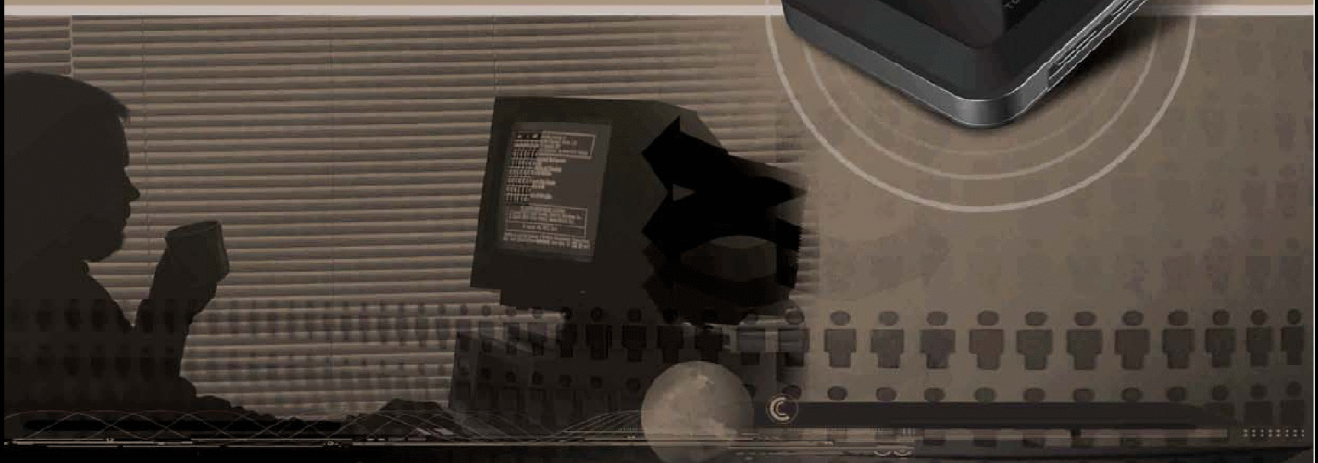




Your data stays yours!

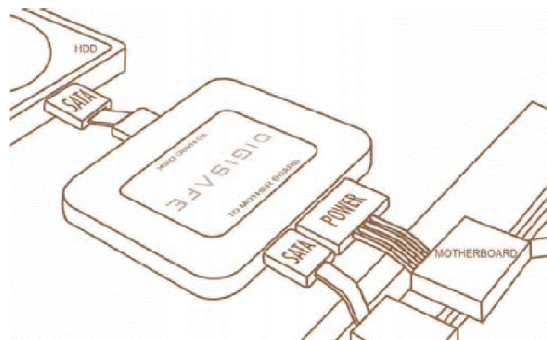
DigiSAFE DeskCrypt is a hardware-based encryption device that secures data in a SATA hard disk drive against hackers and information-thieves. Uniquely designed as a bump-in-the-wire device on the SATA cable, the DeskCrypt requires no mounting and simply plugs in-between the SATA connector on the motherboard and the hard disk drive. It operates transparently and encrypts all data written onto the hard disk without any loss in disk performance.

DeskCrypt does not require any additional software drivers or applications to be installed and is fully operating system independent. Once deployed, users would be assured that all the data on their hard disks is fully protected from unauthorized access in the event that the hard disk is lost or stolen.



Real-time Hardware Encryption

DeskCrypt is a hardware-based cryptographic module that encrypts every single byte of data that is written into the hard disk in real-time without any loss in disk performance.



FEATURES	BENEFITS
Real-time hardware-based encryption and decryption	Zero performance degradation
Pure hardware solution	Total transparency to user. Not vulnerable to virus/trojan unlike software-based products
Every single hard disk sector is encrypted	Complete data protection
Platform and operating system independent	Greater operational options and deployment flexibility
No need for software installation, upgrades, or patches	Ease of installation and maintenance, lower total cost of ownership
Pre-boot authentication	Strong hard disk access control
Supports authentication using USB cryptographic token	Rigorous two-factor authentication

Regulatory Compliance

DeskCrypt employs data encryption and pre-boot authentication, allowing organizations to better protect and control access to their corporate and customer data, thus aiding compliance with regulations such as HIPAA, GLB Act, Sarbanes-Oxley Act, EU Data Protection Directive, FISMA and Japan's Personal Information Protection Act.

Pre-boot Authentication

DeskCrypt authenticates the user every time the PC powers on or resumes from hibernation. The PC will only boot into the Operating System on the attached hard disk drive upon successful user authentication. DeskCrypt offers two authentication modes:

Single-Factor Authentication:

In this mode of authentication, the user is prompted for a Password at the pre-boot stage after power-on. DeskCrypt grants access to the user if the correct password is presented.

Two-Factor Authentication:

In this mode, the user is prompted for the KeyCrypt USB cryptographic token (something you have), as well as the password associated with the token (something you know). DeskCrypt grants access only if the correct token and password is presented.

SPECIFICATIONS	
Data transfer rate	• Up to 150MB/s
Interface	• Serial ATA (SATA)
Power	• 5V 400mA
Physical	• Dimensions: 82 mm (L) x 69 mm (W) x 12 mm (H)
Encryption	• NIST ¹ certified AES hardware cipher engine • Supported key strengths: • 128/256 bits
Pre-boot Authentication	• Password • Two-factor authentication with DigiSAFE KeyCrypt
Key Management	• User-configurable encryption key • Hard disk decommissioning
Hard disk drive configuration	• Supports hard disk on primary master
Certifications and Standards	• Supports SATA I/II compliant hard disk drive • Designed to meet FIPS 140-2 Level 2 • FCC, CE tested
Operating Systems	• Operating systems independent • Tested with Windows® 2000, XP, Vista, and Linux
OPTIONAL	
DigiSAFE KeyCrypt	• USB cryptographic token for two-factor authentication

¹NIST – The National Institute of Standards and Technology of the United States of America

Authorized Reseller:

Sold Exclusively in the UK & France by:

iStorage Ltd

Tel: +44 (0) 20 8997 7013 - info@istorage-uk.com - www.istorage-uk.com

