

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.

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. DeltaCrypt public key encryption applications all 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

DUSK USB protection integrates 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).

DUSK for USB Key Protection

DeltaCrypt DUSK USB key encryption solution enables Users to secure their mobile data with simple drag'n drop encryption technology. Provide your Users, DUSK USB Key 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.

DUSK PROTECTION FEATURES

Drag'n Drop USB Key Protection

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

Corporate Master Key to recuperate Users' data

DUSK solution comes in two modules: an **Admin Module** to create Master keys and a **User Module** for USB Keys. Using the Administrator Module to create the DUSK Master Keys enables IT Administrator to recover encrypted information on Users' USB keys 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 key encryption protection runs on the key itself to simplify implementation in corporate environment, particularly if your workstations have limited privileges (User account). This way your USB keys will not become the weakest security link in your organization.

No Unprotected Partition

When organizations choose to apply security measures to protect sensitive mobile data on USB keys, they cannot risk a User misplacing sensitive files to an unprotected section of his USB Key. DUSK Solution leaves no unprotected space on a USB Key. It fills the whole key with encryption protection regardless of the key size. With this approach, no file may be left unprotected on a DUSK protected USB key. One must open DUSK application to get to a file on his USB key.

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.

User Password

When DUSK protection is launched for the first time, it lets Users configure their own password to protect their USB keys. This feature reduces IT Administrator intervention to a strict minimum.

Automatic Re-Encryption of Files

Double-click to decrypt an encrypted file, and the DUSK solution will automatically open the decrypted file using the proper editing software (as long as you have it installed on the PC your USB key is connected to). Then, when you're finished and have closed the file, the DUSK solution automatically re-encrypts it to maintain a high level of security at all time.

Can be combined to DUSKWatch for USB keys control

Used in conjunction with DUSK Drag'n Drop Encryption for USB Keys, DUSKWatch will only allow protected Keys 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 keys or you may want your IT Administrator to keep control over DUSK installation.

If you choose to combine DUSK protection with DUSKWatch to control USB devices within your organization, it may even be possible to have DUSK installed using DUSKWatch.

USER INSTALLATION

From a workstation with restricted privileges

If you choose to have your Users install DUSK application from a workstation with restricted privileges, we recommend that you hand them a USB key already formatted in NTFS. DeltaCrypt will provide you with an executable file to install the DUSK application and to configure the Master Key given your User. If the computer is connected to the Internet, the registration will be automatically executed. If you send us the Master Key, we will gladly include it directly in our installer for you.

It is also possible to incorporate DUSK installation to the DUSKWatch if installed on Users' workstations. In such a case, as soon as a USB key will be connected to the USB port, DUSKWatch will prompt Users to install DUSK protection on their keys. It is also possible for DUSKWatch to install a DUSK installer icon on the User desktop so that one can choose when to install the DUSK protection on his USB key.

From a workstation with unlimited privileges

If you choose to have your Users install DUSK from a workstation with unlimited privileges, DeltaCrypt can provide you with an executable file that with a single click will automatically format the USB key in NTFS, install DUSK protection and configure the Master Key. If the computer is connected to the Internet, it will automatically register the application without any other intervention on the User's part.

ADMINISTRATOR 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 and DUSK application registration for all the USB keys you need to protect. All you have to do is to connect your USB keys to the installing PC, one after the other and DUSK bulk installer will do the rest.

Using the DUSKWatch

If you choose to combine USB Keys protection together with USB device control in order to have the assurance that only protected keys will be used within your organization; it is possible to combine DUSK installation on your Users' USB keys to DUSKWatch running on Users' workstations. When a USB key is connected to the USB port, you may choose to have DUSKWatch application offer your Users the option to proceed with installing DUSK on their USB keys. It is also possible to have DUSKWatch install a DUSK installer icon on Users' desktops to have them launch DUSK installation whenever they choose.

Log journal of DUSK licenses installed within your organization

When one registers DUSK protection licenses, the following data is gathered for registration purposes, namely, installation date and time, account and computer names and finally, the USB key serial number. It is therefore possible to send you a weekly journal of such installation logs. Of course this report will also inform you of the total license installed together with the number of the purchased licenses available left for installation.

DUSK SPECS	
Support	USB flash memory drive, USB hard disk drive, memory card reader, Firewire.
Operating systems	Windows 2000, XP and Vista
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 1024 bits keys.
Use	With unlimited privileges (administrator account) and limited privileges (User account)
Security	Public key encryption protection generated by a 6 to 1024 characters 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.
Bulk installation	For NTFS formatting, application installation, Master Key configuration and DUSK application registration
Registration	Automatic registration / Manual registration
Complement	DUSKWatch for USB Mass Storage control
Languages available	English, French
Updates	12 months included

HOW DUSK WORKS

DUSK fills the whole USB key with DeltaCrypt protection

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

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 key. The reverse action is also true to decrypt files placed on DUSK protected USB keys.

IT Administrator Master Key

When installing DUSK, a Master Key is coupled with the application. This Master Key allows IT Administrators to recover data when Users forget or lose their passwords. In an event where a User does lose or forget their password, the administrator would enter the Master Key password instead of the User password which will open the DUSK application to not only access files on the USB key but to change User's password.

Can be combined with DeltaCrypt DUSKWatch control

Combined with the DUSKWatch application installed on Users' workstations, only your DUSK protected USB keys will 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.



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 keys protected with DUSK protection now.

DUSKWatch to Control USB Keys

If your organization is concerned about its mobile data on USB keys or any other USB mass storage peripherals, the DeltaCrypt DUSKWatch application will let you control the USB keys on which your corporate data is copied to.

Used alone, DUSKWatch will not permit the copying of corporate data out to unprotected USB mass storage peripherals. Used in conjunction with DUSK protected keys or hard disks, DUSKWatch will allow Users to access and copy files on such protected USB devices.

DUSKWATCH FEATURES

Get the assurance that corporate mobile data is protected at all time

As soon as the computer is turned on, DUSKWatch blocks all unprotected USB Mass storage devices. It authorizes the copy of data only if a personalized DUSK protected USB device is detected. Not only does the USB mass storage device need to be DUSK protected, but the protection must be personalized to your organization. Without this double recognition, no copy on any USB keys will be granted.

Read files on unprotected mass storage devices (XP SP2 & Vista only)

By clicking on the DUSKWatch icon in the computer tray and selecting the read-only mode Users will be able to see, consult and copy files from the next unprotected device to be connected to the computer without needing to disable DUSKWatch control. Even when the read-only mode is used, DUSKWatch will keep Users from copying data out on such unprotected devices.

Transparent to your Users

Once installed on your Users' workstations, DUSKWatch becomes completely transparent to them. DUSKWatch works quietly in the background. No training is needed!

Updates DUSK Protection on USB keys

When used in conjunction with DUSK protection for USB keys, DUSKWatch updates DUSK version without needing to recuperate all your protected USB keys in circulation and with no User intervention too.

Enable to perform unlimited privilege functions

DUSKWatch functions at the same time in local User mode and in system mode enabling a limited computer privileges to perform functions needing unlimited computer privileges such as application installation, USB key formatting to name a few.

Can install DUSK protection onto USB keys

The DUSKWatch can install DUSK protection onto a USB key in one of these two ways: either by directly installing DUSK on unprotected USB keys when connected to the computer or by placing a DUSK installer icon on the User desktop so that a User may launch DUSK installation himself whenever he wants.

DUSK Log Journal

DUSKWatch may gather names of files copied onto DUSK protected keys in order to reconstruct most of the content of a lost USB key.

Illegal intrusion attacks

DUSKWatch can inform management if an unprotected USB key or hard disk was connected to a workstation to help an organization determine which workstation is more vulnerable to illegal intrusion attacks.

DUSKWATCH SPÉCS	
Operating systems	Windows 2000, Win Server 2003, XP and Vista
Application volume size:	3.1 MB
Security	<ul style="list-style-type: none"> - Authorizes DUSK protected USB mass storage devices - Blocks any unprotected USB peripherals - Read-only option for unprotected USB mass storage device (XP feature only)
Use	Transparent to User. Automatically launched when opening a session, unlimited privileges (administrator account) and limited privileges (User account)
Distribution	Download
Installation	MSI file, unlimited privileges required (administrator account)
Registration	Automatic registration done by Internet
Updates	12 months included.
Other	May install and update DUSK protection on USB keys (optional)

Control USB keys within your corporate environment with DUSKWatch solution now!

INSTALLATION

You may choose to have Users install DUSKWatch on their workstation or you may decide to have your IT Administrator remotely install DUSKWatch on all workstations.

USER INSTALLATION

From unlimited privilege computer

If you prefer to have your User perform DUSKWatch installation, all he will have to do is execute the .msi file on his workstation. If he is connected to the Internet, DUSKWatch registration will be automatically done without any other intervention.

ADMINISTRATOR INSTALLATION

Using GPO or SMS

If DUSKWatch installation is remotely performed by your IT Administrator, DUSKWatch .msi installer can be pushed using GPO or SMS. If workstations are connected to the Internet, DUSKWatch registration will be automatically done.

Log journal of DUSKWatch licenses installed within your organization

When one registers DUSKWatch application licenses, the following data is gathered for registration purposes, namely, installation date and time, account and computer names. It is therefore possible to send you a weekly journal of such installation logs. Of course this report will also inform you of the total license installed together with the number of the purchased licenses available left for installation.



Many medium and large corporations prohibit iPods, portable computers and even USB keys, reports a recent Ipsos-Reid survey. With DeltaCrypt DUSKWatch control, get peace of mind without having to police your User community.

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

DeltaCrypt Technologies Inc.

Contact us at <http://www.deltacrypt.com/english/contactus/contact.html>