



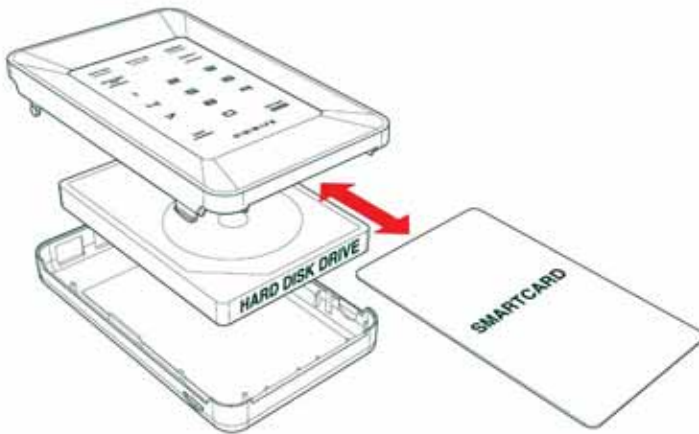
Simply Secure!

Your data on the go

DigiSAFE DiskCrypt *Mobile* (DCM300) is the world's first encrypting hard drive enclosure with smartcard protection. It employs real-time hardware encryption for protecting the data on the hard drive and smartcard technology for authentication. Designed to encrypt all data on-the-fly, DCM300 requires no software installation and operates independently of the operating system.

A unique feature of DCM300 is that it carries a keypad allowing you to key in your PIN directly onto the unit. This ensures protection from key-loggers that may be recording your keystrokes. Together with full disk encryption and smartcard based authentication, DCM300 gives you the ultimate level of protection with an unrivalled ease of use.





FEATURES	BENEFITS
Authentication using smartcard and PIN	Requiring a smartcard and a PIN offers a high level of security, equivalent to using your ATM card and PIN
Built-in keypad for PIN entry	Safety of PIN from trojans/key-loggers
Real-time hardware-based encryption and decryption	Zero performance degradation
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 low maintenance cost. Lower total cost of ownership

Real-time Hardware Encryption

DigiSAFE DCM300 consists of a hardware-based encryption module that performs full disk encryption, i.e. it encrypts every byte and every sector of data that is written into the hard drive. Encryption and decryption happen on-the-fly in hardware such that the process is completely transparent to the user.

Hardware encryption also provides a lower cost of ownership as it is completely Operating System independent and requires no installation of software drivers, thus doing away with the hassle of software upgrades and OS patches.

Two-factor Authentication

DigiSAFE DCM300 enforces two-factor authentication to provide a higher security protection. It requires the users to present the smartcard ("something you have") and enter the correct PIN ("something you know") using the built-in keypad to unlock the data on the encrypted hard disk. This unique feature of PIN entry using the built-in keypad enables DCM300 to be safe from potential trojans and key-loggers that may be recording users' keystrokes.

SPECIFICATIONS	
Enclosure type	• 2.5" external USB enclosure
Bus Interface	• USB 2.0 • Firewire 400/800
Interface Transfer Rate	• USB - 12Mbps / 480Mbps • Firewire - 100/200/400/800 Mbps
Compatible drives	• 2.5" SATA-I/II
Encryption	• NIST ¹ certified AES hardware cipher engine • Supported key strengths • 128/256 bits
Operating Systems	• Operating System independent • Tested with Windows 7, Vista, XP, Linux, Mac OS
Smartcard Authentication	• Two-factor authentication with DigiSAFE certified smartcard
Power	• 5V 400mA (excluding the power drawn by the HDD)
Physical	• Dimensions: 130mm (L) x 78mm (W) x 22mm (H)

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

Regulatory Compliance

DigiSAFE DCM300 employs smartcard technology to protect data in external USB hard disk drives. Its usage by enterprises will allow compliance with regulations such as HIPAA, GLB Act, Sarbanes-Oxley Act, EU Data Protection Directive, FISMA and Japan's Personal Information Protection Act.

Authorised Reseller: