

KASPERSKY LAB

---

# **Kaspersky KryptoStorage 1.0**

**Manuel de l'utilisateur**

**KASPERSKY KRYPTOSTORAGE 1.0**

---

# **Manuel de l'utilisateur**

© Kaspersky Lab

<http://www.kaspersky.com>

Date d'édition : Mars 2009

# Table des matières

CHAPITRE 1. INTRODUCTION .....	5
1.1. Composants de Kaspersky KryptoStorage.....	7
1.2. Objets protégés.....	7
1.3. Droits d'accès aux objets protégés.....	8
1.4. Recommandations pour la création de mots de passe.....	9
CHAPITRE 2. INSTALLATION DE KASPERSKY KRYPTOSTORAGE .....	10
2.1. Configuration minimum requise.....	10
2.2. Description de l'installation.....	11
2.3. Gestion des licences.....	13
2.4. Activer une licence à partir d'un code d'activation .....	15
2.5. Mise à jour des versions du produit.....	17
CHAPITRE 3. INTERFACE PRINCIPALE.....	18
3.1. Menu contextuel de l'explorateur.....	18
3.2. Fenêtre principale de Kaspersky KryptoStorage .....	19
CHAPITRE 4. PROTECTION DES DONNÉES. UTILISER LES OBJETS PROTÉGÉS .....	21
4.1. Dossiers protégés .....	21
4.1.1. Création de dossiers.....	22
4.1.2. Utilisations des dossiers protégés .....	24
4.1.3. Connexion des dossiers protégés .....	26
4.1.4. Déconnexion des dossiers protégés .....	26
4.2. Conteneurs protégés .....	27
4.2.1. Création d'un conteneur .....	27
4.2.2. Préparer le conteneur avant de l'utiliser.....	30
4.2.3. Règles de fonctionnement pour les conteneurs.....	30
4.2.4. Connexion du conteneur.....	30
4.2.5. Formatage du conteneur.....	32
4.2.6. Déconnexion du conteneur .....	33
4.2.7. Protection contre la suppression.....	34
4.3. Protection des disques et des supports amovibles .....	34

---

4.3.1. Spécificités pour l'utilisation d'utilitaire de gestion des disques durs .....	36
4.3.2. Chiffrement d'une partition .....	36
4.3.3. Arrêt du chiffrement .....	38
4.3.4. Reprendre le chiffrement.....	39
4.3.5. Revenir à un état non protégé.....	39
4.3.6. Déchiffrement .....	40
4.3.7. Démarrage à partir d'un disque système et/ou de démarrage protégé... 41	
4.3.8. Connexion des partitions et des supports amovibles.....	41
4.3.9. Déconnexion des partitions et des supports amovibles.....	42
4.3.10. Utilitaire de restauration des disques.....	43
4.4. Destruction des objets protégés et non protégés .....	44
CHAPITRE 5. CONFIGURATION DES SERVICES.....	45
CHAPITRE 6. DÉSINSTALLATION DE KASPERSKY KRYPTOSTORAGE .....	48
ANNEXE A. GLOSSAIRE .....	50
ANNEXE B. INFORMATIONS DIVERSES .....	52
B.1. Contacter nous .....	52
B.2. License sur la bibliothèque Windows Installer XML (WiX).....	53

# CHAPITRE 1. INTRODUCTION

Kaspersky KryptoStorage (ci-après Kaspersky KryptoStorage ou « l'application ») est un système de protection cryptographique des données confidentielles se trouvant sur un ordinateur personnel contre les accès non autorisés.

Le système est destiné à protéger les données confidentielles de l'utilisateur contre les accès non autorisés et à éviter une fuite de données lors de la sauvegarde des données utilisateurs par le système d'exploitation sur le disque ou lors d'une destruction partielle des fichiers de l'utilisateur.

Le mécanisme utilisé pour protéger les informations est **le cryptage transparent**.

**Le cryptage transparent** est un mécanisme dans lequel les informations sont sauvegardées dans un objet protégé exclusivement par un chiffrement. Lors d'opérations sur les données d'un objet protégé, celles-ci sont automatiquement déchiffrées dans la mémoire vive lorsque cela est nécessaire, et les données sont automatiquement chiffrées lors de leurs copies dans un objet protégé.

L'algorithme AES qui fonctionne avec une clé de 128 bits est utilisé en tant qu'algorithme de cryptage. Cet algorithme est approuvé par la communauté cryptographique internationale et il est devenu un standard dans la cryptographie. AES est validé par l'Institut national des standards et des technologies des Etats-Unis (Standards and Technology (NIST) Federal Information Processing Standards (FIPS) PUB 197 26/11/2001).

La clé cryptographique est générée à partir du mot de passe défini par l'utilisateur. En raison de cela, il est possible d'imposer des restrictions sur la longueur de ce mot de passe, en raison des exigences légales locales.

Les fonctions principales du Système sont énumérées ci-dessous.

## Protection des données

Le Système permet les opérations suivantes:

- créer des dossiers virtuels protégés dans le système de fichiers NTFS pour stocker des données confidentielles ;
- créer des disques virtuels protégés (conteneurs protégés) pour stocker des données confidentielles.
- protéger toutes les informations contenues sur un disque dur (ou une partition), y compris le système d'exploitation et les sections de démarrage du disque, sur les clés USB, ou tout autre système de stockage amovible;

La protection du disque système assure la confidentialité:

- du contenu de la mémoire vive conservée sur le disque lors de la mise en veille du système d'exploitation;
- des données collectées lors d'une défaillance du système (crash dump) ;
- des données contenues dans les fichiers temporaires et les fichiers d'échange du système ou des applications.

### **Travailler avec les données protégées.**

Le système permet :

- de délimiter l'accès aux informations protégées grâce à un mot de passe personnel;
- de stocker des objets protégés les uns à l'intérieur des autres sans aucune restriction ;
- d'éviter la suppression volontaire ou involontaire des objets protégés en limitant l'accès à ces objets ;
- d'utiliser les dossiers et conteneurs protégés ou les partitions protégées présentées sur l'ordinateur de l'utilisateur ;
- de transférer les données protégées ainsi que l'objet protégé les contenant (dossier, conteneur, partition), sur un autre ordinateur où Kaspersky KryptoStorage est également installé. Ces objets protégés pourront être utilisés sur le nouvel ordinateur;
- de forcer la suppression des fichiers et des dossiers.

# 1.1. Composants de Kaspersky KryptoStorage

Les composants de Kaspersky KryptoStorage sont énumérés dans le tableau.

Composant	Description
Les composants intégrés dans les menus contextuels du système d'exploitation	Création d'objets protégés, actions sur les objets protégés, déconnexion d'un objet protégé, suppression forcée des fichiers et des dossiers.
L'interface principale de Kaspersky KryptoStorage	Activation de l'application, opérations sur les licences, configuration des services de Kaspersky KryptoStorage, création d'objets protégés, restauration de disques protégés
L'aide Kaspersky KryptoStorage	Fichier d'aide au format .CHM

## 1.2. Objets protégés

Par **objets protégés** nous entendons n'importe quels objets, destinés à stocker les données protégées par Kaspersky KryptoStorage.

**Les objets protégés** peuvent être des types suivants.

- **Le dossier protégé** est un dossier spécifique dans le système de fichiers NTFS qui est créé par l'utilisateur à l'aide de Kaspersky KryptoStorage sur son ordinateur. Après avoir connecter le dossier à l'aide de Kaspersky KryptoStorage, ce dossier est alors utilisable comme n'importe quel autre dossier.
- **Le conteneur protégé** est un fichier particulier créé par l'utilisateur à l'aide de Kaspersky KryptoStorage sur son ordinateur. Après la connexion du conteneur à l'aide de Kaspersky KryptoStorage, il est possible de l'utiliser comme un disque dur normal (ou un disque amovible). En outre, les conteneurs peuvent être copiés, gravés sur des CD et des DVD, envoyés par email, transférés vers un autre ordinateur sur lequel Kaspersky KryptoStorage est installé. Cela sans avoir à déconnecter le conteneur au préalable.

- **La partition protégée (disque logique)** est obtenue par voie de transformation (le cryptage) au moyen de Kaspersky KryptoStorage des partitions existantes sur le disque dur incluant les données qui y sont installées. La protection des sections système et/ou de démarrage est également possible, ainsi que celle des installations de type Mass Storage (Flash-accumulateurs, dispositifs de sauvegarde USB et autres). Après l'activation de la section protégée au moyen de Kaspersky KryptoStorage, la possibilité de travailler avec elle comme avec une section ordinaire apparaît.

**Important !**

Après la création de l'objet protégé, toutes les données qui y seront incluses seront automatiquement protégées, à savoir cryptées. Pendant la copie des données de l'objet protégé dans une zone non protégée, les données seront placées dans la zone non protégée sous forme décryptée (non protégée).

## 1.3. Droits d'accès aux objets protégés

Afin de préserver les objets protégés des actions non autorisées, l'accès s'effectue uniquement après l'autorisation de l'utilisateur.

L'autorisation est exigée lors de l'exécution des opérations suivantes:

- Connexion des objets protégés;
- Changement du mot de passe;
- Désactivation de la protection, le lancement ou l'arrêt du processus de chiffrement ou déchiffrement, restauration d'un disque protégée (partition).

Pour une l'autorisation par l'utilisateur, il faut saisir le mot de passe défini pour l'objet en question.

**Remarque :**

Si l'utilisateur a saisi un mot de passe incorrect (par exemple, lors de l'oubli du mot de passe), l'application avertit alors l'utilisateur du refus d'accès à l'objet et affiche également l'indice de mot de passe si il a été défini lors de la création de l'objet.



## 1.4. Recommandations pour la création de mots de passe

L'accès à tous les objets protégés s'effectue uniquement l'autorisation de l'utilisateur. Le mot de passe est le paramètre obligatoire pour l'autorisation. Voici les conseils à suivre pour définir un nouveau mot de passe:

- le mot de passe doit contenir au moins sept caractères;
- dans la composition du mot de passe, il est possible d'utiliser des chiffres, des lettres, des espaces, ainsi que des caractères spéciaux (« . », « , », « ? », « ! », « < », « > », « " » etc...);
- il est recommandé lors de la création d'un mot de passe d'utiliser au minimum des chiffres, des lettres majuscules et minuscules.

Ce qu'il faut éviter lors de la création d'un mot de passe:

- des mots communs et des locutions;
- des suites de caractères suivant le positionnement des touches du clavier, par exemple : *azerty*, *123456789*, etc.
- des données personnelles : noms et prénoms, adresses, numéro de carte d'identité, de téléphone, etc.
- également, il est déconseillé d'utiliser des mots de passe déjà utilisés pour d'autres programmes (courrier électronique, site web, etc.).

### Important !

En cas de perte de mot de passe, il sera alors impossible de restaurer les informations contenus dans un objet protégé!

Il est possible de définir un indice pour se souvenir du mot de passe. L'indice correspond à une phrase qui est affichée dans un champ spécifique et qui peut être défini lors de la création du mot de passe. Si vous avez défini cet indice, il sera affiché automatiquement par l'application après une erreur de saisie du mot de passe. L'indice doit contenir des informations qui vous permettront de vous souvenir du mot de passe.

### Important !

Lors de la création de l'indice de mot de passe, il faut bien prendre en compte que quiconque tentant d'accéder à vos données protégées aura accès à cet indice. Pour cela, l'indice ne doit pas contenir d'informations trop directes permettant de reconnaître votre mot de passe.

# CHAPITRE 2. INSTALLATION DE KASPERSKY KRYPTOSTORAGE

Cette section contient les informations sur les conditions de configuration matérielle et logicielle requises. Elle contient aussi la description de l'installation, de la mise à jour du produit et de la gestion des licences.

## 2.1. Configuration minimum requisite

Pour que Kaspersky KryptoStorage puisse fonctionner normalement, l'ordinateur doit répondre aux exigences de configuration matérielle et logicielles suivantes:

### Configuration matérielle minimum requisite:

- processeur Intel Celeron 1 GHz minimum ou plus;
- 256 Mo de mémoire vive disponible;
- 10 Mo d'espace libre du disque pour l'installation des applications.

### Configuration logicielle minimum requisite:

- L'un des systèmes d'exploitation suivants:
  - Microsoft Windows 2000 Server Service Pack 4;
  - Microsoft Windows 2000 Professional Service Pack 4;
  - Microsoft Windows XP (Service Pack 2);
  - Microsoft Windows Vista (Service Pack 1);
  - Microsoft Windows 7.

Kaspersky KryptoStorage supportent aussi bien les plateformes x86 (32 bits) et x64 (64 bits).

## 2.2. Description de l'installation

### Important !

Pour l'installation de Kaspersky KryptoStorage, les droits de l'administrateur local de l'ordinateur sont nécessaires.

L'installation de l'application se déroule sous la forme d'un assistant d'installation. Chaque fenêtre contient une série de boutons permettant d'agir le processus d'installation :

- **Suivant** : exécute l'action et passe à l'étape suivante de l'installation.
- **Précédent** : revient à l'étape précédente de l'installation.
- **Annuler** : annule l'installation du logiciel.

Chacune des étapes de la procédure d'installation de l'application est présentée en détail ci-dessous.

### Etape 1. Début de l'installation

Installez le CD d'installation Kaspersky KryptoStorage dans le lecteur de CD ou exécutez vous-même le fichier d'installation `kksVVVfr.exe`.

VVV correspondant à la version du logiciel.

### Remarque :

Les utilisateurs peuvent télécharger les mises à jour de Kaspersky KryptoStorage à l'adresse suivante : <http://www.kaspersky.com/fr/downloads>.

Après cela, la fenêtre de bienvenue de l'assistant d'installation **Kaspersky KryptoStorage** s'ouvre.

Cliquez sur le bouton **Suivant** pour continuer l'installation. Ou cliquez sur le bouton **Annuler** pour annuler l'installation.

### Etape 2. Validation du contrat de licence.

Après avoir pris connaissance du contrat de licence, cochez la case adéquate pour l'accepter et cliquez sur le bouton **Suivant**.

### Etape 3. Choix du répertoire d'installation

Le chemin vers le répertoire dans lequel Kaspersky KryptoStorage sera installé est indiqué dans le champ **Dossier de destination** de la fenêtre.

Il est possible de modifier le répertoire d'installation par défaut en cliquant sur le bouton **Modifier...** et en sélectionnant le répertoire d'installation souhaité.

Pour continuer l'installation, cliquez sur le bouton **Suivant**.

## Etape 4. Fin de l'installation

A l'étape **Programme prêt pour l'installation**, cliquez sur le bouton **Installer** pour commencer l'installation de Kaspersky KryptoStorage.

Suivez les dernières indications de l'assistant pour terminer l'installation de Kaspersky KryptoStorage.

A la fin de l'installation, il vous sera proposé d'activer le logiciel. Vous pouvez choisir une des possibilités suivantes :

- Activer la version d'évaluation de 30 jours.
- Activer la version complète.

Pour l'activation de la version complète, il est nécessaire d'avoir et d'installer la licence à partir du code d'activation. Les informations détaillées sur la licence et l'activation se trouve au paragraphe 2.4 p. 15.

Après avoir sélectionné le mode d'activation, cliquez sur le bouton **Suivant**.

Pour terminer l'installation du logiciel, il est nécessaire de redémarrer l'ordinateur. Une notification à cet effet vous proposera de redémarrer l'ordinateur après l'installation.

### **Important !**

N'arrêtez pas l'ordinateur pendant le redémarrage (pendant que Microsoft Windows est en train de s'arrêter). Cela pourrait provoquer une erreur lors du redémarrage du système d'exploitation.

Si cela se produit, alors cliquez sur le bouton **F8** pendant le redémarrage du système d'exploitation. Ensuite, depuis le menu Démarrage, choisissez la commande **Chargement de la dernière bonne configuration connue**. Enfin, installez à nouveau Kaspersky KryptoStorage.

## 2.3. Gestion des licences

Afin de bénéficier de tous les avantages qu'offre le logiciel Kaspersky KryptoStorage, il faut obtenir et enregistrer une licence commerciale.

### Remarque :

L'activation de la licence d'évaluation (Trial) permet pendant une durée de 30 jours d'utiliser pleinement les fonctionnalités de Kaspersky KryptoStorage. Les mots de passe sont limités à un caractère durant cette période.

A l'expiration de la licence (peu importe son type), les fonctionnalités du produit sont alors limitées. L'utilisateur garde la possibilité d'utiliser normalement les objets (protégés) déjà créés. Notamment, d'accéder aux données et de décrypter ses données. Cependant, il ne pourra pas créer de nouveaux objets protégés, ni contacter le support technique.

Vous pouvez accéder à la fenêtre de gestion des licences à partir de la fenêtre principale de Kaspersky KryptoStorage.

### Pour ouvrir la fenêtre des licences de Kaspersky KryptoStorage,

1. Dans le menu **Démarrer**, choisissez **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.
2. Dans la fenêtre ouverte, cliquez sur le bouton **Licences**.

La fenêtre des **Licences** apparaît alors (voir image 1).

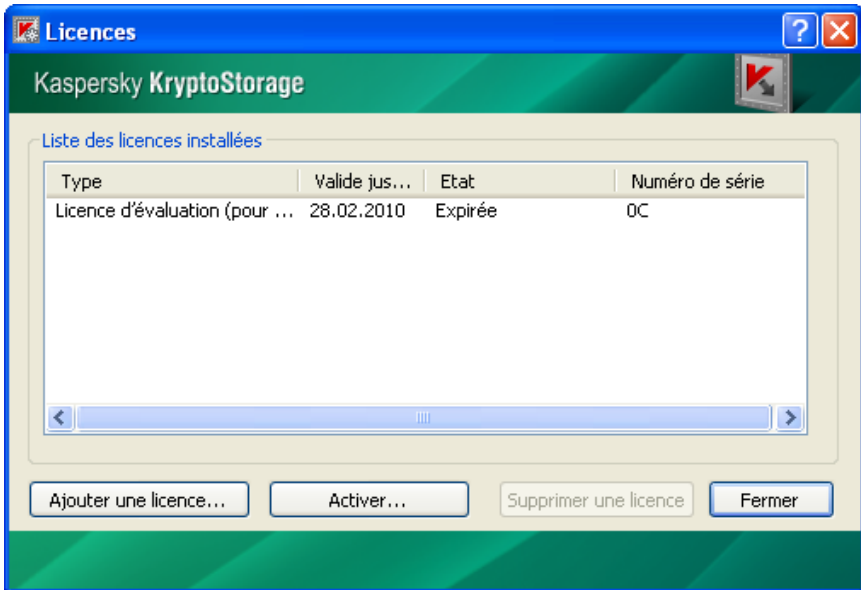


Image 1. Licences

Cette fenêtre présente la liste des licences installées, avec son type, son numéro de série, son statut actuel et sa période de validité pour chaque licence.

Pour ajouter une licence au format fichier, il faut utiliser le bouton **Ajouter une licence**. Dans la fenêtre de dialogue, indiquez le chemin vers le fichier de licence et cliquez sur le bouton **Ouvrir**.

**Remarque :**

La licence ajoutée doit être délivrée au même utilisateur que les autres licences de la liste ; dans le cas contraire, l'ajout de licence sera impossible.

Pour supprimer une licence de la liste, sélectionnez-la et cliquez sur le bouton **Supprimer une licence**.

**Remarque :**

La licence d'évaluation (Trial) ne peut pas être supprimée de la liste des licences installées.

**Important !**

Ne supprimez pas une licence encore valide de la liste des licences. Les fonctionnalités du produit pourraient alors être limitées comme après l'échéance d'une licence.

Pour activer une licence à partir d'un code d'activation, cliquez sur le bouton **Activer**. La procédure d'activation de la licence à partir du code d'activation est expliqué au paragraphe 2.4 p. 15.

Pour fermer la fenêtre, cliquez sur le bouton **Fermer**.

## 2.4. Activer une licence à partir d'un code d'activation

L'utilisation du code d'activation pour l'activation des licences est possible à la fin de l'installation du logiciel, ou à partir de la fenêtre de gestion des licences (voir paragraphe 2.3 p. 13).

**Important !**

Pour activer une licence à partir du code d'activation, l'ordinateur doit posséder une connexion Internet.

Pour activer la licence, entrez le code, composé de cinq blocs de cinq caractères chacun, dans la fenêtre d'activation du logiciel (voir image 2). Le code est composé de chiffres (à l'exception du zéro) et de lettres majuscules.

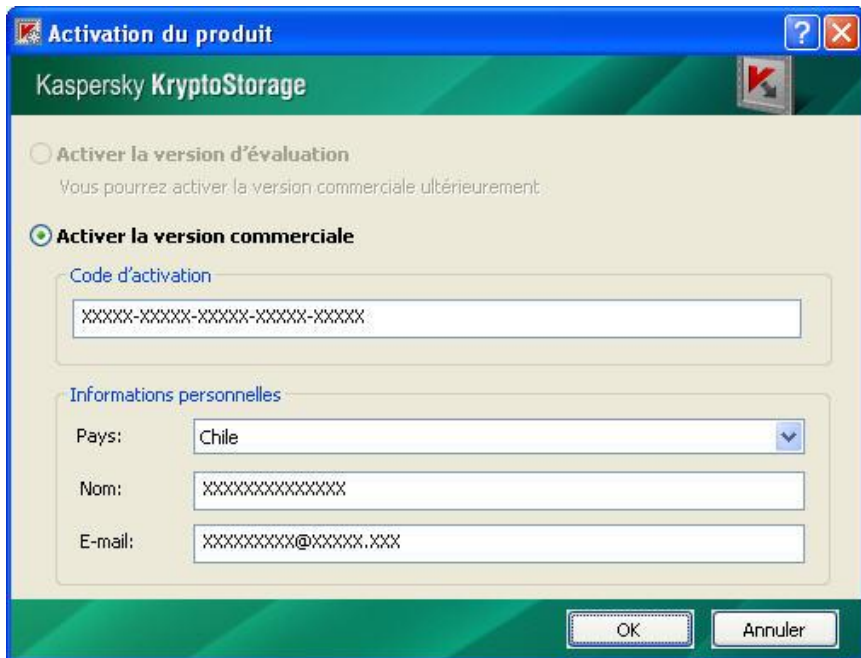


Image 2. Activation du produit.

Précisez ensuite votre pays de résidence ainsi que votre nom et votre adresse email. Cliquez sur le bouton **OK**.

L'activation de la licence se déroulera alors automatiquement.

**Important !**

Une activation est autorisée pour chaque code d'activation. Ne divulguez pas le code d'activation de votre produit.

Vous pouvez copier le fichier de la licence reçu sur un support externe. Cette copie pourra être nécessaire pour la restauration du système après un bug.



## 2.5. Mise à jour des versions du produit

Les utilisateurs peuvent télécharger les mises à jour de Kaspersky KryptoStorage à l'adresse suivante : <http://www.kaspersky.com/fr/downloads>.

Pour effectuer la mise à jour du produit, exécutez simplement le programme d'installation de la nouvelle version.

**Remarque :**

Une nouvelle version du produit ne peut pas être installée par dessus une ancienne version. Il faut d'abord désinstaller l'ancienne version avant d'installer la nouvelle (voir Chapitre 6 p. 48).

# CHAPITRE 3. INTERFACE PRINCIPALE

La section ci-après contient la description de l'interface principale de l'application.

## 3.1. Menu contextuel de l'explorateur

L'accès aux fonctions de l'application s'effectue à travers un menu contextuel dans l'explorateur de fichiers de Microsoft Windows.

**Pour ouvrir le menu Kaspersky KryptoStorage:**

1. Choisissez l'objet nécessaire (dossier, conteneur, partition) et cliquez sur le bouton droit de la souris.
2. Choisissez dans le menu contextuel ainsi ouvert le menu **Kaspersky KryptoStorage** (voir image 3).

Ce menu contient un sous-menu dont la liste dépend du type de l'objet et de l'état de l'objet en question (connecté/déconnecté).

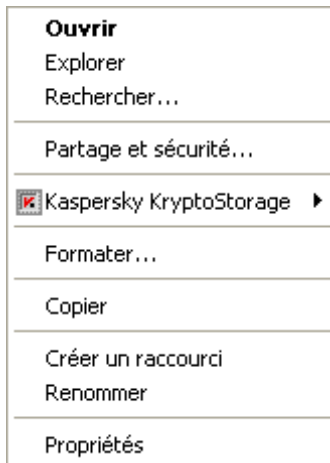


Image 3. Menu Kaspersky KryptoStorage

### Pour créer un dossier ou un conteneur protégé,

Cliquez avec le bouton droit de la souris dans une quelconque partie libre d'un dossier ouvert ou du bureau, et choisissez ensuite la commande **Créer ► Dossier Kaspersky KryptoStorage** ou **Créer ► Conteneur Kaspersky KryptoStorage** dans le menu contextuel.

## 3.2. Fenêtre principale de Kaspersky KryptoStorage

### Pour ouvrir la fenêtre principale de Kaspersky KryptoStorage,

dans le menu **Démarrer**, choisissez **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.

La fenêtre de Kaspersky KryptoStorage s'ouvrira alors (image 4).

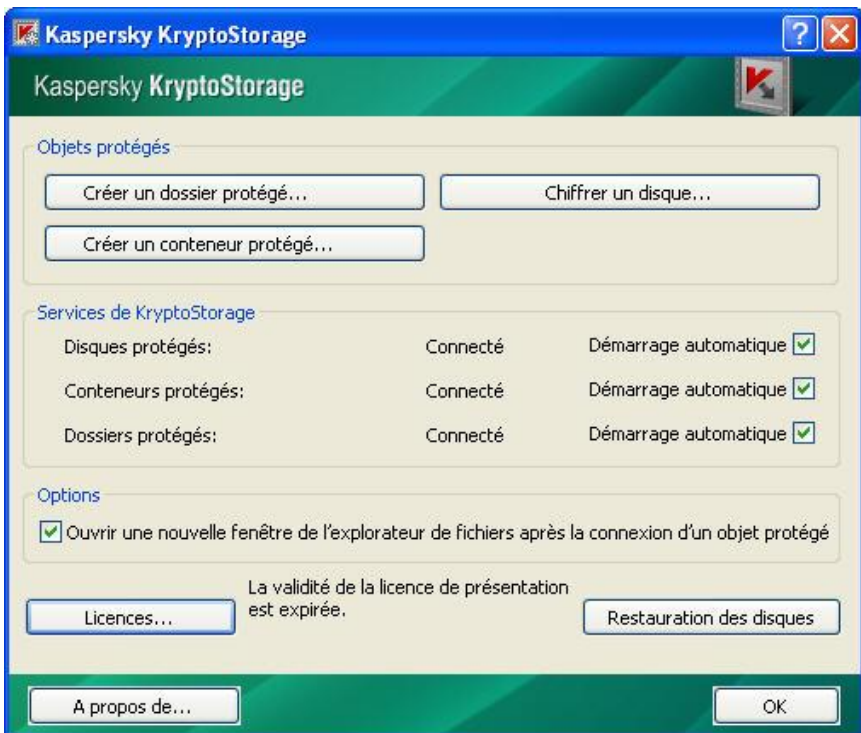


Image 4. Fenêtre principale

Le programme permet les actions suivantes:

- Création de dossiers protégés (voir paragraphe 4.1.1 p. 22)
- Création de conteneurs protégés (voir paragraphe 4.2.1 p. 27)
- Chiffrement d'un disque (partition) (voir paragraphe 4.3.2 p. 36)
- Configuration des services (voir Chapitre 5 p. 45)
- Possibilité d'ouvrir l'objet après la connexion dans une nouvelle fenêtre de l'explorateur de fichier.
- Gestion des licences, activation (voir paragraphe 2.3 p. 13)
- Restauration des disques (partitions) (voir paragraphe 4.3.10 p. 43)

# CHAPITRE 4. PROTECTION DES DONNEES. UTILISER LES OBJETS PROTEGES

Le chapitre ci-après décrit le fonctionnement des objets protégés suivants:

- Dossiers protégés (voir paragraphe 4.1 p. 21)
- Conteneurs protégés (voir paragraphe 4.2 p. 27)
- Disques (partitions) et supports amovibles chiffrés (voir paragraphe 4.3 p. 34).

## 4.1. Dossiers protégés

Conditions de création d'un dossier protégé:

- Si le service de Kaspersky KryptoStorage *Dossiers protégés* (voir Chapitre 5 p. 45) est démarré sur l'ordinateur, le fonctionnement des dossiers protégés est alors possible. Par défaut, le service est démarré.
- Le matériel (disque dur ou support amovible) sur lequel le dossier protégé est créé ne doit pas être protégé contre l'écriture. L'utilisateur créant le dossier protégé doit posséder les droits en ce qui concerne la création du dossier.
- Le dossier protégé ne peut être créé que dans un système de fichiers NTFS.
- Il ne peut pas être créé dans un dossier protégé Kaspersky KryptoStorage existant.
- Il ne peut pas être créé dans un dossier protégé par EFS (système de cryptage de données faisant partie de Microsoft Windows).
- La longueur du nom du dossier ne doit pas dépasser 255 caractères.

## 4.1.1. Création de dossiers

### Important !

Avant de commencer, prenez connaissance des contraintes pour la création de dossiers protégés (paragraphe 4.1 p. 21).

Un dossier protégé peut être créé sur un disque dur ou sur un support amovible. En outre, le dossier protégé peut être créé à l'intérieur d'un autre objet protégé (disque chiffré ou conteneur protégé).

### Remarque :

Si le dossier est créé à l'intérieur d'un autre objet protégé, celui doit être connecté avant l'opération.

### Pour créer un dossier protégé:

1. Exécutez l'une des opérations suivantes:
  - Cliquez avec le bouton droit de la souris dans une quelconque partie libre d'un dossier ouvert ou du bureau, et choisissez ensuite la commande **Créer ► Fichier Kaspersky KryptoStorage** dans le menu contextuel ouvert.
  - Ouvrez la fenêtre Kaspersky KryptoStorage, en allant dans **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**, et dans la fenêtre ouverte, utilisez le bouton **Créer un fichier protégé**.

La fenêtre de dialogue suivante sera alors affichée à l'écran: **Création d'un dossier protégé** (voir image 5).

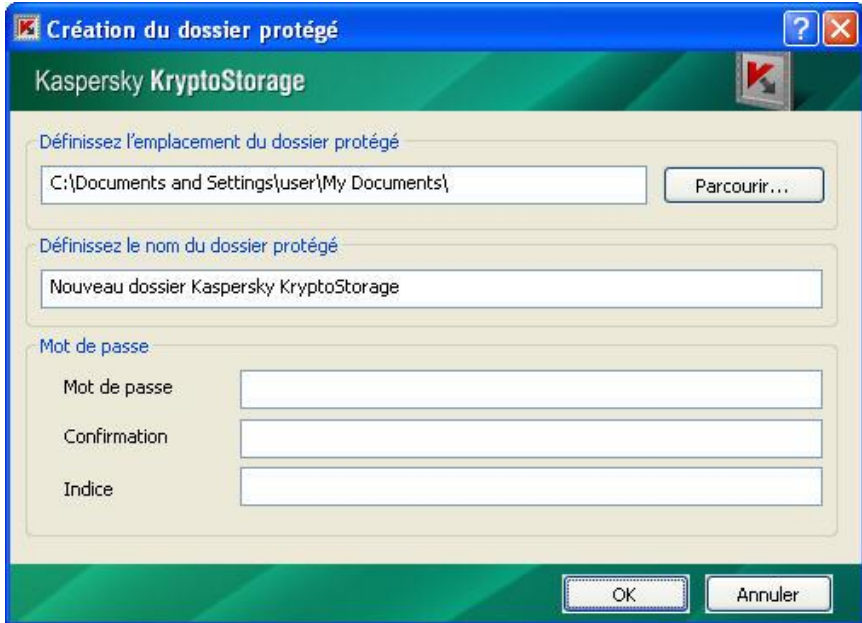


Image 5. Création d'un dossier protégé

2. Indiquez les paramètres du dossier protégé en cours de création:

- **Choix du dossier.** Il faut indiquer le dossier dans lequel le dossier protégé sera placé. Par défaut, si le dossier protégé est créé par le menu contextuel de l'explorateur de fichiers, le dossier choisi est celui dans lequel le menu est ouvert. Si le dossier protégé est créé dans la fenêtre principale, alors le dossier **Mes documents** est choisi par défaut. Il est possible de modifier l'emplacement de ce dossier.
- **Nom du dossier protégé.** Il faut indiquer le nom du dossier protégé.

**Remarque :**

Vous pouvez changer les noms des dossiers protégés grâce au système d'exploitation.

- **Mot de passe, Confirmation du mot de passe, Indice pour le mot de passe.** Indiquez le mot de passe et l'indice de mot de passe (optionnel). Ces paramètres seront utilisés lors des accès au dossier.

**Remarque :**

Les recommandations pour la création du mot de passe sont présentées dans le paragraphe 1.4 p. 9.

3. Quand tous les paramètres nécessaires sont indiqués, cliquez sur le bouton **OK**.

Le dossier protégé est alors créé. Après sa création, le dossier se trouve dans un état connecté ; il est alors prêt pour son utilisation.

## 4.1.2. Utilisations des dossiers protégés

Pour utiliser les dossiers protégés, il est nécessaire de prendre les points suivants en considération:

- Tous les fichiers et les dossiers qui se trouvent à l'intérieur du dossier protégé sont chiffrés et demeurent protégés.
- L'exécution de n'importe quelles actions (lecture, écriture, changement de nom, archivage, suppression, etc.) concernant le dossier protégé n'est possible qu'après la connexion de ce dossier.
- Le dossier connecté est accessible à tous les utilisateurs et à tous les programmes qui peuvent s'exécuter localement sur l'ordinateur au nom de l'utilisateur courant. L'accès vers les dossiers protégés par le réseau est interdit par l'application.

**Remarque :**

Il est recommandé de déconnecter le dossier protégé après avoir fini de l'utiliser.

- Les fichiers et les dossiers sont protégés uniquement par les objets dans lesquels ils se trouvent.

**Remarque :**

Les fichiers ou dossiers copiés en dehors d'un objet protégé ne sont pas protégés par l'application.

- Le système ne permet pas d'accomplir les actions suivantes avec les dossiers protégés et leur contenu : supprimer vers la corbeille, déplacer des fichiers et des dossiers à l'intérieur d'un objet protégé.



**Remarque :**

Si l'on essaye de déplacer un dossier contenant des fichiers, le dossier initial restera intact. Dans le dossier protégé cible, un dossier du même nom sera créé et protégé.

Certains gestionnaires de fichiers, par exemple Total Commander, peuvent lors du déplacement des fichiers et des dossiers utiliser la copie avec suppression ultérieure des objets initiaux. Dans ce cas, un déplacement est possible et les fichiers déplacés, ainsi que les dossiers bénéficient d'une protection pour les objets dans lesquels ils se trouvent.

- Il est possible de déplacer un dossier non protégé contenant un dossier protégé dans un autre dossier non protégé. Dans ce cas, le dossier protégé ne doit pas être connecté.
- Un dossier non protégé contenant un dossier protégé peut être déplacé dans la corbeille si le dossier protégé est attaché.

**Remarque :**

Il est possible de supprimer ou de restaurer un dossier protégé déplacé dans la corbeille. Lors de la restauration, tous les objets protégés de ce dossier seront connectés. Après redémarrage de l'ordinateur ou après la fermeture de la session, il est impossible de supprimer le dossier placé dans la corbeille, mais il est possible de le restaurer. Lors de la restauration, tous les objets protégés de ce dossier seront déconnectés. Dans les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7, après le redémarrage ou la fermeture de la session, la suppression ou la restauration du dossier en dehors de la corbeille restent possibles.

Total Commander ne peut pas accomplir le déplacement d'un tel dossier vers la corbeille.

### 4.1.3. Connexion des dossiers protégés

Les opérations (lecture, écriture, changement de nom, copie, suppression, etc...) avec un dossier protégé ne sont possibles que si le dossier est connecté.

**Pour connecter un dossier:**

1. Sélectionnez le dossier à connecter.
2. Cliquez avec le bouton droit de la souris sur le dossier sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Connecter le dossier**.
3. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le mot de passe pour accéder au contenu protégé du dossier.
4. Cliquez sur le bouton **OK**.

### 4.1.4. Déconnexion des dossiers protégés

Après avoir déconnecté le dossier protégé, il devient impossible de l'utiliser de quelque manière que ce soit, jusqu'à ce qu'il soit reconnecté.

#### **Important !**

**Avant de déconnecter le dossier, il est impératif de fermer toutes les applications pouvant utiliser des fichiers ou des dossiers contenus dans le dossier protégé. Certaines applications peuvent conserver un accès exclusif aux données même après avoir fini de les utiliser.**

**Pour déconnecter un dossier protégé:**

1. Sélectionnez le dossier protégé à déconnecter
2. Cliquez avec le bouton droit de la souris sur l'objet sélectionné, et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Déconnecter le dossier**.

Si vous souhaitez déconnecter plusieurs objets protégés simultanément, cela peut réclamer un peu plus de temps. Pourtant dans certains cas, il peut être nécessaire de déconnecter tous les objets protégés simultanément. Dans ce cas, il est préférable de redémarrer l'ordinateur (après avoir sauvegardé les changements effectués). Une fois l'ordinateur redémarré, tous les objets protégés seront déconnectés. On peut également déconnecter tous les dossiers protégés en fermant la session.

## 4.2. Conteneurs protégés

Le composant (disque dur ou support amovible), sur lequel le conteneur protégé est créé, ne doit pas être protégé en écriture. L'utilisateur, créant le conteneur protégé, doit posséder les droits de création des fichiers.

La création des conteneurs protégés sur les disques CD/DVD n'est pas prise en charge. Néanmoins, ces supports peuvent être utilisés pour la sauvegarde de conteneurs existants.

Les actions sur les conteneurs protégés ne sont possibles que sur un ordinateur sur lequel l'application Kaspersky KryptoStorage est installé et pour lequel le service suivant est démarré: *Conteneurs protégés*.

### 4.2.1. Création d'un conteneur

#### Important !

Avant de commencer, prenez connaissance des contraintes pour la création des conteneurs protégés, décrites dans l'art. 4.2 p. 27.

Le conteneur protégé peut être créé sur le disque dur ou sur un support amovible. Egalement, le conteneur protégé peut être créé à l'intérieur d'un autre objet protégé (disque chiffré (partition), dossiers ou conteneur protégé).

#### Remarque :

Si le conteneur est créé à l'intérieur d'un autre objet protégé, cet objet doit être connecté avant la création.

#### Pour créer un conteneur:

1. Procédez d'une des manières suivantes:
  - Cliquez avec le bouton droit de la souris dans une quelconque partie libre d'un dossier ouvert ou du bureau, et choisissez ensuite la commande **Créer ► Conteneur Kaspersky KryptoStorage** dans le menu contextuel ouvert.

- Ouvrez Kaspersky KryptoStorage en choisissant dans le menu **Démarrer** l'option **Tous les programmes** ► **Kaspersky KryptoStorage** ► **Kaspersky KryptoStorage**. Dans la fenêtre ouverte, utilisez le bouton **Créer un conteneur protégé**.

La fenêtre de dialogue suivante sera alors affichée à l'écran : **Création d'un conteneur protégé** (voir image 6).

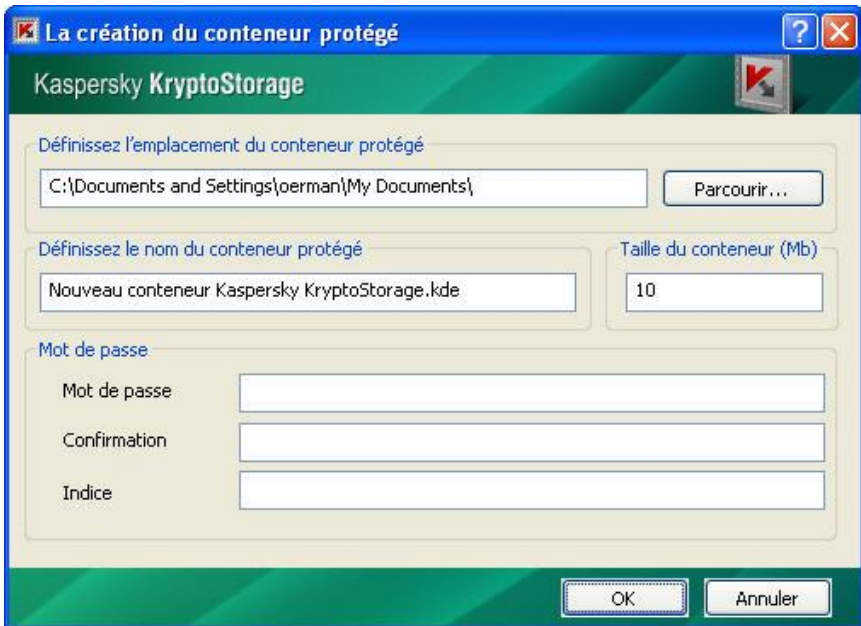



Image 6. Création d'un conteneur protégé

## 2. Définissez les paramètres du conteneur protégé à créer:

- **Sélection du dossier.** Il faut indiquer le dossier, dans lequel le conteneur protégé sera placé. Par défaut, si le conteneur protégé est créé à partir du menu contextuel de l'explorateur de fichiers, le dossier sélectionné est celui dans lequel le menu a été ouvert. Si le conteneur protégé est créé à partir de la fenêtre principale, alors le conteneur sera placé par défaut dans Mes Documents. Il est possible de modifier l'emplacement du conteneur en cliquant sur le bouton **Parcourir**.
- **Nom du conteneur protégé.** Nom et extension du fichier correspondant au conteneur protégé.

Par défaut, le nom du fichier du conteneur porte l'extension `.kde` (pendant l'installation de Kaspersky KryptoStorage, les fichiers avec une telle extension sont enregistrés dans le système d'exploitation comme Conteneurs Kaspersky KryptoStorage). Dans le système d'exploitation, ces fichiers sont reconnaissable avec l'icône .

Si à la place de `.kde` une extension non enregistrée dans le système d'exploitation est indiquée, alors le fichier du conteneur sera marqué comme fichier de type inconnu.

**Remarque :**

La connexion des conteneurs portant l'extension `.kde` possède certaines différences avec la connexion de conteneurs portant une autre extension (voir paragraphe 4.2.4 p. 30).

Après la création, vous pourrez changer les noms et les extensions des conteneurs grâce à la fonction **Renommer** de Windows.

- **Taille du conteneur.** Taille souhaitée pour le conteneur en mégaoctets.
- **Mot de passe, Confirmation du mot de passe, Indice pour le mot de passe.** Définissez le mot de passe pour l'accès au conteneur protégé et l'indice de mot de passe (optionnel). Ces paramètres seront utilisés pour accéder au conteneur.

**Remarque :**

Les recommandations pour la création du mot de passe sont présentées dans le paragraphe 1.4 p. 9.

3. Une fois tous les paramètres nécessaires définis, cliquez sur le bouton **OK**.

Après la création du conteneur protégé, il vous sera proposé de le connecter (voir paragraphe 4.2.4 p. 30) et de le reformater (voir paragraphe 4.2.5 p. 32).

## 4.2.2. Préparer le conteneur avant de l'utiliser

Avant de pouvoir utiliser le conteneur, il est nécessaire de le formater. Pour cela:

1. Connecter le conteneur (voir paragraphe 4.2.4 p. 30)
2. Formater le lecteur auquel est connecté le conteneur protégé (voir paragraphe 4.2.5 p. 32).

## 4.2.3. Règles de fonctionnement pour les conteneurs

Il est nécessaire de connecter le conteneur pour pouvoir l'utiliser.

### **Important !**

La connexion et l'utilisation des conteneurs protégés n'est possible que sur un ordinateur sur lequel Kaspersky KryptoStorage est installé et si le service *Conteneurs protégés* est lancé.

Lorsque le conteneur est connecté, il n'est plus protégé et est accessible à tous les utilisateurs, ayant accès à l'ordinateur. Pour cette raison, il est recommandé de le déconnecter après avoir fini de l'utiliser.

Lorsque vous utilisez un conteneur, n'oubliez pas que tous les fichiers et dossiers qu'il contient sont chiffrés et donc protégés également. Cependant, si vous déplacez des objets en dehors du conteneur, ils ne seront plus protégés.


## 4.2.4. Connexion du conteneur

Vous ne pouvez utiliser le container ou les fichiers qu'il contient qu'après l'avoir connecté.

**Pour connecter un conteneur protégé:**

1. Sélectionnez le conteneur protégé.
2. Cliquez avec le bouton droit de la souris sur le conteneur sélectionné et dans le menu contextuel, choisissez l'option **Kaspersky KryptoStorage**  
▶ **Connecter le conteneur.**

**Remarque :**

Si le conteneur possède l'extension `.kde` (avec l'icône ) , vous pouvez connecter le conteneur en double-cliquant simplement dessus..

3. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le mot de passe pour accéder au conteneur protégé.
4. Puis cliquez sur le bouton **OK**.

La fenêtre de dialogue suivante sera alors affichée à l'écran : **Paramètres du conteneur** (voir image 7).

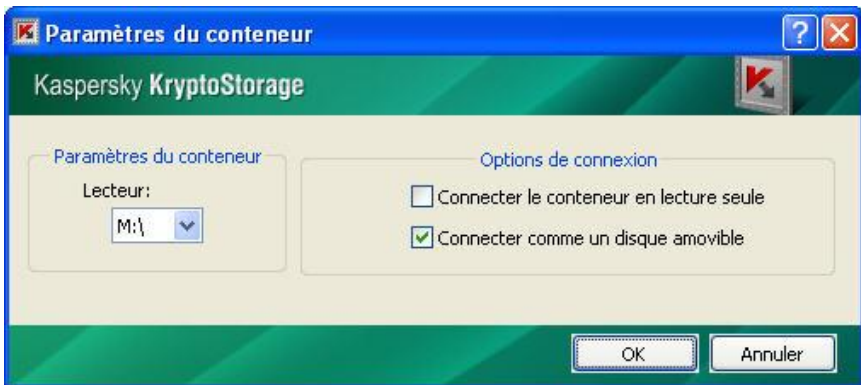


Image 7. Configuration des paramètres du conteneur protégé

5. Dans la fenêtre de dialogue ouverte, indiquez les paramètres souhaités pour la connexion:
  - **Lecteur.** Choisissez la lettre du lecteur pour conteneur protégé. Le conteneur est connecté comme un disque dur (on peut utiliser n'importe quelle lettre de lecteur libre).
  - **Options de connexion.** Spécifiez les options additionnelles de connexion du conteneur protégé :
    - **Lecture seule.** Si la case est cochée, tout le contenu du conteneur protégé sera accessible en lecture seule uniquement. L'écriture et la suppression des données seront impossible.

**Remarque :**

La case sera automatiquement cochée si le fichier du conteneur est déjà en *Lecture seule*.

Microsoft Windows 2000 ne permet pas d'utiliser le mode *Lecture seule* avec les conteneurs formatés en NTFS.

- **Connecter comme un disque amovible.** Par défaut, le conteneur protégé est connecté comme un disque amovible (affiché dans la liste des périphériques amovible dans le **Poste de travail**). Toutefois, si la case n'est pas cochée, il sera connecté comme un disque dur (affiché dans la liste des disques durs dans le **Poste de travail**).

6. Une fois terminé, cliquez sur le bouton **OK**.

Lors de la connexion à un conteneur non formaté, vous serez invité à le formater (voir paragraphe 4.2.5 p. 32).

## 4.2.5. Formatage du conteneur

**Important !**

Pendant le formatage du disque auquel le conteneur protégé est connecté, toutes les données stockées dans ce conteneur seront supprimées.

L'utilisateur peut formater le conteneur connecté de la même manière qu'un disque standard. Le formatage est effectué avec les commandes standard de Microsoft Windows. Lors de la configuration, les paramètres suivants du formatage doivent être pris en compte:

- Avec Microsoft Windows 2000, pour que le conteneur soit formaté en FAT et FAT32, il faut le connecter en tant que disque amovible (lors de la connexion, cochez la case **Connecter comme un disque amovible**).
- Lors d'un formatage complet, le fichier du conteneur protégé aura la taille indiquée au moment de la création de ce conteneur.
- Lors d'un formatage rapide et en choisissant FAT ou FAT32, le fichier du conteneur protégé aura la taille minimale, et augmentera au fur et à mesure du remplissage du conteneur (ce qui permet d'économiser l'espace sur le disque).
- Lors d'un formatage rapide du conteneur en NTFS, le fichier du conteneur protégé aura la taille indiquée au moment de la création de ce conteneur.



**Remarque :**

Quel que soit le type du formatage, la taille du conteneur protégé en tant que disque virtuel sera toujours égale à la taille choisie au moment de la création du conteneur, seule la taille du fichier du conteneur peut changer.

**Important !**

Lors de l'utilisation du conteneur, il est possible que l'espace libre du conteneur devienne insuffisant. Dans ce cas, il vous sera proposé de sauvegarder les données à un autre emplacement. Si l'emplacement sur lequel il vous est proposé de sauvegarder les données n'est pas protégé, alors les données sauvegardées ne seront pas non plus protégées. Si vous les déplacez vers un autre objet protégé, les données resteront protégées.

## 4.2.6. Déconnexion du conteneur

Avant la déconnexion du conteneur protégé, il faut s'assurer que qu'aucune action n'est en cours avec les éléments qu'il contient.

**Pour déconnecter le conteneur protégé:**

1. Sélectionnez le disque correspondant au conteneur protégé ou bien le fichier du conteneur protégé.
2. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Déconnecter le conteneur**.

Si vous souhaitez déconnecter plusieurs objets protégés simultanément, cela peut réclamer un peu plus de temps. Pourtant dans certains cas, il peut être nécessaire de déconnecter tous les objets protégés simultanément. Dans ce cas, il est préférable de redémarrer l'ordinateur (après avoir sauvegardé les changements effectués). Une fois l'ordinateur redémarré, tous les objets protégés seront déconnectés. On peut également déconnecter tous les conteneurs protégés en fermant la session.

## 4.2.7. Protection contre la suppression

Etant donné que le conteneur protégé est un fichier ordinaire, il peut être supprimé par n'importe quel utilisateur. On peut éviter une suppression non souhaitée du conteneur protégé en plaçant le fichier du conteneur dans un dossier protégé ou sur un disque protégé.

### **Important !**

Ce type de protection nécessite que l'application Kaspersky KryptoStorage soit installée.

## 4.3. Protection des disques et des supports amovibles

Vous pouvez protéger n'importe quel type de partition d'un disque dur (y compris les partitions système et de démarrage), ainsi que les autres types de stockage externe.

Les partitions protégées et les supports amovibles protégés ont les particularités suivantes:

- Si vous protégez la partition système et/ou de démarrage, vous devez d'abord autoriser le chargement du système d'exploitation pour accéder au volume (voir le graphique 4.3.7 p. 41).
- Egalement, la protection de la partition système par Kaspersky KryptoStorage assure également la protection des fichiers de vidages mémoire (crash dump), ainsi que le contenu de la mémoire vive enregistrée sur le disque système lors du passage en veille. La protection de la partition système permet de prévenir contre la fuite de données confidentielles à travers les informations système conservées sur le disque dur.
- Le service *Disques protégés* de Kaspersky KryptoStorage doit être démarré pour pouvoir utiliser une partition ou un disque protégé (voir chapitre 5 p. 45). Si le service est arrêté, l'accès aux informations est impossible. Le système d'exploitation présentera cette partition comme étant non formatée ou contenant des erreurs. Si une partition système et/ou de démarrage du disque est protégée, alors il sera impossible d'arrêter le service *Disques protégés*.

- Il est déconseillé d'utiliser Kaspersky KryptoStorage sur des ordinateurs ayant plusieurs systèmes d'exploitation et de protéger les partitions du disque nécessaires pour le chargement des systèmes d'exploitation installés.
- Les données de l'application sur toutes les partitions protégées d'un support physique (disque dur, mémoire Flash, etc.), se trouvent à la racine de la première partition du support physique dans le fichier `iwcs.bin`. En cas de formatage de la partition contenant `iwcs.bin`, ou en cas de suppression ou corruption de `iwcs.bin`, l'accès à toutes les partitions protégées du support sera perdu. Si le service *Disques protégés* de Kaspersky KryptoStorage est démarré l'application protégera le fichier `iwcs.bin` des suppressions et des modifications. Pour cette raison, l'arrêt du service *Disques protégés* est vivement déconseillé. Si le formatage de la partition contenant `iwcs.bin` est nécessaire, il faut préalablement supprimer la protection de toutes les partitions du disque.

Les limitations pour la protection des partitions et des supports amovibles :

- La taille des partitions doit être au moins de 512 octets pour pouvoir être chiffrées (taille standard des partitions pour la plupart des supports de ce type).
- Le chiffrement des partitions dynamique n'est pas pris en charge.
- La protection peut être utilisée uniquement sur les disques locaux. La protection des disques de réseau n'est pas prise en charge.
- On ne peut pas lancer simultanément des opérations de chiffrement/déchiffrement pour plusieurs partitions d'un même disque physique. Mais cela est possible avec les partitions de disques différents.
- La protection de la partition du disque sur laquelle Kaspersky KryptoStorage est installé n'est possible que si cette partition est la partition système et/ou de démarrage.
- Le chiffrement est autorisé si le volume chiffré a les droit d'écriture.
- Lancer le chiffrement d'un disque amovible est possible que si il n'est utilisé par aucun programme. L'utilisation du disque est possible pendant le chiffrement.
- Dans Windows 7, lors de la connexion physique des supports amovibles protégés, le système d'exploitation prévient que le support n'est pas formaté et que son accès ne sera pas possible qu'après l'avoir connecté avec l'application (cf. p. 4.3.8 p. 41).

- L'application ne prend pas en charge la protection des CD/DVD. Néanmoins, on peut graver un conteneur protégé sur un CD/ DVD (voir paragraphe 4.2 p. 27).

### 4.3.1. Spécificités pour l'utilisation d'utilitaire de gestion des disques durs

Certains utilitaires permettent de changer les tailles des partitions du disque dur. Ne changez pas les tailles des partitions protégées par Kaspersky KryptoStorage. Cela peut provoquer la perte de données.

Si vous devez réaliser absolument cette opération, supprimez la protection des partitions avant de procéder au changement de la taille de la partition.

### 4.3.2. Chiffrement d'une partition

#### **Important !**

Avant de commencer, prenez connaissance des spécificités pour la protection des partitions et des supports amovibles (voir paragraphe 4.2 p. 27).

Le chiffrement des partitions et des supports amovibles sont accompli en tâche de fond. C'est pourquoi vous pouvez continuer à utiliser l'ordinateur pendant cette opération.

En cas de nécessité, le processus de chiffrement peut être interrompu (voir paragraphe 4.3.3 p. 38). Il est également possible de le reprendre plus tard (voir paragraphe 4.3.4 p. 39), ou de l'annuler (voir paragraphe 4.3.5 p. 39).

#### **Remarque :**

La mise en veille de l'ordinateur interrompt le chiffrement. A la sortie de la mise en veille, vous pouvez reprendre l'opération ou l'annuler.

#### **Pour chiffrer une partition ou un support amovible:**

1. Exécutez l'une des opérations suivantes:
  - Sélectionnez dans l'explorateur de la partition ou le support amovible à protéger. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Chiffrer le disque**.

- Ouvrez Kaspersky KryptoStorage, à partir du menu **Démarrer**. Choisissez **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**. Dans la fenêtre ouverte, cliquez sur le bouton **Chiffrer un disque...**, choisissez le disque à protéger et cliquez sur **OK**.

La fenêtre de dialogue suivante sera alors affichée à l'écran : **Chiffrement du disque** (voir image 8).

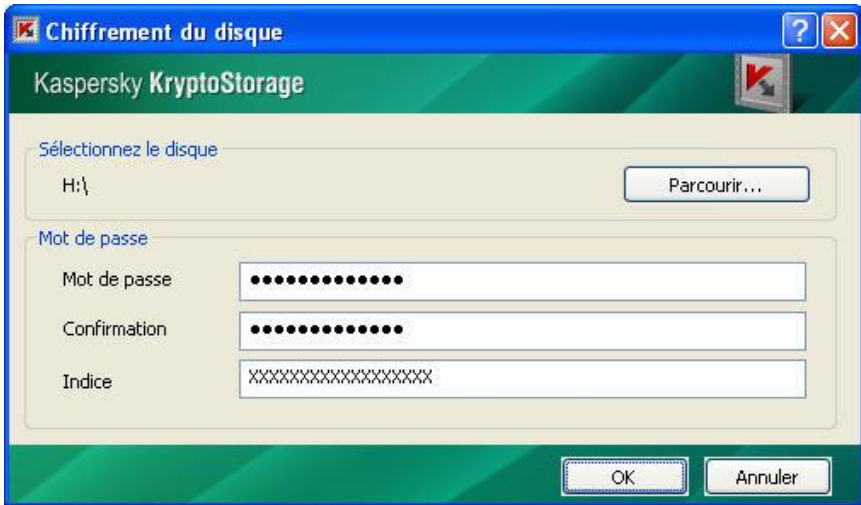


Image 8. Protection d'un disque logique

2. Dans cette fenêtre, indiquez les paramètres du disque à protéger:
  - **Sélection du disque.** Sélectionnez le disque à protéger en cliquant sur le bouton **Parcourir...**
  - **Mot de passe, Confirmation, Indice.** Spécifiez un mot de passe pour l'accès au disque protégé et un indice de mot de passe (optionnel). Ces paramètres seront utilisés lors de l'accès au disque.

**Remarque :**

Les recommandations pour la création du mot de passe sont présentées dans le paragraphe 1.4 p. 9.

3. Une fois terminé, cliquez sur le bouton **OK**.

Après cela, le chiffrement du disque démarre. A partir de ce moment, le disque logique (le support amovible) devient un objet protégé.

**Important !**

Si vous chiffrez la partition système ou de démarrage, vous devrez autoriser l'accès avant de démarrer le système (voir le paragraphe 4.3.7 p. 41). Le contrôle de l'autorisation s'effectue à chaque démarrage, à la sortie de mise en veille.

### 4.3.3. Arrêt du chiffrement

Pendant le chiffrement du disque, vous pouvez avoir besoin de l'interrompre manuellement ou il peut s'interrompre automatiquement (par exemple, lors d'un arrêt inattendu de l'ordinateur). Vous pourrez reprendre le chiffrement plus tard.

**Important !**

Le disque (le support amovible) est un objet protégé indépendamment du fait que le chiffrement soit réalisé entièrement ou partiellement. C'est pourquoi même si le chiffrement était interrompu, l'utilisation du disque sera possible uniquement après la connexion. De plus, si le chiffrement n'est pas terminé, certaines informations de la partition ne seront pas protégées.

**Pour interrompre l'installation de la protection:**

1. Sélectionnez l'objet en cours de chiffrement.
2. Exécutez l'une des actions suivantes:
  - Cliquez sur le bouton **Arrêt** dans la fenêtre de dialogue dans laquelle la progression de l'installation de la protection apparaît.
  - Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Arrêter le chiffrement**.
3. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le **Mot de passe** pour accéder à l'objet protégé. Puis cliquez sur le bouton **OK**.

Après cela, le chiffrement sera interrompu. Le disque protégé (le support amovible) reste connecté, et vous pouvez continuer à l'utiliser.

## 4.3.4. Reprendre le chiffrement

L'objet sera correctement protégé qu'une fois le chiffrement terminé. Si le chiffrement a été interrompu pour une raison quelconque, une partie du contenu restera non protégée.

### Pour reprendre le chiffrement:

1. Sélectionnez l'objet dont le chiffrement a été interrompu.
2. Connectez l'objet protégé si nécessaire (voir paragraphe 4.3.8 p. 41).
3. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez option **Kaspersky KryptoStorage ► Reprendre le chiffrement du disque**.
4. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le **Mot de passe** pour accéder à l'objet protégé. Puis cliquez sur le bouton **OK**.

Après cela, le chiffrement reprend. Le disque protégé (le support amovible) reste connecté, et il est toujours possible de l'utiliser.

## 4.3.5. Revenir à un état non protégé

Si l'installation de la protection a été interrompue, on peut refuser de reprendre le chiffrement et revenir à un état non protégé.

### Pour revenir à un état non protégé:

1. Sélectionnez l'objet dont le chiffrement a été interrompu.
2. Connectez l'objet protégé si nécessaire (voir paragraphe 4.3.8 p. 41).
3. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Annuler le chiffrement**.
4. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le **Nom** et le **Mot de passe** du propriétaire de l'objet protégé. Puis cliquez sur le bouton **OK**.

Après cela, l'annulation du chiffrement démarre. Le disque protégé (le support amovible) reste connecté, utilisable.

## 4.3.6. Déchiffrement

Le déchiffrement n'est possible que si le disque est connecté (voir paragraphe 4.3.8 p. 41).

### Remarque :

Il n'est possible que de déchiffrer une seule partition d'un disque à la fois. Si plusieurs partitions doivent être déchiffrées, vous devez les faire une par une.

### Pour déchiffrer un disque:

1. Sélectionnez l'objet à déchiffrer.
2. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Déchiffrer le disque**.
3. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le **Mot de passe** pour accéder à l'objet protégé. Puis cliquez sur le bouton **OK**.

Le déchiffrement de la partition ou du support amovible s'effectue en tâche de fond. En conséquence, il est possible d'utiliser le disque pendant l'opération.

Si cela est nécessaire, le déchiffrement peut être interrompu. L'interruption du déchiffrement se réalise de la même manière que pour le chiffrement (voir paragraphe 4.3.3 p. 38).

La reprise du déchiffrement peut se faire ultérieurement. L'annulation est similaire à l'annulation du chiffrement (voir paragraphe 4.3.4 p. 39).

En outre, il est possible de refuser le décryptage et revenir à l'état précédent. La procédure d'interruption du processus de décryptage s'accomplit de la même manière que la procédure d'interruption du cryptage (voir paragraphe 4.3.5 p. 39). Après le refus du décryptage, l'objet se retrouvera dans un état protégé.



### 4.3.7. Démarrage à partir d'un disque système et/ou de démarrage protégé

Si le disque système et/ou le disque de démarrage sont protégés par Kaspersky KryptoStorage, alors le chargement du système d'exploitation installé sur ce disque n'est possible seulement qu'après la connexion du disque protégé. Pour la connexion du disque protégé, il est nécessaire de passer par l'autorisation effectuée avant le chargement du système d'exploitation.

**Pour connecter le disque système et/ou le disque de démarrage protégé :**

Indiquez le **Mot de passe** : le mot de passe de la partition protégée.

**Remarque :**

Si sur votre ordinateur, les partitions système et de démarrage se trouvent sur différents disques et que les deux partitions sont protégées, il est nécessaire de connecter chacune de ces partitions.

Ensuite, après l'autorisation positive de l'utilisateur le système d'exploitation pourra démarrer.

**Remarque :**

Si au moment de l'autorisation, un mot de passe incorrect est saisi, un avertissement sera présenté à l'écran et l'indice de mot de passe sera affiché si il a été défini à la création du mot de passe. Vous pourrez alors saisir à nouveau le mot de passe. Si l'application ne vous propose pas de saisir une nouvelle fois le mot de passe, il faut redémarrer l'ordinateur en utilisant la combinaison de touches <CTRL+ALT+DEL>.

### 4.3.8. Connexion des partitions et des supports amovibles

Les opérations (lecture, écriture, changement de nom, copie, suppression, etc.) avec tout disque protégé ne sont possibles qu'à condition que l'objet soit connecté.

**Pour connecter la partition ou le support amovible :**

1. Sélectionnez le disque protégé à connecter.

2. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Connecter le disque**.
3. Dans la fenêtre de dialogue qui s'est ouverte, saisissez le mot de passe pour accéder au disque protégé. Puis cliquez sur le bouton **OK**.

Lorsque l'objet est connecté, il n'est plus protégé et est accessible à tous les utilisateurs, ayant accès à l'ordinateur. Pour cette raison, il est recommandé de le déconnecter après avoir fini de l'utiliser.

## 4.3.9. Déconnexion des partitions et des supports amovibles

Après la déconnexion, il devient impossible d'utiliser le disque ou les informations qu'il contient avant qu'il soit reconnecté.

### **Important !**

**Avant de déconnecter un objet, il est nécessaire de sauvegarder toutes les modifications et de fermer les applications utilisant l'objet.**

### **Pour déconnecter le partition ou le support amovible :**

1. Sélectionnez l'objet protégé (la partition ou le support amovible).
2. Cliquez avec le bouton droit de la souris sur le disque sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Déconnecter le disque**.

Si vous déconnectez plusieurs objets simultanément, l'opération pourra prendre plus de temps. Cependant, dans certains cas, il peut être nécessaire de déconnecter tous les objets rapidement. A cette fin, on peut redémarrer l'ordinateur (après avoir sauvegardé les changements effectués). Après le redémarrage de l'ordinateur, tous les objets protégés seront déconnectés.

## 4.3.10. Utilitaire de restauration des disques

### Important !

Les droits d'administrateur local de l'ordinateur sont nécessaires pour utiliser cet utilitaire.

Dans Kaspersky KryptoStorage, on peut utiliser l'outil qui permet de libérer de l'espace sur les disques durs, les clés USB, ou autres stockages externes protégés par Kaspersky KryptoStorage et dont l'accès ne peut être rétabli.

Vous pouvez avoir besoin de supprimer des données d'un disque protégé sans les déchiffrer dans les cas suivants :

- Vous avez perdu le mot de passe d'accès au disque protégé et donc la connexion est impossible.
- Le disque a été formaté sans utiliser le service *Disque protégé* de Kaspersky KryptoStorage. Par conséquent, toutes les données de ce secteur ont été perdues, mais l'application à conserver les informations de protection du disque.
- La taille de la partition protégée a été changée (voir paragraphe 4.3.1 p. 36). En conséquence, il y a une différence entre la taille réelle de la partition et celle reconnue par l'application.

Vous ne pouvez pas réaliser l'opération citée ci-dessus si l'application Kaspersky KryptoStorage est installée. Et l'espace supplémentaire alloué à la partition n'est pas utilisable. L'utilitaire de restauration des disques permet de rendre utilisable dans Kaspersky KryptoStorage ce nouvel espace alloué.

Avant de commencer, procédez comme-suit :

1. Terminez toutes les opérations de chiffrement ou de déchiffrement du disque en question.
2. Déconnectez toutes les partitions protégées pour lesquelles vous voulez supprimer des informations à l'aide de l'utilitaire.

### Important !

Faites bien attention lorsque vous sélectionnez un disque protégé. Après la suppression des informations de protection du disque, il sera impossible de récupérer les données déchiffrées à partir de celui-ci. De la même manière, si le disque est chiffré, il apparaît non formaté.

**Pour libérer l'espace utiliser par un disque protégé:**

1. Ouvrez Kaspersky KryptoStorage. Pour cela, à partir du menu **Démarrer**, choisissez **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.
2. Cliquez sur le bouton **Utilitaire de restauration des disques** dans la fenêtre de Kaspersky KryptoStorage
3. Dans la fenêtre **Utilitaire de restauration des disques**, choisissez le disque dont les données de l'application doivent être supprimées du disque. Puis, cliquez dessus avec le bouton droit de la souris et dans le menu contextuel, choisissez l'option **Supprimer les informations de protection**.

## 4.4. Destruction des objets protégés et non protégés

Les fichiers et les dossiers supprimés par la voie habituelle peuvent par la suite être restaurés à l'aide d'utilitaire spécifique. Par conséquent, les informations se trouvant dans l'objet supprimé peuvent être accessibles à certaines personnes non souhaitées. On peut régler ce problème par la destruction de l'objet.

La fonction de destruction est accessible aux objets protégés ou non.

### **Important !**

Lors de la destruction d'un dossier, l'intégralité de son contenu est supprimée.

Un dossier protégé ne peut être détruit que lorsqu'il est connecté.

Un conteneur protégé ne peut être détruit que lorsqu'il est déconnecté.

**Pour supprimer un fichier ou un dossier et garantir l'impossibilité de restauration ultérieure:**

1. Sélectionnez l'objet (le fichier, le dossier ou le conteneur protégé) qu'il faut supprimer.
2. Cliquez avec le bouton droit de la souris sur l'objet sélectionné et dans le menu contextuel qui s'ouvre, choisissez l'option **Kaspersky KryptoStorage ► Détruire**.
3. Dans la fenêtre qui s'ouvre, à la question concernant la suppression, cliquez sur le bouton **Oui**.

# CHAPITRE 5. CONFIGURATION DES SERVICES

Kaspersky KryptoStorage inclut trois services permettant chacun de prendre en charge un type d'objet donné. Les services sont détaillés ci dessous.

Sous-système	Destination
Disques protégés	Protection des partitions et des supports amovibles
Conteneurs protégés	Création de conteneurs protégés et gestion de ces conteneurs protégés
Dossiers protégés	Création de dossiers protégés et gestion de ces dossiers protégés

La configuration des services faisant partie de Kaspersky KryptoStorage est accessible dans l'interface principale de **Kaspersky KryptoStorage**.

Pour ouvrir **Kaspersky KryptoStorage** à partir du menu **Démarrer**, choisissez **Tous les programmes ► Kaspersky KryptoStorage ► Kaspersky KryptoStorage**.

Ensuite, vous trouverez détaillé les options sur les services Kaspersky KryptoStorage sur la fenêtre principale (voir image 9).

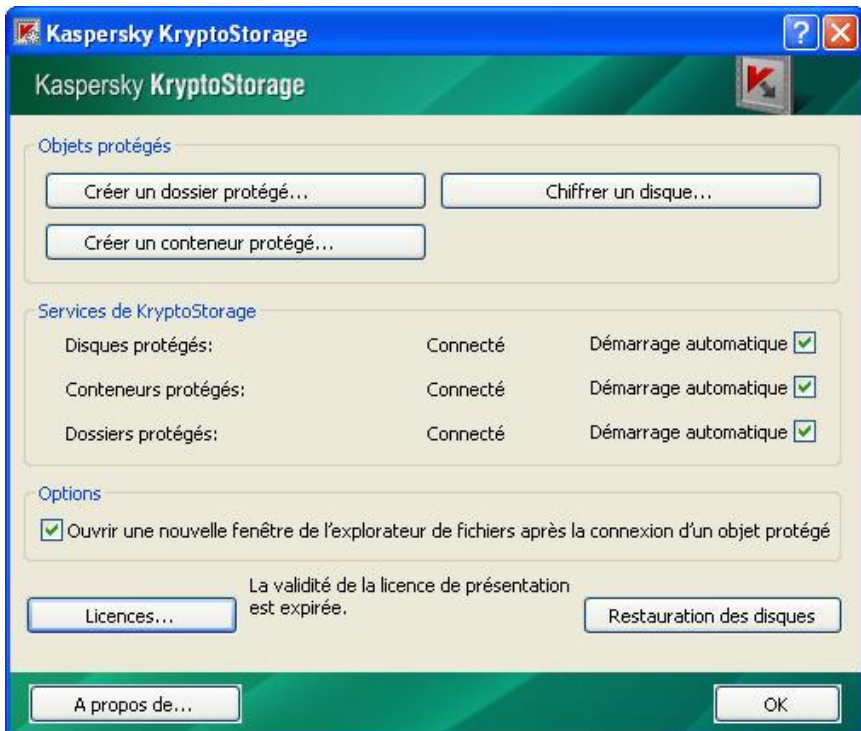


Image 9. Configuration des services de Kaspersky KryptoStorage

À droite du nom de chaque service est placée l'option **Démarrage automatique**. L'option cochée dans ce champ précis signifie que le démarrage automatique du service est activé.

Après l'installation de Kaspersky KryptoStorage, tous les services sont configurés pour démarrer automatiquement. Néanmoins, on peut changer les paramètres de démarrage automatique du service:

- désactivez le démarrage automatique en cochant la case **Démarrage automatique** ;
- activez le démarrage automatique en cochant la case **Démarrage automatique**.

#### Remarque :

Les paramétrages liés au démarrage automatique des services sont pris en compte seulement après le redémarrage de l'ordinateur.

Lors de la désactivation du démarrage automatique des services, il est nécessaire de prendre en considération les particularités du fonctionnement des services Kaspersky KryptoStorage. Dans le tableau ci-après, les conséquences de la désactivation pour chaque service sont décrites.

Service	Résultat de la désactivation du service
Disques protégés	<p>Le système d'exploitation identifie les disques protégés comme non formatés. Le contenu est chiffré.</p> <p>Les fonctions de l'application sont inaccessibles pour les opérations sur les partitions et sur les supports amovibles.</p> <p><b>Remarque :</b> Il est impossible de désactiver le service si la partition système et/ou de démarrage est protégée.</p>
Conteneurs protégés	<p>L'accès vers le contenu des conteneurs protégés est impossible. Le contenu est chiffré.</p> <p>Les fonctions de l'application pour l'utilisation des conteneurs protégés sont inaccessibles</p>
Dossiers protégés	<p>Les dossiers protégés et les fichiers leur appartenant peuvent être supprimés de votre ordinateur par n'importe quel utilisateur.</p> <p>Le contenu des fichiers est chiffré, il demeure possible de voir la structure des sous-dossiers.</p> <p>Les fonctions de l'application pour utiliser les fichiers et les dossiers protégés sont inaccessibles.</p>

# CHAPITRE 6. DESINSTALLATION DE KASPERSKY KRYPTOSTORAGE

La désinstallation de Kaspersky KryptoStorage signifie que tous les services pour tout type d'objets protégés seront supprimés (voir chapitre 5 p. 45) :

- Les dossiers protégés et les fichiers qu'ils contiennent peuvent être supprimés de votre ordinateur par n'importe quel utilisateur. Le contenu des fichiers reste chiffré, il demeure possible de voir la structure des sous-dossiers.
- Les conteneurs restent chiffrés, et il devient impossible de les connecter pour voir leur contenu.
- La protection établie pour les partitions et les supports amovibles reste présente. Mais il ne sera plus possible d'accéder aux données contenues dans ces objets.

## **Important !**

Ces objets seront vus comme non formatés par le système d'exploitation et lorsque vous essayerez d'y accéder, il sera proposé d'effectuer un formatage. Pendant le formatage de l'objet, toutes les données seront perdues. C'est pourquoi, si l'objet contient des informations importantes pour vous, il est nécessaire de refuser le formatage.

Il n'est pas possible de supprimer l'application, si la partition système et/ou de démarrage sont protégées. Puisque dans ce cas, le chargement du système d'exploitation et, par conséquent, l'accès aux données se trouvant sur ce disque, sera impossible.

Préalablement à la désinstallation de l'application vous devez :

- Supprimer la protection de la partition système et/ou de démarrage, des disques non-système et des supports amovibles.
- Connectez les conteneurs protégés et les dossiers, et copiez le contenu dans des dossiers non protégés dans un emplacement non protégé.

## **Important !**

Pour la désinstallation de Kaspersky KryptoStorage, les droits de l'administrateur local de l'ordinateur sont nécessaires.



La désinstallation de Kaspersky KryptoStorage se fait avec les fonctions standard de Microsoft Windows.

**Pour supprimer Kaspersky KryptoStorage:**

1. Ouvrez le menu **Installation et suppression des programmes**. Pour cela, à partir du menu **Démarrer**, choisissez **Paramètres ► Panneau de configuration**. Dans la fenêtre Panneau de configuration, double-cliquez sur l'icône **Ajout/suppression des programmes**.
2. Dans la fenêtre **Ajout/suppression des programmes**, sélectionnez **Kaspersky KryptoStorage** et cliquez sur le bouton **Supprimer**.

Pour terminer la désinstallation de l'application, il faut redémarrer l'ordinateur.

# ANNEXE A. GLOSSAIRE

## **Kaspersky KryptoStorage**

Application destinée à la protection cryptographique des données confidentielles sur l'ordinateur de l'utilisateur contre un accès non autorisé.

## **Destruction de l'objet**

C'est une fonction de destruction des fichiers et des dossiers qui supprime non seulement l'objet, mais efface également son contenu..

## **Protection des informations**

Mesures pour la restriction de l'accès aux informations par les utilisateurs.

## **Conteneur protégé**

Fichier d'un format spécifique, qui est géré par l'application comme un disque virtuel. Les données sont stockées dans ce fichier.

## **Objet protégé**

Par objets protégés, nous entendons n'importe quels objets destinés à stocker des données protégées par Kaspersky KryptoStorage.

## **Données confidentielles**

Données dont l'accès est limité. Les données confidentielles ne sont accessibles qu'aux utilisateurs pour lesquels ils sont destinés.

## **Mot de passe**

Suite de caractères utilisés pour l'accès au contenu d'un objet protégé. L'utilisateur doit garder son mot de passe secret.

**Cryptage transparent**

Le cryptage transparent est un mécanisme qui permet de stocker des informations chiffrées à l'intérieur d'objet chiffré. Les données protégées sont gérées ainsi : elles sont automatiquement déchiffrées en mémoire, et lors de l'enregistrement elles sont automatiquement chiffrées.

# ANNEXE B. INFORMATIONS DIVERSES

## B.1. Contacter nous

Si vous avez des questions, des commentaires, ou des suggestions, nous vous invitons à nous les communiquer.

Si vous avez acheté Kaspersky KryptoStorage, vous pouvez contacter les experts du service d'assistance technique par téléphone ou par Internet afin d'obtenir des informations sur cette application.

<b>Support technique</b>	<b>Base de connaissance:</b> <a href="http://support.kaspersky.com/fr/">http://support.kaspersky.com/fr/</a> <b>Pour contacter le support technique:</b> <a href="https://my.kaspersky.com/fr/">https://my.kaspersky.com/fr/</a>
Informations générales	WWW: <a href="http://www.kaspersky.fr">http://www.kaspersky.fr</a> <a href="http://www.viruslist.com/fr/">http://www.viruslist.com/fr/</a> <a href="http://www.kaspersky.com/fr/contacts">http://www.kaspersky.com/fr/contacts</a>

## B.2. License sur la bibliothèque Windows Installer XML (WiX)

L'annexe ci-après contient le texte de la licence sur la bibliothèque Windows Installer XML (WiX) 2.0 Copyright (c) 2005-2008 Microsoft Corporation.

### Remarque:

Le texte de la licence est présenté également sur le lien suivant : <http://www.opensource.org/licenses/cpl1.0.php>.

### Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

### 3. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
  - i) changes to the Program, and
  - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

#### 4. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

#### 5. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

- i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;
- ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;
- iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and
- iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

- a) it must be made available under this Agreement; and
- b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

## 6. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

## 7. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.



## **8. DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## **9. GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.