Szyfrowane pamięci Kingston – 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, wprowadzając jako firmowy standard szyfrowane pamięci Kingston® DataTraveler® i IronKey™ lub zewnętrzne dyski 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 urządzenia pamięci DataTraveler i IronKey oferują legendarną niezawodność produktów firmy Kingston i są objęte pięcioletnią gwarancją (modele IronKey Keypad 200 i IronKey Vault Privacy 80 ES podlegają trzyletniej gwarancji) oraz bezpłatną pomocą techniczną. Wszystkie wymienione niżej urządzenia pamięci są w pełni szyfrowane, dzięki czemu są zgodne z najbardziej restrykcyjnymi wymogami bezpieczeństwa. Więcej informacji jest dostępnych na stronie **kingston.com/encryptedsecurity**






Opis polecanych produktów	IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	IronKey Keypad 200	DataTraveler 4000G2	IronKey D300S	IronKey S1000
Numer katalogowy	IKVP50/xxxGB	IKVP80ES/xxGB	IKKP200/xxGB	Opis polecanych produktów Numer katalogowy Poziom bezpieczeństwa	IKD300S/xxGB Standard IKD300SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Poziom bezpieczeństwa	Klasa korporacyjna do standardowych zastosowań	Małe/średnie firmy, standardowe zastosowania	Klasa wojskowa	Klasa wojskowa	Klasa wojskowa/ podwyższona	Klasa wojskowa/najlepszy produkt w swojej klasie
Pojemności[1]	8-256GB	480-1 920GB	8-128GB	8-128GB	8-128GB	4-128GB
256-bitowe sprzętowe szyfrowanie AES	XTS	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
Pojemności[2]	FIPS 197	FIPS 197	FIPS 140-3 Poziom 3 (Oczekujące)	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3
Obsługa wielu haseł (Multi-Password)	Administratora/użytkownika/ jednorazowe	Administratora/użytkownika	Administratora/użytkownika			
Tryb wyrażenia hasłowego i maksymalna długość	√ Do 64	√ Do 64				√ 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]	√	√	√	√	√	√
Montaż/COO	USA	USA	Chiny	USA	USA	USA
Dostęp tylko do odczytu	√	√	√	√	√	√
Ochrona przed nieuprawnionym manipulowaniem		Zabezpieczony mikroprocesor z certyfikatem CC EAL5+	√ Żywica epoksydowa	√ Żywica epoksydowa	√ Wypełnienie żywicą	√ Wypełnienie żywicą
Wodoodporność[3]	do ok. 1,2 m		do ok. 90 cm	do ok. 1,2 m	do ok. 1,2 m	do ok. 90 cm
Opcje personalizacji[4]	√		√	√	√	
Wirtualna klawiatura	Windows® i macOS	Ekran dotykowy			Tylko Windows®	Tylko Windows®
Opcja zarządzania na poziomie korporacyjnym	Opcja zarządzania lokalnego dla małych i średnich firm			Opcjonalne zarządzanie (SafeConsole)	√ D300SM (SafeConsole / IronKey EMS)[6]	√ S1000E (SafeConsole / IronKey EMS)[6]
Niestandardowy identyfikator PID – zgodność z punktem końcowym/DLP	√		√	√	√	√
Materiał obudowy	Anodyzowane aluminium	Cynk i tworzywo sztuczne	Anodyzowane aluminium	Stal nierdzewna z powłoką tytanową	Cynk	Anodyzowane aluminium
Interfejs USB	USB 3.2 Gen 1	USB 3.2 Gen 1 (zewnętrzny dysk SSD)	USB 3.2 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1
Obsługiwane systemy operacyjne						
Windows® 11, 10, 8.1	√	√ (niezależność od systemu operacyjnego)	√ (niezależność od systemu operacyjnego)	√	√	√
macOS® wer. 10.14.x – 12.x.x	√	√ (niezależność od systemu operacyjnego)	√ (niezależność od systemu operacyjnego)	√	√	√
Jądro systemu Linux5 wer. 4.4+		√ (niezależność od systemu operacyjnego)	√ (niezależność od systemu operacyjnego)		√[7,8]	√[8]

1 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.

2 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.

3 S1000: zgodność z MIL-STD-810F, IKKP200: zgodność z IP57, pozostałe urządzenia są zgodne ze standardem IEC 60529 IPX8. Należy używać wyłącznie czystego i suchego produktu.

4 Więcej informacji: kingston.com/usb/encrypted_security.

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

6 Kompatybilność na potrzeby obecnych klientów korzystających z rozwiązania IronKey EMS Cloud/ On-Prem.

7 DTVP30 / IKD300S: Obsługiwane 32- i 64-bitowe wersje systemu Linux. Ograniczona liczba funkcji. Więcej informacji: kingston.com/usb/encrypted_security.

8 IKD300SM i IKS1000B: obsługa 32- i 64-bitowych wersji systemu Linux / IKS1000E: obsługa 32-bitowych wersji systemu Linux. Ograniczona liczba funkcji.

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