

MANUEL UTILISATEUR DES CLES DE CHIFFREMENT DES PRODUITS KRYPTKEY ET KRYPTKEY II

Prérequis techniques

- PC : système d'exploitation Windows7 et suivant
- Mac : MacOS 10.10 (Yosemite) et 10.11 (El Capitan)

En résumé

Vous venez d'acquérir une solution qui permet de chiffrer et déchiffrer très simplement des fichiers de votre ordinateur ou de tout autre périphérique connecté à ce dernier, grâce aux clés USB intelligente **KryptKey II**

Pour lui attribuer toutes ces capacités, vous devez activer **KryptKey II** lors de sa première utilisation et ensuite, à chaque nouvel usage, vous allez vous authentifier pour garantir que vous en êtes bien son propriétaire.

Lorsque KryptKey II est activée, vous avez toute latitude d'utiliser ou non ses fonctions de chiffrement.

Vous pouvez sauvegarder les documents chiffrés sur la clé, sur un disque dur (interne ou externe) ou sur vos serveurs dans le Cloud.

Cette clé vous permet également de créer un disque virtuel sur votre ordinateur (MAC ou PC). Ce dernier est visible uniquement si votre KryptKey II est activée.

Plusieurs moyens très simples permettent de gérer le chiffrement des documents :

- Simple « Glisser » vers la partie USB de la clé ou vers le Disque Virtuel (Chiffrement Automatique)
- Menu contextuel du fichier (clic droit) (sur Mac et sur PC quand l'extension MDKC est installée sur le PC) Pour Chiffrement sur l'ordinateur*
- Simple « Glisser » vers le coffre-fort (sur PC). Chiffre le dossier/fichier sur son emplacement.*

Votre **KryptKey II** est unique, vous ne pourrez déchiffrer que les fichiers préalablement chiffrés avec cette dernière.

Dans le détail,

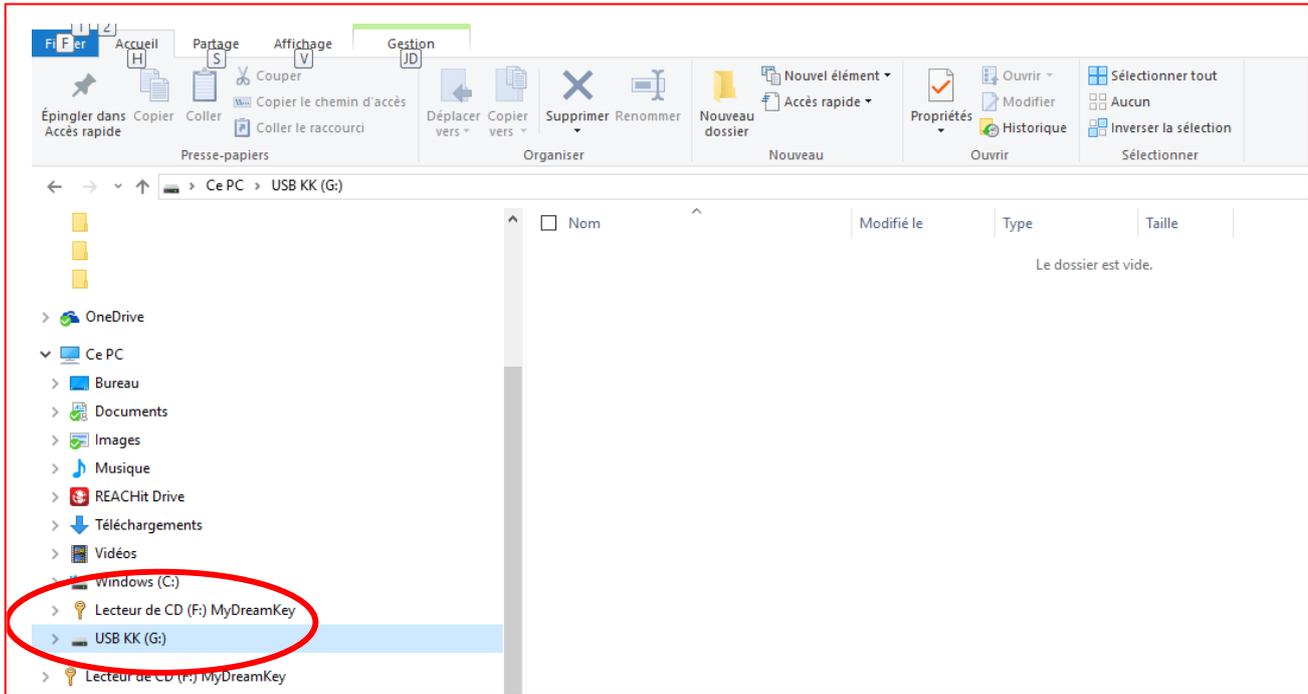
PROCEDURE INITIALE	3
USAGE COURANT	5
Chiffrement/déchiffrement	5
Installation de l'extension MDKC sur votre PC	6
Chiffrement des noms de fichiers/dossiers	7
Exclure des dossiers du chiffrement automatique	7
Utilisation d'un disque virtuel*	8
Gestion du disque virtuel (Création / suppression /Augmentation taille)*	8
Création d'un disque virtuel*	9
Déconnexion du disque virtuel*	9
Agrandissement du disque virtuel*	10
Suppression du disque virtuel*	10
Gestion du mot de passe	11
Changement de mot de passe	11
Mot de passe oublié	11
PERTE DE VOTRE CLE KRYPTKEY	12
DEBRIDAGE DE VOTRE CLE KRYPTKEY Essential EN CLE KRYPTKEY	13

PROCEDURE INITIALE

Pour cette première utilisation, une connexion Internet depuis votre PC ou Mac est requise.

1- Connectez votre clé KryptKey II à votre PC/Mac.

Cette clé contient 2 partitions. Une partition USB permettant le stockage et une partition MyDreamKey contenant l'application **MyDreamKey.exe** (PC) ou **MyDreamKey** (Mac).



2- Dans la partition MyDreamKey, lancez l'application MyDreamKey.exe (PC) ou MyDreamKey (Mac).



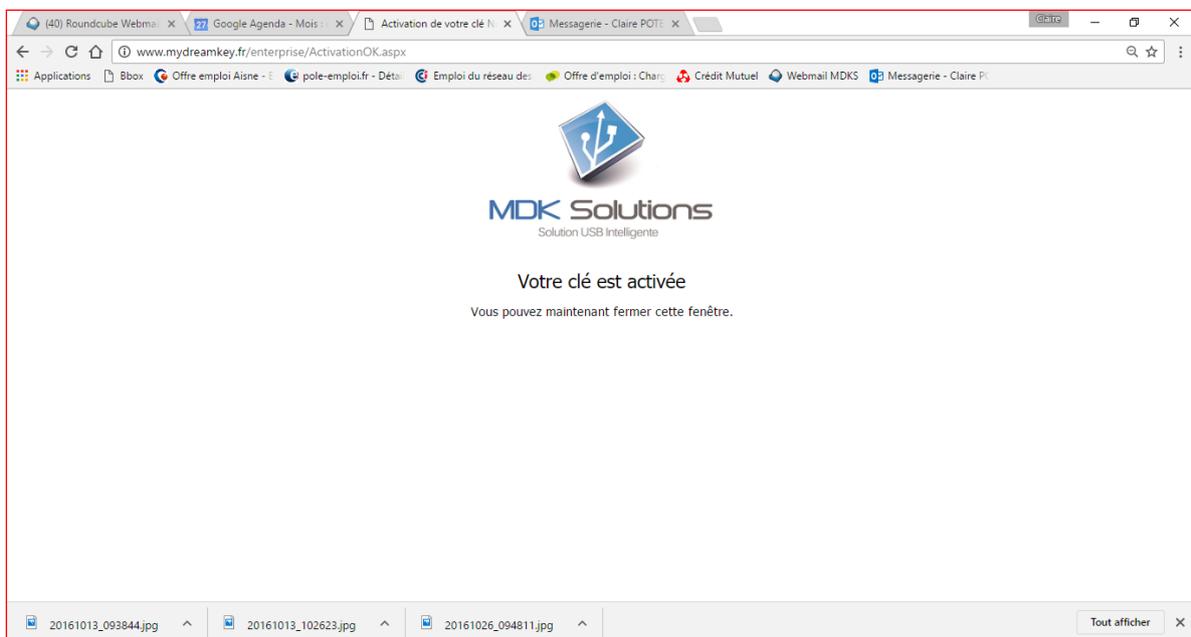
3- La fenêtre suivante apparaît.



The screenshot shows a web browser window displaying the MDK Solutions activation page. At the top, the MDK Solutions logo and tagline 'Solution USB Intelligente' are visible. Below this, the title 'Activation de votre clé MDK Solutions' is centered, followed by the serial number 'Votre numéro de série : 058F,6387,EDK1618801000002'. A message states: 'En cas d'oubli de mot de passe, MDK Solutions doit pouvoir vous contacter afin de réactiver votre clé.' The form contains several input fields: 'Nom, prénom', 'Adresse e-mail', 'Choisissez un mot de passe', 'Confirmez votre mot de passe', 'Question secrète', and 'Réponse secrète'. To the right of these fields, there are instructions: 'Saisissez une adresse e-mail valide. Votre nouveau mot de passe vous sera envoyé à cette adresse en cas d'oubli.'; 'Choisissez un mot de passe d'au moins 8 caractères. Il doit contenir 3 des 4 catégories suivantes : minuscules, majuscules, chiffres et caractères spéciaux.'; 'Confirmez la saisie de votre mot de passe.'; 'Cette question vous sera posée en cas d'oubli de mot de passe. Saisissez une question (ex: Nom de jeune fille de votre mère).'; and 'Saisissez ici la réponse que vous devez fournir pour valider le mot de passe de votre clé.' At the bottom, there is a checkbox for 'J'accepte les conditions générales de vente et d'utilisation.' and a 'Valider' button.

Remplissez l'écran d'activation avec votre nom, votre email, votre mot de passe et les question/réponse secrètes.

Ces données seront utilisées dans les procédures de réactivation et de ré-initialisation de mot de passe.



USAGE COURANT

Lancez l'application MyDreamKey.exe, fichier présent sur la partition CD/MyDreamKey, de KryptKey, de votre ordinateur.

Saisissez votre mot de passe.

Si vous avez une connexion Internet active, l'application va accéder au serveur MDK Solutions pour mettre à jour la clé avec les éventuelles dernières mises à jour logicielles. Windows peut vous poser des questions. Répondez aux éventuels messages Windows.

Sur votre PC, une icône « coffre-fort » apparaît en haut à droite de votre écran.

Sur un MAC, l'application KryptKey est alors accessible depuis le menu contextuel.



Vous pouvez alors utiliser les fonctions de chiffrement.

Chiffrement/déchiffrement

Pour chiffrer un dossier ou un fichier, glissez-le directement sur la clé USB si vous voulez que le fichier/dossier chiffré soit sur la clé, ou dans le coffre-fort* pour un chiffrement sur votre ordinateur, ou sélection/clic-droit/crypter (si MAC, ou l'extension MDKC installée sur votre PC via menu Coffre-fort).

Pour le déchiffrer, glissez-le sur le coffre-fort ou double-cliquez dessus (si MAC ou l'extension MDKC est installée sur votre PC).

Votre document s'ouvre automatiquement dans son format d'origine avec l'application associée (word, excel, ppt, pdf, ...)

A la fermeture du document, celui-ci est automatiquement chiffré sur son support et prend une extension **.mdkc**

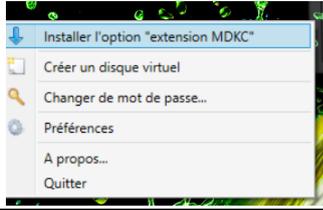
Les fichiers cryptés peuvent être stockés :

- sur la clé KryptKey
- sur votre disque dur interne*
- sur un support externe*
- dans le cloud*
- sur un disque virtuel sur votre ordinateur*.

** Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir des KryptKey Essential et KryptKey II Essential, vous devez acheter en ligne la mise à jour à partir du Menu / A propos.*

Installation de l'extension MDKC sur votre PC

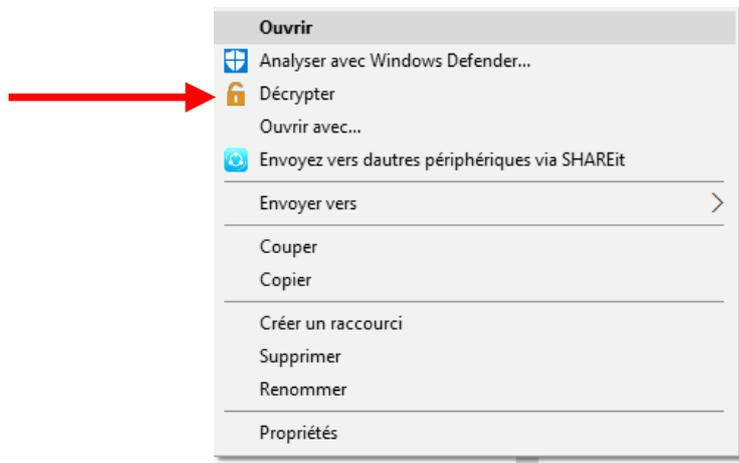
Vous pouvez installer « l'extension MDKC » sur votre PC (OPTIONNEL et gratuit).



Cette solution, facultative, vous apporte encore plus de simplicité dans la gestion des fichiers.

Lorsque la clé est activée, un simple double-clic sur le fichier chiffré entraîne l'ouverture du document dans son format d'origine avec l'application associée (word, excel, ppt, pdf, ...).

Un clic-droit sur le fichier vous permet d'accéder à la fonction Chiffrer/Déchiffrer.

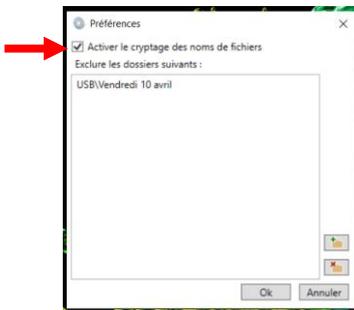


A la fermeture de l'application, le document est automatiquement sauvegardé chiffré.

** Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir des KryptKey Essential et KryptKey II Essential, vous devez acheter en ligne la mise à jour à partir du Menu / A propos.*

Chiffrement des noms de fichiers/dossiers

Cette fonction est optionnelle. Elle s'active en via « Menu / Préférences » puis cocher la case « Activer le cryptage des noms de fichiers ».



ATTENTION une fois cette option activée, après chaque utilisation de votre **KryptKey** vous devez quitter l'application via « Menu / Quitter », pour déclencher la procédure de chiffrement, et attendre sa fin avant de retirer la clé. Si la clé est retirée pendant la procédure de chiffrement, des noms ne seront pas chiffrés, et surtout vous risquez de corrompre le fichier/dossier en cours de traitement.

De même, après la validation de votre mot de passe, vous devez attendre la fin de la procédure de déchiffrement avant d'accéder à vos fichiers.

Le temps de chiffrement et de déchiffrement dépend du nombre de fichier et de dossier, de la configuration de votre ordinateur et de la performance de votre connecteur USB.

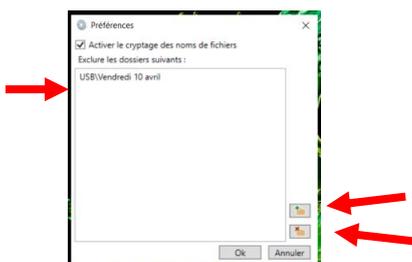
Exclure des dossiers du chiffrement automatique

Pour certain Usage vous pouvez vouloir ne pas chiffrer automatiquement des fichiers. Par exemple une vidéo qui doit être lu directement sur une Box, ou un fichier qui doit pouvoir être lu directement par une imprimante.

Il est possible d'exclure des Dossiers du chiffrement automatique. Les fichiers déposés dans ces dossiers ne seront donc pas chiffrés.

Pour sélectionner les dossiers à exclure du chiffrement automatique, vous devez aller sur « Menu / Préférences » puis sélectionner les dossiers, sur la clé, que vous souhaitez exclure du Chiffrement. Vous pouvez également créer directement un dossier. Une fois le Dossier sélectionner, faite OK

Si vous avez sélectionné un dossier contenant déjà des fichiers chiffrés, ils ne seront pas déchiffrés par « l'exclusion ». Vous devrez les déplacer hors du dossier, les ouvrir puis « enregistrer sous » dans le dossier. Il est conseillé de sélectionner des dossiers vide et de mettre ensuite les fichiers concernés.



Utilisation d'un disque virtuel*

Un disque virtuel est une partition du disque interne d'un PC. Cette partition et son contenu ne sont visibles qu'après l'activation de la clé KryptKey II.

Le disque virtuel permet de créer un environnement de sauvegarde de fichiers sur n'importe quel ordinateur (PC ou MAC), espace qui ne sera visible lorsque la clé sera correctement identifiée. Pour une sécurité renforcée, les documents sont chiffrés.

Gestion du disque virtuel (Création / suppression /Augmentation taille)*

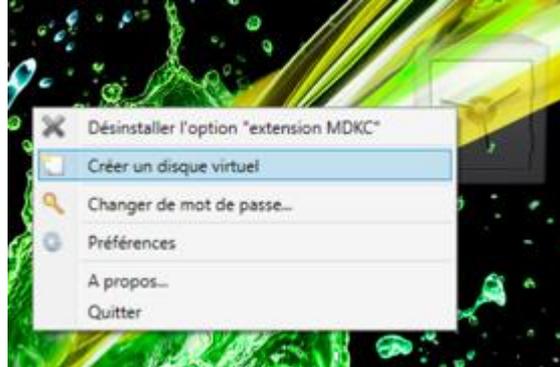


* Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir de KryptKey Essential et KryptKey II Essential, il faut d'acheter en ligne la mise à jour à partir du Menu KryptKey / A propos.

Création d'un disque virtuel*

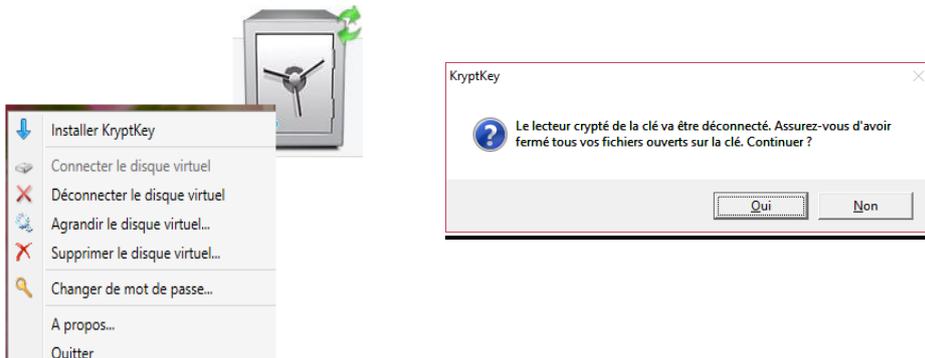
NB : Pour créer un disque virtuel, vous devez avoir le droit d'administrateur de votre PC.

Pour créer un disque virtuel sur votre PC, allez dans le menu du coffre-fort (clic droit sur le coffre-fort) et sélectionner « Créer un disque virtuel ».



Tous les dossiers/fichiers créés/déposés sur ce disque virtuel sont automatiquement chiffrés. Pour lire/modifier ces fichiers, il suffit de les glisser sur l'icône « coffre-fort ».

Déconnexion du disque virtuel*



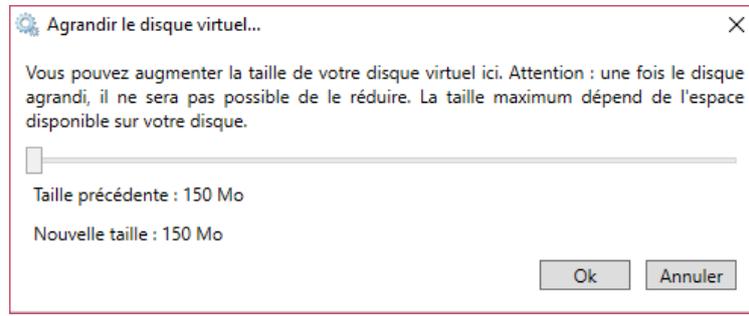
Après cette opération, le disque virtuel n'est plus visible.

* Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir de KryptKey Essential et KryptKey II Essential, il faut d'acheter en ligne la mise à jour à partir du Menu KryptKey / A propos.

Agrandissement du disque virtuel*

Par défaut, le disque virtuel occupe un espace de 150 Mo.

Vous pouvez agrandir sa taille afin d'y stocker un volume plus important de données.

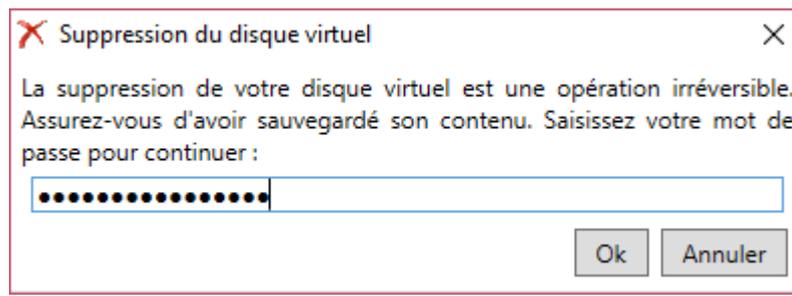


En déplaçant le curseur, vous augmentez la capacité de stockage du disque virtuel.

Cette opération est irréversible. Vous ne pourrez plus réduire la taille de ce disque virtuel.

Suppression du disque virtuel*

La suppression du disque virtuel entraîne la perte des fichiers qui y sont stockés.



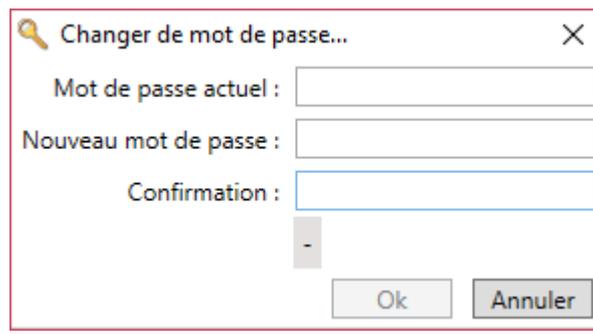
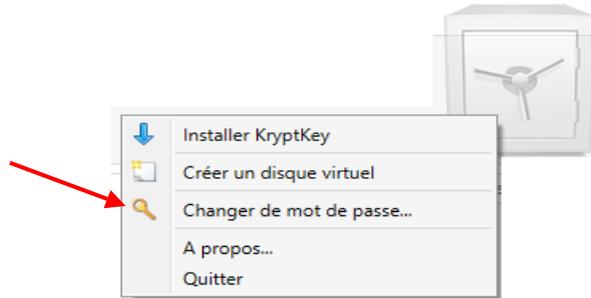
* Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir de KryptKey Essential et KryptKey II Essential, il faut d'acheter en ligne la mise à jour à partir du Menu KryptKey / A propos.

Gestion du mot de passe

Changement de mot de passe

Cette opération nécessite une connexion Internet. Elle ne concerne pas le mot de passe de la fonction **Email sécurisé**.

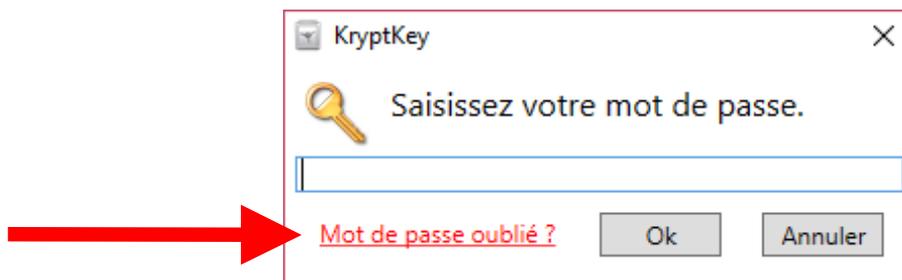
Un mot de passe efficace fait au moins 8 caractères, contient des minuscules, des majuscules et au moins un chiffre et un caractère spécial par exemple !, :, @,%, \$



Saisissez votre mot de passe actuel.

Saisissez votre nouveau mot de passe et confirmez-le.

Mot de passe oublié





Lancez le lien contenu dans le mail que vous avez reçu à l'adresse mail que vous avez fournie lors de l'activation de votre KryptKey.



Vous recevez alors un mail avec un nouveau mot de passe.
Relancez MyDreamKey.exe en saisissant ce mot de passe attribué.
Procédez ensuite à son changement.

PERTE DE VOTRE CLE KRYPTKEY

Si vous avez perdu ou si vous vous êtes fait voler votre KryptKey, contactez-nous à partir du lien suivant <http://www.mdkolutions.com/sav/>, ou bien en envoyant un mail à contact@mdksolutions.com.

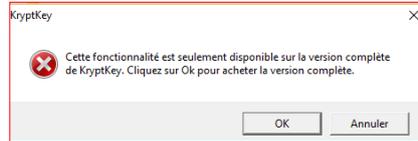
Après nous être assuré que vous étiez bien le possesseur de la KryptKey (question/réponse secrètes), nous vous adressons une nouvelle clé qui est identique à celle perdue (clône avec la même clé de chiffrement) contre un montant de 30 € HT pour le modèle 16 Go ou 50 € HT pour le modèle 64 Go.

Cette nouvelle KryptKey vous permettra d'accéder à l'ensemble de vos fichiers chiffrés et à votre disque virtuel.

Nous vous conseillons de procéder au changement de mot de passe de votre nouvelle clé.

DEBRIDAGE DE VOTRE CLE KRYPTKEY Essential EN CLE KRYPTKEY

KryptKey Essential et KryptKey II Essential peuvent être 'débridées' pour avoir accès à l'ensemble des fonctionnalités de KryptKey (stockage sécurisé sur tous supports, gestion d'un disque virtuel, ...).



Pour cela, répondez OK à la fenêtre précédente, vous accédez alors au site Internet de MDK Solutions et à l'achat en ligne de Kryptkey depuis KryptKey Essential.



(*) Ces fonctionnalités ne sont disponibles que sur les versions KryptKey et KryptKey II PRO. Pour y accéder à partir de KryptKey Essential et KryptKey II Essential, il faut d'acheter en ligne la mise à jour à partir du Menu KryptKey / A propos.