**Veracrypt : Comment crypter ses données facilement ?**

1. **Un mot sur le chiffrement :**

Qu’est ce qu’on entend par chiffrement ? Le chiffrement désigne la pratique consistant à coder et décoder des données. Des données chiffrées sont des données qui ont été codées à l'aide d'un algorithme de sorte qu'elles ne se présentent plus sous leur forme d'origine et ne soient donc plus lisibles. En termes simples, le chiffrement consiste donc à protéger les fichiers dans le but de ne les montrer qu’aux personnes concernées.

1. **Présentation de Veracrypt**
   1. **Historique**

VeraCrypt est un utilitaire sous licence [libre](https://fr.wikipedia.org/wiki/Logiciel_libre" \o "Logiciel libre) utilisé pour le chiffrement et la dissimulation des fichiers et dossiers sensibles. Il a pour objectif principal de sécuriser vos données.

Il a été développé par la société française IDRIX et permet de créer un [disque virtuel](https://fr.wikipedia.org/wiki/Disque_virtuel" \o "Disque virtuel) chiffré dans un fichier ou une partition. L'ensemble du dispositif de stockage demande une [authentification](https://fr.wikipedia.org/wiki/Authentification" \o "Authentification) avant de [monter](https://fr.wikipedia.org/wiki/Point_de_montage" \o "Point de montage) le disque virtuel.

VeraCrypt est un [fork](https://fr.wikipedia.org/wiki/Fork_(d%C3%A9veloppement_logiciel)" \o "Fork (développement logiciel)) qui a été initialement publié le 22 juin 2013 pour faire suite au projet [TrueCrypt](https://fr.wikipedia.org/wiki/TrueCrypt" \o "TrueCrypt) interrompu subitement quelques mois plus tard. Selon ses développeurs, des suspicions sur l'origine de plusieurs failles de sécurité ont été soulevées à la suite d’un [audit](https://fr.wikipedia.org/wiki/Audit_de_s%C3%A9curit%C3%A9" \o "Audit de sécurité) du [code source](https://fr.wikipedia.org/wiki/Code_source" \o "Code source) de TrueCrypt. Elles ont donné lieu à des améliorations de sécurité mises en œuvre dans sa dernière version.

* 1. **Systèmes d’Exploitation compatibles :**

Voici les systèmes d’exploitation compatibles avec Veracrypt.

* Compatibilité Mac OS X  10.6 à 10.10
* Compatibilité Windows XP à 8.1 en 32 et 64 bits
* Compatibilité Linux kernel 2.6+ en 32 et 64 bits
  1. **Lien de téléchargement officiel :**

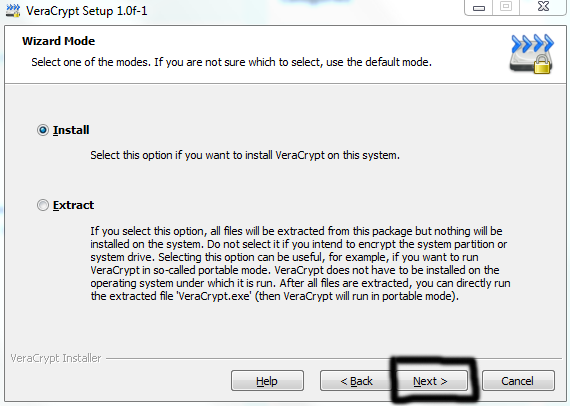
Vous téléchargerez le logiciel librement en tapant sur.

**VeraCrypt**1.19 ([https://veracrypt.codeplex.com](https://veracrypt.codeplex.com/)) – le package d’installation fait environ 23 Mo. C’est la version la plus recente compatible avec Windows7.

1. **Installation :**

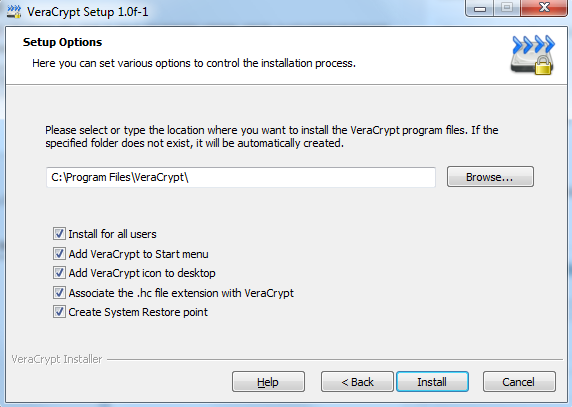
Voici les quelques étapes de l’installation.

Il faudra être administrateur du poste (uniquement durant la phase d’installation). Après avoir accepté la licence, un premier choix s’impose:

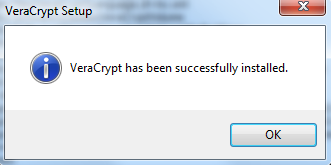


Vous pouvez choisir de poursuivre une installation classique ou d’extraire VeraCrypt. Le choix de l’extraction est utile si vous souhaitez utiliser VeraCrypt ponctuellement sans installer quoique soit sur l’ordinateur (utilisation dans un cadre mobile).

Choisissons cependant le cas le plus répandu : « **install »**



Comme vous le voyez, cliquez sur “Install” puis voilà le logiciel installé dans votre ordinateur.



Vous aurez ensuite cette icône apparaître sur votre bureau :



**NB: Pour avoir une interface en autre langue que l’anglais américain => Allez simplement dans Settings / Langages.**

1. **Présentation de l’interface du logiciel :**

Trois choix s’offrent à vous :

1 – « Créer un fichier conteneur  chiffré», vous choisirez cette option si vous voulez créer un volume qui sera associé à un fichier unique de type confidentiel.tc qui contiendra les fichiers chiffrés sur votre volume habituel (par exemple sur C).

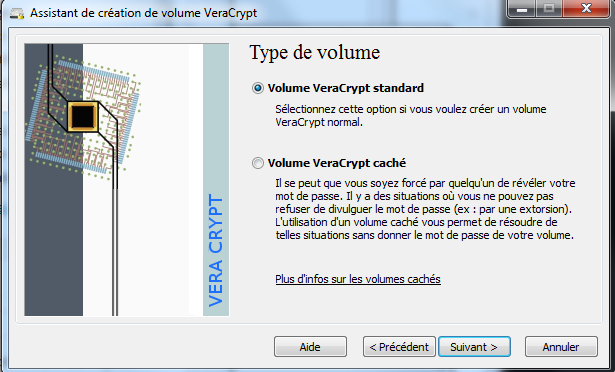
2 – « Chiffrer une partition / un disque non système », si vous désirez créer un volume complet sur un espace disque disponible tel que une clé USB, une partition de disque non-utilisée ou un disque externe.

3 – « Chiffrer la partition ou l’intégralité du disque système », pour modifier une partition actuelle afin de la rendre chiffrée en totalité. Cette partition peut-être la partition système ou le disque système.

**Ces 3 choix définissent ce à quoi ressemblera le container chiffré qui stockera les fichiers chiffrés.**

 Choisissons la première option notamment « Créer un fichier conteneur  chiffré ».

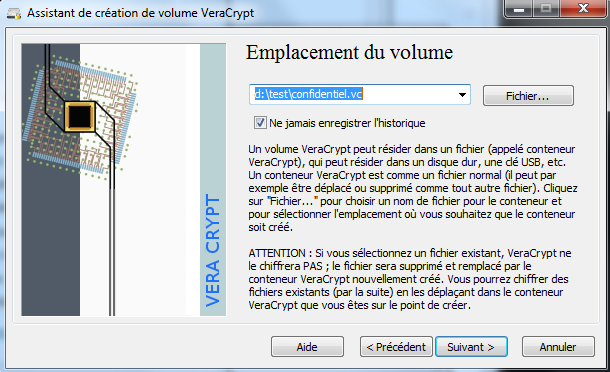
 L’écran suivant vous propose deux options (disponibles également pour les autres choix précédents) :



–  Standard TrueCrypt Volume : globalement, vous allez créer un espace (fichier ou partition) qui sera visible en tant qu’élément chiffré. C’est plus standard comme son nom l’indique.

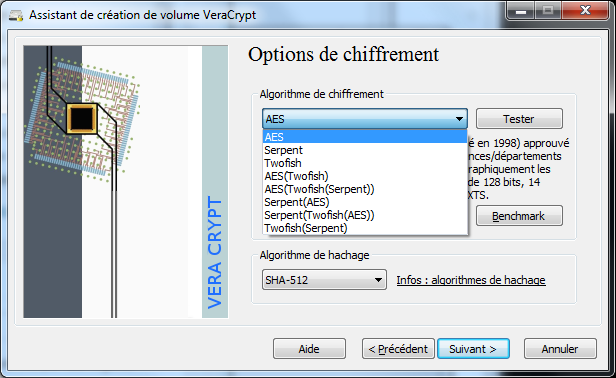
–   Hidden TrueCrypt Volume (ou mode paranoïa) : le container qui recevra les fichiers chiffrés sera « invisible ». Cet espace sera plus précisément sur un espace de disque non partitionné donc non visible sous Windows. Dans le détail, c’est un schéma de fonctionnement un peu plus compliqué mais davantage sécurisé puisqu’une analyse rapide d’un ordinateur ne permettra pas de repérer l’existence d’un volume chiffré.

sous slocauxdisques s etc. P et **déjà**



L’étape suivante consiste à sélectionner en premier le **type de chiffrement**que vous souhaitez utiliser. AES, Serpent ou TwoFish, mais plus amusant encore, vous pouvez choisir d’additionner séquentiellement 1 ou 2 voire 3 de ces algorithmes déjà forts puissants utilisés de manière individuelle.

Partons sur AES, un système de chiffrement à clé symétrique très répandu dans maintes applications informatiques, système robuste et approuvé par le NIST, le FIPS et la NAS comme algorithme de chiffrement fort. Pour l’anecdote, l’algorithme a été conçu par deux Belges Vincent Rijmen et Joan Daemen.



Le menu Outils / Banc de Test vous permettra d’évaluer le chiffrement le plus rapide.

Sélectionnez aussi le **type de hachage** retenu. Le hachage étant l’algorithme qui permet de définir une empreinte « unique » pour un fichier donné. Si le contenu du fichier est modifié, le hachage ne sera plus vérifiable et confirmera que le fichier a été modifié.

Choisissez SHA-512, relativement répandu et très fiable (produit un condensat ou Hash de 512 bits, ce qui est assez important).

Définissez ensuite le volume que fera votre conteneur (en Ko ou Mo ou Go). L’espace sera alors alloué dans son intégralité sur le disque mais comme une coquille vide.

Petit rappel :

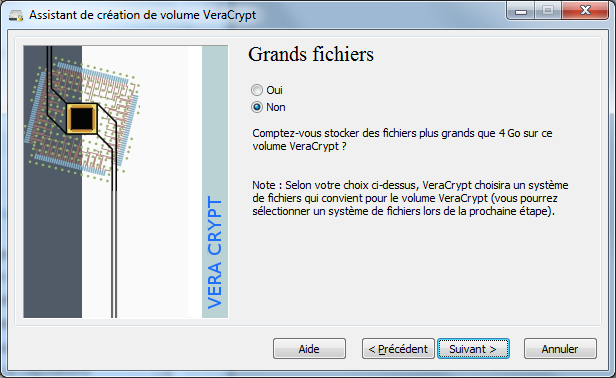
Un Ko (Kilo Octet) = 1000 octets et qu’il ne faut pas confondre avec un Kibi Octet = 1024 octets. Le CEI a normalisé tout ceci (le kibi octet, le mebioctet,…) en 1998.

Sur le choix du mot de passe, inutile de préciser que plus c’est long plus c’est bon. Mais si c’est trop long et trop compliqué on est obligé de le noter sur un post-it. Cela n’empêche pas pour autant d’y glisser quelques caractères exotiques comme les chiffres, les majuscules, les minuscules, etc.

Le mot de passe est limité à 64 caractères. C’est ce mot de passe qui vous sera demandé pour accéder au volume chiffré à chaque fois que vous y accédez.

Si vous cochez « Fichier Clé », vous devrez indiquer un fichier qui servira de « clé » supplémentaire au mot de passe. Ce fichier sera ensuite toujours nécessaire pour pouvoir ouvrir le fichier TrueCrypt. Cela peut-être un fichier mp3, avi, texte… Mais un fichier qui ne sera plus modifié !

En fonction de l’utilisation de votre conteneur (notamment si la taille des fichiers hébergés dans le volume sont supérieurs à 4 Go, TrueCrypt utilisera le système de fichier adapté (exclusion de FAT).

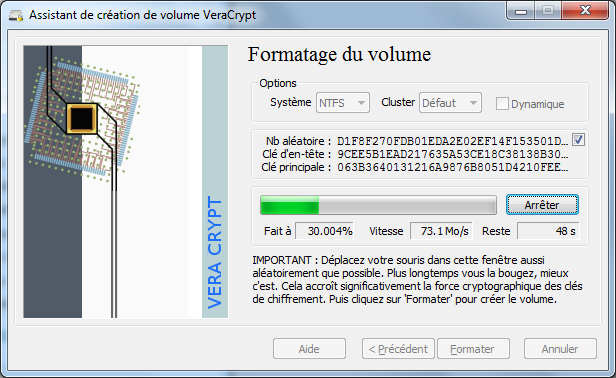


L’étape suivante est de générer les clés nécessaires au chiffrement du volume sur un modèle le plus aléatoire possible sans utiliser la fonction pseudo aléatoire de votre ordinateur. Plus le mouvement de la souris sera long, plus la clé sera difficile à reproduire.

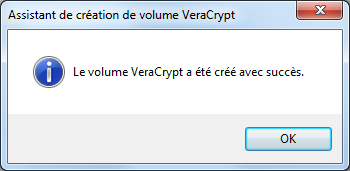
Sélectionnez également le système de fichier retenu (FAT, NTFS)

**L’option « Dynamique » permet de créer un conteneur de taille limité qui grossira au fur et à mesure des besoins (mais ne diminuera pas) : cette fonction mérite de ne pas occuper la totalité du volume spécifié au départ, en revanche cela a un impact sur les performances.**

Vous devez donc bouger la souris puis faire « Formater »



Le container sera formaté et l’espace sera chiffré.



Vous pouvez ensuite quitter sans quoi l’assistant vous re-proposera de créer un nouveau volume.

1. **Les limites de VeraCrypt**

Comme tout logiciel dédié à la sécurité et exploitant des procédures de chiffrement, VeraCrypt correspond ne protège pas de tout. Ainsi, l'équipe[détaille dans sa documentation](https://veracrypt.codeplex.com/wikipage?title=Security%20Requirements%20and%20Precautions" \t "_blank)les éléments importants à prendre en compte, les mesures de sécurité à respecter et même les limites de l'outil.

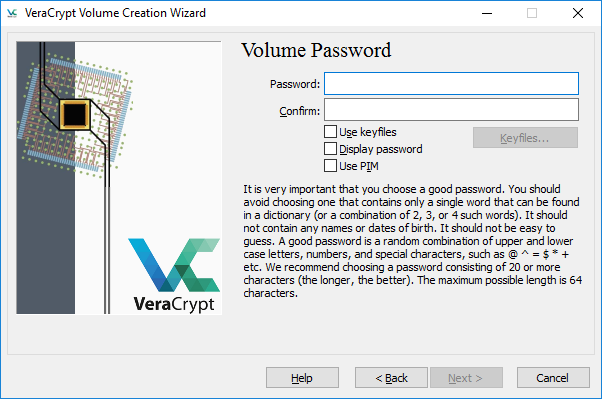
Il est particulièrement recommandé de faire attention à l'utilisation de périphériques de stockage à base de mémoire Flash lorsqu'ils utilisent **[la fonction TRIM](https://veracrypt.codeplex.com/wikipage?title=Trim%20Operation" \t "_blank)** ou **le [Wear-leveling](https://veracrypt.codeplex.com/wikipage?title=Wear-Leveling" \t "_blank).**

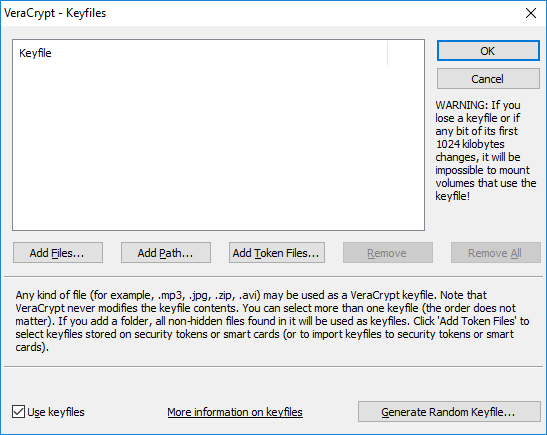
1. **Les éléments de sécurité à prendre en compte:**

Pour assurer le [chiffrement](https://www.nextinpact.com/news/99777-chiffrement-notre-antiseche-pour-expliquer-a-vos-parents.htm" \t "_blank) de conteneurs, disques et partitions, VeraCrypt permet d'utiliser trois éléments qui peuvent être combinés : un mot de passe, un ou plusieurs fichiers clefs, un PIM (Personal Iterations Multiplier). Ce dernier correspond à une valeur prise en compte pour la dérivation de clef au niveau de l'en-tête du volume.

Le nombre par défaut peut être celui de votre choix mais attention plus il sera élevé, plus le temps nécessaire pour monter votre volume sera important. Cela peut néanmoins permettre de renforcer une phrase de passe un peu faible. Il est conseillé par l'équipe de VeraCrypt d'utiliser une phrase de passe d'au moins 20 caractères **(voir [notre guide pratique](https://www.nextinpact.com/news/100871-choisir-bon-mot-passe-regles-a-connaitre-pieges-a-eviter.htm" \t "_blank) ci-dessus).**

Les fichiers clefs peuvent être n'importe quels fichiers de votre choix (texte, vidéo, photo, etc.), mais attention, les premiers 1024 kilobytes ne devront jamais être modifiés (pensez donc à bien les sauvegarder). Il peut aussi s'agir de fichiers contenant des données aléatoires générés par VeraCrypt. Dans ce cas, ils peuvent être stockés sur une smart card pour peu qu'elle gère le standard [PKCS #11](https://en.wikipedia.org/wiki/PKCS_11" \t "_blank).



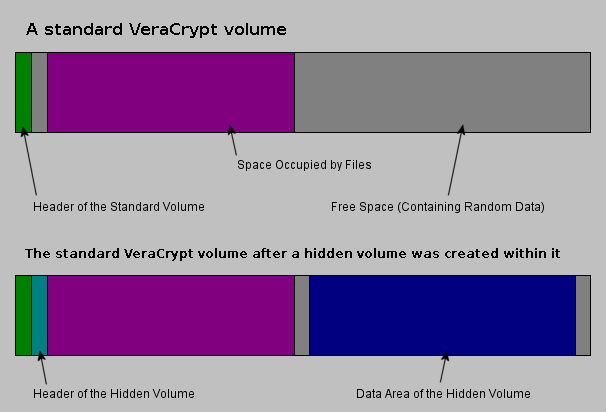


1. **Partitions cachées et deni plausible**

VeraCrypt propose de « cacher » les volumes chiffrés qu'il génère. Dans la pratique, il s'agit de placer un élément protégé dans un autre, de plus grande taille mais de manière invisible (à moins d'une analyse complète du disque). La seule manière d'accéder à l'un ou à l'autre étant les éléments de sécurité utilisés, ce qui constitue une sorte de tiroir à double fond pour vos données. Un concept connu sous le nom [de déni plausible](https://fr.wikipedia.org/wiki/D%C3%A9ni_plausible_(cryptologie)" \t "_blank).

Pour créer un conteneur caché, deux possibilités s’offrent à vous : le faire au sein d'un conteneur VeraCrypt déjà existant (mode direct) ou suivre une procédure entièrement automatisée (mode normal). Dans ce second cas, l'application vous guidera dans la création du conteneur principal puis du conteneur caché.

Pour rappel, le second devra forcément être de plus petite taille. On peut ainsi placer des fichiers dans le conteneur principal qui peuvent paraitre crédible, puis les données que l'on veut protéger dans le conteneur caché.



1. **Peut-on stocker un conteneur chiffré dans le « cloud » ?**

La plupart du temps, il n'est pas conseillé de stocker des conteneurs tels que ceux générés par VeraCrypt dans des services de stockage en ligne et d'utiliser plutôt des outils tels que [BoxCryptor](https://www.boxcryptor.com/fr" \t "_blank)ou [Cryptomator](https://cryptomator.org/" \t "_blank) qui sont prévus à cet effet et chiffrent les données fichier par fichier.

Les conteneurs [VeraCrypt](http://www.nextinpact.com/recherche?_search=VeraCrypt&RubriqueId=&Author=&OrderType=date&DateStartPeriod=&DateEndPeriod=&ListTypeContent.actus_view=true&ListTypeContent.dossiers_view=true&ListTypeContent.bonsplans_view=true&ListTypeContent.archives_view=true" \t "_blank) prennent en effet la forme d'un fichier unique et la modification du moindre élément implique le besoin d'un nouvel upload complet. Ce n'est néanmoins pas le cas avec certains services qui proposent la synchronisation différentielle et analysent l'évolution des fichiers dans le détail. Ainsi, ils n'envoient que les différences relevées. C'est notamment [le cas de Dropbox](https://www.dropbox.com/help/8" \t "_blank).

1. **Les autres logiciels de cryptage de fichiers**

* Folder Lock 7.6.1
* BitLocker
* [AxCrypt](http://www.clubic.com/telecharger-fiche12208-axcrypt.html)
* [Advanced ZIP Password Recovery](http://www.clubic.com/telecharger-fiche10139-advanced-zip-password-recovery.html)

Etc.

**Conclusion :**

Veracrypt est un logiciel de cryptage de données parmi la multitude qui existe dans le paysage informatique. Il sert à cacher, chiffrer et sécuriser vos données. Sa particularité tient en son téléchargement rapide et son usage facile.