



**SECUREDIVES**



## **SDSRDD**

# **SECURE DATA STORAGE - REMOTE DATA DESTRUCTION**

**SDSRDD to zewnętrzne/wewnętrzne 2,5-calowe samoszyfrujące dyski SSD, które zostały opracowane specjalnie dla potrzeb zapewnienia bezpieczeństwa danych rządów i organizacji komercyjnych.**

**Dysk SDSRDD zabezpiecza przed:**

- **Bezpośrednim zagrożeniem stwarzanym przez keyloggery sprzętowe i programowe (rejestrujące informacje o klawiszach naciskanych przez użytkownika komputera) – uwierzytelnianie za pomocą Tokenu a nie hasła wprowadzanego za pośrednictwem komputera**
- **Przypadkową utratą lub kradzieżą – zdalne niszczenie danych za pośrednictwem sieci GSM**
- **Technikami odzyskiwania danych – poprzez fizyczne zniszczenie układów NAND flash**
- **Uzyskaniem dostępu do Dysku przy użyciu siły – obudowa zabezpieczona przed ingerencją uruchamiającą procedurę natychmiastowego fizycznego zniszczenia**
- **Usunięciem z komputera – monitorowanie obecności wtyczki SATAII**

**Jednolite podejście do bezpieczeństwa danych**

[www.securedrives.co.uk](http://www.securedrives.co.uk)

**SecureDrives – Security by design**



SECUREDRIVES

## Wewnętrzny/Zewnętrzny Dysk Twardy

### Pojemności

- Dyski SSD 64GB i 128GB

### Wymiary

- 100,5mm x 69,85mm x 9,5mm

### Interfejsy danych

- Micro USB 3.0 (Zewnętrzny)
- SATAII (Wewnętrzny)

### Zabezpieczenia

- Uwierzytelnianie niezależne od komputera
- Uwierzytelnianie dwuskładnikowe z użyciem Tokenu
- Sprzętowe szyfrowanie całego dysku
- Fizyczne zniszczenie układów NAND flash
- Niszczenie danych na żądanie za pośrednictwem sieci GSM
- Monitorowanie złącza SATAII
- Wspomaganie bateryjne

### Szyfrowanie

- 256-bitowy tryb wiązania bloków zaszyfrowanych AES
- Standard przetwarzania informacji FIPS 140-2 – poziom 3
- Funkcja kasowania/nadpisania klucza szyfrowania
- Generowanie klucza szyfrowania z ciągiem zaburzającym (tzw. solą) wprowadzanym przez użytkownika
- Komunikacja pomiędzy Tokenem a Dyskiem za pomocą modułu TPM

### Niezależny od platformy

- Nie wymaga oprogramowania
- Niezależny od systemu operacyjnego
- Nie wymaga aktualizacji ani poprawek

### Bezdotykowy zestaw do wykonywania kopii zapasowych (Wyposażenie dodatkowe)

- Automatyczne tworzenie kopii zapasowych z Dysku na Dysk w postaci zaszyfrowanej
- Zapewnia spójność bezpieczeństwa danych
- Nie wymaga oprogramowania ani komputera

Setting a new bench mark for  
security of Data-at-Rest

- Uwierzytelnianie za pomocą Tokenu – zabezpiecza przed keyloggerami. Pozwala na bezpiecznie przenoszenie danych pomiędzy lokalizacjami, w których znajdują się Tokeny
- Uwierzytelnianie dwuskładnikowe z użyciem Tokenu i kodu PIN – kod PIN może zawierać do 22 znaków
- Próby wprowadzenia kodu PIN – liczba prób wprowadzenia kodu PIN jest ograniczona zanim dysk zainicjuje procedurę fizycznego samozniszczenia. Funkcja zabezpiecza przed zbyt dużą liczbą prób wprowadzenia kodu PIN w celu uzyskania nieupoważnionego dostępu
- Sprzętowe szyfrowanie całego dysku za pomocą silnika szyfrującego FIPS 140-2 poziom 3 – zapewnia szybki transfer danych
- Generowanie klucza szyfrowania przez generator liczb losowych TPM, do których następnie za pomocą interfejsu Tokenu wprowadzany jest ciąg zaburzający. W linii Dysków SDS nie stosuje się automatycznego generowania kluczy szyfrowania używanego przez silniki kryptograficzne z powodu przewidywalności kluczy
- Dwa interfejsy danych – elastyczne opcje podłączenia pozwalające na pracę wewnętrzną i zewnętrzną
- Oprogramowanie Windows nie jest stosowane w celu zarządzania Dyskiem z powodu słabości zabezpieczeń. Brak poprawek oprogramowania oraz oprogramowania układowego (firmware)
- Natychmiastowe fizyczne zniszczenie układów przechowywania NAND flash – zapobiega zastosowaniu technik odzyskania danych z Dysku
- Zdalne polecenie zniszczenia za pośrednictwem sieci GSM przez SMS. Oferowana przez sieć GSM opcja wartości granicznej detekcji zaniku sygnału zapobiega celowemu zagłuszeniu sygnału GSM w celu ominięcia zabezpieczeń
- Monitorowanie interfejsu SATAII – zabezpiecza przed usunięciem Dysku z komputera umożliwiającym skopiowanie danych z Dysku. W momencie usunięcia interfejsu z Dysku ulega on samozniszczeniu
- Wspomaganie bateryjne – zabezpiecza przed utratą zasilania sieciowego umożliwiającą obejście zabezpieczeń. Opcja monitorowania poziomu naładowania baterii zabezpiecza przed wyczerpaniem baterii umożliwiającym obejście zabezpieczeń
- Obudowa zabezpieczona przed ingerencją – uruchamia procedurę nadpisania klucza szyfrowania przy próbie uzyskania dostępu do obudowy przy użyciu siły