

# DeltaCrypt Technologies inc.



## **Custom-Built Solution**

Don't let your company's special requirements keep you from protecting sensitive corporate data. Have any of the DeltaCrypt public key encryption solutions adapted to your environment.

## **Complete Range of Encryption Products**

DeltaCrypt offers a complete range of encryption applications. Whether you want to protect your PC, data exchanges, emails, USB flash memory drives as well as your backups; DeltaCrypt has the right solution for you.

## **Strong Presence in Security-conscious Organizations and Industries**

Governments, R&D, High Tech, Financial Institutions, Lotteries, Oil & Gas, etc.

## DeltaCrypt Encryption Protection

DeltaCrypt is a privately owned corporation. Our dedicated team has been developing cryptographic applications for nearly 10 years. DeltaCrypt's mission is to develop new and innovative public key encryption technologies of the highest quality suited for medium, large & enterprise clients.

### **Public Key Encryption**

DeltaCrypt applications offer public key encryption to secure exchanges and to protect sensitive files. Public key cryptography is an encryption method that uses two unique keys which are related: a public key which is used for encryption and a secret key (password) used to decrypt the data. As per its name, the public key is available to anyone wanting to cipher a message. However, the encrypted message can only be decrypted using the private key, which remains confidential.

### **1024bits RSA Keys**

At encryption, a RSA public key is used by DeltaCrypt to cipher the symmetrical key included in the encryption key. At decryption, a RSA private key is used to decipher the symmetrical key. To maintain a high level of security, DeltaCrypt does not save the RSA private key on the hard drive conversely, it generates one each time the private key is required. In both cases, DeltaCrypt uses 1024bits RSA keys.

### **Hashing**

DeltaCrypt uses a hash function to ensure the encryption integrity. All DeltaCrypt public key encryption applications benefit from a choice of hashing algorithms (SHA-1 SHA-256 and MD-5). This hashing produces a message digest to protect the encryption and the public key file integrity. For the DUSK USB protection, Encrypted Backup Solution and DEOS, DeltaCrypt strictly uses SHA-256.

### **AES Rijndael Encryption**

DeltaCrypt applications integrate the Rijndael Algorithm (128-bit, 192-bit and 256-bit keys). The high security Rijndael algorithm is the new Advanced Encryption Standard (AES) chosen by the National Institute of Standards and Technology (NIST, FIPS-197).

### **FIPS 140-2 Certification**

DeltaCrypt is currently undergoing a FIPS 140-2 Certification. The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to accredit cryptographic modules.

### **Patent-pending technology**

DeltaCrypt DUSK is patent-pending.

# DUSK Corporate Edition for USB Mobile Device Protection

DeltaCrypt DUSK USB Mobile Device Protection enables Users to secure their mobile data with simple drag'n drop encryption technology. Provide your Users with DUSK USB Mobile Device Protection to secure corporate mobile data. These mobile devices have become essential working tools in today's business world however; they are also the cause of many security breaches and lost data. Dusk for USB quickly and cost effectively provides the security your corporate data requires. DeltaCrypt DUSK Protection is patent-pending.

## DUSK PROTECTION FEATURES

### **Drag'n Drop USB Mobile Device Protection**

To encrypt, drag files and folders from DUSK left pane (representing your PC) to its right pane (representing the USB drive). No other training required. Easy as 1, 2, 3!

### **Reads, Writes, Encrypts/decrypts Outside the Network Without Restrictions**

Not only can anyone decrypt and read files on the DUSK-protected device from anywhere but DUSK protection encrypts any newly added files from any computer inside or outside the network without any restrictions!

### **Valorize Initial Investments Made in USB Mass Storage Devices**

DUSK software protects not only your future USB flash drive or other USB devices acquisitions but all your previous investments made in such devices as well, no matter what their brand, size and capacities.

### **Corporate Master Key to Recuperate Users' Data**

DUSK solution comes in two modules: an **Admin Module** to create Master keys and a **DUSK User Module** for USB drives. Using the Administrator Module to create the DUSK Master Keys enables IT Administrator to recover encrypted information on Users' USB drives at any time, if needed.

### **No Software on Host PC Needed**

There is no need to install any application on any host PC. The DeltaCrypt DUSK USB drive protection runs on the drive itself to simplify implementation in corporate environment, particularly if your workstations have limited privileges (User account). This way your USB flash drives will not become the weakest security link in your organization.

### **No Unprotected Partition to Mislplace Sensitive Files**

When organizations choose to apply security measures to protect sensitive mobile data on USB drives, they cannot risk a User misplacing sensitive files to an unprotected section of his USB stick. DUSK Solution leaves no unprotected space on a USB Drive. It fills the whole drive with encryption protection regardless of the drive size. With this approach, no file may be left unprotected on a DUSK-protected USB drive.

### **Works with User (limited) and Administrator (unlimited) Accounts**

DeltaCrypt DUSK USB encryption protection works with any computers even those that administrative privileges have been deactivated to make the operating system more resistant to viruses and other malicious software.

### **Active Directory Configuration New**

With the .ADM file inserted to the Active Directory Group Policy Management, DUSK options are easily configured by the IT Administrator. From the encryption algorithm to the User password structure, DUSK configuration is shaped according to your security needs.

### **Logs Journal New**

Logs of files copied onto and deleted from your mobile devices are recorded, allowing your Administrator to identify your flash drive content. Details such as the file name, its last modification date, and file size are made available to Administrators in a log journal.

### **Transparent Updates New**

When used together with DUSKWatch on a workstation, DUSK updates are accomplished transparently without any other intervention or User knowledge. As soon as a new DUSK version is available, DUSKWatch automatically makes sure that all connected DUSK-protected drives are up to date.

### **Can Be Combined to DUSKWatch for USB Mobile Device Control**

Can be used in conjunction with DUSKWatch to only allow DUSK-protected Mobile Devices to be used. Any other unauthorized USB mass storage devices will be rejected. This way, you'll get the assurance that all your mobile data is protected at all time.

## **INSTALLATION**

You may choose to have your Users install DUSK protection on their USB drives or you may want your IT Administrator to keep control over DUSK installation.

### **USER INSTALLATION (DECENTRALIZED INSTALLATION)**

#### **From a Workstation with Restricted or Unlimited Privileges**

When choosing a decentralized installation, DUSKWatch is required to allow Users to install themselves DUSK protection onto their USB flash drives.

Once configured, DUSKWatch will place a DUSK installer icon onto Users desktops. Once installed, Users will simply have to double click on the icon to launch DUSK installation onto their USB drives.

### **ADMINISTRATOR INSTALLATION (CENTRALIZED INSTALLATION)**

#### **Using a Bulk Installer**

If you prefer having your IT department perform numerous installations, DeltaCrypt will provide you with a bulk installer allowing your IT Administrator to automatically accomplish the following tasks: : NTFS formatting, application installation, Master Key configuration for all the USB drives you need to protect. All you have to do is to connect your USB drives to the installing PC, one after the other and DUSK bulk installer will do the rest.



Small USB keys may contain up to 160,000 documents. One can no longer underestimate the consequences of losing such a large amount of data. Have your corporate USB drives protected with DUSK protection now.

DUSK CORPORATE EDITION SPECS	
Support Type	<ul style="list-style-type: none"> <li>• USB flash memory drive</li> <li>• USB hard disk drive</li> <li>• Memory card</li> <li>• Firewire</li> </ul>
Operating systems	Windows 2000, XP and Vista <b>New</b>
USB interface	USB 2.0 / USB 1.1 / USB 1.0
File systems	FAT / FAT32 / NTFS (recommended)
Application volume	2.3 Mb
Hashing algorithm	Sha-256
Encryption type	Choice between AES 128-bit, 192-bit and 256-bit (Rijndael). All encryption methods are protected with RSA public and private 1024bit keys.
Use	With unlimited privileges (Administrator account) and limited privileges (User account)
Security	Public key encryption protection generated by password or pass phrase
Protection	User password / Administrator Master Key and Private Key File (if configured)
Interface	Drag'n drop / Copy / Paste / Cut
Distribution	Download
Installation	Executable file. Unlimited and limited privileges.
Active Directory Configuration (Activation / deactivation)  Policies applicable to : - User groups - Workstation groups	<ul style="list-style-type: none"> <li>• User Password Structure <ul style="list-style-type: none"> <li>○ Character minimum</li> <li>○ Lower case letter minimum</li> <li>○ Upper case letter minimum</li> <li>○ Number minimum</li> </ul> </li> <li>• Language</li> <li>• Encryption algorithm</li> <li>• Log parameters</li> <li>• Log recording</li> <li>• Master key use</li> <li>• Option to view the User password at DUSK opening</li> </ul>
Bulk installation	For NTFS formatting, application installation, Master Key configuration
Complement	DUSKWatch for USB Mass Storage control
Languages available	English, French
Updates	12 months included

## HOW DUSK WORKS

### **DUSK Fills the Whole USB Mobile Device with DeltaCrypt Protection**

At installation, DUSK fills the entire USB drive with its protection forcing Users to open the DUSK application to access any files on their USB drive. It will not be possible for any User to copy files on a protected USB device without first opening the DUSK application. When opened, DUSK evaluates the file volume it needs to copy any file onto the USB drive and automatically generates sufficient space on the protected drive.

### **Public Key Protection**

Entering a User password opens the DUSK application. Once opened, to encrypt files, the User needs to drag'n drop files from DUSK left pane representing the User workstation to DUSK right pane representing the USB drive. The reverse action is also true to decrypt files placed on DUSK protected USB drives.

### **IT Administrator Master Key**

When installing DUSK, a Master Key is coupled with the application. This Master Key allows the IT Administrator to recover data when Users forget or lose their passwords. In an event where a User does lose or forget his password, the Administrator would enter the Master Key password instead of the User password to open the DUSK application.

### **Can be Combined with DeltaCrypt DUSKWatch Control**

Combined with the DUSKWatch application installed on Users' workstations, only your DUSK-protected USB devices can be permitted. Your Users will be prevented from using any unprotected USB mass storage device and consequently, they will not be able to contravene corporate security policies. You will get the assurance that your corporate data will always be protected when being copied to portable USB mass storage devices.

## Custom-Built Solution

Don't let your specific requirements keep you from protecting your sensitive data, contact DeltaCrypt instead. It will be our pleasure to study the possibility to adapt our technology to meet your special needs.



### Contact us

DeltaCrypt Technologies Inc.  
By phone at 1-888-500-3563  
By email at [dtiinfo@deltacrypt.com](mailto:dtiinfo@deltacrypt.com)