SECUREDRIVES

SDSDSP

SECURE DATA STORAGE DATA SECURITY PROTOCOL DRIVE

The SDSDSP is an external / internal 2.5" Self-Encrypting solid-state disk drive which has been specifically developed for use with the Data Security Protocol Switch (DSPS) to meet and exceed the data security needs of government and commercial organisations.

The SDSDSP safeguards against:

- **The direct threat of keyloggers hardware & software** – via Token authentication and not PC based password authentication
- **Data recovery techniques** – via physical destruction of the NAND-Flash SIMs
- **Brute force access to Drive** – via anti-tamper case activating instant physical destruction
- **Removal from PC** – via monitoring for the presence of the SATAII connector
- **Theft or removal from a specific location** – via monitoring for the presence of the DSPS

A unified approach to data security

SECUREDRIVES

Internal / External Hard Drive

Capacities
- 64GB, 128GB solid-state drive

Dimensions
- 100.5mm x 69.85mm x 9.5mm

Data Interfaces
- Micro USB 3.0 (External)
- SATAII (Internal)

Security Features
- PC Independent authentication
- 2 Form factor Token authentication
- Full disk hardware encryption
- Physical destruction of NAND-Flash SIMs
- SATAII monitoring
- Battery backup

Encryption
- 256-bit AES Cipher-block chaining
- FIPS 140-2 - level 3
- Encryption key erase /flip function
- Encryption key generation salted via user input
- TPM Token to Drive communication
- TPM Drive to DSPS communication

Non Platform dependent
- No software required
- O/S independent
- No upgrading or patching

Zero Touch Backup Pod (Accessory)
- Automatic Drive to Drive backup in encrypted form
- Ensures data security integrity
- No software or computer required

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

- Token-based authentication – safeguards against keyloggers
- 2 Form factor Token & PIN code authentication – PIN code up to 22 characters
- PIN code retries – limited number of PIN code retries before Drive initiates physical self-destruction. This safeguards against extended PIN retries in an attempt to gain unauthorised data access
- Hardware level full disk encryption via FIPS 140-2 level 3 cryptographic engine – ensures high speed data transfer rates
- Encryption key generation from TPM random number generator which is further salted via user input from Token interface. The automatic encryption key generation facility of cryptographic engines is not used in the SDS range of Drives
- Dual data interfaces – flexible deployment options allowing for internal and external use
- No Windows-based software to manage Drive due to security weaknesses. No software or firmware patches
- Instant physical destruction of storage NAND-Flash SIMs – prevents data recovery techniques being applied to the Drive
- Signal Proximity (SP) – SDSDSP drive will initiate automatic self-destruction in the event of signal lose of the Data Security Protocol Switch (DSPS). Either by proximity (being taken away from the DSPS) or signal jamming (3rd party attempt to block data destruction command)
- SATAII interface monitoring – safeguards against Drive removal from PC to stream data off the Drive. Drive self-destructs on removal of interface
- Battery backup – safeguards from mains power loss circumventing security. Battery level monitoring option safeguards against running down of battery to circumvent security
- Anti-tamper case – initiates physical data destruction on brute force entry to case