

DeltaCrypt Technologies inc.



Solution sur mesure

Ne laissez pas des exigences particulières vous empêcher de protéger vos renseignements corporatifs sensibles. DeltaCrypt peut adapter ses protections spécifiquement à vos besoins. Offrez à vos utilisateurs des outils de sécurité spécialement adaptés à leur environnement de travail.

Gamme complète de produits de cryptage

DeltaCrypt offre une gamme complète de protection cryptographique. Que ce soit pour protéger votre ordinateur, vos échanges de fichiers, vos courriels, vos clés USB ainsi que vos copies de sauvegarde, DeltaCrypt a la solution pour vous.

La Protection de Cryptage de DeltaCrypt

Les Technologies DeltaCrypt Inc. est une société privée qui développe des applications cryptographiques depuis 2000. L'expertise de la société réside dans la technologie de cryptage et sa principale force se situe dans la transformation de cette technologie de cryptage de fichiers dans des applications logicielles pratiques pour la protection d'information.

Cryptage à clé publique

La cryptographie à clé publique est une méthode de chiffrement qui emploie deux clés différentes mais inter-reliées: la clé publique étant employée pour le chiffrement seulement et la clé secrète (mot de passe) étant employée pour déchiffrer les données. Cette méthode est particulièrement bien adaptée pour le stockage et/ou l'échange des données privées et confidentielles entre deux parties ou plus.

Sécurité intégrée RSA de 1024 bits

Une clé publique RSA est utilisée par DeltaCrypt pour crypter la clé symétrique incluse dans la clé de cryptage de DeltaCrypt. Une clé privée RSA est utilisée pour décrypter la clé symétrique pour le décryptage. Pour maintenir un haut niveau de sécurité, DeltaCrypt ne sauvegarde pas la clé privée RSA sur votre disque dur mais elle la régénère à chaque fois. Dans tous les cas, DeltaCrypt utilise des clés RSA de 1024bits.

Hachage

La fonction de hachage dans les logiciels de DeltaCrypt est utilisée pour vérifier l'intégrité du cryptage. Les applications de cryptage à clé publique de DeltaCrypt pour le Pc bénéficient tous d'un choix d'algorithme de hachage (SHA-1 SHA-256 et MD-5). Ce hachage produit un résumé de message (« message digest ») pour la protection de l'intégrité du cryptage et de ses clés publiques. Pour la Protection DUSK, la solution de copie de sauvegarde cryptée ainsi que DEOS, seul SHA-256 est utilisé.

Cryptage AES Rijndael

La protection DUSK offre maintenant une solution de cryptage avec l'algorithme Rijndael (AES 128bits, 192bits et 256bits). Cet algorithme est le nouveau standard de cryptage choisi par le NIST (National Institute of Standards and Technology) (FIPS-197).

Certification FIPS 140-2

DeltaCrypt est sur le point de produire une demande de certification FIPS 140-2. Le « Federal Information Processing Standard (FIPS) Publication 140-2 est un standard de sécurité informatique gouvernemental américain utilisé pour accréditer des modules cryptographiques.

Protection DUSK pour Clés USB

La Solution DUSK de DeltaCrypt permet aux sociétés de sécuriser leurs informations mobiles et en transit. Offrez à vos utilisateurs, la protection pour clés USB DUSK afin de sécuriser les informations qui quittent l'enceinte des bureaux de votre société. Les dispositifs mobiles sont désormais des outils incontournables dans le monde des affaires. En vous permettant de travailler à la maison comme si vous étiez au bureau, les clés USB emportent avec elles les informations sensibles de votre organisation. Une demande de brevet a été produite pour la protection DUSK.

LES PARTICULARITÉS DE LA PROTECTION DUSK

Cryptage glisser-déposer ("drag'n drop") pour clés USB

Protégez votre clé USB à l'aide du cryptage glisser-déposer ("drag'n drop") de la protection DUSK. Aucune formation nécessaire. Simple comme 1, 2, 3!

Clé Maître de l'Administrateur qui agit comme passe-partout

La Solution DUSK de DeltaCrypt se décline en deux modules: un Module Administrateur pour créer la Clé Maître qui sera utilisée comme passe-partout et un Module Utilisateur pour protéger les clés USB. La Solution DUSK permet donc à l'Administrateur TI de récupérer l'information sur les clés USB de ses utilisateurs au besoin.

Aucun logiciel n'est requis sur le poste de travail

Pas besoin d'installer d'application sur les postes de travail où votre clé sera branchée. La protection DUSK pour clés USB de DeltaCrypt s'exécute à même la clé et simplifie son implantation en milieu corporatif, particulièrement si votre parc d'ordinateurs ne possède que des privilèges limités (comptes utilisateur).

Aucun espace non protégé sur la clé USB

Lorsqu'une entreprise choisit d'appliquer des mesures de sécurité pour protéger l'information sur ses clés USB, elle ne peut se permettre qu'un utilisateur sauvegarde par mégarde ses données sensibles sur une partition non protégée de sa clé USB. Pour éviter cette situation, la protection DUSK remplit toute la clé USB de sa protection faisant en sorte qu'aucun fichier ne peut demeurer non protégé par erreur ou par mégarde.

Mobilité assurée: S'utilise à partir de n'importe quel ordinateur avec ou sans privilèges illimités

Vous pouvez utiliser votre clé USB sans avoir à installer de pilote, à partir d'ordinateurs ayant les privilèges de l'administrateur ou ceux dont les privilèges administrateurs sont désactivés pour rendre le système d'exploitation plus résistant aux virus et autres logiciels malicieux.

Mot de passe de l'utilisateur

Lorsque la protection DUSK est lancée pour la première fois, l'Utilisateur crée lui-même son mot de passe pour protéger sa clé USB. Cette particularité réduit l'intervention de l'Administrateur au strict minimum.

Configurable à l'aide d'Active Directory **Nouveau**

A l'aide d'un fichier .ADM inséré à la console de gestion des stratégies de groupe d'Active Directory, les options de DUSK peuvent être aisément configurées par votre Administrateur. De l'algorithme de cryptage à la structure du mot de passe Utilisateur, la configuration de la protection DUSK peut être façonnées selon vos besoins de sécurité.

Journal des logs **Nouveau**

Lorsqu'utilisée avec DUSKWatch installé sur les postes de travail, des logs des fichiers copiés et supprimés de vos dispositifs mobiles seront colligés, vous permettant d'identifier le contenu de vos dispositifs mobiles. Des données telles que le nom du fichier, la date de sa dernière modification, le volume du fichier sont mis à la disposition de votre Administrateur dans un journal des logs.

Mises à jour transparente **Nouveau**

Lorsqu'utilisée avec DUSKWatch, les mises à jour de DUSK se font de façon transparente sans aucune intervention ni connaissance de votre utilisateur. Dès qu'une nouvelle version est disponible, DUSKWatch vérifiera toute clé branchée et en fera la mise à jour.

Peut se combiner au DUSKWatch pour contrôler les clés USB

Installé sur le PC, le DUSKWatch n'autorise que l'utilisation de clés USB protégées par la protection DUSK identifiée à votre société. Vous obtiendrez ainsi l'assurance que toute l'information dont vous permettez la copie sur ces dispositifs mobiles sera protégée en tout temps.

INSTALLATION

Il est possible de décider si vous désirez que vos utilisateurs fassent eux-mêmes l'installation de la protection DUSK sur leurs clés USB. Vous pouvez également préférer garder le contrôle de l'installation en choisissant que votre Administrateur TI fasse l'installation de la protection DUSK sur toutes les clés de votre organisation.

PAR L'UTILISATEUR (INSTALLATION DÉCENTRALISÉE)

A partir d'un ordinateur avec privilèges limités ou illimités

Lorsqu'une installation décentralisée est privilégiée, DUSKWatch est requis afin de permettre à vos utilisateurs d'installer eux-mêmes la protection DUSK sur leurs dispositifs mobiles USB.

Une fois DUSKWatch installé sur vos postes de travail et qu'il est configuré pour placer un icône sur le bureau de vos utilisateurs, ces derniers n'auront qu'à cliquer deux fois sur cet icône pour installer eux-mêmes la protection DUSK après avoir été dûment autorisés par le système.

PAR L'ADMINISTRATEUR TI (INSTALLATION CENTRALISÉE)

A l'aide d'un installateur en série

Si vous préférez que votre Administrateur TI fasse une multitude d'installation de la protection DUSK, DeltaCrypt offre un installateur en série permettant à votre Administrateur TI d'effectuer automatiquement les fonctions suivantes : formatage en NTFS, installation de l'application, configuration de la clé maître pour toutes les clés USB que vous avez à protéger. Vous n'aurez qu'à brancher vos clés de mémoire flash USB, les unes après les autres et cet installateur en série se chargera de tout.



Petits et performants, les clés USB peuvent contenir jusqu'à 160,000 documents. On ne peut sous-estimer les conséquences engendrées par leur perte. Protégez vos clés USB dès maintenant avec la protection DUSK de DeltaCrypt.

SPÉCIFICATIONS DE LA SOLUTION DUSK	
Type de support	Clé USB, disque dur USB, lecteur de carte mémoire, Firewire
Système d'exploitation	Windows 2000, XP et Vista Nouveau
Interface USB	USB 2.0 / USB 1.1 / USB 1.0
Système de fichier	FAT / FAT32 / NTFS (recommandé)
Taille de l'application	2.3 Mo
Algorithme de hachage	Sha-256
Type de cryptage	Choix entre AES 128bits, 192bits, 256bits (Rijndael). Tous ces cryptages sont protégés par clés publique et privée RSA de 1024 bits.
Mode d'utilisation	Tant avec des privilèges illimités que des privilèges limités
Sécurité	Protection de cryptage à clé publique générée par mot de passe ou phrase de 6 à 1024 caractères
Protection	Mot de passe de l'utilisateur / Clé Maître (passe-partout)/ Clé privée (si configurée)
Interface	Glisser-Déposer / Copier / Coller / Couper
Distribution	Téléchargement
Installation	Fichier exécutable, privilèges illimités et privilèges limités
Installation automatique en série pour administrateurs	Formatage en NTFS, installation, configuration de la clé Maître et enregistrement des clés protégées par DUSK
Complément	DUSKWatch pour contrôler les clés USB
Langues d'utilisation	Français, anglais
Mises à jour	12 mois inclus

COMMENT FONCTIONNE DUSK

DUSK remplit toute la clé USB

Lors de l'installation, DUSK remplit toute la clé USB de sa protection faisant en sorte qu'un utilisateur doit impérativement utiliser par la protection DUSK pour accéder à un fichier placé sur la clé USB ou pour y copier un fichier. Il ne pourra copier ses fichiers sur sa clé USB sans qu'ils ne soient protégés. DUSK évaluera le volume du fichier à copier et générera automatiquement l'espace nécessaire pour le placer sur la clé protégée. Ainsi pas d'oubli possible...

DUSK sécurise les fichiers à l'aide de cryptage à clé publique

Le mot de passe saisi par l'utilisateur lors de l'ouverture du DUSK, permet d'ouvrir l'application DUSK. Une fois ouverte, l'utilisateur pourra crypter les fichiers en les copiant et les glissant de la fenêtre gauche du DUSK représentant le poste ordinateur sur lequel la clé USB est branchée vers la fenêtre de la droite du DUSK représentant le contenu protégé sur la clé USB. L'inverse est également vrai pour décrypter.

Récupération possible des fichiers par l'Administrateur TI

Lors de l'installation, une clé Maître est combinée à la protection DUSK. Cette clé Maître permet à l'Administrateur TI de récupérer l'information se trouvant sur la clé de l'utilisateur dans les cas où ce dernier aurait oublié son mot de passe. Il n'aura qu'à saisir le mot de passe ayant servi à dériver la clé Maître en lieu et place du mot de passe de l'utilisateur (ainsi qu'à indiquer le fichier de clé privée si configuré lors de la création de la clé Maître) pour ouvrir la protection DUSK.

Peut se combiner à l'application DUSKWatch pour une protection optimale

Lorsque combinée à l'application DUSKWatch installée sur le parc d'ordinateurs de votre organisation, seule l'utilisation de clés USB protégées par la protection DUSK identifiée à votre société ne sera permise. Vos utilisateurs ne pourront utiliser des clés USB non-protégées et ainsi contrevenir à vos politiques de sécurité. Vous obtiendrez ainsi l'assurance que toute l'information dont vous permettez la copie sur ces dispositifs mobiles sera protégée en tout temps.

DUSKWatch pour Contrôler l'Utilisation des Clés USB

Si votre organisation est préoccupée par l'information qui sort de ses bureaux sur des clés USB ou tout autre périphérique USB de stockage de masse, notre logiciel de prévention DUSKWatch vous permettra de contrôler les clés USB sur lesquelles vos informations sont copiées.

Utilisé seul, le DUSKWatch ne permet pas l'utilisation de périphériques de stockage de données USB. Combiné à la protection DUSK de DeltaCrypt protégeant les clés USB, le DUSKWatch permettra l'utilisation des périphériques ainsi protégés et autorisés. Une demande de brevet a été produite pour le DUSKWatch.

LES PARTICULARITÉS DU DUSKWATCH

Assurance que vos informations mobiles sont protégées en tout temps

Au démarrage du système d'exploitation, DUSKWatch bloque les périphériques de stockage de masse USB non protégés et non autorisés. Il n'autorise que l'utilisation de périphériques de stockage de données USB protégés par la protection DUSK et identifiée à votre société. Votre organisation aura ainsi l'assurance que toute l'information copiée sur ces dispositifs mobiles sera protégée en tout temps.

Bloque les dispositifs mobiles USB non autorisés

Le DUSKWatch bloquera tout dispositif USB non autorisés ni protégés tels que clés USB, Disque Dur USB, lecteurs de cartes de mémoire, iPods, cameras, pour n'en nommer que quelques-uns.

Lecture des dispositifs non protégés

Cliquer sur l'icône de DUSKWatch situé dans la zone de notification de l'ordinateur pour permettre la lecture de la prochaine clé USB non-protégée tout en empêchant la copie de vos fichiers sur celle-ci. Pas besoin de désactiver DUSKWatch pour consulter un fichier placé sur un dispositif USB non protégé.

Utilisation transparente pour vos utilisateurs

Une fois installé sur l'ordinateur de vos utilisateurs, le DUSKWatch devient complètement transparent pour l'utilisateur. Le DUSKWatch surveille et fonctionne discrètement en arrière-plan. Vous n'avez donc aucune formation à déployer.

Utilitaire de la protection DUSK **Nouveau**

Lorsqu'utilisé avec la protection DUSK pour les clés USB, DUSKWatch effectue les mises à jour de DUSK sans avoir à récupérer toutes vos clés en circulation et cela sans intervention de la part de vos utilisateurs.

Lors d'une installation décentralisée de DUSK, DUSKWatch permet également à vos utilisateurs d'installer eux-mêmes la protection DUSK sur leurs clés USB en plaçant un icône d'installation sur leurs bureaux. L'installation de la protection DUSK sera lancée en cliquant deux fois sur cet icône.

Configuration à l'aide d'Active Directory **Nouveau**

A l'aide d'un fichier .ADM inséré à la console de gestion des stratégies de groupe d'Active Directory, les options de DUSKWatch peuvent être aisément configurées par votre Administrateur. De l'icône d'installation de la protection DUSK à l'option de lecture seulement des dispositifs non protégés, la configuration de DUSKWatch peut être façonnée selon vos besoins de sécurité.

Journal des Logs **Nouveau**

DUSKWatch recueille les détails des fichiers copiés sur les dispositifs protégés par DUSK afin de vous permettre d'identifier le contenu de vos clés USB perdues ou volées.

Le Journal des Logs de DUSKWatch vous informe également sur les dispositifs non protégés et non autorisés qui ont été branchés sur votre réseau. Votre organisation pourra désormais identifier ses postes les plus vulnérables.

Décèle les tentatives d'intrusions illégales

DUSKWatch peut informer si une clé ou un disque dur USB non protégés a été branché à un poste de travail faisant en sorte qu'il peut être plus facile d'identifier les postes vulnérables de votre organisation.

SPÉCIFICATIONS DE LA SOLUTION DUSKWATCH

Système d'exploitation	- Windows 2000, Win Server 2003, XP et Vista Nouveau
Taille de l'application	3.1 Mo
Sécurité	<ul style="list-style-type: none">- Autorise l'utilisation de périphériques de stockage de données USB protégés par DUSK de DeltaCrypt- ne permet pas l'accès aux périphériques non protégés ni autorisés- Permet la lecture seulement des dispositifs non protégés (disponible que pour XP et Vista)
Mode d'utilisation	Se lance automatiquement à l'ouverture de session, privilèges illimités (compte administrateur) et privilèges limités (compte utilisateur)
Distribution	Téléchargement
Installation	Fichier MSI, privilèges illimités (compte administrateur)
Utilisation	Transparente pour l'utilisateur. Privilèges illimités et limités.
Enregistrement	L'enregistrement se fait automatiquement par Internet
Mises à jour	12 mois inclus

INSTALLATION

Il est possible que vos utilisateurs fassent eux-mêmes l'installation de l'application DUSKWatch sur leur poste de travail. Vous pouvez également préférer garder le contrôle de l'installation en choisissant que votre Administrateur TI fasse l'installation de DUSKWatch sur tous les postes de travail de votre organisation en même temps.

PAR L'UTILISATEUR

A partir d'un ordinateur avec privilèges illimités

Si vous préférez que votre utilisateur fasse lui-même son installation à partir d'un ordinateur, il n'aura qu'à exécuter le fichier d'installation .msi du DUSKWatch à partir de son ordinateur.

PAR L'ADMINISTRATEUR TI

A l'aide de GPO ou de SMS

Si vous préférez que votre Administrateur TI fasse l'installation du DUSKWatch sur tout votre parc d'ordinateurs en même temps, il pourra combiner l'installateur .MSI du DUSKWatch à des applications telles que GPO ou SMS afin de procéder aux installations à distance.



Plusieurs moyennes et grandes entreprises canadiennes refusent que leurs employés amènent au bureau des iPod, des ordinateurs portatifs ou même des clés de mémoire à bus sériel universel (USB), indique un sondage effectué par la maison Ipsos-Reid. Avec le DUSKWatch de DeltaCrypt ayez l'esprit tranquille !

Solution de Cryptage sur Mesure de DeltaCrypt

Ne laissez pas vos besoins particuliers vous empêcher d'obtenir la sécurité dont vos fichiers ont besoin, communiquez avec DeltaCrypt. Il nous fera plaisir d'étudier vos contraintes et vos demandes pour adapter notre technologie pour répondre à vos besoins.



Contact

Pour nous rejoindre

1-888-500-3563

<http://www.deltacrypt.com/francais/contactus/contact.html>