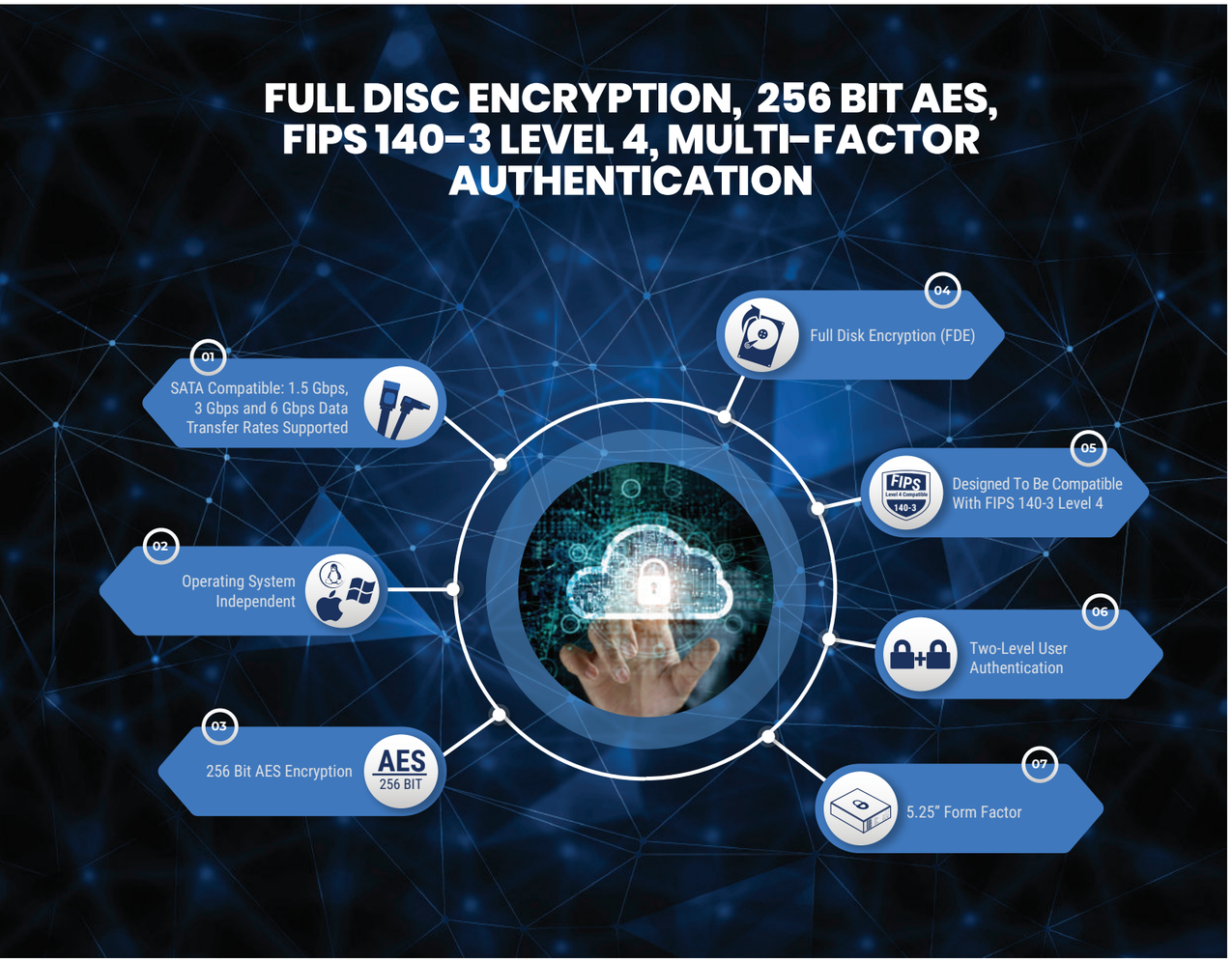
HOW IT WORKS

DISKRIPTO® is installed on a free 5.25" slot on your machine. Connect first SATA cable between DISKRIPTO® and the Main Board, and second data cable between Hard Drive and DISKRIPTO®. Plug in the USB Key Token and use key pad to enter the Pin Code while booting the machine to authenticate and enable the device. USB Key Token must be plugged in all times during normal operation.



Dimensions WxDXH	• 146 x 214 x 42 mm	Regulatory Compliance	• Designed for FIPS 140-3 Level 4
Power Consumption	• 15 watts (max)	Vibration Certifcations	• EN 68/ IEC 60068-2-6/27
Weight	• 1,090 g	Operating Temperature	• 0°C to +55°C
EMC/EMI Certifications	• EN 55024, EN 55022	Storage Temperature	• -10°C to +70°C

Teknopark İstanbul 1. Blok Kat 2, Pendik, İstanbul / TURKEY
T : +90 850 480 77 44 | +90 216 290 52 86

www.ctech.com.tr

CYBER SECURITY

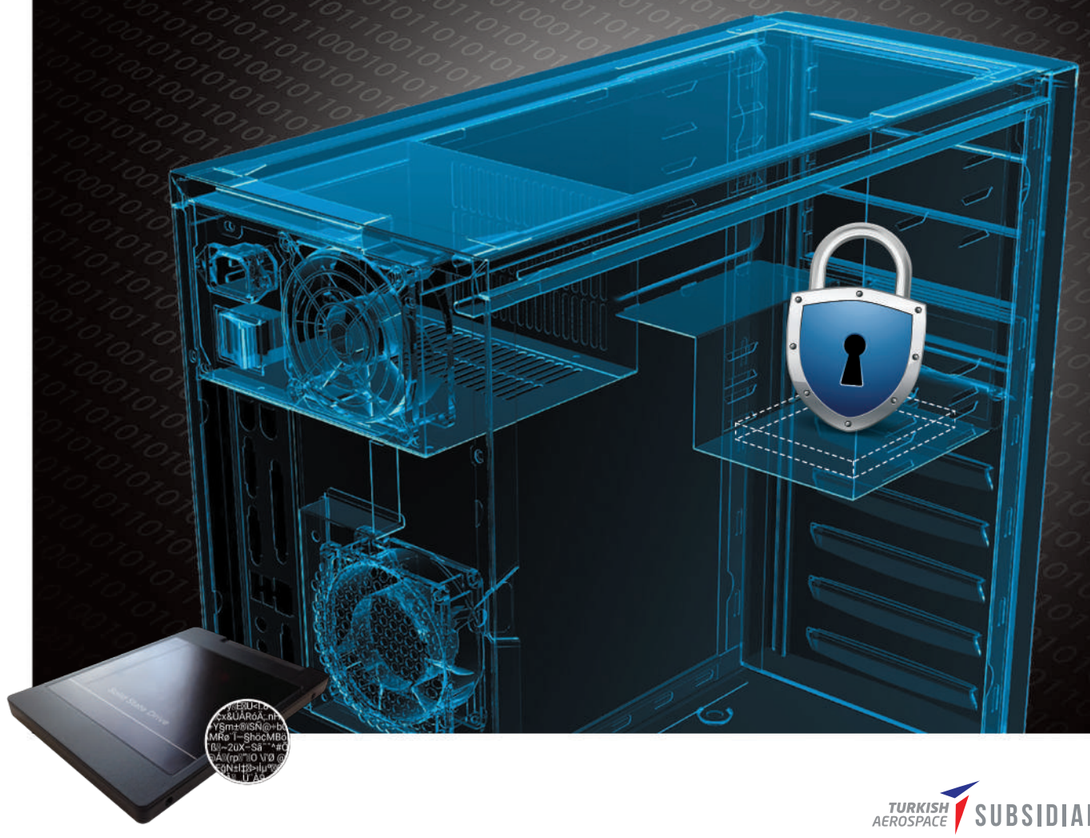
DISKRIPTO®

HIGH SECURITY DATA PROTECTION SOLUTION FOR PCS

FOR YOUR EYES ONLY

OVERVIEW

DISKRIPTO® is an hardware-based Full Disk Encryption device that is designed to protect Data-at-Rest by encrypting content and securely sharing sensitive information, and can be used for several data categories including protection of Financial Data, Private Individual Data, Military Data, Government Data to meet regulatory and contractual requirements, and comply with audits.

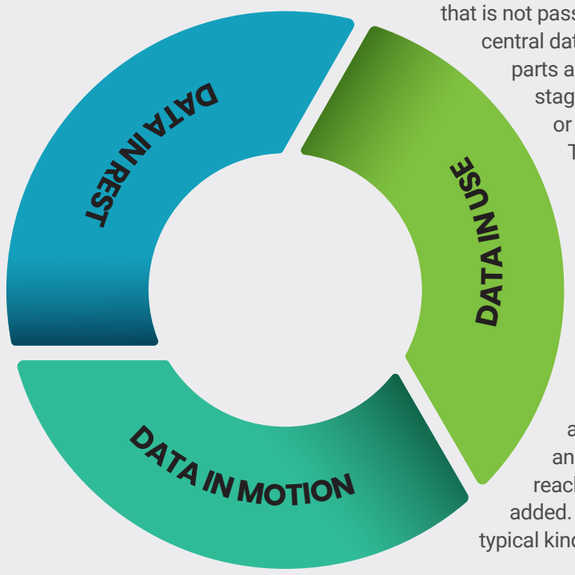


TURKISH AEROSPACE SUBSIDIARY

DATA CLASSIFICATION

Data that need to be protected can be classified into several categories such as Financial Data, Personal Health Data, Private Individual Data, Military Data, Government Data and Confidential or Sensitive Business Data. Besides, there are a lot of International (Basel III, Euro-Sox, 95/46/EC EU Directive) and national (US: Pci Dss, Glba, Sox, Hipaa, FDA 21 CFR; JP: Fiea, Pipl; DE: Bdsg; CA: Pipeda; UK: Dpa) regulations mandating the protection of data and placing significant requirements on government or private sector institutions, for encrypting content and securely sharing sensitive information.

DATA PROTECTION



Data can be protected at three different states. Data-in-Use refers to data that is not passively stored at a stable destination, such as a central data warehouse, but is being processed at different parts and levels of IT architecture. Data in use may be in the stage of being generated, amended or updated, erased, or viewed through various interface endpoints. Typically, these interface endpoints are computer memory, processor cache or registers. Data-in-Transit is the term used for data on the move. The transfer of the data may be on a public and unsecure network such as the Internet, or may be on private networks such as corporate Local Area Networks (LANs). It is data that is exiting the network via email, web or other secure or unsecure Internet protocols. On the other hand Data-at-Rest refers to computer data in persistent storage such as hard drives, USB sticks, backup tape and disks, and even storage area networks (SAN). When data reaches a storage destination, new layers of security can added. Encryption and password protection is the most typical kind of security procedure that is applied to data-at-rest.

FULL DISK ENCRYPTION

For maximum data protection, all information on the persistent storage, that is hard drive in our case, including the operating system, user data, temporary files and deleted files need to be encrypted. This process is called Full Disk Encryption (FDE). During system initialization the user needs to present an encryption key.

After successful authorization and authentication the system boots up and the standard operation begins. As data is fetched from the disk, it is decrypted simultaneously, and handled by the appropriate process. Any data that is stored on the disk is also encrypted simultaneously. Without the key used in encryption, all information on the hard drive is undecipherable to anyone including hackers and thieves.

PURE HARDWARE BASED

DISKRIPTO®, being a hardware-based Full Disk Encryption solution, has many advantages over software-based solutions. FDE leads to some processor (and therefore power) overhead to perform the simultaneous data encryption and decryption, and this is dependent on the amount of disk I/O that individual processes request. This overhead can reach up to 20% percent for data-intensive applications, such as video processing. However, with DISKRIPTO®, which is a pure hardware-based real-time encryption & decryption solution, zero performance degradation is ensured.

It does not need any software setup, upgrades or fix packs. It is very easy to install and maintain DISKRIPTO® for data protection, and it lowers the total cost of ownership. DISKRIPTO® is totally user transparent, therefore unlike any software-based solution, it is not subject to any software-based threats such as viruses and trojans.Since DISKRIPTO® is a pure hardware-based device, it is platform independent, and provides great flexibility under different deployment and operation scenarios. DISKRIPTO® offers perfect data protection by encrypting every single sector of a hard disk including the master boot record. DISKRIPTO® is a SATA3 compatible device with max data transfer rate of 600 MB/s.

AUTHENTICATION

Multi-factor authentication requires the presentation of two or more of the three independent authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). DISKRIPTO® supports two-factor authentication, by combining a secret numeric password, PIN, used in pre-boot authentication and a USB authentication token used in real-time encryption and decryption process. If the USB authentication token is removed during a normal operation, the user will hear an audio buzzer warning, and will be given a chance to reinsert the token in a very short grace time, before the system inhibits any transaction with the hard disk.

LOADING MANAGEMENT SYSTEM

DISKRIPTO® is bundled with a carefully designed Loading Management System (LMS) that handles key initialization, device activation, maintenance, device revocation, data backup and data recovery operations. The system depends on True Random Generators for System and User Encryption Key creation. Loading any of the secrets to either hardware unit or the USB authentication token can only be performed through the application of the LMS, which should be placed in the physically secure Trust Centre areas. Security clearance and physical security are required to access the Trust Centre, where the LMS is located. Backup of all system secrets is performed in an encrypted manner.

FIPS-140 COMPLIANCE

DISKRIPTO® components and functionality, including the employed algorithms, are designed to be compatible with FIPS-140.3 Security Level 4. The unit is powered from the host system's power supply with backup battery power for tamper monitoring when the host system is switched off. The system detects and prevents any intrusion/breach of crypto security. AES-256, the encryption algorithm used by DISKRIPTO®, is a proven, trusted and validated algorithm chosen by the National Institute of Standards and Technology (NIST) and is a FIPS-approved symmetric encryption algorithm that is used for protecting sensitive information.