# Pendrive 8GB D500S AES-256 FIPS 140-3 Lvl 3




| | |
|---|---|
| Cena brutto | **486,99 zł** |
| Cena netto | **395,93 zł** |
| Numer katalogowy | **SGKIN3G08IKD5S0** |
| Kod producenta | **IKD500S/8GB** |
| Kod EAN | **740617334869** |
| Uwaga | **CE+WEEE** |
| Gwarancja | **60 mc.** |
| Szyfrowanie danych | **Tak** |
| Pojemność pamięci flash | **8** |
| Prędkość zapisu | **190** |
| Prędkość odczytu | **260** |
| Interfejs (pamięci) | **USB 3.0/USB 3.1 gen 1/USB 3.2 gen 1** |
| Obsługiwane systemy operacyjne | **Linux** |
| Wymiary | **77,9 x 21,9 x 12,0 mm** |
| Kolor (wyliczeniowy) | **Czarny** |

## Opis produktu

**Pamięć z funkcją 256-bitowego szyfrowania sprzętowego XTS-AES i certyfikatem FIPS 140-3 Level 3 (w toku) we wzmocnionej cynkowej obudowie**

Pamięć flash USB Kingston IronKey D500S/SM jest wyposażona w zaawansowane zabezpieczenia spełniające wojskowe normy bezpieczeństwa, dzięki którym marka IronKey cieszy się największym zaufaniem w dziedzinie ochrony informacji niejawnych. Pamięć z certyfikatem FIPS 140-3 Level 3 (w toku), uwzględniającym nowe wymogi NIST dotyczące aktualizacji oprogramowania bezpiecznego mikroprocesora w celu zwiększenia bezpieczeństwa i ochrony przed atakami w zastosowaniach rządowych i wojskowych. Dane są szyfrowane i odszyfrowywane w pamięci D500S bez pozostawiania jakichkolwiek śladów w systemie hosta. Oprócz funkcji 256-bitowego szyfrowania sprzętowego XTS-AES pamięć ma wytrzymałą cynkową obudowę, która jest wodoodporna, pyłoszczelna, odporna na zgniecenie i wypełniona specjalną żywicą epoksydową w celu ochrony wewnętrznych komponentów przed atakami penetracyjnymi.

Dzięki wyposażeniu w najbardziej skuteczne zabezpieczenia spełniające wymogi wojskowych norm bezpieczeństwa, które zapewniają zgodność z przepisami i regulacjami dotyczącymi szyfrowania danych, takimi jak RODO (GDPR), HIPAA, SOX i CCPA, pamięć IronKey D500S jest niezbędnym elementem w stosowaniu najlepszych praktyk ochrony przed utratą danych. Pamięć D500S oferuje więcej funkcji niż jakiekolwiek inne urządzenie w swojej klasie, co czyni ją kompletnym rozwiązaniem do ochrony danych o wysokiej wartości.

Po uruchomieniu pamięć D500S przeprowadza autotesty i w przypadku wykrycia zbyt wysokiej temperatury lub napięcia samoczynnie się wyłącza. Dodatkowo pamięć D500S wykorzystuje podpisane cyfrowo oprogramowanie sprzętowe, dzięki czemu jest odporna na ataki z wykorzystaniem złośliwego oprogramowania BadUSB oraz metodą Brute Force. Stale włączona funkcja ochrony przed atakami metodą Brute Force zapobiega wielokrotnym próbom wprowadzenia hasła i po przekroczeniu ich dozwolonej liczby wymazuje zawartość pamięci metodą kryptograficzną.

Urządzenie oferuje także funkcję obsługi wielu haseł, która umożliwia uzyskanie dostępu do danych z wykorzystaniem hasła administratora, użytkownika lub jednorazowego hasła odzyskiwania. Administrator może zresetować hasło użytkownika oraz utworzyć jednorazowe hasło odzyskiwania, aby umożliwić dostęp użytkownika do danych w przypadku zapomnienia przez niego hasła.

Pamięć D500S może działać w trybie obsługi tradycyjnych haseł złożonych lub wyrażeń hasłowych2. Tryb tradycyjnego hasła złożonego umożliwia wprowadzenie hasła składającego się z 8-16 znaków przy użyciu 3 z 4 rodzajów znaków. Wyrażenie hasłowe może mieć długość od 10 do 128 znaków. Możliwość użycia zdania ze spacjami, listy słów, a nawet fragmentu tekstu piosenki pozwala łatwiej zapamiętać takie znaczące i jednocześnie bardzo bezpieczne hasło. FBI zaleca stosowanie wielowyrazowych, składających się z 15 lub więcej znaków wyrażeń hasłowych, ponieważ są trudniejsze do odgadnięcia i łatwiejsze do zapamiętania niż hasła złożone.

Pamięć D500S, jako pierwsza na rynku, oferuje funkcję dwóch ukrytych partycji, która pozwala administratorowi utworzyć dwie bezpieczne partycje o niestandardowym rozmiarze dla administratora i użytkownika. Powstały ten sposób ukryty magazyn plików może być w razie potrzeby wykorzystywany do udostępniania plików na partycji użytkownika. Podczas korzystania z nieznanych systemów lub udostępniania pamięci ukryte magazyny plików, do których można uzyskać dostęp tylko w określony sposób, zapewniają bezpieczeństwo danych, które pozostają niewidoczne.

Używając specjalnej sekwencji klawiszy, administrator może wprowadzić hasło Crypto-Erase, które powoduje bezpowrotne usunięcie danych z pamięci metodą kryptograficzną i jej zresetowanie, aby zapobiec nieuprawnionemu dostępowi.

W celu ograniczenia błędów podczas wprowadzaniu hasła na wszystkich ekranach dostępna jest opcja jego podglądu (symbol oka). Przydatna jest także funkcja wirtualnej klawiatury w języku angielskim, która chroni hasła przed oprogramowaniem rejestrującym naciśnięcia klawiszy (keylogger) lub zawartość ekranu (screenlogger).

Pamięć D500S obsługuje również dwa poziomy trybów tylko do odczytu (ochrony przed zapisem). Zarówno administrator, jak i użytkownik mogą ustawić tryb tylko do odczytu w danej sesji, aby w nieznanych systemach chronić pamięć przed złośliwym oprogramowaniem. Administrator może także włączyć ogólny tryb tylko do odczytu, który pozostanie aktywny do czasu zresetowania pamięci.

Oprócz bezpieczeństwa zapewnia on także dużą szybkość odczytu danych. Pamięć ma unikalny 8-cyfrowy numer seryjny zapisany w urządzeniu, wygrawerowany na obudowie oraz dostępny w postaci kodu kreskowego, który można zeskanować w celu rejestracji lub na potrzeby audytu.

Pamięć D500S oferuje wiele opcji personalizacji, jest zgodna z wymogami TAA/CMMC i montowana w USA.

**Wersja przystosowana do zarządzania**

Pamięć Kingston IronKey D500SM (M = Managed (pamięć zarządzana)) wymaga użycia oprogramowania SafeConsole5. Pozwala ono na scentralizowane zarządzanie dostępem i sposobem użytkowania wielu urządzeń pamięci w dużej firmie lub instytucji rządowej. Opcjonalna wersja pamięci przystosowanej do zarządzana jest również oferowana z możliwością personalizacji.