



Simply Secure!

Your notebook data with DigiSAFE DiskCrypt, the encrypted hard disk.

DigiSAFE DiskCrypt is a secure storage device that consists of a hard disk drive with a hardware-based cryptographic module that encrypts all data that is written into the hard disk to provide total data protection. DiskCrypt encrypts every single sector transparently in hardware without any loss in disk performance.

DiskCrypt is a drop-in and easy-to-install replacement for standard 2.5" notebook hard disk drives. DiskCrypt does not require any software drivers or applications to be installed and is operating system independent. After installation, users use their notebooks as usual with the assurance that their data is fully protected should their notebooks be stolen or lost.

Real-time Encryption



Two-factor Authentication

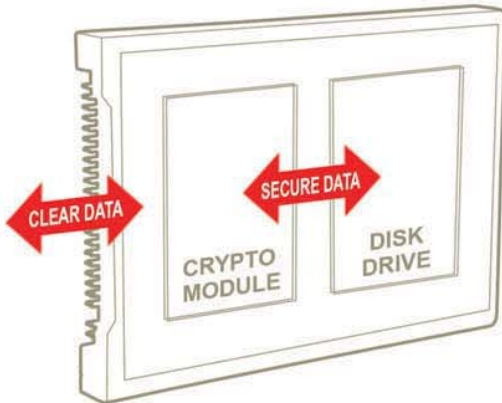


Pre-boot Authentication



Real-time encryption

DigiSAFE DiskCrypt consists of a hard disk drive and a hardware-based cryptographic module that encrypts every single byte of data that is written into the hard disk in real-time without loss in disk performance.



FEATURES	BENEFITS
Real-time hardware-based encryption and decryption Pure hardware solution	Zero performance degradation
Every single hard disk sector is encrypted	Total transparency to user, immune to virus/trojan attacks against software
Platform and operating system independent	Complete data protection
No need for software installation, upgrades, or patches	Greater operational options and deployment flexibility
Tamper-resistant hardware cryptographic module	Ease of installation and maintenance, lower total cost of ownership
Pre-boot authentication	Robust physical protection
Supports authentication using USB cryptographic token	Strong hard disk access control
Supports data migration and backup	Rigorous two-factor authentication
	Total data protection, migration, backup, and recovery solution for the notebook

DiskCrypt Toolkit

The DiskCrypt Toolkit consists of an external USB hard disk enclosure and a data cloning software.

Migration:

This enables the user to migrate seamlessly from the original hard disk to DiskCrypt, preserving the existing software operating environment and user data.

Backup and Recovery:

User can also backup their DiskCrypt data onto another external drive that can be stored securely.

Pre-boot Authentication

DiskCrypt authenticates the user every time the notebook powers on or resumes from hibernation. The notebook will only boot into the Operating System upon successful user authentication. DiskCrypt 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. DiskCrypt grants access to the user if the correct password is presented.

Two-Factor Authentication:

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

SPECIFICATIONS	
Storage Capacity	• 20GB, 30GB, 40GB
Data Transfer Rate	• 100 MB/sec Ultra DMA
Interface	• ATA-2/3/4/5/6, SATA 1.0
Rotational Speed	• 4200 rpm
Buffer	• 2MB
Physical	• Standard 2.5" HDD • Conforms to SFF-8200, SFF-8201, SFF-8212 • Dimensions: 100 mm (L) x 70 mm (W) x 9.5 mm (H)
Power	• 5V 900mA
Operating Systems	• Operating Systems independent • Tested with Windows® XP, 2000, ME, 98SE, 98, and Linux
Encryption	• NIST ¹ & CSE ² certified TDES hardware cipher engine • Supported key strengths: - 64-bits DES - 128-bits 3DES - 192-bits 3DES
Pre-boot Authentication	• Password • Two factor authentication with DigiSAFE KeyCrypt
DigiSAFE KeyCrypt USB Cryptographic token	• Two-factor pre-boot authentication
OPTIONAL	
DigiSAFE DiskCrypt Toolkit	• Utility Kit with - Disk cloning software for migration, backup and recovery of data - External USB hard disk enclosure

¹NIST – The National Institute of Standards and Technology of the United States of America
²CSE – The Communications Security Establishment of the Government of Canada

Regulatory Compliance

DiskCrypt combines notebook data encryption and pre-boot authentication to allow organizations to better protect and control access to their corporate and customer data to comply with regulations such as Sarbanes-Oxley, HIPAA, and EU Data protection Directive.

Authorized Reseller:

ST Electronics (Info-Security) Pte Ltd (Formerly known as DigiSAFE Pte Ltd)

100 Jurong East Street 21, ST Electronics Jurong East Building, Singapore 609602 Tel: (65) 6568 7118
Fax: (65) 6568 7226 Email: info@digisafe.com URL: www.digisafe.com (Regn. No.: 199902746G)



ST Electronics

A company of ST Engineering

The development of DigiSAFE products and services is continuous and published information may not be up to date. All rights to the mentioned trademarks reside with their respective owners. DigiSAFE logo, DiskCrypt and KeyCrypt are registered trademarks of ST Electronics (Info-Security) Pte Ltd. Printed by ST Electronics (Info-Security) Pte Ltd in January 2007. Information is correct at the time of printing. © 2006-2007