

FAQ for DigiSafe DiskCrypt Mobile – DCM300

Q: What is DigiSAFE DiskCrypt MOBILE?

A: DigiSAFE DiskCrypt MOBILE is a smartcard authenticated USB external storage enclosure that offers real-time full disk encryption capability to the enclosed 2.5" hard drive. Two factors authentication, the presence of the smartcard and the knowledge of the PIN, is a standard implementation.

Q: How does DigiSAFE DiskCrypt MOBILE work?

A: The DigiSAFE DiskCrypt MOBILE works just like a regular external USB drive except that it requires user to authenticate before disk access is allowed. It houses any standard 2.5" SATA drive (no disk capacity limitation) and offers real-time hardware full disk encryption capability. Only upon successful authentication, does DigiSAFE DiskCrypt MOBILE allow normal disk access. The embedded encryption real time crypto engine offers transparent cryptographic operations to the entire addressable sectors of the drive, providing NIST & CSE certified AES strength.

Q: How easy it is to use DigiSAFE DiskCrypt MOBILE?

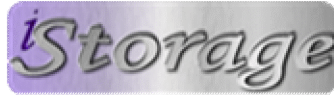
A: The engineering of the DigiSAFE DiskCrypt MOBILE is simple and straight forward. Simply connect the provided USB cable; Insert the smartcard; then press the PIN on the keypad. There is no additional software to install, making it completely OS independent.

Q: What are the advantages of using DigiSAFE DiskCrypt MOBILE as compare to other USB drive enclosures?

A: The DigiSAFE DiskCrypt MOBILE offers strong security, period. It does that through an industrial strength smartcard/PIN authentication and real-time cryptographic engine that encrypts the entire drive.

Q: What are the advantages of using smartcard/PIN two factors authentication?

A: Smartcards are a proven technology for secure storage of information. DigiSAFE DiskCrypt MOBILE stores the secret key (for both encryption and decryption) in smartcards. The secret key will not be released from the smartcard unless a valid PIN attempt releases it. The power of using two factors authentication is obvious as the lost of entire unit is simply a loss of hardware, not the data.



Q: What is two-factor authentication?

A: Two-factor authentication is an authentication protocol that requires two independent methods (something you have and something you know) to establish one's identity and privileges. DigiSAFE DiskCrypt MOBILE requires both the presence of the correct smartcard (something you have) and PIN (something you know) to enable its functions. In certain applications, the DigiSAFE DiskCrypt MOBILE can be sent out via regular parcel services and the PIN can then be properly advised through the phone.

Q: What are the advantages of real-time full disk encryption over software encryption solutions?

A: Unlike existing software solutions,

- the embedded crypto chip encrypts every addressable sector of the enclosed hard drive, including boot sector, FAT and temporary files;
- DigiSAFE DiskCrypt MOBILE is OS independent;
- DigiSAFE DiskCrypt MOBILE does not involve with tedious and error-prone software installation and configuration. Simply plug in the DigiSAFE DiskCrypt MOBILE to the host USB2.0 interface or FireWire (subjected to certain model); authenticate yourself and you are ready to go;
- DigiSAFE DiskCrypt MOBILE does not require any maintenance or patches thus reduce the total cost of ownership over years;
- DigiSAFE DiskCrypt MOBILE offers no performance degradation while performing real time cryptographic operations.

Q: What happens when DigiSAFE DiskCrypt MOBILE malfunctions?

A: Every DigiSAFE DiskCrypt MOBILE is subjected to a stringent quality assurance process prior to shipment. Just in case the unit might suffer electronic malfunctions, simply remove the disk drive and place it over to the other DigiSAFE DiskCrypt MOBILE that comes with the same cryptographic strength (for instance, AES 128-bit). Insert smartcard and present the same PIN to access the protected data. However, hard drives have a limited lifetime. As such, users are advised to backup their data regularly.



Q: Is the boot sector encrypted?

A: Yes, DigiSAFE DiskCrypt MOBILE employs full disk encryption, meaning every addressable sector of your hard drive is encrypted.

Q: Does the process of cryptographic operations decrease drive performance?

A: No. The hardware cryptographic engine offers real-time no performance loss operation. As a matter of fact, it offers a lot more bandwidth than a USB2.0/ FireWire connection. As the hardware is OS independent, the CPU interrupt and memory overhead are completely eliminated.

Q: How strong is the encryption of DigiSAFE DiskCrypt MOBILE?

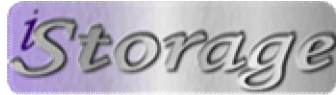
A: Very strong. DigiSAFE DiskCrypt MOBILE offers NIST (National Institute of Standards and Technology of United States) and CSE (Communication Security Establishment of Canada) certified AES 128-bit hardware strength.

Q: Can the PIN be changed later without data loss?

A: Yes, the smartcard PIN may be easily changed during the time of authentication without any data loss. Please note that PIN is smartcard specific so changing the PIN with one smartcard does not automatically change the PIN of another. As the DigiSAFE DiskCrypt MOBILE comes with two smartcards as a standard package, change one PIN does not automatically associate the change of the other. You must manually change the PIN of both smartcards issued to you.

Q: Can I use my *DigiSAFE DiskCrypt MOBILE* with various OS?

A: Yes! DigiSAFE DiskCrypt MOBILE is OS independent. As long as the USB Mass Storage class specification is supported in your specific OS, you may use your purchase with it. Being said, the DigiSAFE DiskCrypt MOBILE has been tested under Windows XP, 2000, Mac OS and Linux.



Q: What happens if I lose my smartcard?

A: The secret key to operate the cryptographic engine *resides on the* smartcards and it is protected by your specific PIN. There are two ways to deal with the issue:

- 1) If you lose your 1st card, please continue to use the 2nd card to access your drive.
Meanwhile, purchase an additional pair of cards and follow the instructions in the user's guide to initialize the new smartcards. Please note that new cards will come with new secret key. So please backup your data with your existing smartcard before using the new one; or,
- 2) Work with our engineering team to produce a customized smartcard key management system to allow the same secret key been issued at your convenience.