

**CKM<sup>®</sup> Secrypt<sup>®</sup> Mobile** is a disc encryption product that provides protection of sensitive information at rest. All user information on the machine is automatically encrypted using TecSec's standards-based CKM technology. Once CKM Secrypt Mobile is installed, all data related files are encrypted. Only users holding the proper Credentials will be able to access the information contained on the machine. CKM Secrypt Mobile is ideal for use on a laptop by a frequent traveler, ensuring that the entire hard disc content is secure, not just drives or folders. Thus, stolen laptops will yield nothing to the thief.

CKM Secrypt Mobile goes beyond other conventional disc encryption tools that encrypt program files as well as data; thus causing users extended wait times during boot up and restarts. CKM Secrypt Mobile does not encrypt Direct Library Link (.dll) files or other associated program related files. This ensures that the programs startup quickly and get you to your data faster.

CKM Secrypt Mobile goes even further; its operation is transparent to users. And furthermore, any file copied from the machine to any other device or location maintains its encryption... preventing unauthorized or accidental sharing of sensitive information. This means that you can be safe knowing that you data is always safe.

Some Key Features of CKM Secrypt Mobile:

- The operation is transparent to users.
- Operating System files are not encrypted meaning;
  - OS updates are smother and quicker.
  - The OS is not slowed down by the encryption of DLLs and other system files.
- Users are prevented from storing any files unencrypted, except by specific administrator managed policy.
- The files that are encrypted are clearly delineated in two ways:
  - The file name appears in green text in Windows Explorer
  - In the file properties, there is a CKM Secure tab.
- The Single Sign-on feature ensures that users do not have to independently enter their password for every application that CKM Enabled, or able to access encrypted files.
- If users Tokens or passwords are lost, the system administrator can reset the password or issue another Token. The control of the encryption of the data is always in the hands of the enterprise, not users.
- System Administrators are provided with a utility that provides:
  - The ability to encrypt all existing data files on a machine in the background.
  - The ability to decrypt all data files on a machine should that ever be necessary.
  - Log files to assist in the administration and validation of the security features.