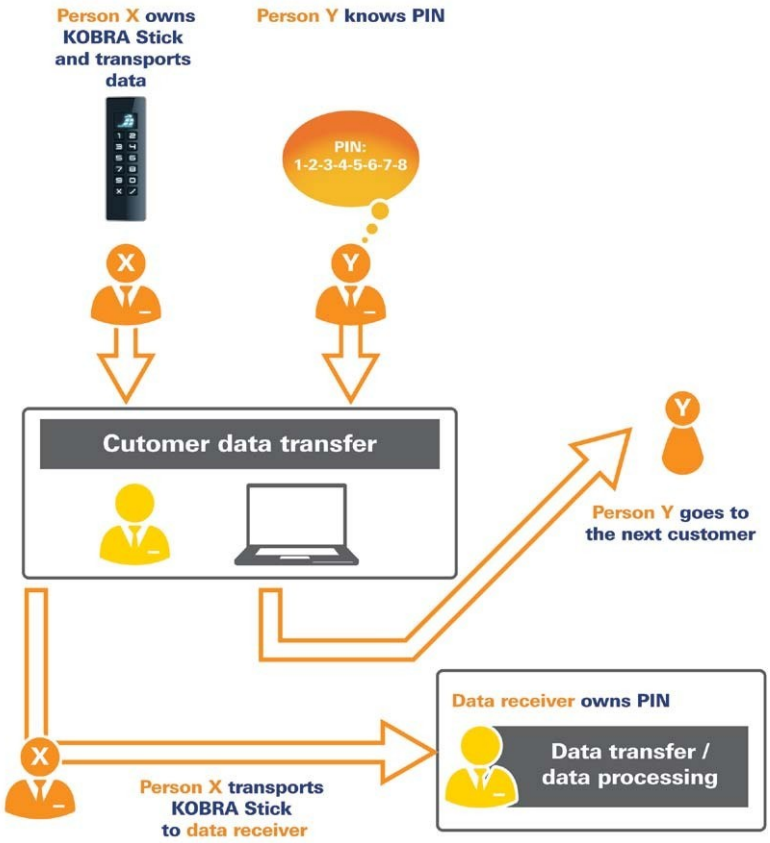
Nový zaměstnanec poté změní PIN uživatele a může na KOBRA Stick bezpečně ukládat svá data. Pokud musí být prezentace provedeny na externích počítačích nebo pokud mají uložené soubory zůstat nezměněny z jiných důvodů, lze také aktivovat ochranu proti zápisu.

Zaměstnanec po použití vrací KOBRA Stick. Před vrácením zničí aktuální šifrovací klíče a data uložená na KOBRA Stick vytvořením nových šifrovacích klíčů. (Kapitola 5.5)

KOBRA Stick je poté během několika minut připravena k použití dalším kolegou, jak je popsáno výše. To znamená, že pro každého zaměstnance není nutná samostatná KOBRA Stick a lze snížit počet datových nosičů potřebných ve společnosti.

7.5 Oddělení datového nosiče od autentizace

Přístup k údajům lze regulovat například spojením dvou konkrétních osob. Osoba X (např. Kurýr) má krypto klíč, osoba Y zná PIN uživatele. Oba lidé se tak spojí pouze, aby pomocí jeden druhého přenesli data a pak se znovu oddělili. Přitom osoby X a Y nemají individuální přístup k datům.



7.6 Použití jako šifrované bootovací zařízení

Integrovaný autonomní zdroj napájení umožňuje ověření KOBRA Stick před spuštěním počítače (ověření před spuštěním). Tato funkce umožňuje ukládat operační systémy v šifrované podobě na KOBRA Stick a poté je spouštět přímo z ní.
Operační systémy jako Windows To Go, Linux, ECOS Secure Linux a další, stejně jako požadovaná data, lze uložit na disk. Tato aplikace je vhodná pro stacionární i mobilní počítače. Musí být dodržena minimální požadovaná skladovací kapacita. Operační systém Windows To Go lze použít pouze na KOBRA Stick s kapacitou paměti 32 GB nebo vyšší a vyžaduje speciální konfiguraci zařízení, která musí být provedena před dodáním.

7.7 Použití v různých operačních systémech a chytrých telefonech

KOBRA Stick pracuje prostřednictvím hardwarového šifrování nezávisle na operačním systému a lze ji použít na téměř jakémkoli zařízení, které podporuje USB média.

Optimalizovaná spotřeba energie umožňuje použití KOBRA Stick pro výměnu dat pomocí smartphonu nebo tabletu.

7.8 Integrace stávajících softwarových řešení

Všechna stávající softwarová řešení v organizaci mohou být nadále používána k vylepšení bezpečnostních funkcí a metod použití. Integrovaná baterie umožňuje autentizaci před připojením zařízení k počítači nebo jinému externímu zdroji napájení (např. Napájení USB nebo rozbočovač USB). Tato funkce datového nosiče se nazývá pre-boot autentizace (kapitola 3).

KOBRA Stick lze také použít jako bootovací médium s nainstalovaným operačním systémem. Když je KOBRA Stick připojena k libovolnému počítači, spustí se operační systém nainstalovaný na jednotce. Když je KOBRA Stick odpojena od PC, zůstanou data, programy a dočasné soubory zašifrovány na KOBRA Stick a nejsou přístupné neoprávněným osobám.

7.9 Použití VID a PID k ochraně firemních dat

Volitelně lze přizpůsobit implementaci ID dodavatele (VID) a ID produktu (PID). Tato informace umožňuje, aby byla KOBRA Stick přiřazena různým oddělením a skupinám uživatelů. Mohou mít také různá oprávnění pro připojení USB v interní síti společnosti.

To umožňuje určit, které KOBRA Stick lze připojit ke kterým rozhraním USB ve společnosti. Tím lze zabránit připojení jiných „neautorizovaných“ datových nosičů USB. K ovládání portů USB v hostitelských systémech může být vyžadován další software.

7.10 Použití jako datová dioda

Aktivovaná ochrana proti zápisu datových nosičů KOBRA Stick poskytuje bezpečnou ochranu před nežádoucím tokem informací ze systémů s vyšším hodnocením do systémů s nižším hodnocením.

Aby se toho dosáhlo, jsou data ze zdrojového systému zapsána na datový nosič a poté je na tyči aktivována ochrana proti zápisu. Poté je datový nosič připojen k systému s vyšším hodnocením a požadovaná data jsou přenesena z KOBRA Stick do hostitelského systému. Poté může být datový nosič znovu normálně použit ve zdrojovém systému.

Stále jsou ale nutná jakákoli další bezpečnostní opatření, jako je například antivirová kontrola. Volitelně může být datový nosič vymazán rychle a bezpečně před a poté regenerací šifrovacích klíčů.

8. Technické specifikace

Přenosová rychlost:	USB 3.0 max. 5 GBit/s USB 2.0 max 480 MBit/s Skutečná rychlost zápisu a čtení, které lze dosáhnout, závisí na vybrané velikosti paměti, typu paměti, portu USB a hostitelském systému.
Šifrování:	Hardwarové šifrování 256 bitů AES, XTS režim, s 2 x 256-bit krypto klíči
Úložiště:	4 GB, 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Typ úložiště:	3D TLC, MLC a pSLC

9. Bezpečnost dat a vyloučení zodpovědnosti

Doporučujeme také pravidelně zálohovat data na KOBRA Stick na jiná paměťová média. To vás ochrání před úplnou ztrátou dat. Společnost DIGITTRADE GmbH neodpovídá za ztrátu dat ani za náklady a škody z tohoto vyplývající. Kromě toho výše uvedená společnost není odpovědná za uložená data s ohledem na zákon o ochraně dat.

10. Bezpečné ukončení po použití KOBRA Stick

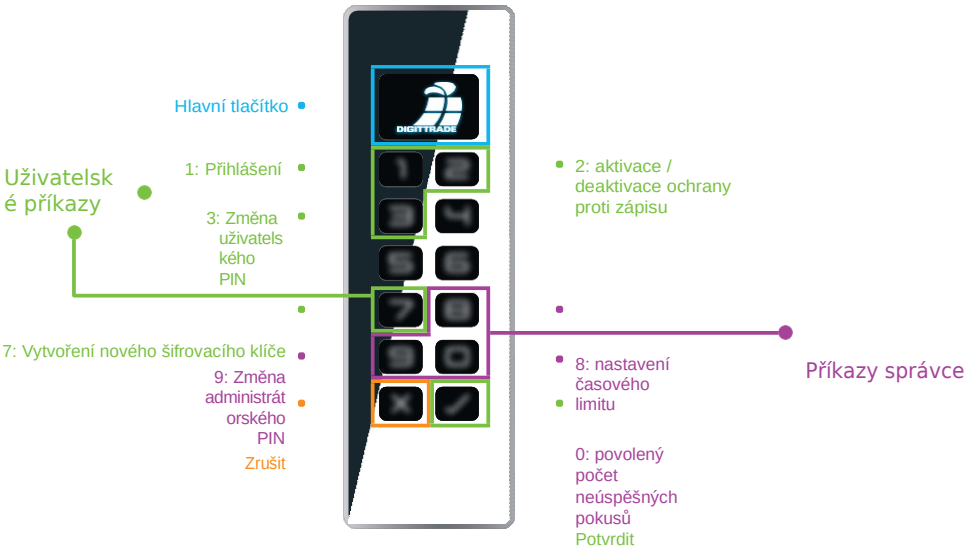
Z bezpečnostních důvodů musí být KOBRA Stick po použití virtuálně nebo fyzicky oddělena od hostitelského systému. To se doporučuje zejména v případě ukončení, krátkodobého přerušení nebo při opuštění pracoviště. Při aktivaci funkce time-out může pomoci zajistit účinnou ochranu dat.

Můžete se také rychle odhlásit dvojitým kliknutím na tlačítko X během 2 sekund (funkce rychlého odhlášení).

Aby bylo zajištěno bezpečné fyzické oddělení, musí být kabel USB zcela vyjmut z KOBRA Stick.

Poznámka:
Chcete-li zabránit ztrátě dat, před odpojením zkontrolujte, zda je přenos dat a přístup ke KOBRA Stick kompletní.

11. Přehled menu, příkazů a tovární nastavení



Uživatel	Tlačítko 1 – Přihlášení Tlačítko 2 – ochrana zápisu Tlačítko 3 – změna uživatelského PIN Tlačítko 7 – vytvoření nových šifrovacích klíčů

Administrátor	Tlačítko 8 – nastavení časového limitu Tlačítko 9 – změna administrátorského PIN Tlačítko 0 – povolený počet neúspěšných pokusů
Uživatelský PIN	1-2-3-4-5-6-7-8
Administrátorský PIN	8-7-6-5-4-3-2-1
Délka PIN	8 znaků (nastavitelné: 4–16)
Počet neúspěšných pokusů zadání uživatelského PIN	8 x (nastavitelné: 1–16)
Počet neúspěšných pokusů zadání administrátorského PIN	16 x (nelze nastavit)
Time-out	0 minut (nastavitelné: 0–30)

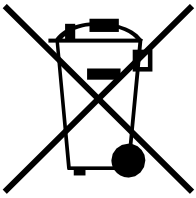
12. Obsah balení

- KOBRA Stick (externě šifrovaná karta USB-C) verze 1.0
- 3 kabely USB (USB-C na USB-C, USB-C na USB-A, USB-C na USB Micro-B)
- Obaly

13. Poznámka k ochraně životního prostředí

Podle směrnice ES nesmí být odpadní elektrická a elektronická zařízení likvidována jako komunální odpad. Abychom se vyhnuli šíření materiálů obsažených v tomto produktu ve vašem prostředí a šetřili přírodní zdroje, žádáme vás, abyste na konci životnosti vrátili tento produkt výhradně do sběrného místa ve vašem okolí.

Takto bude možné materiály ve vašem produktu znovu použít způsobem šetrným
k životnímu prostředí.



Poznámky

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