Dyski Kingston IronKey szyfrowane sprzętowo – rozwiązania z zakresu bezpieczeństwa

Zarządzanie bezpieczeństwem przenoszonych danych i ograniczanie ryzyka

Pracownicy przenoszący firmowe dane między miejscem pracy a domem z wykorzystaniem własnych urządzeń pamięci narażają firmę na ryzyko. Chroń poufne dane, standaryzując szyfrowaną sprzętowo pamięć flash USB IronKey™ firmy Kingston® lub zewnętrzny dysk SSD. Dzięki dostępności kilku modeli i wersji pojemności każda firma może wybrać pamięć idealnie dostosowaną do swoich potrzeb, niezależnie od tego, czy chce zapewnić bezpieczeństwo przenoszonych danych czy musi przestrzegać dyrektyw, przepisów, standardów lub międzynarodowych regulacji, takich jak RODO (GDPR) lub CCPA, dotyczących przechowywanych lub przesyłanych danych.

Wszystkie nośniki pamięci IronKey są objęte pięcioletnią gwarancją (z wyjątkiem urządzeń z serii IronKey Vault Privacy 80 ES i IronKey Keypad 200, które są objęte są trzyletnią gwarancją, oraz IronKey D500SM, które są objęte dwuletnią gwarancją), bezpłatną pomocą techniczną i cechują się legendarną niezawodnością marki Kingston. Wszystkie wymienione niżej urządzenia pamięci są w pełni szyfrowane sprzętowo, dzięki czemu spełniają najbardziej restrykcyjne wymogi bezpieczeństwa. Więcej informacji znajduje się na stronie **kingston.com/ironkey**





Opis polecanych produktów	IronKey Vault Privacy 50 Series	IronKey Vault Privacy 80 ES	IronKey Keypad 200 Series	IronKey D500S	IronKey S1000
Numer katalogowy	IKVP50/xxGB USB-A IKVP50C/xxGB USB-C®[1]	IKVP80ES/xxGB	IKKP200/xxGB	IKD500S/xxGB Serialized IKD500SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Poziom bezpieczeństwa	Klasa korporacyjna do standardowych zastosowań	Klasa korporacyjna do standardowych zastosowań	Klasa wojskowa	Klasa wojskowa/podwyższona	Klasa wojskowa/najlepszy produkt w swojej klasie
Pojemności[2]	8-512GB	480-7680GB	8-256GB USB-A 8-512GB USB-C	8-512GB	4-128GB
256-bitowe sprzętowe szyfrowanie AES	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
Pojemności[3]	FIPS 197	FIPS 197	FIPS 140-3 Poziom 3 (Oczekujące)	Certyfikat FIPS 140-3 Level 3 (w toku)	FIPS 140-2 Level 3
Obsługa wielu haseł (Multi-Password)	Administratora/użytkownika/jednorazowe	Administratora/użytkownika	Administratora/użytkownika	Administratora/użytkownika/jednorazowe	
Tryb wyrażenia hasłowego i maksymalna długość	√ Do 64	√ Do 64	√ Do 15	√ Do 128	√ Do 225
Funkcja podglądu hasła (symbol oka)	√	√			
Oprogramowanie sprzętowe podpisane cyfrowo	√	√	√	√	√
Ochrona przed złośliwym oprogramowaniem BadUSB	√	√	√	√	√
Ochrona hasła przed atakiem siłowym	√	√	√	√	√
Zgodność z przepisami TAA	√	√		√	√
Zgodność z RODO (GDPR)[9]	√	√	√	√	√
Dostęp tylko do odczytu	√	√	√	√	√
Ochrona przed nieuprawnionym manipulowaniem		Zabezpieczony mikroprocesor z certyfikatem CC EAL5+	√ Żywica epoksydowa	√ Wypełnienie żywicą	√ Wypełnienie żywicą
Dwie ukryte partycje				√	
Hasło Crypto-Erase	√			√	
Wodoodporność/pyłoszczelność[4]	IPx8		IP68	IP67, MIL-STD-810F	MIL-STD-810F
Opcje personalizacji[5]	√		Możliwość nadruku logo	√	
Wirtualna klawiatura	Windows® i macOS®	Ekran dotykowy		Windows® i macOS®	Tylko Windows®
Opcja zarządzania na poziomie korporacyjnym	Opcja zarządzania lokalnego dla małych i średnich firm			√ D500SM (SafeConsole)	√ S1000E (SafeConsole)
Niestandardowy identyfikator PID – zgodność z punktem końcowym/DLP	√			√	
Materiał obudowy	Anodyzowane aluminium	Cynk i tworzywo sztuczne	Anodyzowane aluminium	Cynk	Anodyzowane aluminium
Interfejs USB	USB 3.2 Gen 1	USB 3.2 Gen 1 (zewnętrzny dysk SSD)	USB 3.2 Gen 1	USB 3.2 Gen 1	USB 3.1 Gen 1
Obsługiwane systemy operacyjne					
Windows® 11, 10	√	√ Niezależność od Systemu Operacyjnego	√ Niezależność od Systemu Operacyjnego	√	√
macOS® 11.x – 14.x	√	√ Niezależność od Systemu Operacyjnego	√ Niezależność od Systemu Operacyjnego	√	√
Jądro systemu Linux[6] wer. 4.4+		√ Niezależność od Systemu Operacyjnego	√ Niezależność od Systemu Operacyjnego	√[7]	√[8]

1 USB Type-C® i USB-C® to zastrzezone znaki towarowe organizacji USB Implementers Forum.

2 Część podanej pojemności urządzenia z pamięcią flash służy do obsługi formatowania i innych funkcji, co powoduje, że nie jest wykorzystywana do przechowywania danych. Więcej informacji znajduje się w przewodniku po urządzeniach z pamięcią flash pod adresem kingston.com/flashguide.

3 Federal Information Processing Standards (FIPS) 140-2: „Wymagania dotyczące zabezpieczeń modułów kryptograficznych". Aby uzyskać więcej informacji, odwiedź stronę http://csrc.nist.gov/publications/PubsFIPS.html.

4 Certyfikat IEC 60529, potwierdzający wodoodporność urządzenia z założoną nasadką. Przed użyciem produkt musi być czysty i suchy.

5 Więcej informacji znajduje się na stronie kingston.com/ironkey.

6 Polecenia systemu Linux obsługują tylko procesory i386/x86_64 Intel i AMD – ograniczona liczba funkcji.

7 IKD500S i IKD500SM: Obsługa 32- i 64-bitowej wersji systemu Linux. Ograniczona liczba funkcji.

8 IKS1000B i IKS1000E: Obsługa systemu operacyjnego Linux w wersji 32-bitowej (oraz 64-bitowej, jeśli dokonano aktualizacji do wersji 6.xx). Ograniczona liczba funkcji.

9 Szyfrowanie może stanowić element rozwiązania zapewniającego zgodność z rozporządzeniem RODO, jednak samo w sobie nie gwarantuje tej zgodności.