Chiffrer vos données avec VeraCrypt

Le menu :

1 – Intro.

Sur la base de TrueCrypt, VeraCrypt est un logiciel qui permet le cryptage des fichiers et partitions sous forme de conteneur global ou fichier unique.

Dans la continuité de Truecrypt, sans les problèmes identifiés en 2014, une société Française Idrix a développé un produit similaire disponible sur SourceForge et CodePlex. VeraCrypt est sous licence TrueCrypt et surtout MS-PL (Licence Microsoft Public).

Qu'apporte VeraCrypt vis à vis de la version de TrueCrypt ? Les équipes de VeraCrypt ont tenu compte et corrigé un bon nombre de faiblesses/vulnérabilités identifiées par l'Open Crypto Audit Project sur TrueCrypt.

Le rapport d'origine sur l'audit de TrueCrypt : https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf

La liste des corrections apportées suite à l'audit de TruceCrypt :

https://veracrypt.codeplex.com/discussions/569777#PostContent_1313325

Le document présente différentes utilisations possibles de VeraCrypt: un usage classique avec création d'un fichier(volume) crypté et protégé par un mot de passe, la même chose protégé par un

fichier clé (keyfile), le cryptage de tout votre PC ou portable y compris la partition système (!), et le cryptage d'un volume qui sera caché.

VeraCrypt effectue le cryptage/décryptage à la volée après lecture du fichier, avant enregistrement du fichier. C'est aussi ce qu'on appelle le cryptage OFT = On The Fly

La version 1.0f2 présente les fonctionnalités suivantes :

- 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
- Montage automatique des volumes VeraCrypt. Si vous posséder un volume VeraCrypt sur un support amovible que vous connectez celui-ci sur votre PC, le volume *pourra* être monté automatiquement.
- Comptabilité entière des volumes TrueCrypt (merci Korben : http://korben.info/veracrypt-est-maintenant-compatible-avec-les-conteneurs-truecrypt.html)
- Les partitions supportent des secteurs de taille 1024 à 4096 octets.
- La gestion de Volumes Favoris présente de nombreuses options (montage lecture seule, ordre de montage, etc…)
- la possibilité de crypter une partition contenant des données, sans perdre le contenu (sous Vista/Windows 2008)
- le support des tokens et smart cards
- l'interopérabilité d'un volume crypté sous Windows et utilisable sous Linux/Mac
- …

Cette dernière release intègre des corrections aux vulnérabilités identifiées dans la phase II de l'audit de TrueCrypt (https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf)

2 – Modes opératoires possibles avec VeraCrypt

Il existe plusieurs variantes à l'usage de VeraCrypt : certains ont la première utilité de crypter ses fichiers pour se protéger de tout vol alors que d'autres visent à masquer, voire leurrer l'hypothèse que vous puissiez crypter vos fichiers. En voici cinq :

– Créer un **conteneur VeraCrypt dans un fichier visible**. Cette option basique vous permet de vous promener avec votre conteneur (fichier) sur une clé USB, votre disque externe, vos sauvegardes, etc avec un minimum de confidentialité. C'est ce qui est expliqué dans la partie 3

– **Dédier une partition (non système) en tant que conteneur VeraCrypt** . Option similaire à la précédente avec un conteneur qui fera la taille de votre partition ou de votre disque complet, donc particulièrement confortable pour les disques externes par exemple.

– **Mettre sa partition Système dans un conteneur VeraCrypt** . Cette fois-ci, votre système d'exploitation et tout l'environnement/paramètres/données qui se trouvent sur la partition système se trouvent cryptés, de manière transparente pour l'OS, hormis le **VeraCrypt** Boot Loader initial qui vous demandera un mot de passe pour lancer votre OS. Partie 7.

– **Déclarer un conteneur dans un fichier qui contiendra lui-même un autre conteneur caché**. Imaginez un coffre-fort caché derrière un tableau de maitre, ce coffre-fort une fois découvert s'avère posséder quelques documents peu compromettants mais possède surtout un double fond

contenant vos véritables documents confidentiels. A ceci près qu'en fonction du mot de passe du conteneur initial, soit vous ouvrez le conteneur leurre, soit vous ouvrez le conteneur qui vous est cher.

– A l'image de l'option précédente, vous **cryptez votre partition système, qui se trouve contenir également une autre partition systèmes chiffrée** accessibles l'une comme l'autre selon le mot de passe saisi. Cet usage est détaillé en partie 8

Enfin, une fonctionnalité commune à tous les modes ci-dessus concerne la clé d'accès au conteneur chiffré : dans les cas les plus simples, la clé sera un mot de passe mais peut également être un fichier de votre choix.

3 – Installation

Parce que le parc de postes Windows est encore important, c'est cet OS qui est utilisé pour expliquer un peu plus comment çà s'installe.

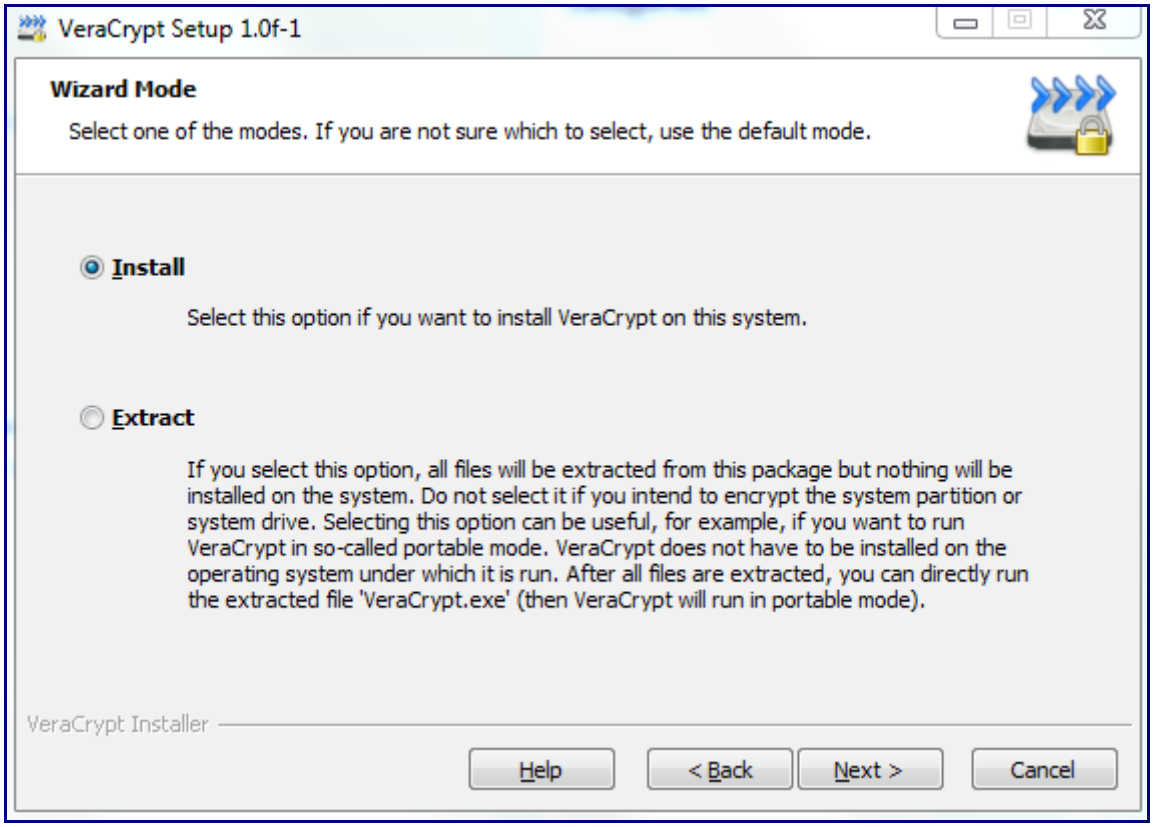
Il vous faudrait donc :

Windows 7+

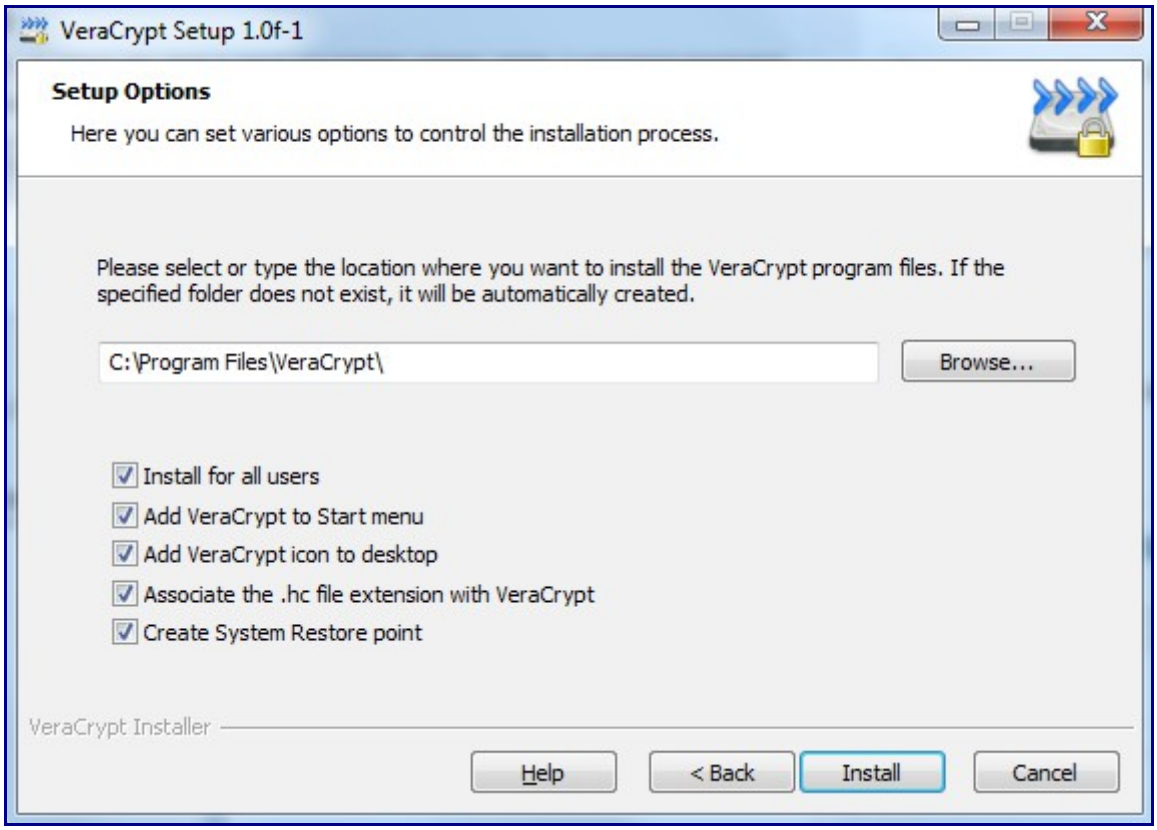
VeraCrypt 1.19 (https://veracrypt.codeplex.com) – le package d'installation fait environ 23 Mo

Etre administrateur du poste (uniquement durant la phase d'installation)

Après avoir accepté la licence, un premier choix :

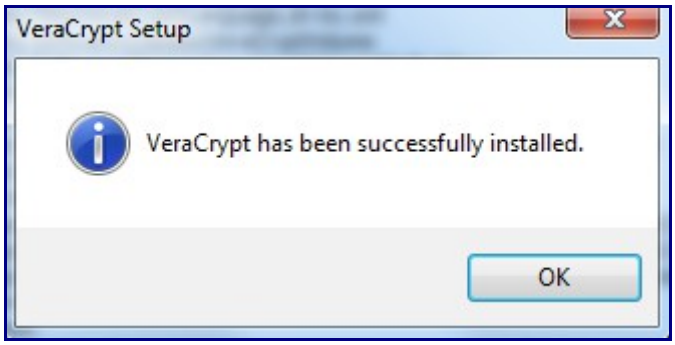


Vous pouvez choisir de poursuivre une installation classique ou d'extraire VeraCrypt: ce choix est utile si vous souhaitez utiliser VeraCryptponctuellement sans installer quoique soit sur l'ordinateur (utilisation dans un cadre mobile). Choisissons le cas le plus répandu : **install**



Rien de particulier dans cet écran sauf à noter la possibilité de forcer un point de restauration Windows.

L'installation finie



Vous aurez cette icône sur votre bureau :

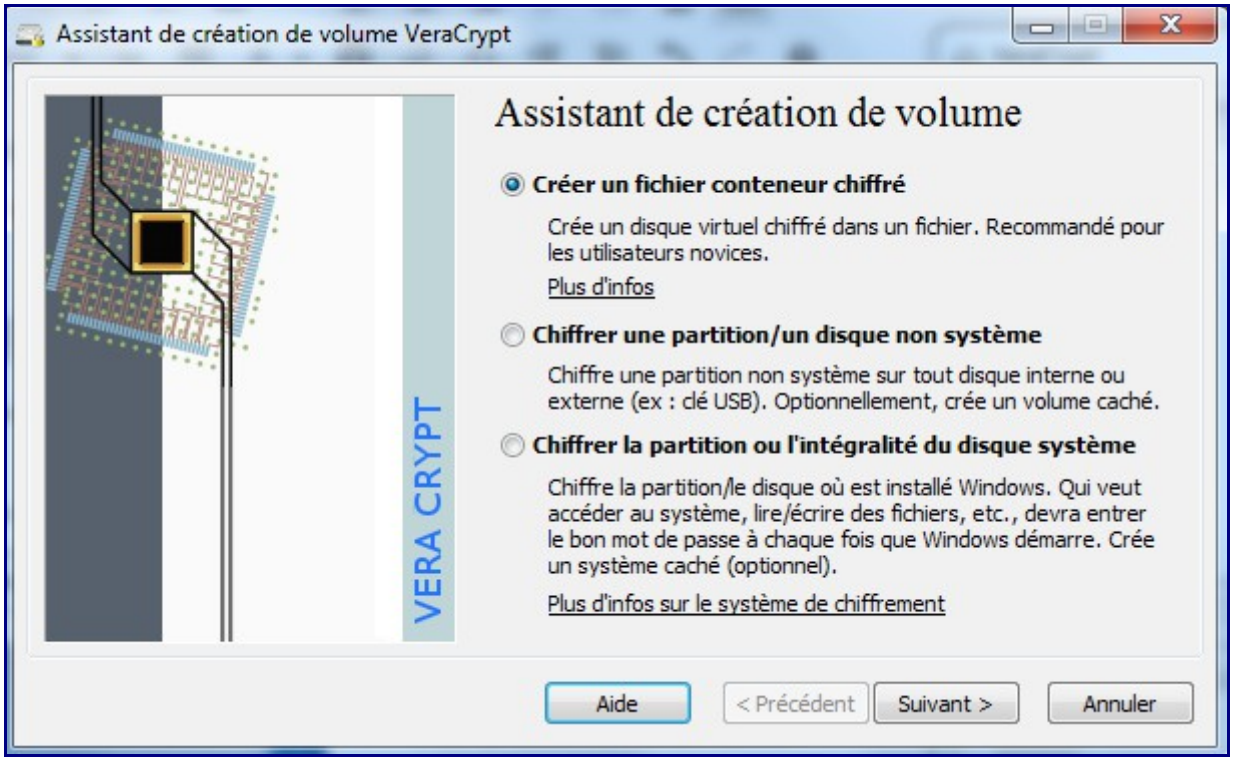
<u>Pour avoir une interface en langue autre qu'US :</u>

Allez simplement dans Settings / Langages….

4 – Configuration

L'étape primordiale est ensuite de créer un volume (unité logique de type e, f, g,…) qui sera cryptée et qui contiendra l'ensemble de vos données protégées.

Allez dans le menu Volumes, Créer un Nouveau Volume ou cliquez sur le bouton « Creer un volume »



Trois choix s'offrent à vous :

1 – « *Créer un fichier conteneur* chiffré», créer un volume qui sera associé à un fichier unique de type *confidentiel.tc* qui contiendra les fichiers cryptés sur votre volume habituel (par exemple sur C

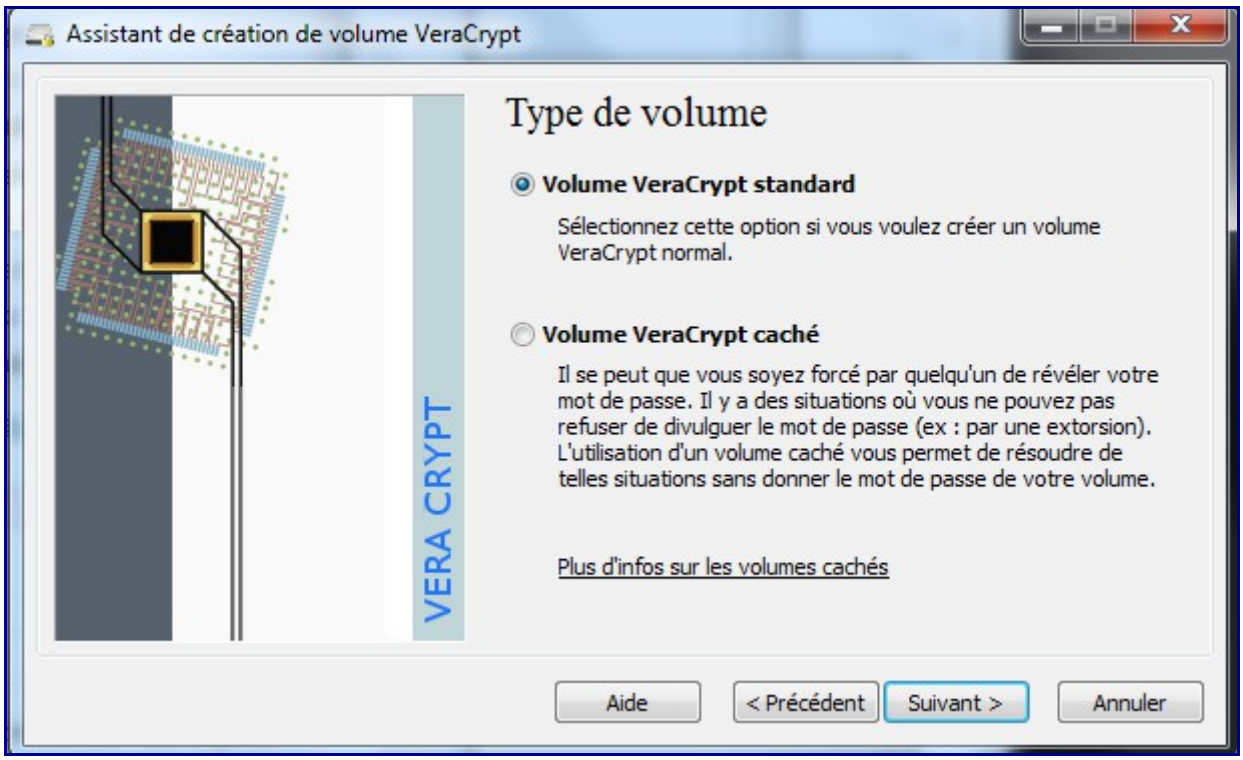
2 – « *Chiffrer une partition/ un disque non système* », créer un volume complet sur un espace disque disponible tel que une clé USB, une partition de disque non-utilisée, un disque externe

3 – « *Chiffrer la partition ou l'intégralité du disque système* », modifier une partition actuelle pour la rendre cryptée en totalité. Cette partition peut-être la partition système ou le disque système.

Ces 3 choix définissent ce à quoi ressemblera le container crypté qui stockera les fichiers cryptés.

Choisissons la première option .

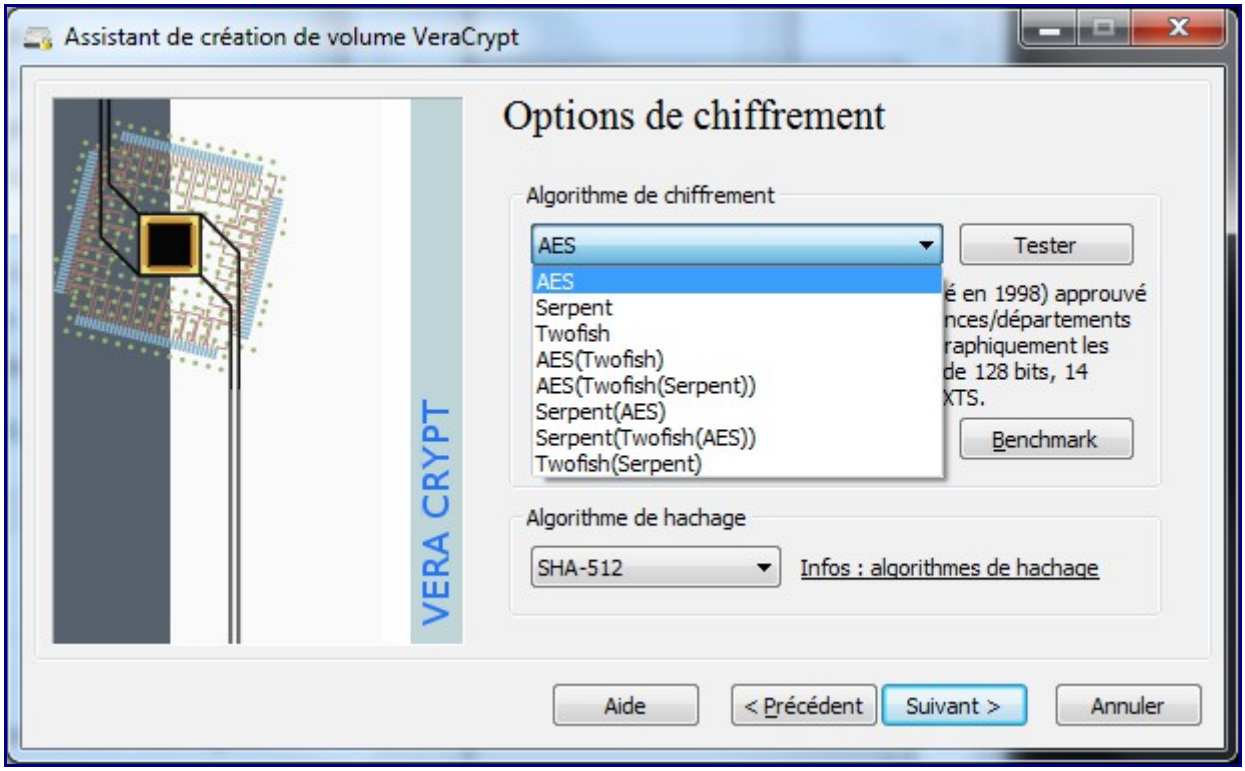
L'écran suivant vous propose deux options (disponibles également pour les autres choix précédents) :



– *Standard TrueCrypt Volume* : globalement, vous allez créer un espace (fichier ou partition) qui sera visible en tant qu'élément chiffré. Traditionnel…

– *Hidden TrueCrypt Volume* (ou mode paranoïa) : le container qui recevra les fichiers cryptés 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 peu plus compliqué mais davantage sécurisé puisqu'une analyse rapide d'un ordinateur ne permettra pas de repérer l'existence d'un volume crypté.

Vous devez ensuite définir de l'emplacement de votre container (ou fichier global) qui contiendra vos éléments à protéger). Cet emplacement peut être vos disque local, externe, USB,… précisez un chemin, voir un nom de fichier. *Si celui-ci existe, il ne sera pas réutilisé mais* ***écrasé*** *par TrueCrypt.*

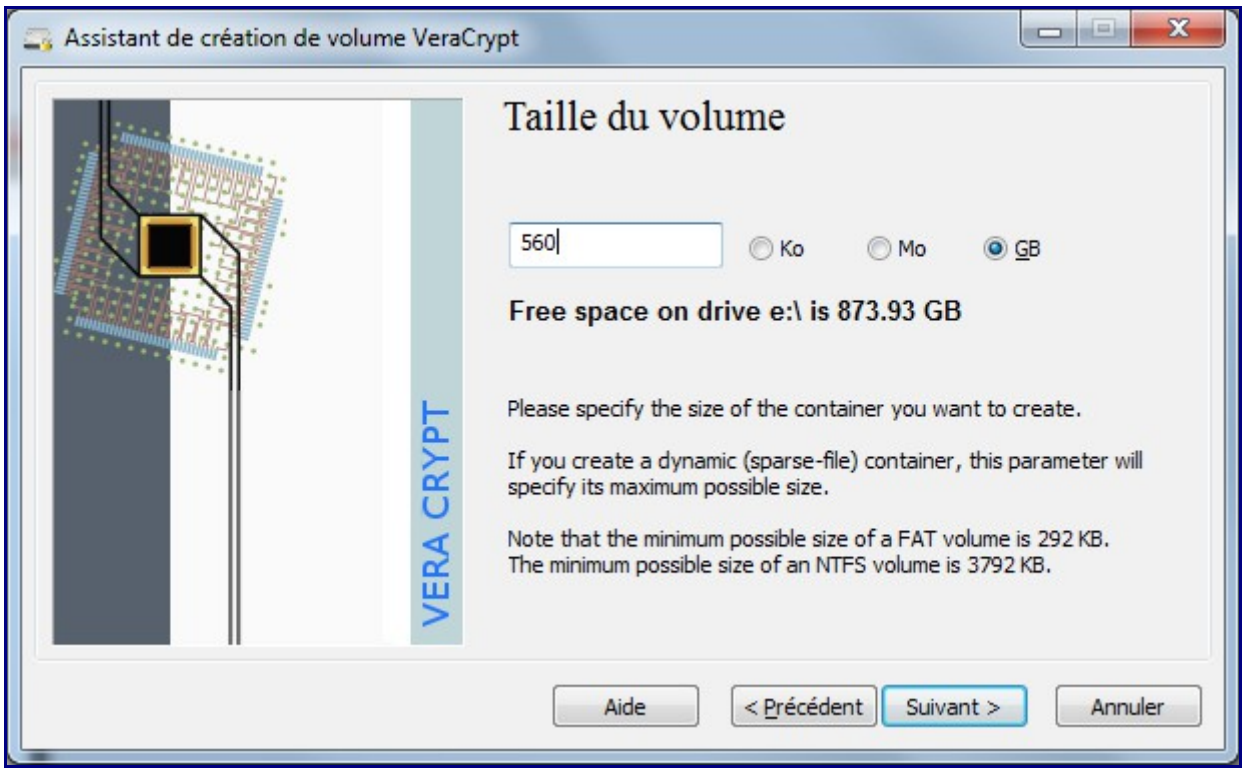


L'étape suivante consiste à sélectionner en premier le **type de cryptage** que vous souhaitez utiliser. AES, Serpent ou TwoFish mais plus amusant encore, vous pouvez choisir d'additionner séquentiellement 1 ou 2 voire 3 de ces algorithmes déjà forts puissants utilisés de manière individuelle. Partons sur AES, un système de cryptage à clé symétrique très répandu dans maintes applications informatiques, système robuste et approuvé par le NIST, le FIPS et la NAS comme algorithme de cryptage fort. Pour l'anecdote qui n'en pas une, l'algorithme a été conçu par deux Belges Vincent Rijmen et Joan Daemen.

Le menu *Outils / Banc de Test* vous permettra d'évaluer le cryptage le plus rapide.

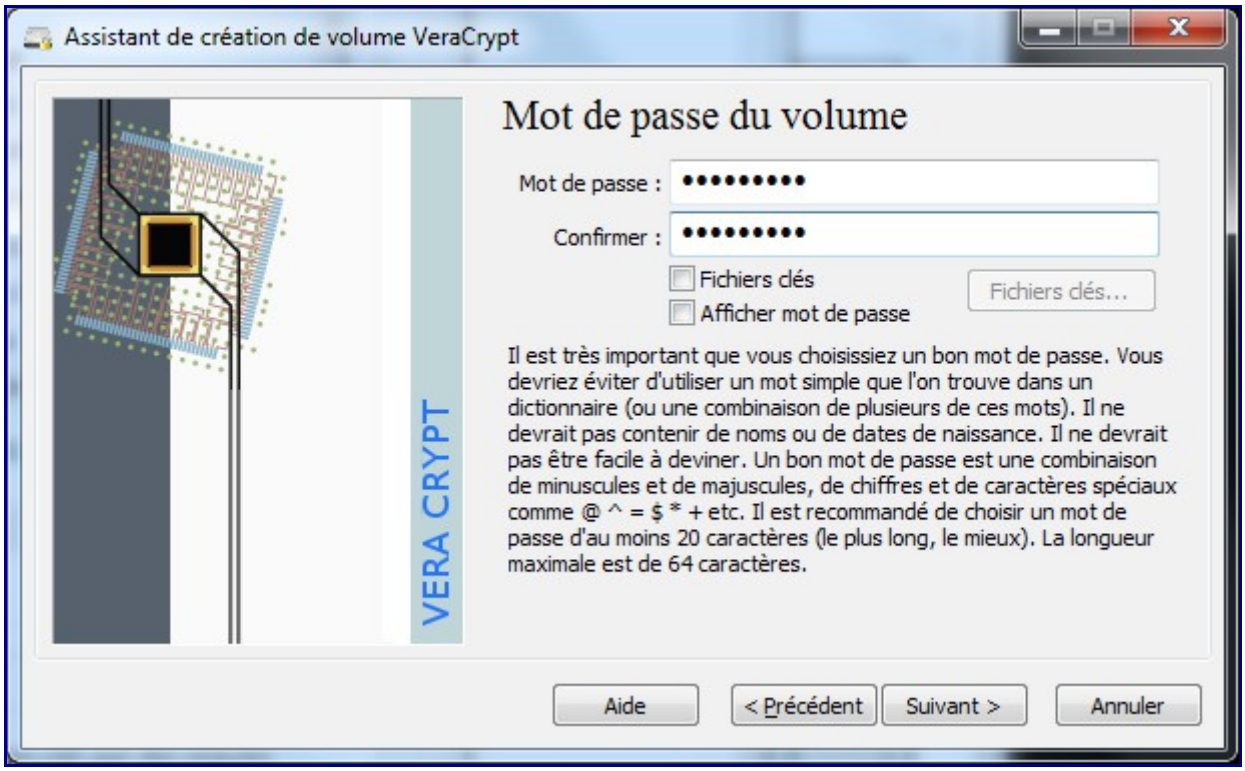
Sélectionnez aussi le **type de hachage** retenu. Le hachage étant l'algorithme qui permet de définir une empreinte « unique » pour un fichier donné. Si le contenu du fichier est modifié, le hachage ne sera plus vérifiable et confirmera que le fichier a été modifié.

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



Définissez 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 est 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.



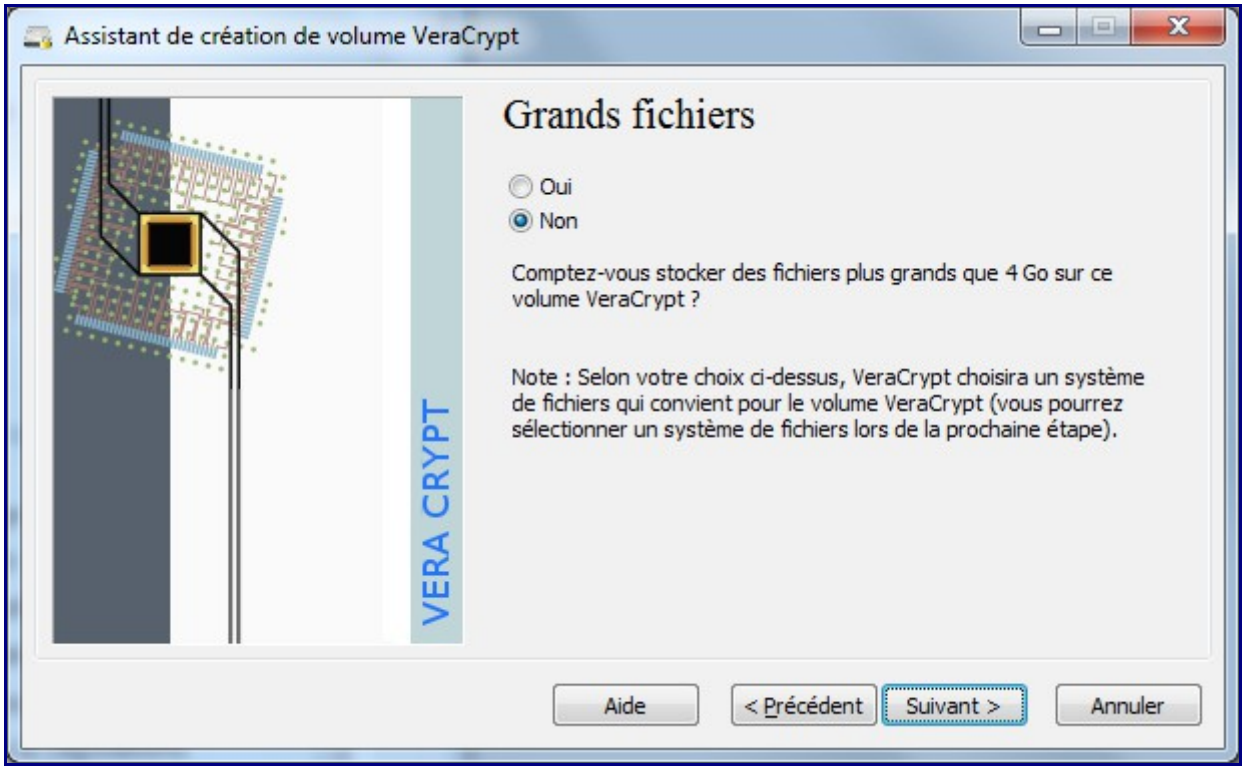
Sur le choix du mot de passe, inutile de préciser que plus c'est long plus c'est bon … mais si c'est trop long et trop compliqué on est obligé de le noter sur un post-it… Cela n'empêche pas pour

autant d'y glisser quelques caractères exotiques, chiffres, majuscules, minuscules,…).

Le mot de passe est limité à 64 caractères. C'est ce mot de passe qui vous sera demander pour accéder au volume crypté.

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 soit plus modifié !

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

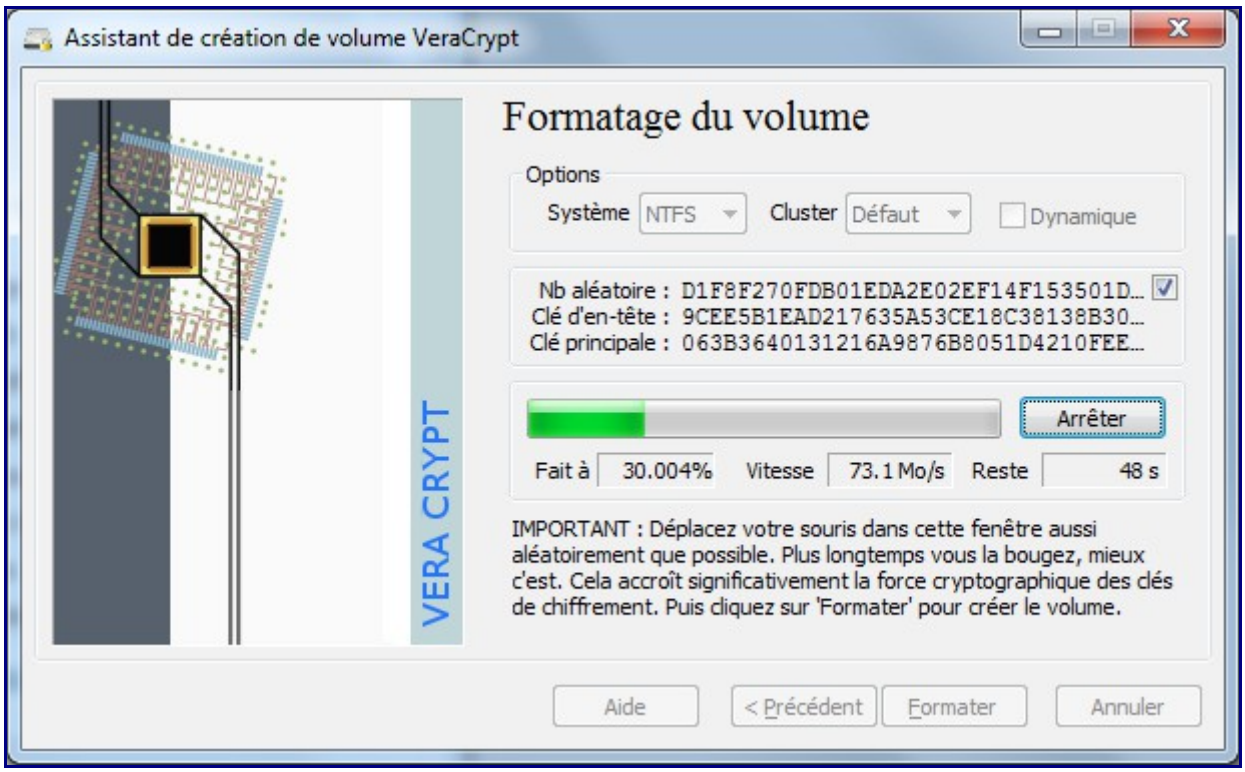


L'étape suivante est de générer les clés nécessaires au cryptage du volume sur un modèle le plus aléatoire possible sans utiliser la fonction pseudo aléatoire de votre ordinateur. Plus le mouvement de la souris sera long, plus la clé sera difficile à reproduire.

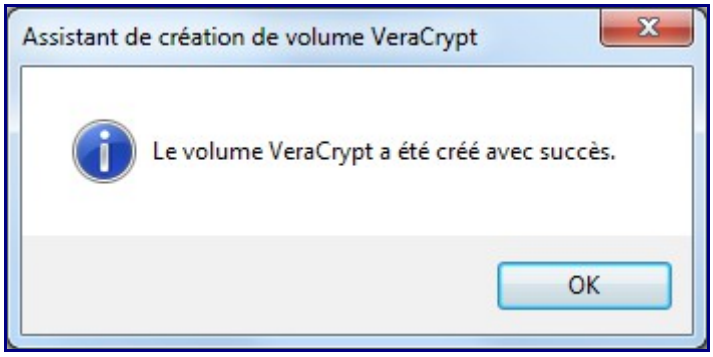
Sélectionnez également le système de fichier retenu (FAT, NTFS)

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.

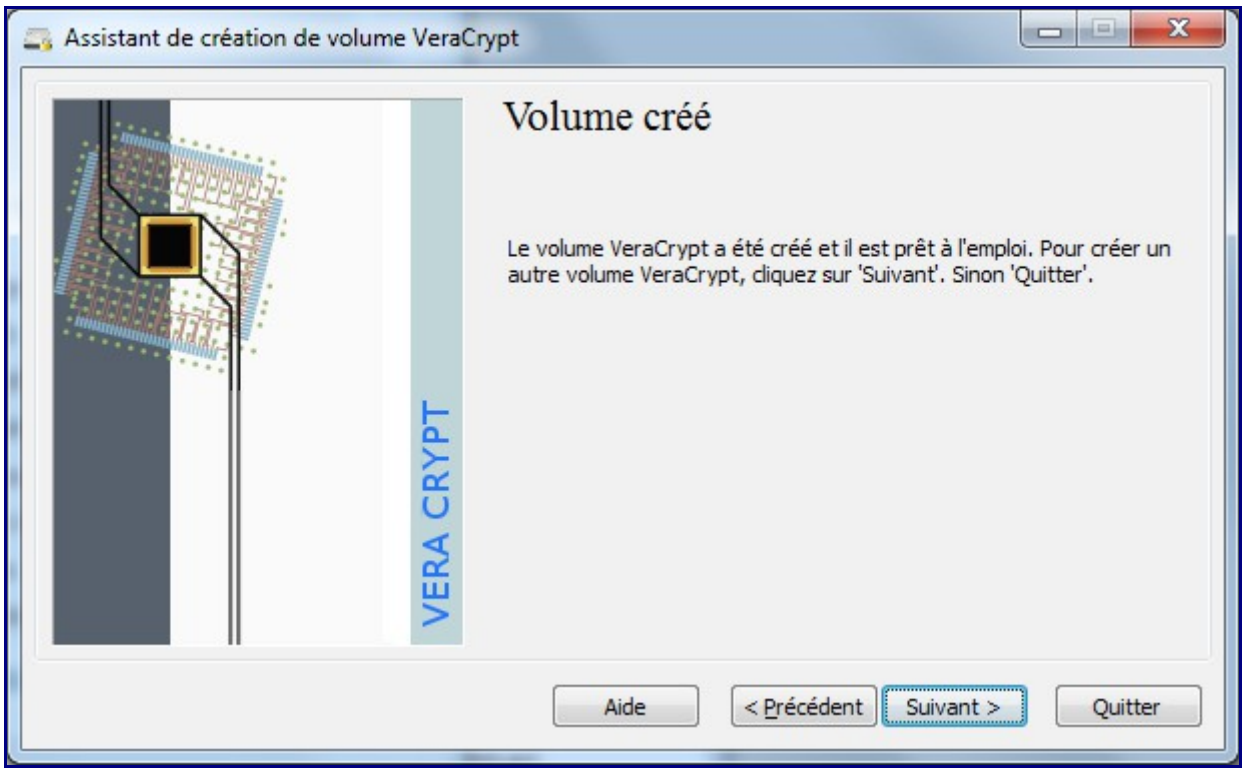
Vous devez donc bouger la souris puis faire « Formater »



Le container sera formaté et l'espace chiffré



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

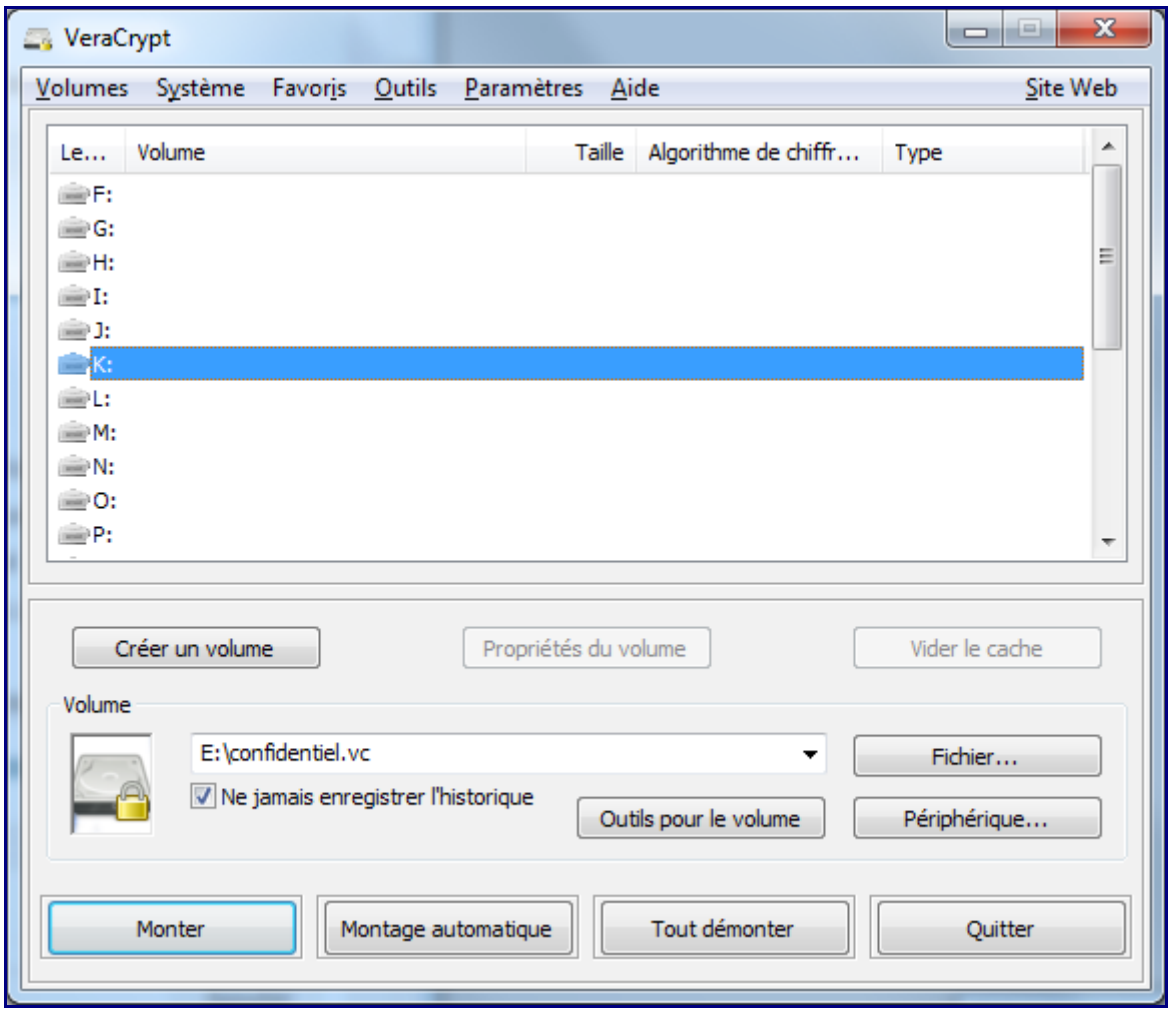


Le conteneur créé (sous forme de fichier) avec l'extension que vous avez choisi.

5 – Montage automatique des volumes

Une icône en bas à droite est apparue : 

Faites un double-click pour accéder à l'interface

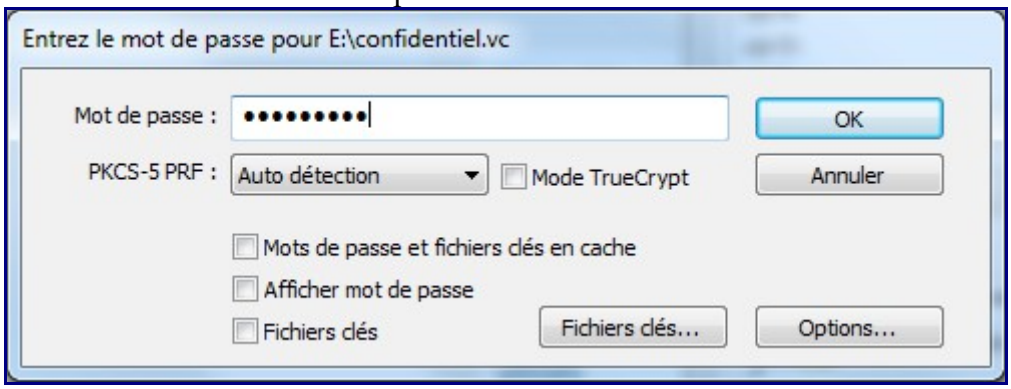


– Sélectionnez la lettre de lecteur qui sera affectée au volume chiffré,

– Dans Volume, sélectionnez le fichier que vous avez généré.

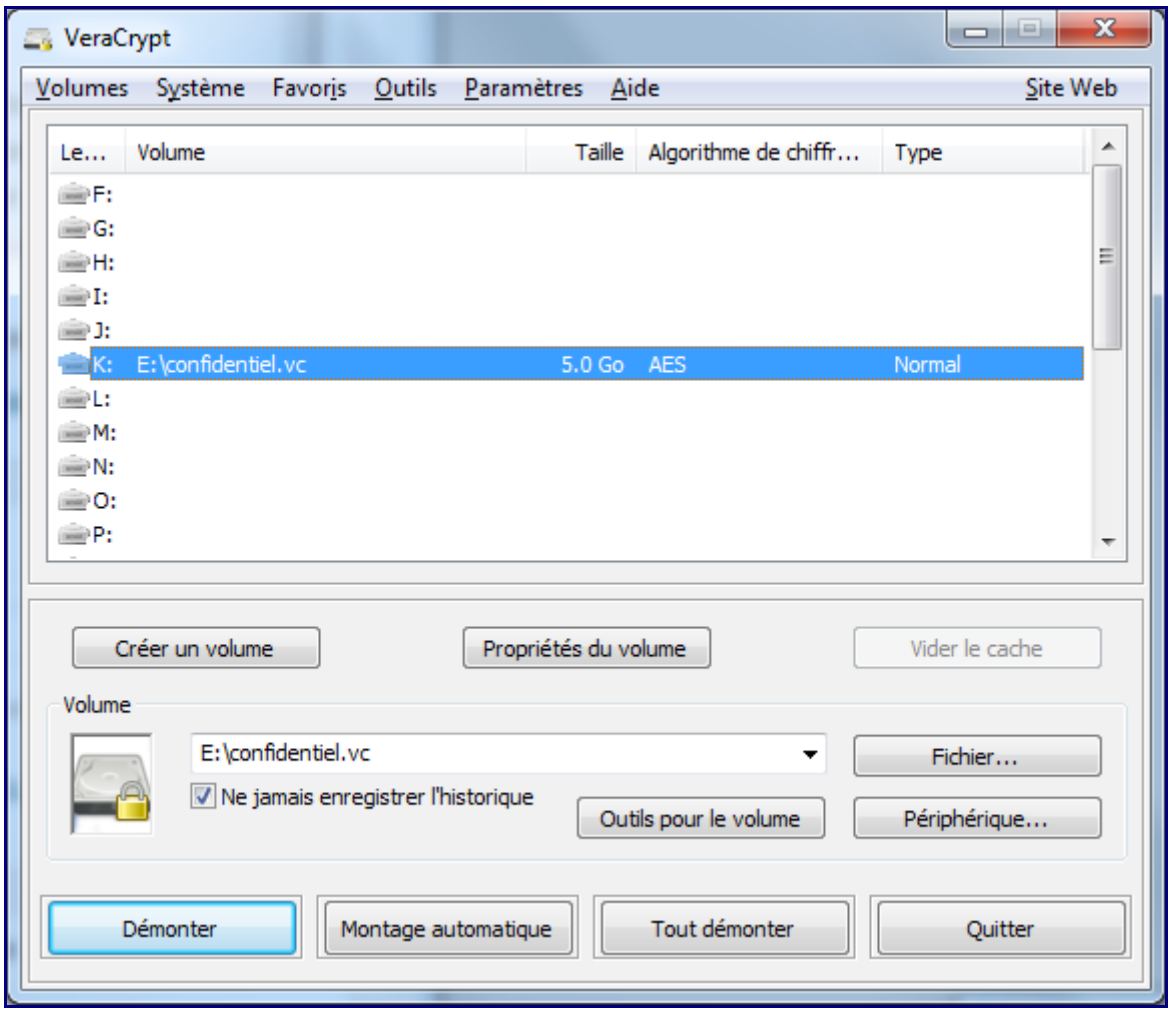
– Cliquez sur « Monter »

– Saisissez votre mot de passe

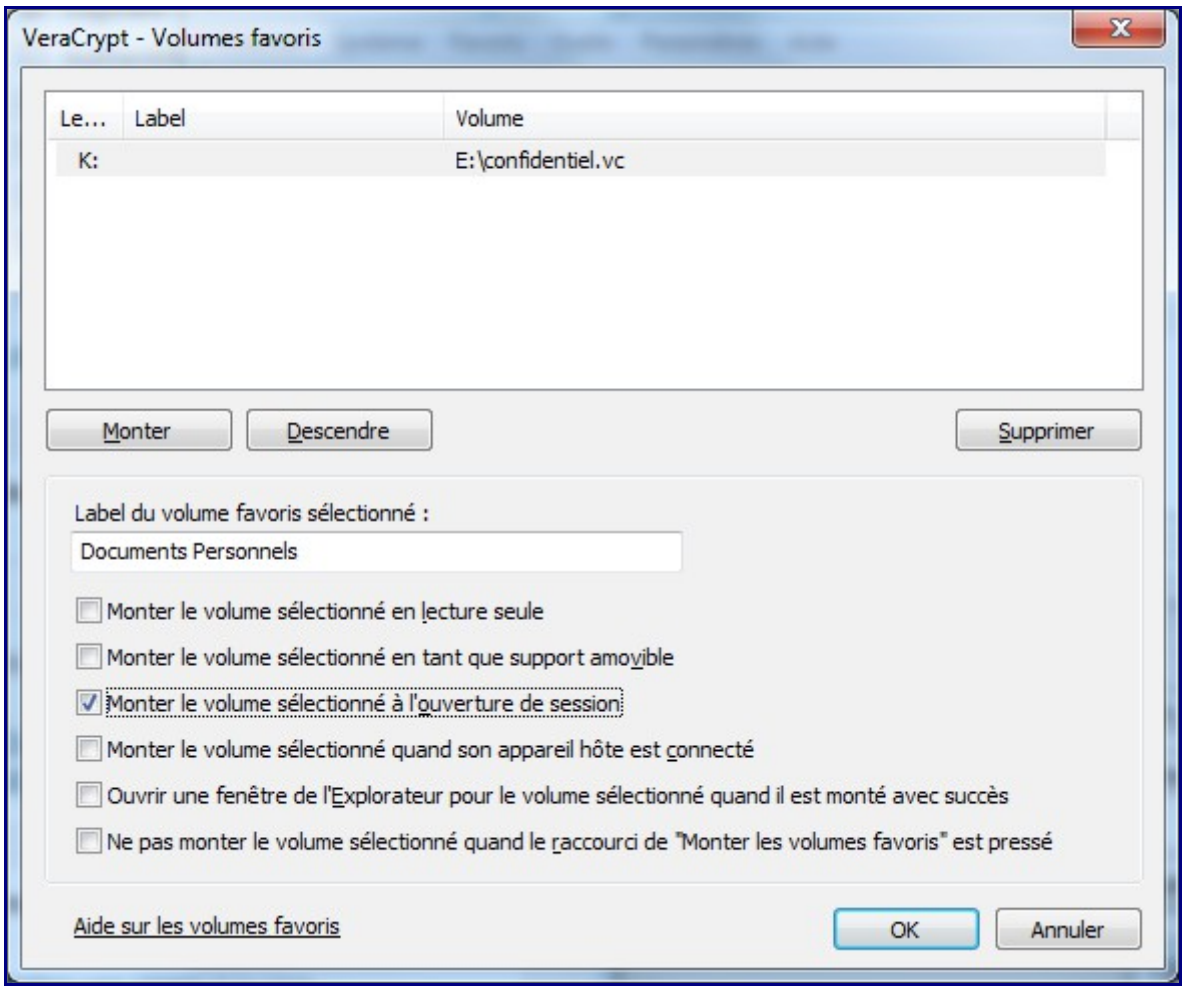


– l'option « Mode Truecrypt » vous permet de spécifier que le volume sélectionné a été créé par TrueCrypt.

– Cliquez sur OK



– Aller ensuite dans le menu *Favorites*, et sélectionnez « Add mounted volumes to Favorites…»



De nombreuses options associables au montage de ce volume favori :

- Mettre un label pour rendre le volume facile à identifier parmi d'autres.
- Monter le volume en lecture seule,
- Préciser que le volume est monté à partir d'un support amovible,
- Ne monter le volume que pendant que la session est ouverte,
- Préciser que le volume est monté à partir d'un lecteur réseau
- Ouvrir l'explorateur Windows dès que le volume est monté,
- Ne pas monter le volume favori quand la hot key est pressée.
- Choisir parmi plusieurs volumes, l'ordre de montage des volumes cryptés.

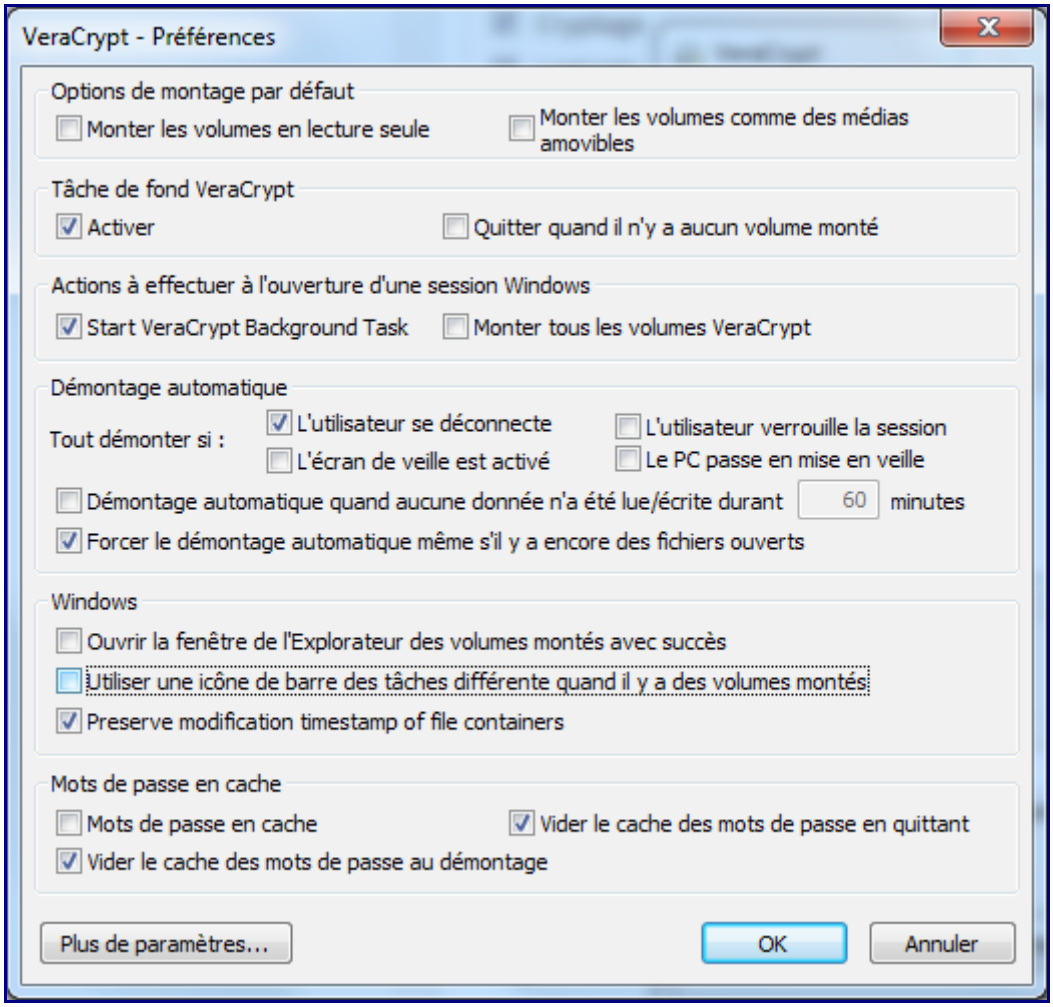
Validez par OK.

Vous trouverez alors l'unité logique montée comme une partition, tout ce que vous y mettrez sera chiffré et accessible uniquement avec VeraCrypt + votre mot de passe (ou votre fichier clé+mot de passe)

Particularités Windows

L'idéal est dans la plupart des cas, d'avoir VeraCrypt exécuté et initialisé à chaque démarrage de Windows.

Dans le menu *Paramètres / Préférences* des options sont à activer pour permettre cela :



Notamment *« Start VeraCrypt Background Task »*

Désormais, à chaque lancement de VeraCrypt , le (ou les) volumes sauvegardés dans les favoris seront montés automatiquement.

6 – Sauvegarde / Restauration

L'essentiel est maintenant d'envisager la situation suivante :

– que faites-vous si votre fichier conteneur est perdu, altéré, effacé ?

Il n'y a pas grand chose à faire dans le cas où le conteneur est un fichier stocké sur un volume windows : sauvegardez le fichier classiquement sur bande, média externe,…Restaurez, réinstallez VeraCrypt et voilà…

7 – Les KeyFiles pour une authentification renforcée

Dans l'étape 3, vous avez associé l'accès au conteneur à un mot de passe. Ce dernier est plus facilement vulnérable (exemple de BrutForce ou Keylogger,….)

Avec VeraCrypt, une utilisation plus sécurisée est possible. L'accès à une donnée confidentielle n'est plus dépendant de *ce que je sais*, mais **aussi** de *ce que je possède* : le keyfile

L'utilisation des keyfiles : c'est associer un fichier ou les fichier d'un répertoire (la clé) qui vous donnera accès au volume crypté à la condition initiale que le mot de passe fourni soit le bon.

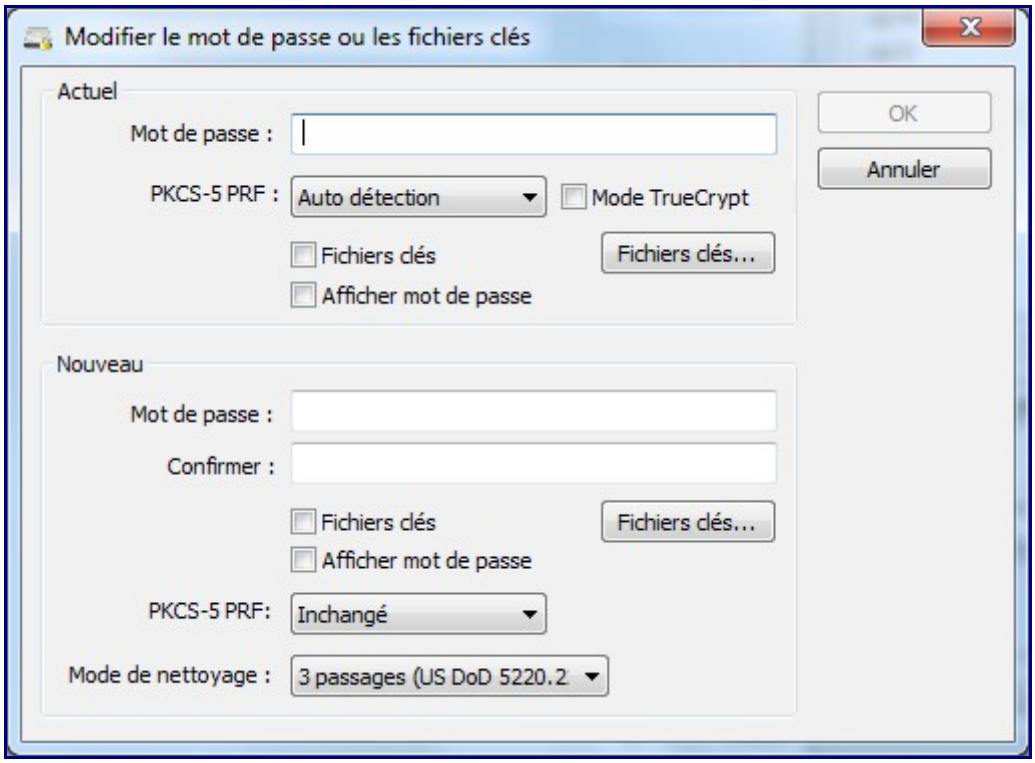
Le fichier peut-être aussi bien un mp3, qu'un avi, qu'un fichier word,… Il doit faire au moins 30 octets et **ne doit plus être modifié**.

Pour basculer d'u simple « mot de passe » au mode « mot de passe + keyfile »

– Ouvrez l'interface VeraCrypt (**ne montez pas le volume**)

– Cliquez sur *Outils pour le Volume (ou dans le menu Volume / Modifier le mot de passe du volume)*

– Choisissez Change Volume Password…

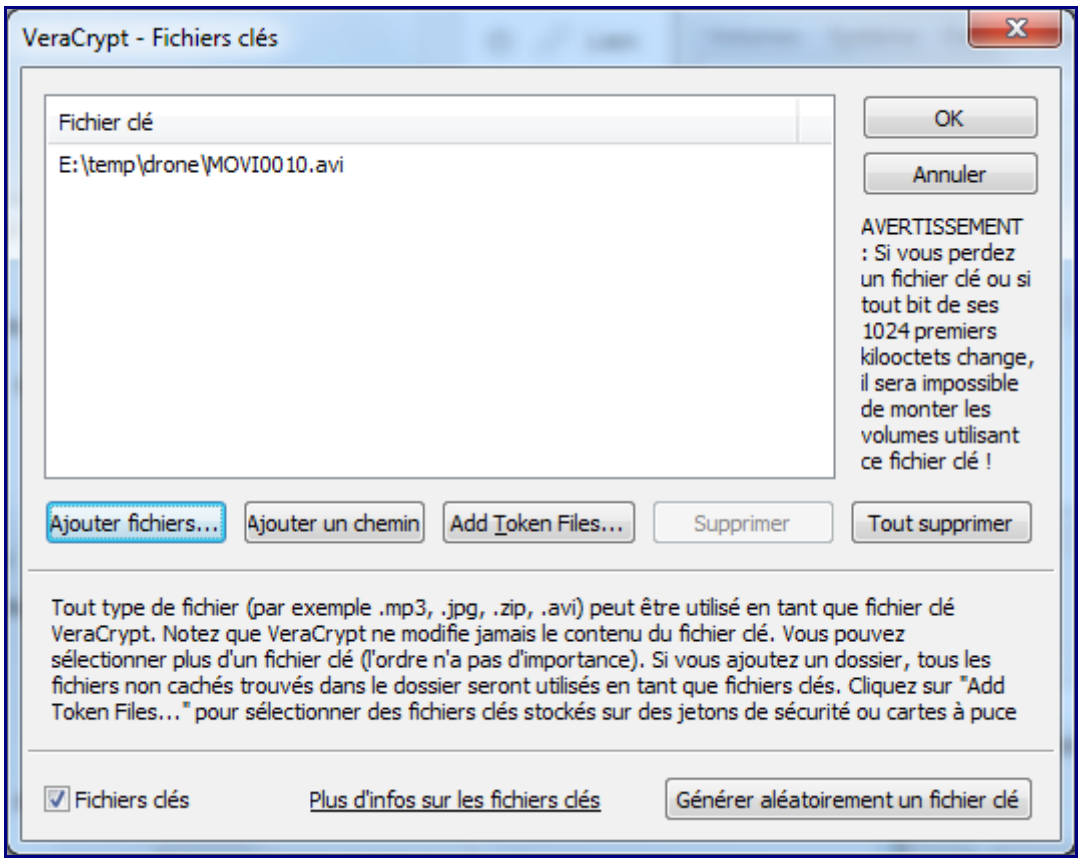


– Dans la zone Actuel, saisissez votre mot de passe actuel

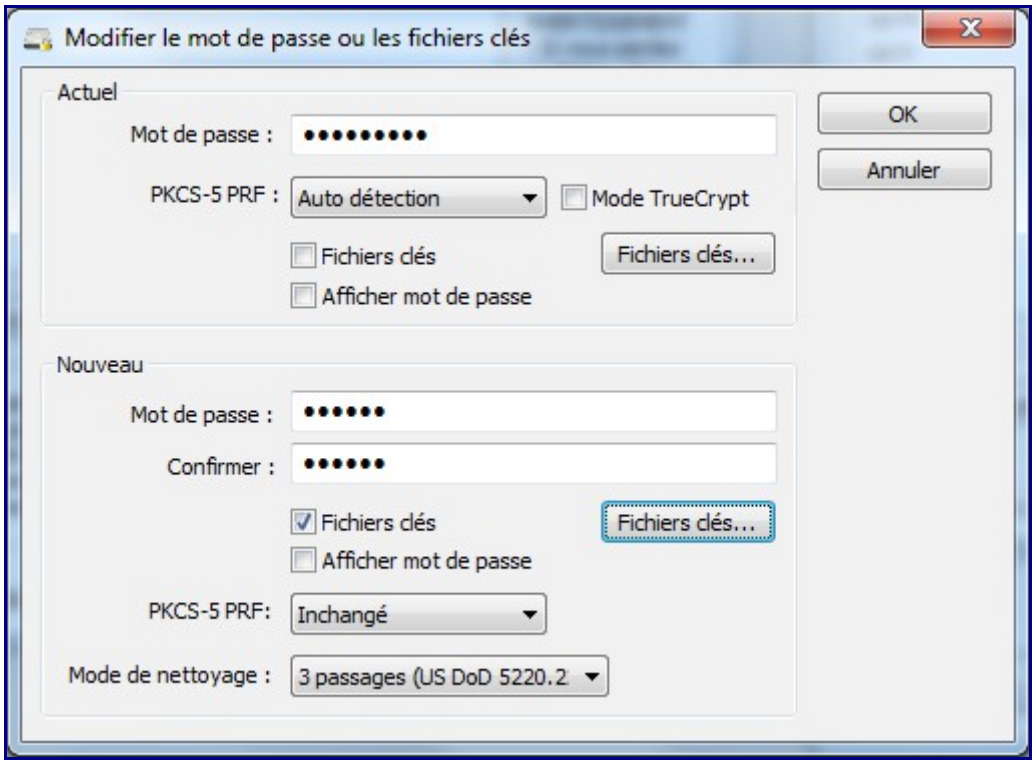
– Dans la zone Nouveau , saisissez avec confirmation votre nouveau mot de passe, puis

– Cliquez sur le bouton Fichiers clés

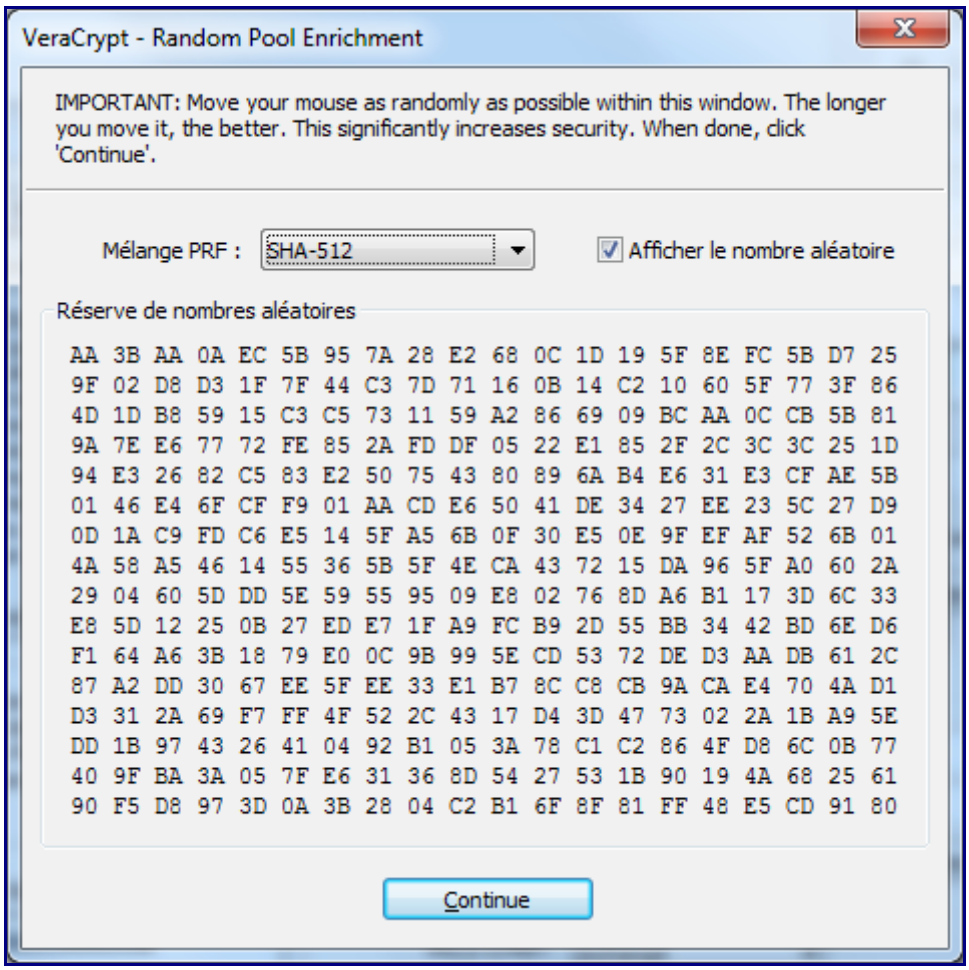
– Sélectionner le fichier (ou le répertoire) qui vous servira de clé



Le fichier sélectionné ne sera pas modifié.



-Validez.



Bougez votre souris de manière aléatoire.

Et c'est tout.

Pour monter le volume crypté, il vous restera à spécifier le fichier clé et le mot de passe comme auparavant.

Pensez à sauvegardez votre fichier clé car il devient désormais une clé essentielle pour l'ouverture de votre conteneur (ainsi que votre mot de passe).

8 – Cryptage du volume contenant le Système d'Exploitation

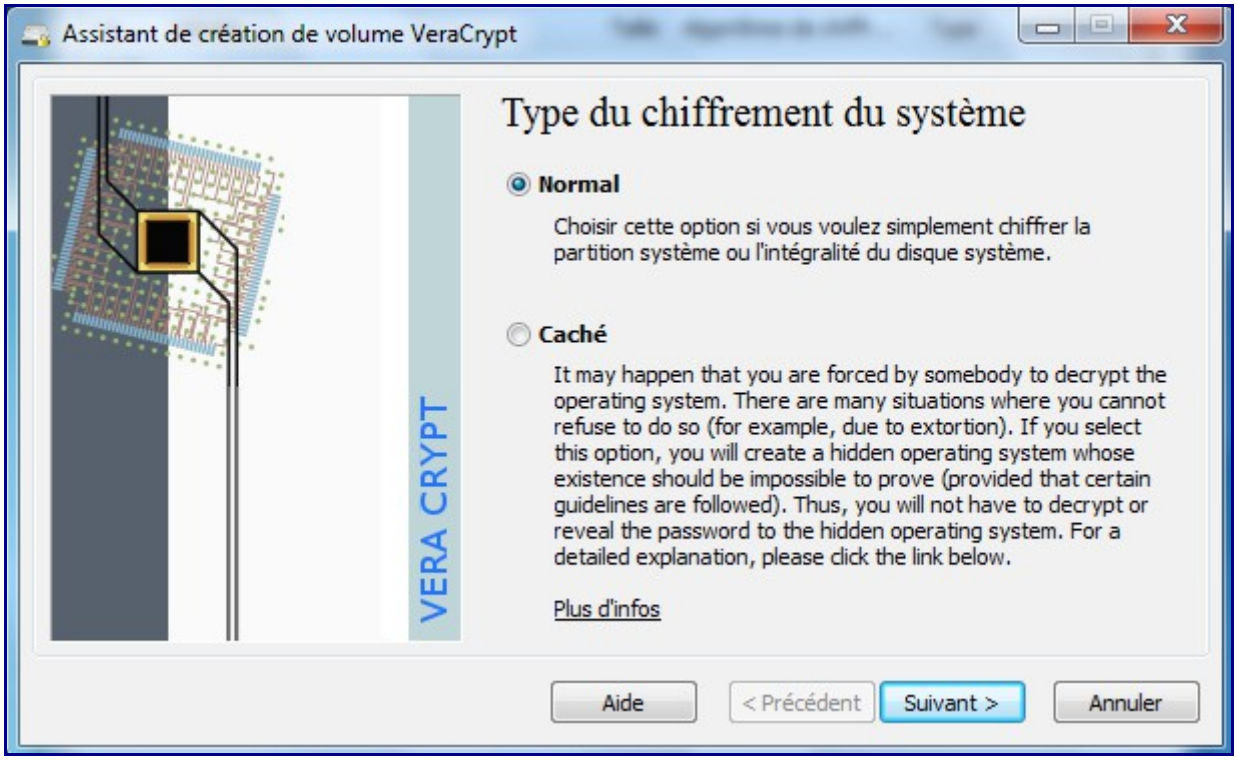
Plus délicat maintenant mais tellement plus efficace, la mise en place du cryptage au niveau du volume complet où se trouve le système d'exploitation.

Autrement dit, le système démarre au sein d'un conteneur chiffré.

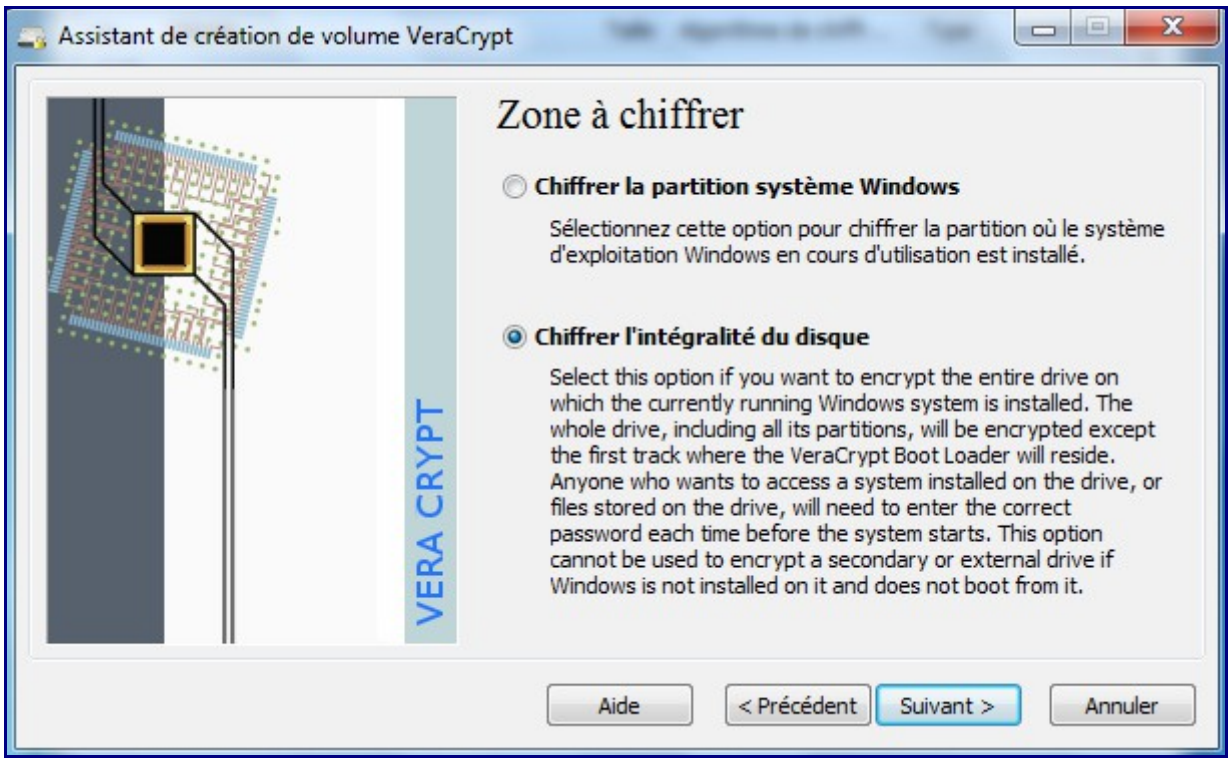
Pour commencer, il faut avoir son OS et VeraCrypt installés normalement.

1 – aller ensuite dans le menu Système / Chiffrer la partition/le disque système…

Choisir « Normal »



– Dans le choix suivant, soit vous décidez de crypter le volume système seulement, à l'exception de toutes les autres partitions présentes, soit « Chiffrer l'intégralité du disque » , soit de « Chiffrer la partition système Windows » . Dans le premier cas vous décidez (et c'est sans doute le meilleur choix) de chiffrer le volume système et TOUTES les partitions présentes sur le disque physique ; dans ce dernier cas, un chargeur VeraCrypt sera installé : à chaque boot du système, le chargeur vous demandera le mot de passe Veracrypt et la séquence de boot système pourra démarrer ensuite.

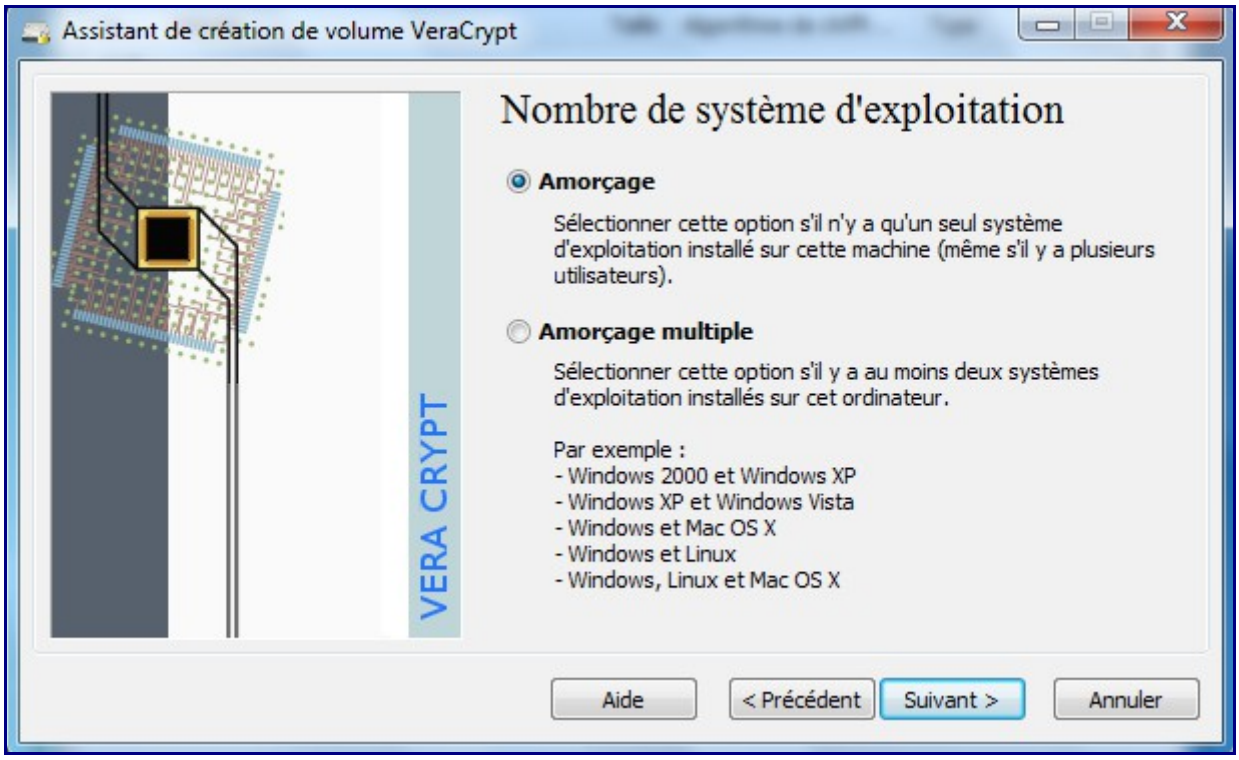


Attention, si vous avez choisi l'option « Chiffrer l'intégralité du disque », VeraCrypt va alors crypter TOUS les volumes du disque physique, y compris les volumes contenant des utilitaires ou boot spécifiques ou systèmes de restauration etc… Donc si pensez être dans cette situation (vérifier avec les DiskManager de Windows), choisissez Yes. Veracrypt va alors détecter ces volumes spécifiques et les exclure.

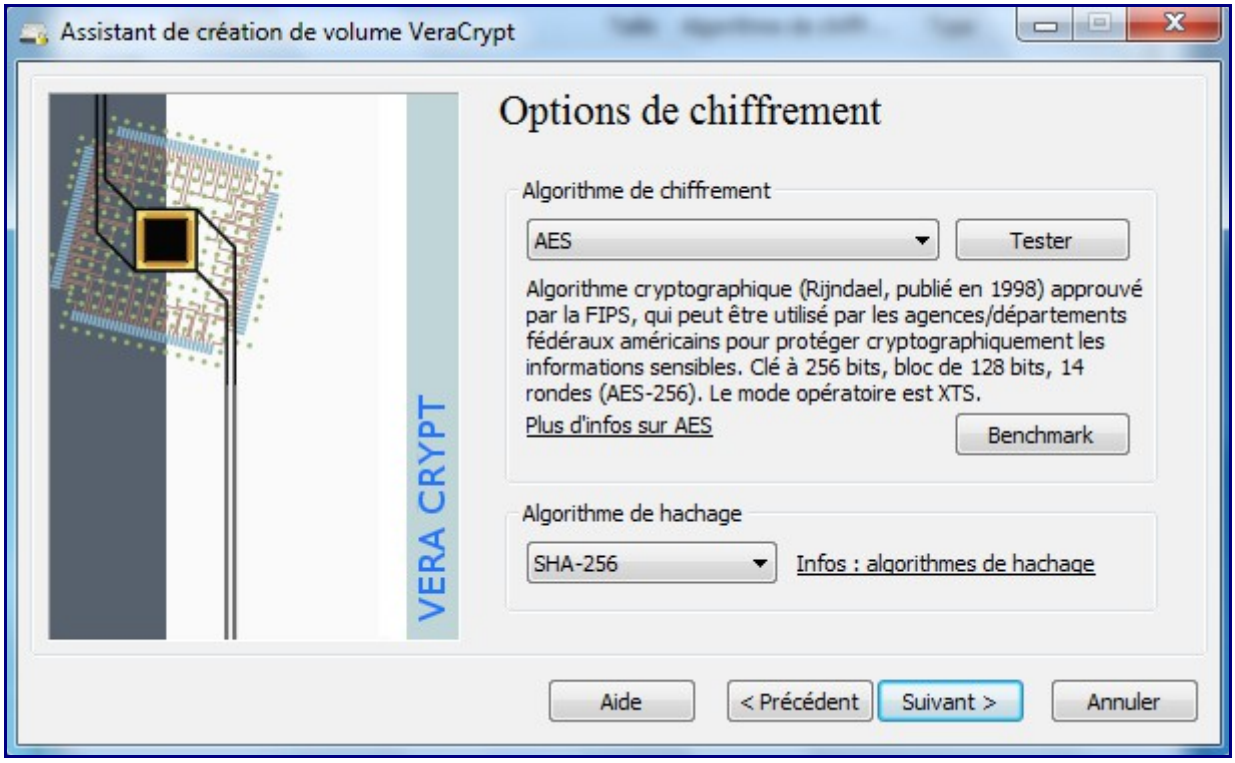
Dans le cas d'un volume sur un disque virtuel, sur certains portables également, on pourra choisir No.

L'écran suivant permet de spécifier si le module de boot doit intégrer la présence de 1 ou plusieurs

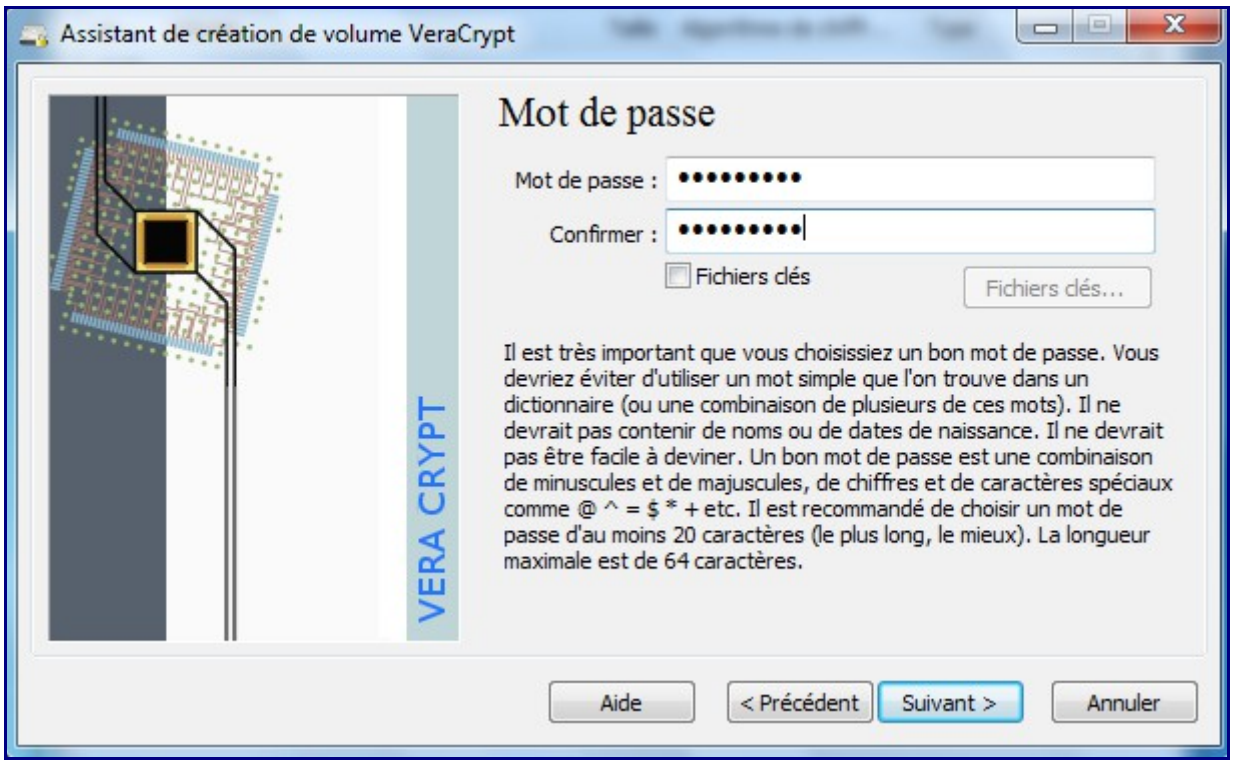
OS déjà installés en multi-boot.



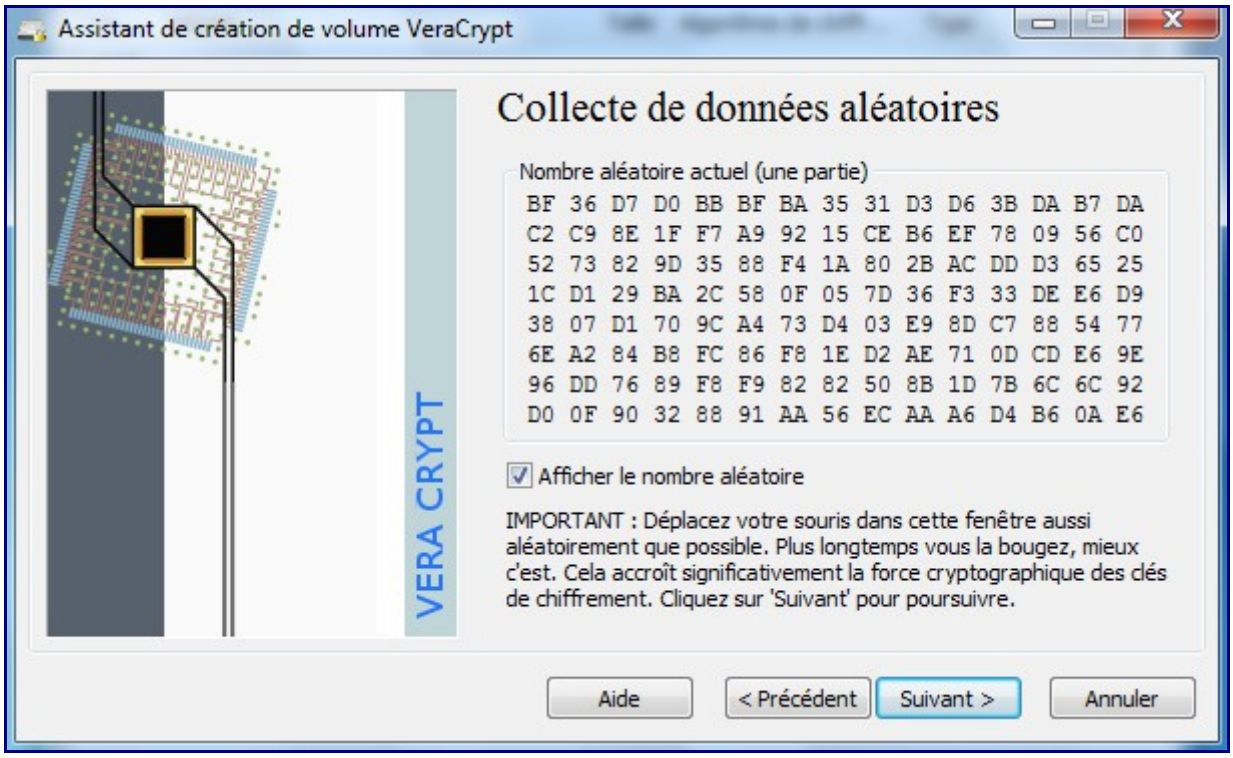
Étapes suivantes, choisissez l'algorithme de cryptage :



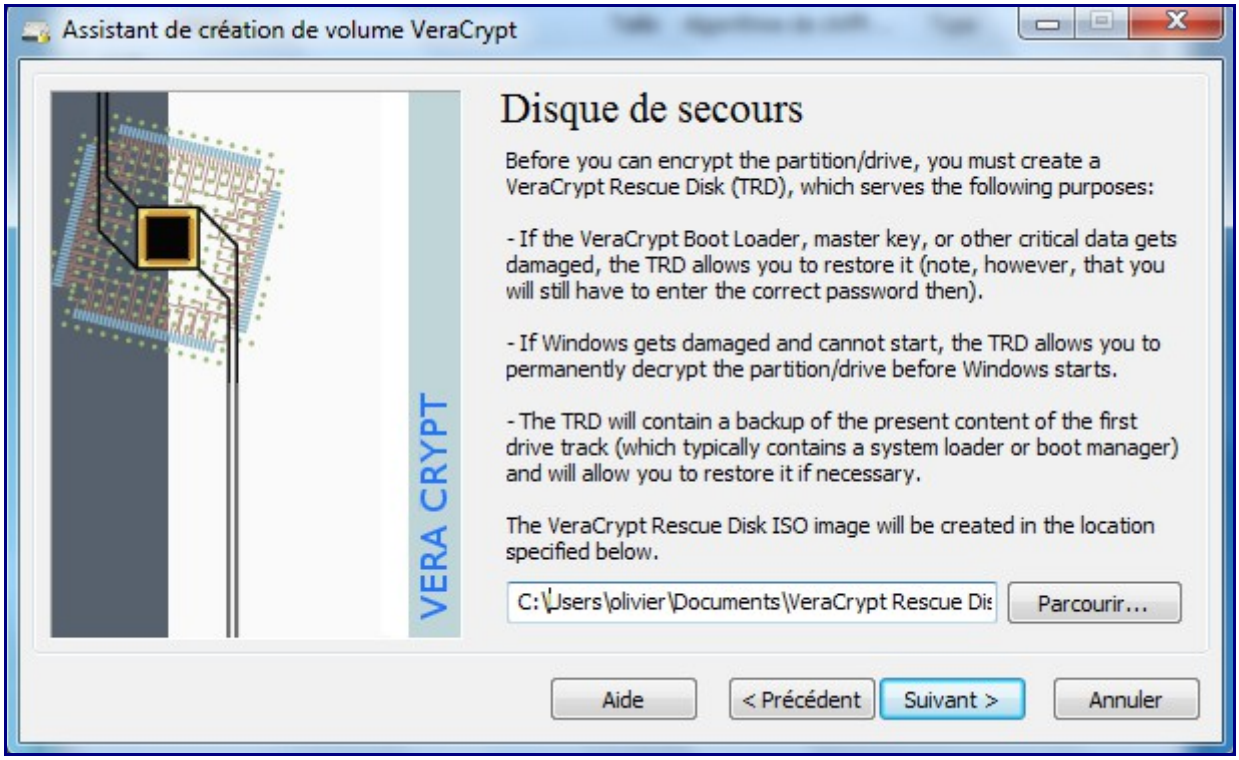
Spécifiez votre mot de passe suffisamment robuste, c'est à dire 20car min avec une complexité habituelle (vous pouvez le tester ici : http://www.passwordmeter.com/)



Puis se démarre les séquences de génération de clés :

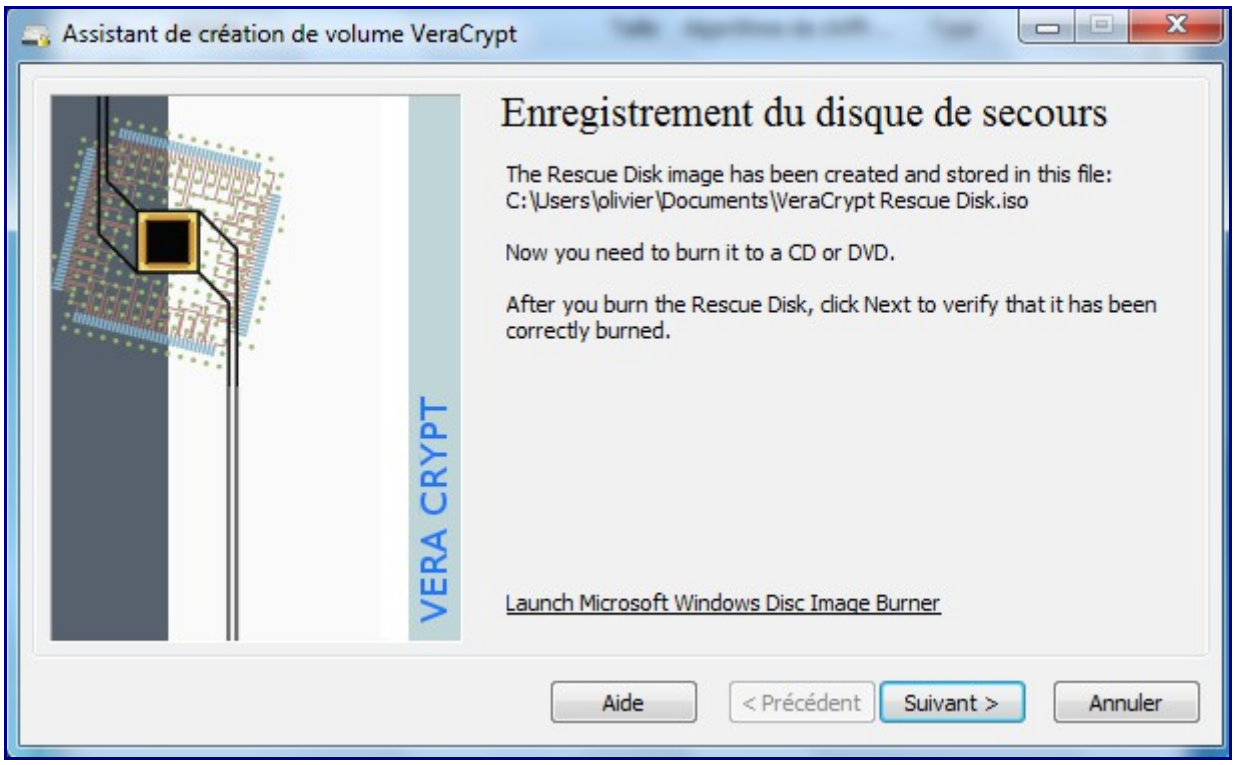


L'étape suivant consiste à créer un fichier ISO de secours – passage obligatoire.

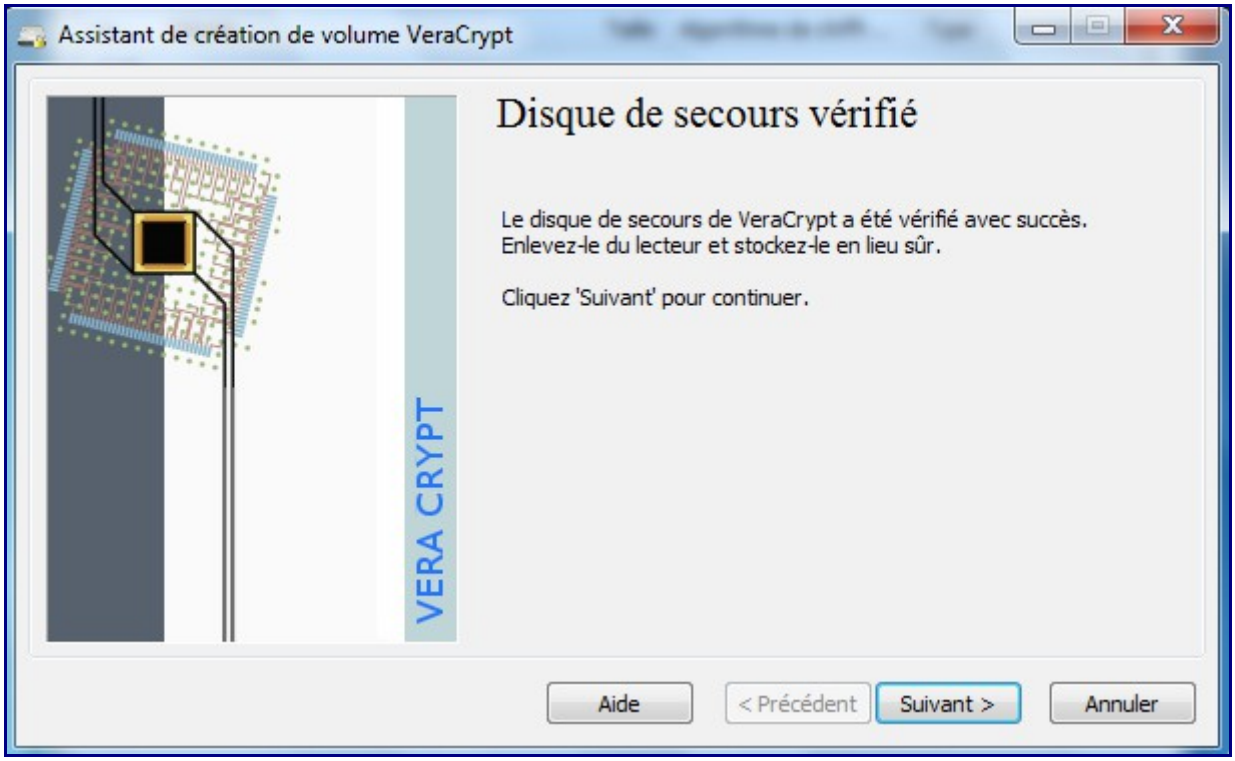


Ce fichier est stocké sur un autre CD ou DVD.

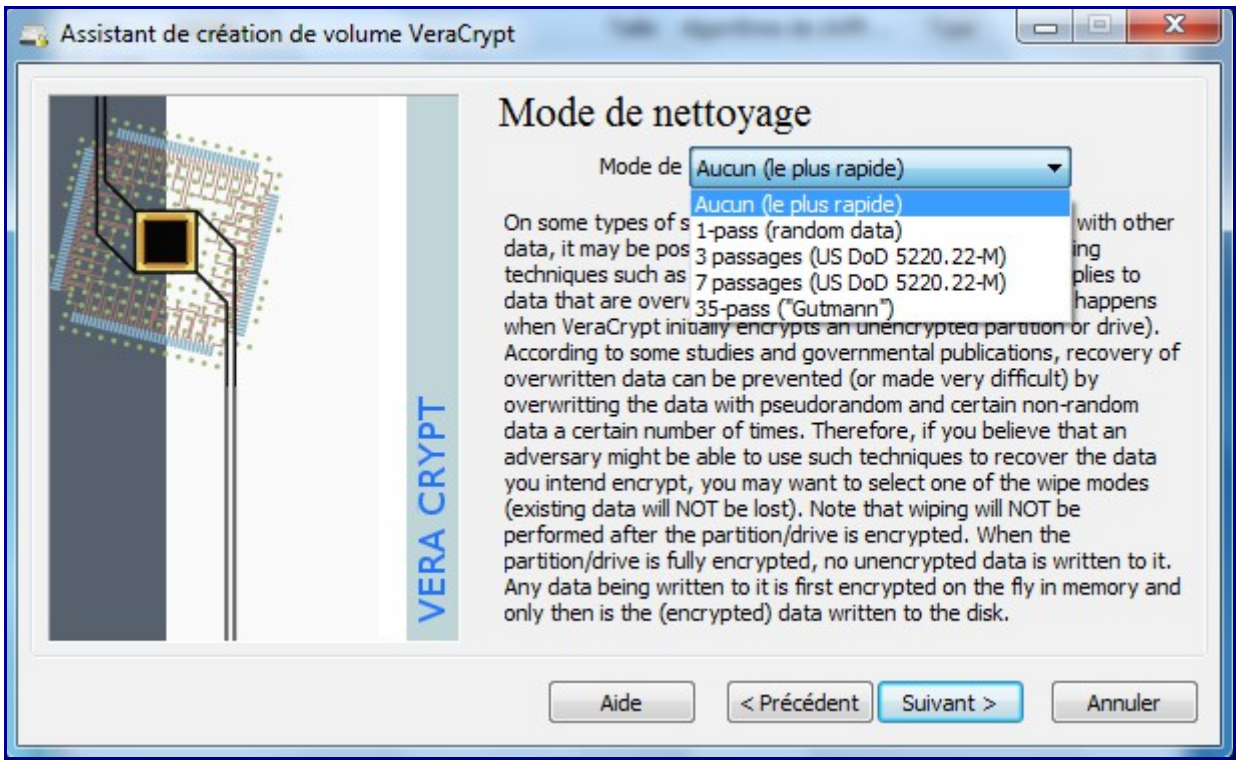
Il vous permettre de booter votre système, de déchiffrer votre partition et contient une sauvegarde des premiers secteurs de boot. Veracrypt vous invitera d'ailleurs à le graver sur un CD ou DVD immédiatement : condition nécessaire pour pouvoir lancer le cryptage de la ou des partitions.



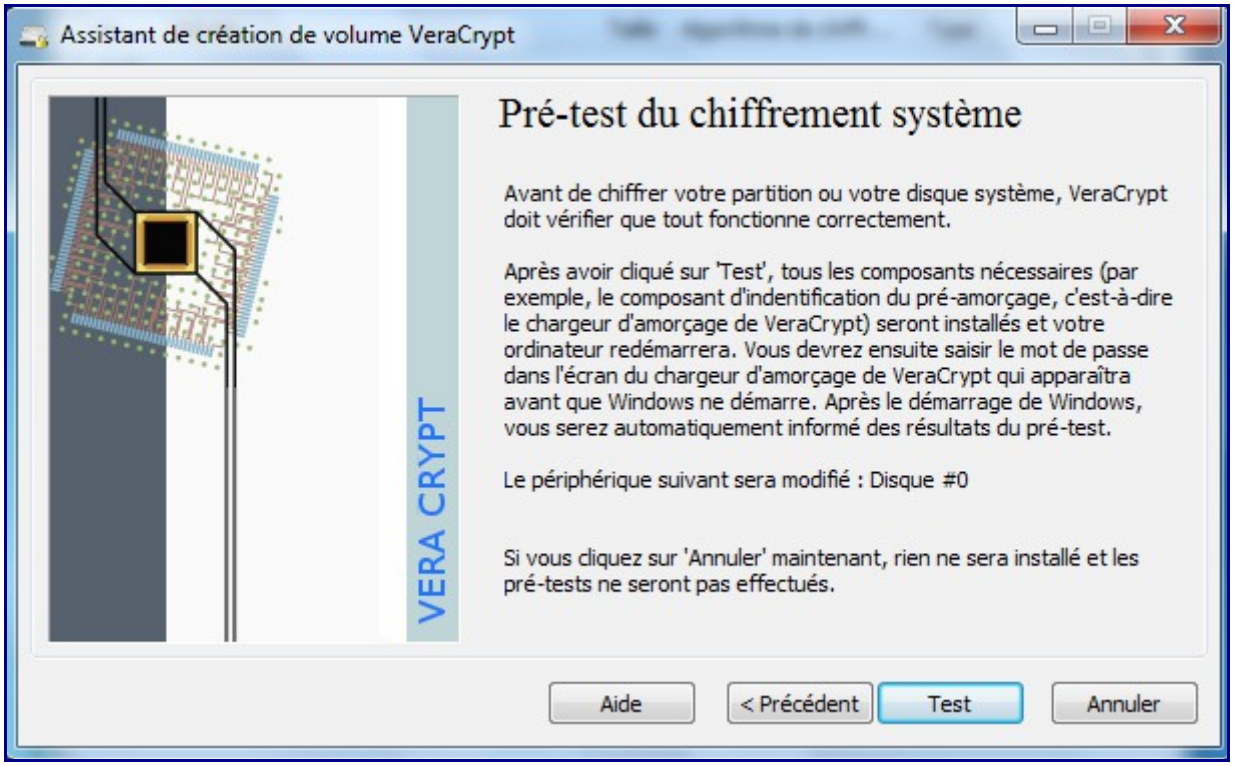
Une fois, le CD gravé, vous devrez vérifier la bonne issue de l'opération.



Dernière opération : VeraCrypt prévoit une passe simple ou complexe de nettoyage du volume afin de réduire toute récupération de donnée non chiffrée.

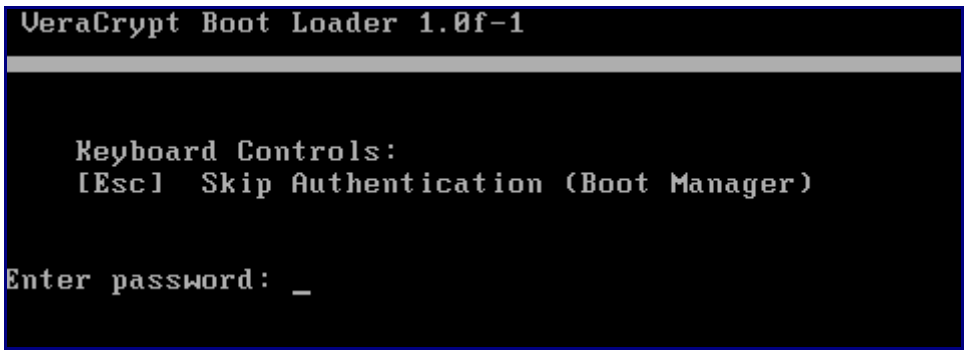


Ensuite, VeraCrypt fera un premier test de chiffrement du système (au prochain reboot) :



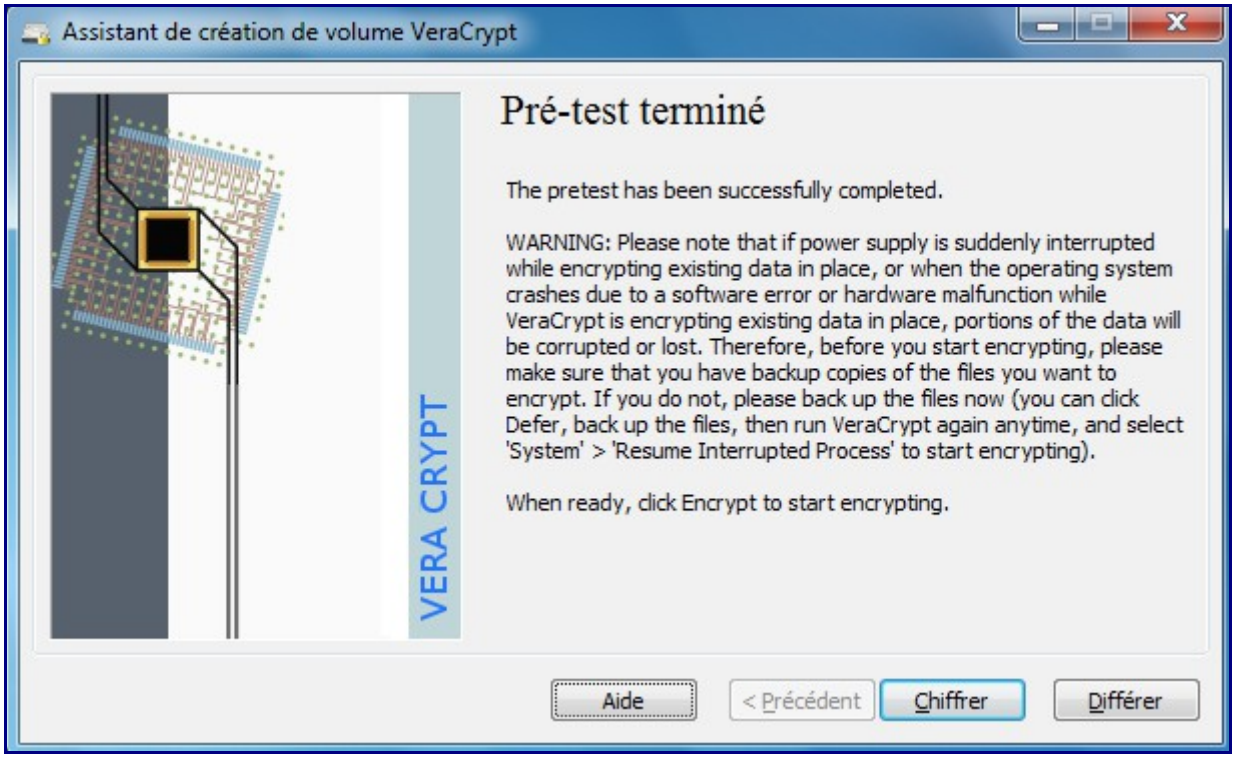
Un dernier click : le reboot de votre système est lancé

Au boot du système, VeraCrypt vous demandera votre mot de passe :



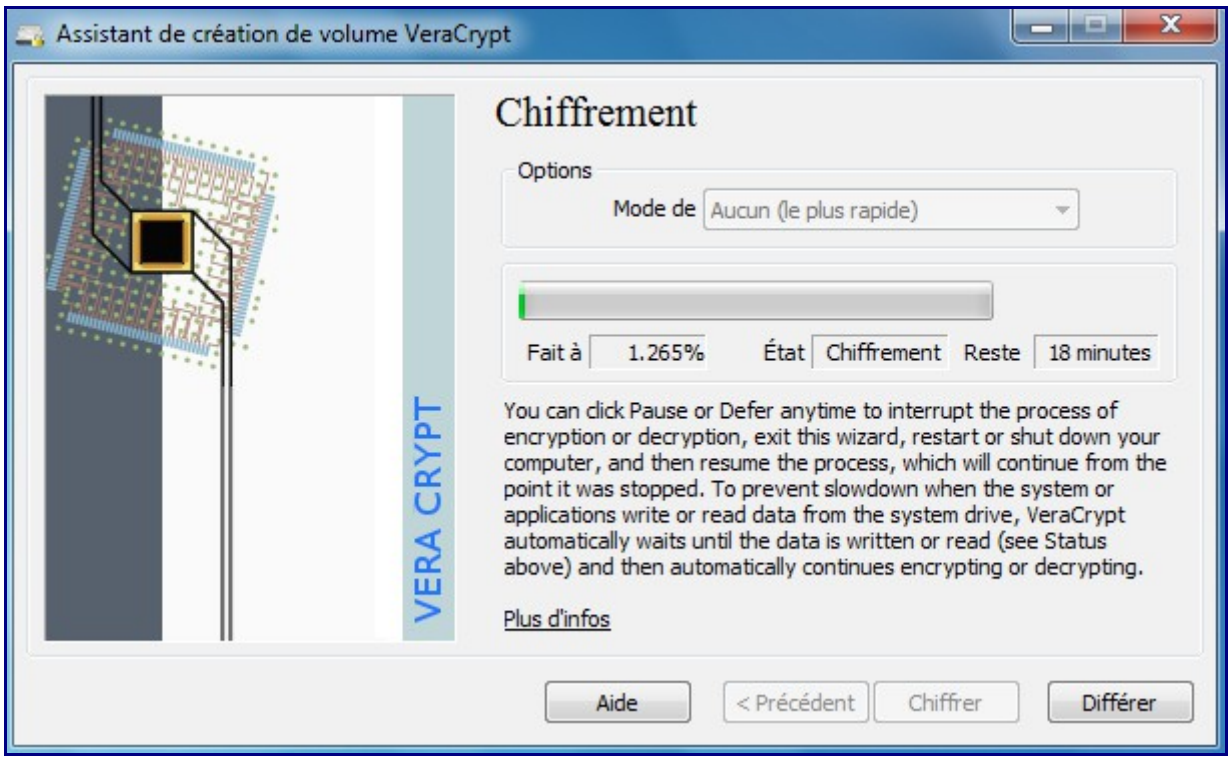
Il suffit de le saisir, et Windows démarrera (pour faire un premier test de boot).

Après ce premier reboot, VeraCrypt doit valider que le prétest est OK puis vous proposera de lancer le cryptage final des partitions.



Appuyez juste sur « Chiffrer » et c’est parti pour le chiffrement des partitions.

Ci-dessous une progression ; environ 25 minutes pour 30 Go.



A la fin :

Vos partitions sont chiffrées !

PS : si la partition est chiffrée, une fois l'OS démarré, les données sont bien entendues en clair accessible depuis l'explorateur, donc également à travers le réseau du PC…

9 – Crypter ET cacher sa partition (système) –

(partie non mise à jour pour VeraCrypt)

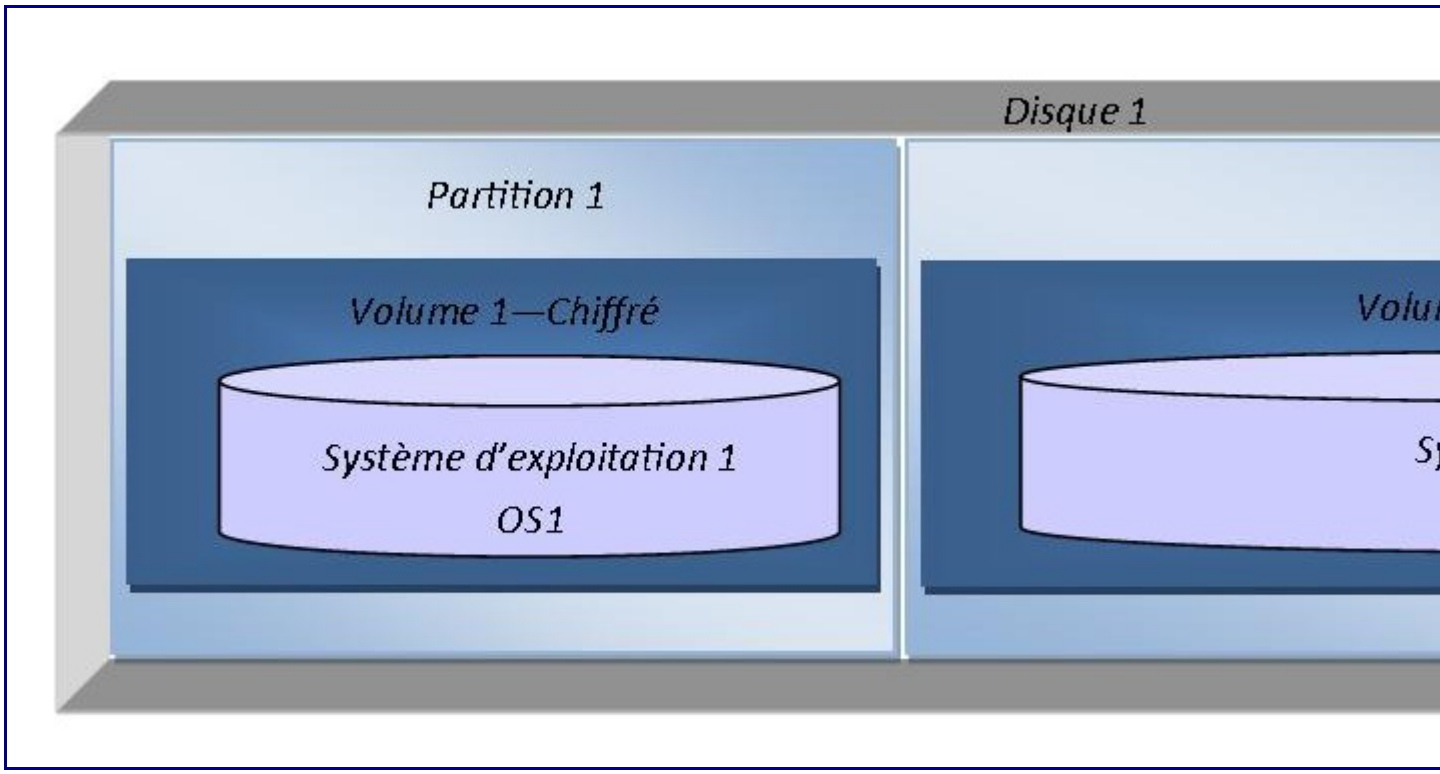
Cela peut s'avérer utile lorsque vous voyagez dans certains pays où on peut légalement vous demander votre portable à la douane : crypter un volume de données, ET le rendre non visible afin

de ne pas susciter d'attention particulière.

Cette méthode est sensiblement plus complexe que l'étape précédente.

Globalement cela consiste à mettre en œuvre un premier OS sur une partition cryptée dans lequel nous insérerons un second volume contenant l'OS final (et donc les données) crypté et caché. Le premier OS sera ensuite formaté et vous devrez réinstaller un OS sur cette première partition !

Voici ce à quoi va ressembler votre partitionnement final :

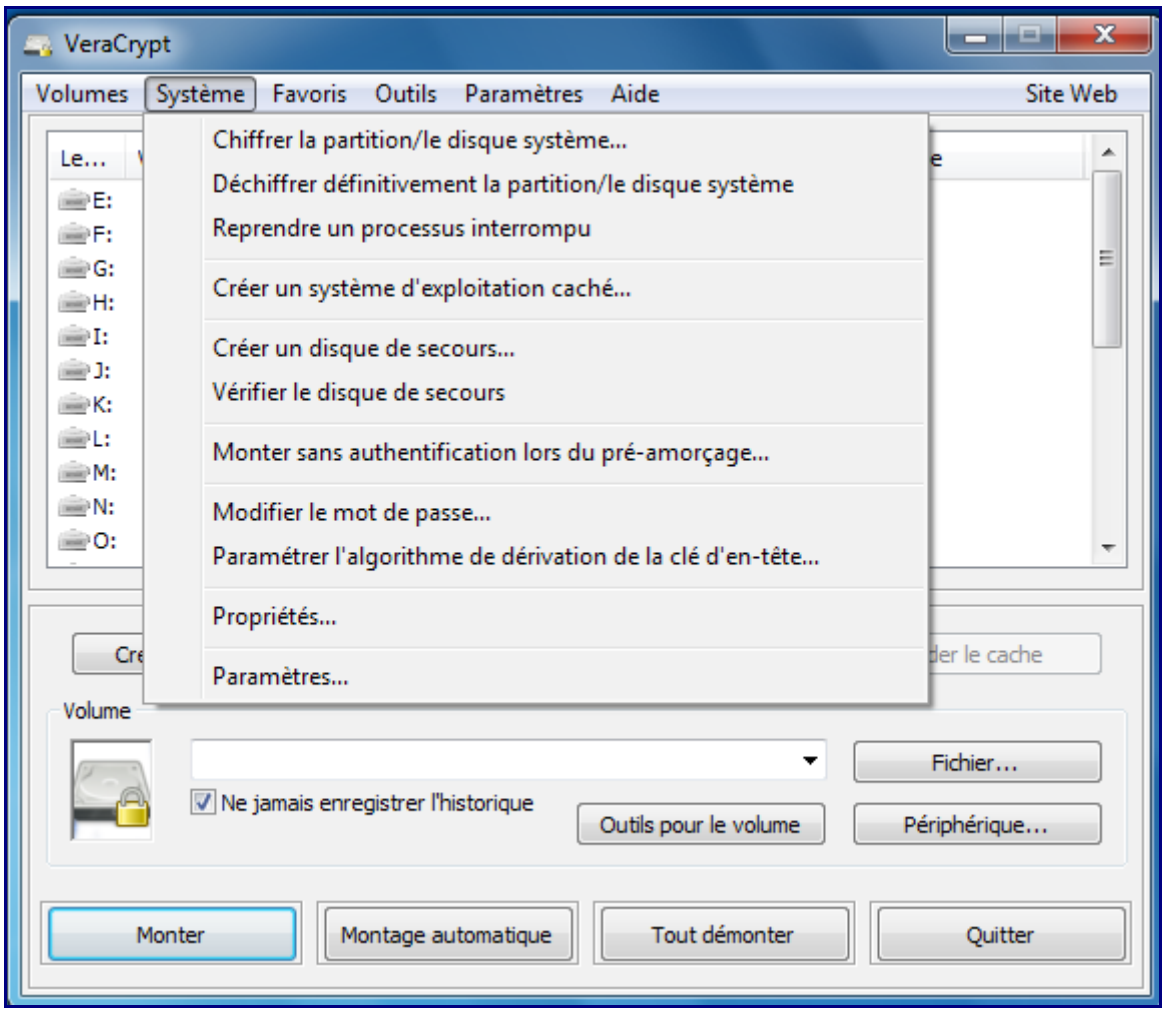


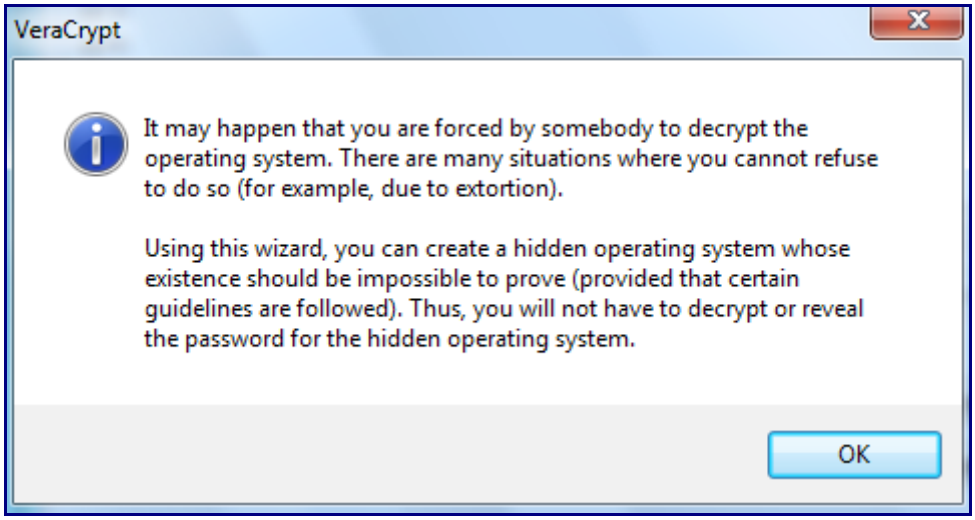
La partition 1 est celle qui reçoit l'OS crypté qui servira de leurre (c'est l'OS1).

La partition 2, juste après la partition 1 est celle qui reçoit l'OS crypté et caché (c'est l'OS2) : sa taille doit être de 2.1 fois la partition 1. La partition 2 doit être créée..

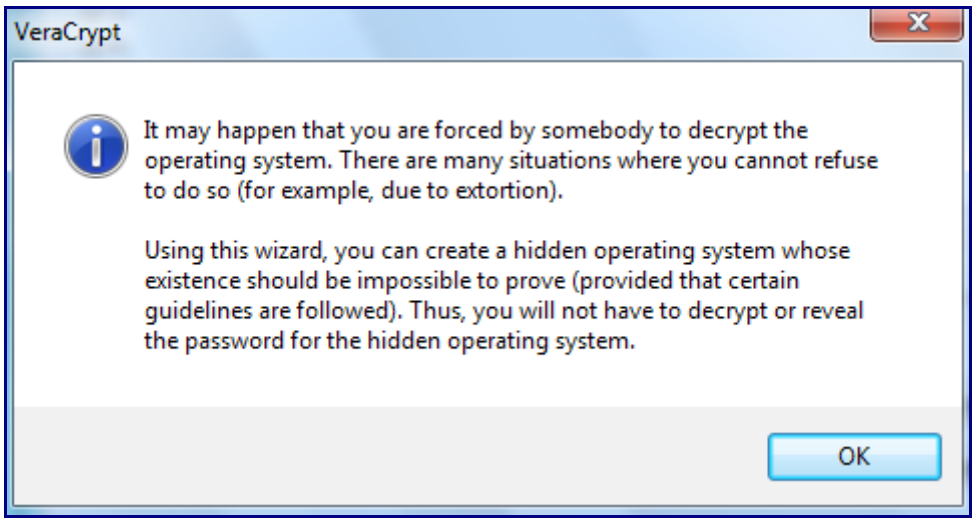
Sur l'OS1, vierge avec VeraCrypt installé :

1 – dans le menu Système, choisissez « Créer un systèmes d'exploitation caché»

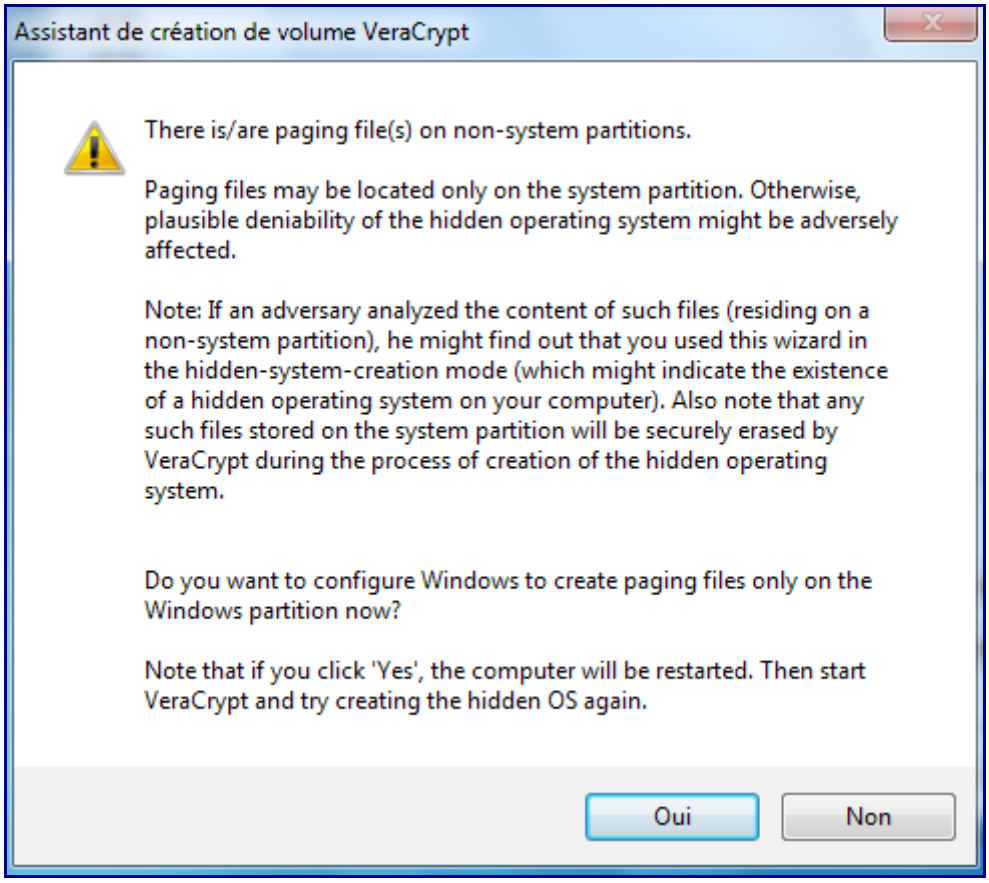




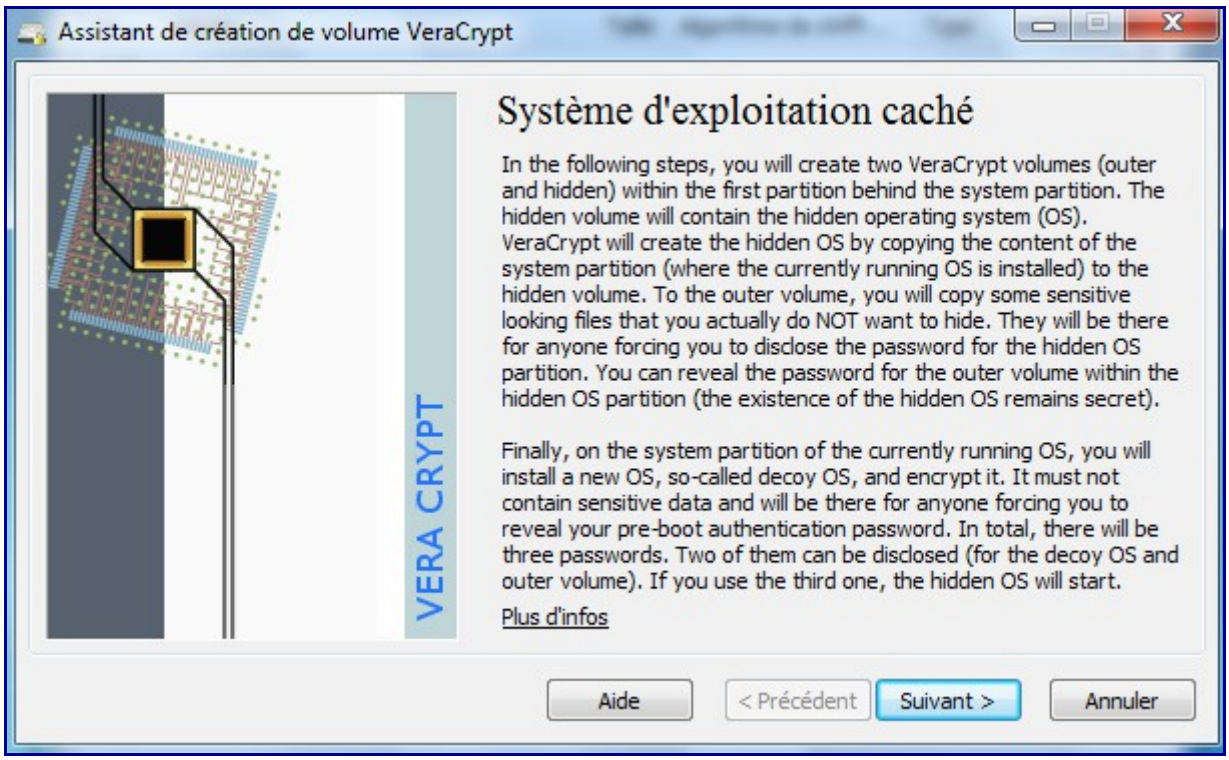
On vous prévient que vous DEVREZ réinstaller vos OS situé sur la première partition. Votre OS1 et le contenu entier de la partition 1 sera recopié sur la partition 2.



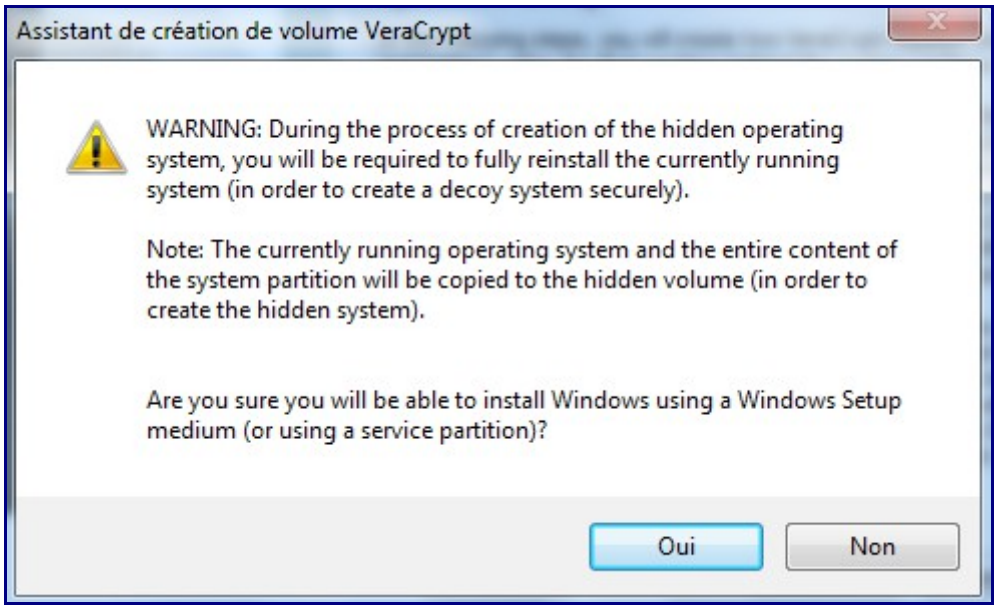
Dans la question suivante, VeraCrypt détecte que le fichier d'échange est sur votre partition system ce qui peut représenter le risque de dévoiler la présence de votre partition système cachée. Si vous répondez Yes, Veracrypt fera la modification nécessaire.



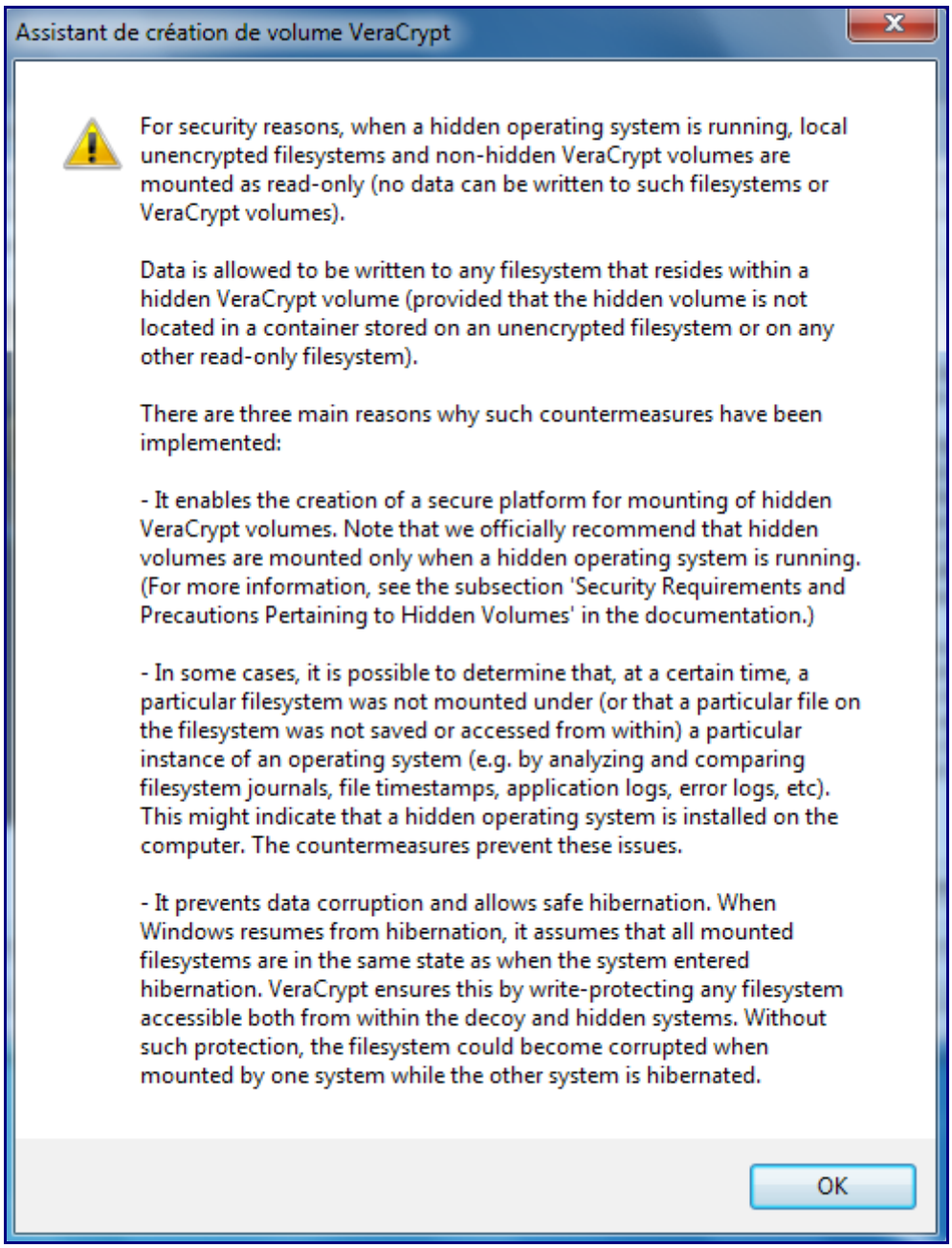
Après le reboot éventuel pour suppression du Pagefile.sys, on peut relancer la séquence :



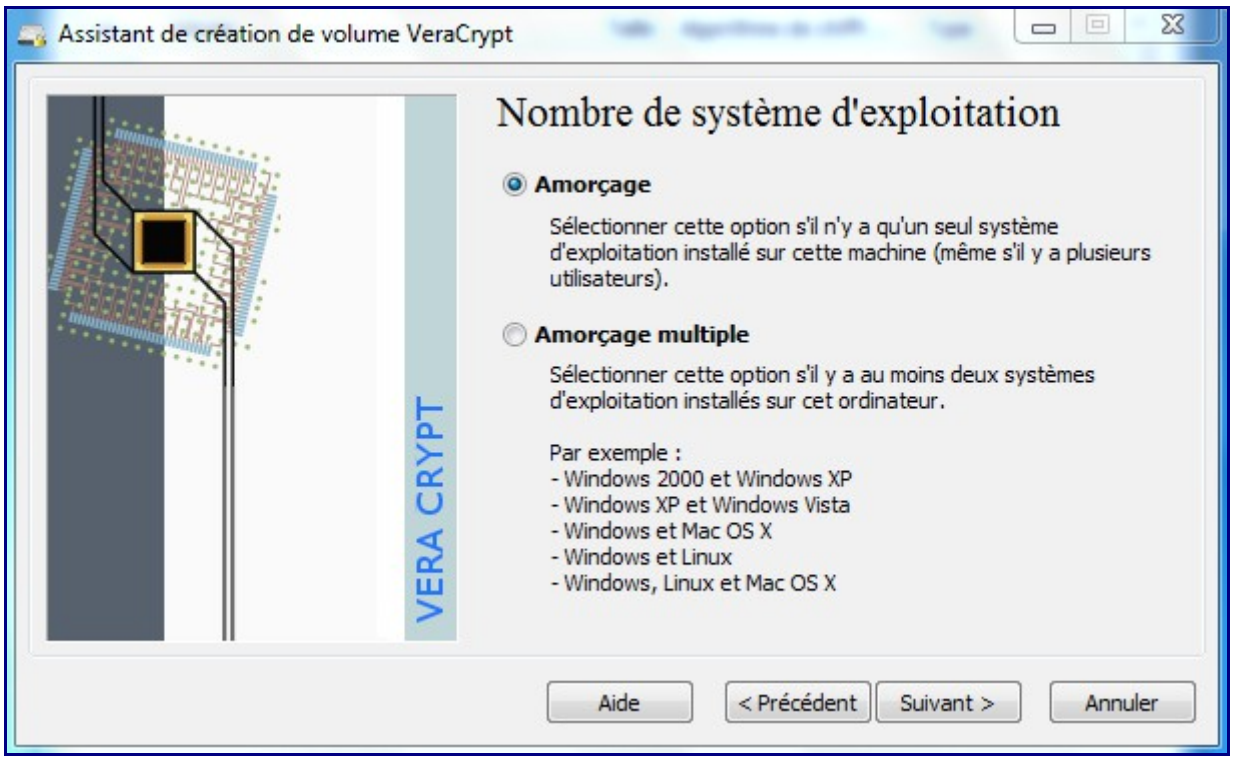
On vous rappelle que l'OS1 sera à réinstaller (donc supprimé)



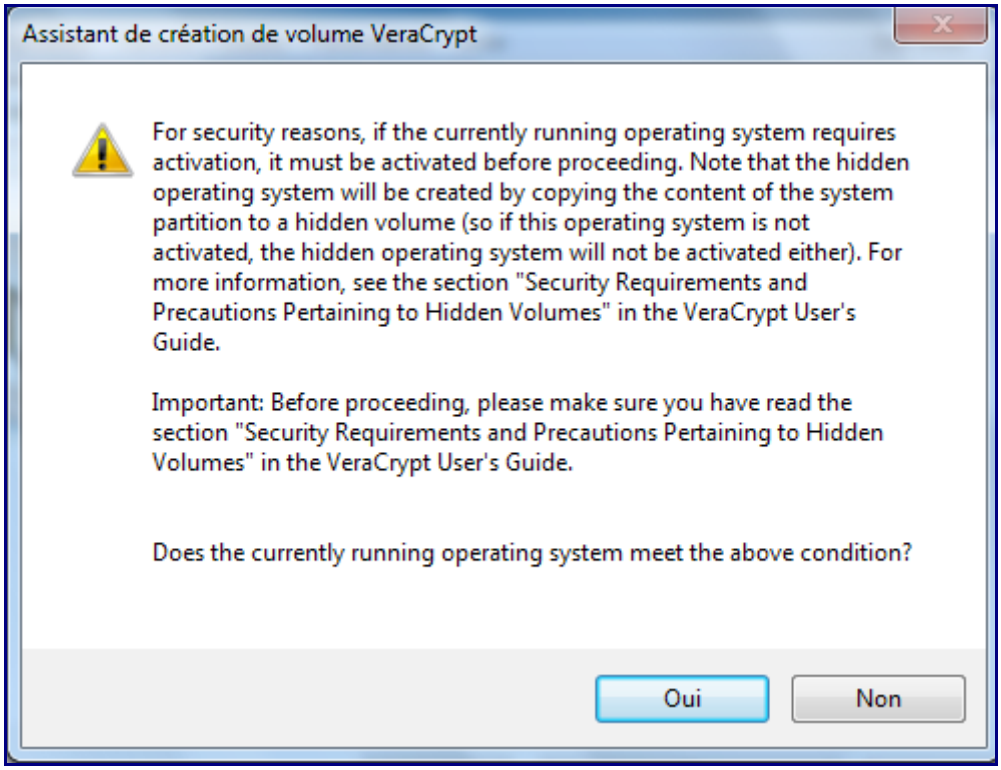
Attention, nombreux avertissements de sécurité qui visent à faire en sortie que l'usage d'un système crypté/caché reste « indétectable » : raison pour laquelle toute écriture en dehors de la partition 2 (typiquement sur la partition 1) ne sera pas possible.



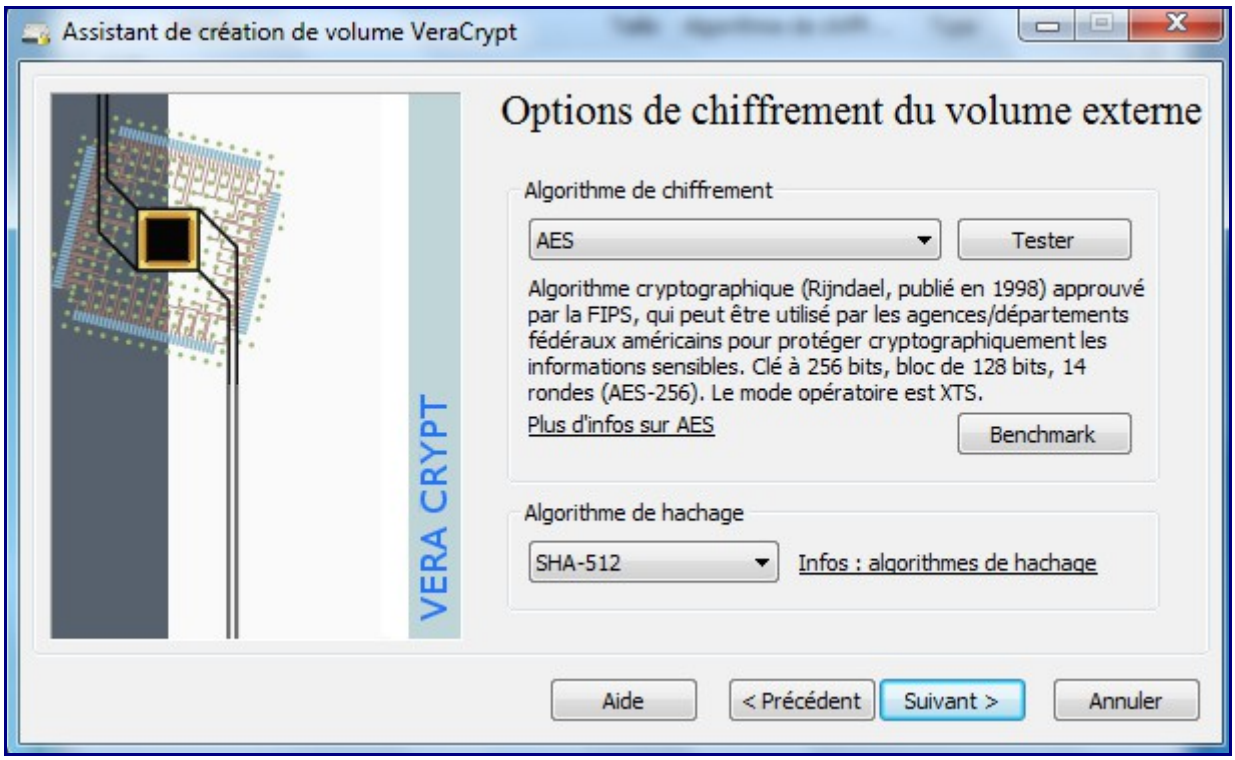
Page suivante : on retrouve l'installation du BootLoader qui sera adapté en fonction votre choix « avez-vous un seul OS ou bien avez-vous plusieurs OS distincts ? »

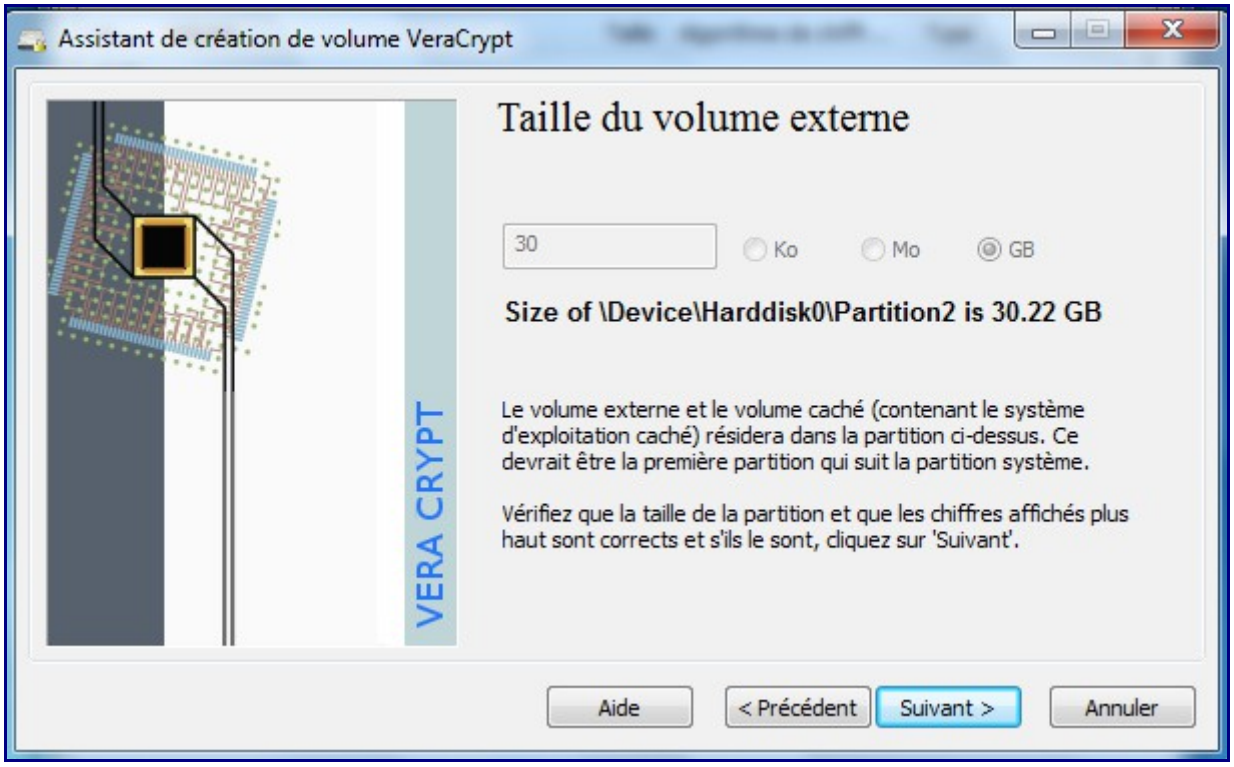


Info importante : sous Windows, assurez-vous d'avoir activé votre système auprès de Microsoft avant de lancer la copie vers la Partition 2. Toujours pour éviter de faciliter la détection de l'existence de cet OS2…

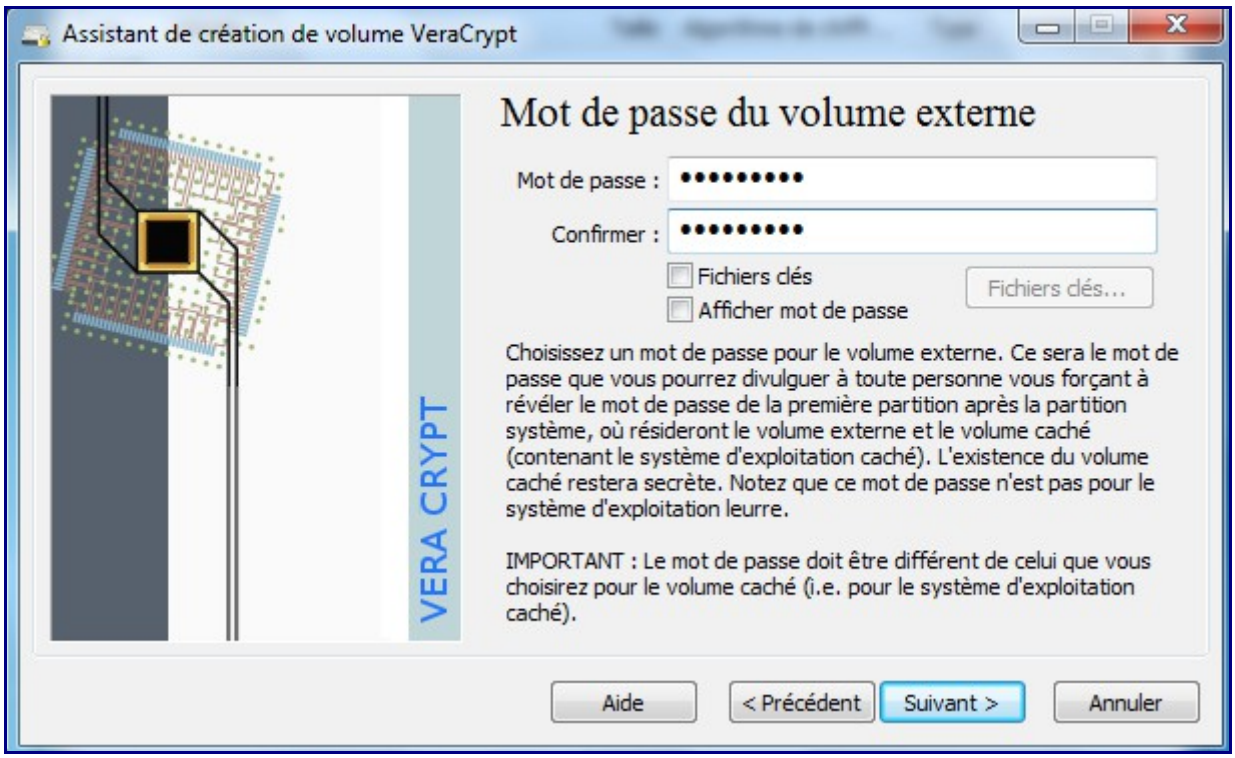


Le « Volume de Chiffrement externe » sera par défaut, la totalité de votre partition 1 (officielle) et partition 2 (cachée).



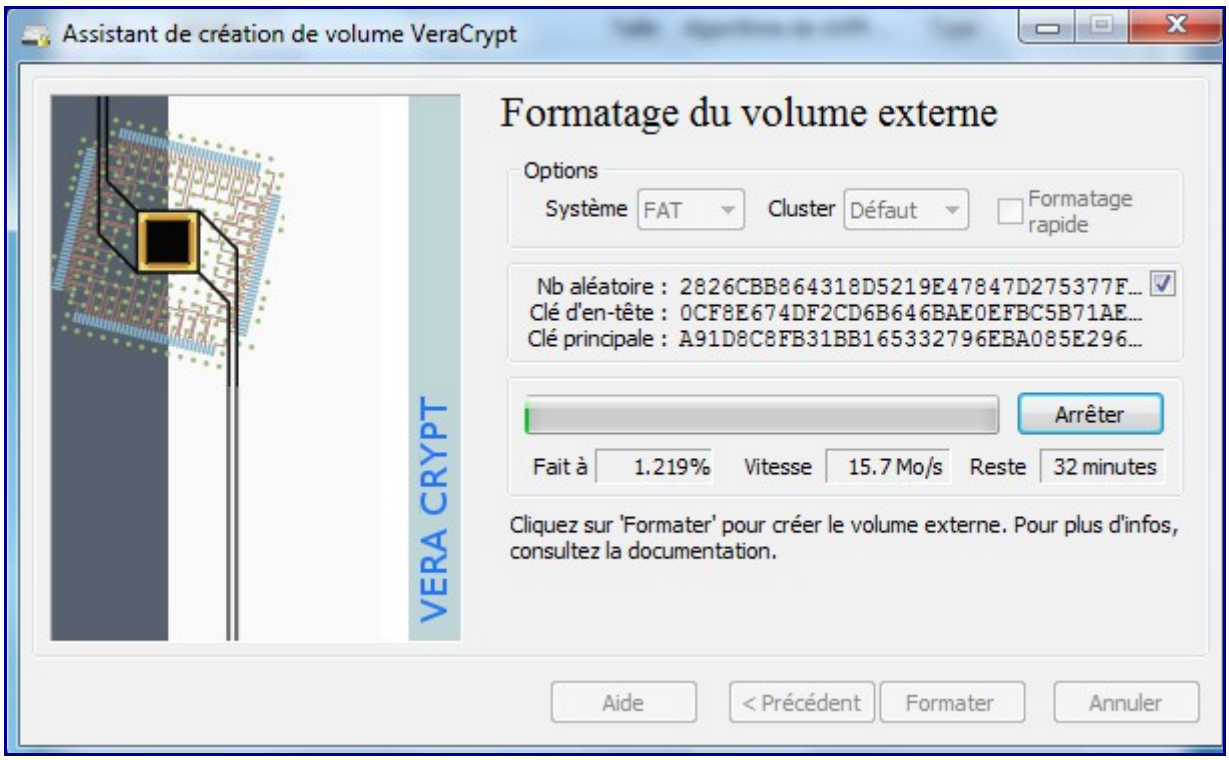


Spécifiez un mot de mot de passe spécifique pour l'accès à ce volume.

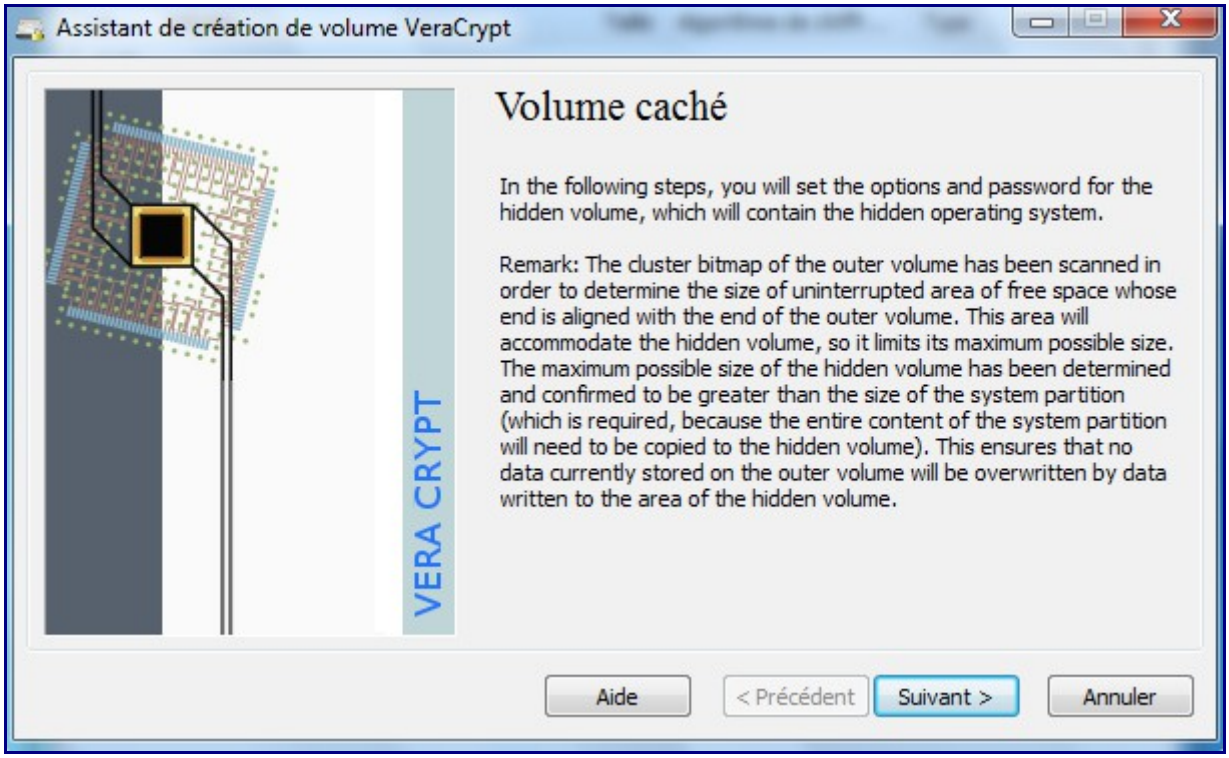


Rappel que tout ce qui se trouve sur votre seconde partition sera effacé.

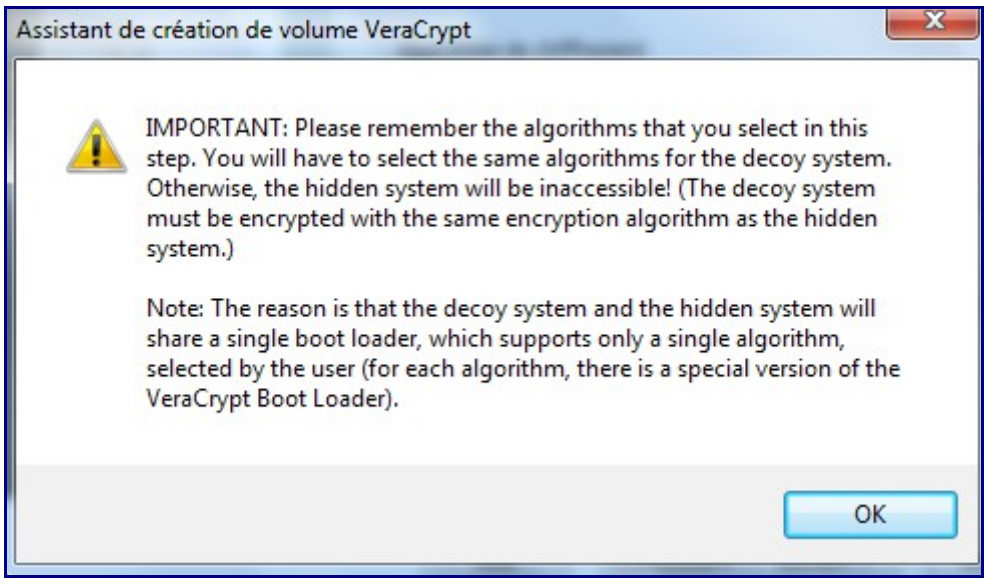
On lance le formatage de la partition dès que vous avez généré assez de mouvement aléatoire avec votre souris.



Maintenant que le volume externe est créé est accessible (par d »faut monté sous Z:), on passe à la création du volume caché de la partition 2.

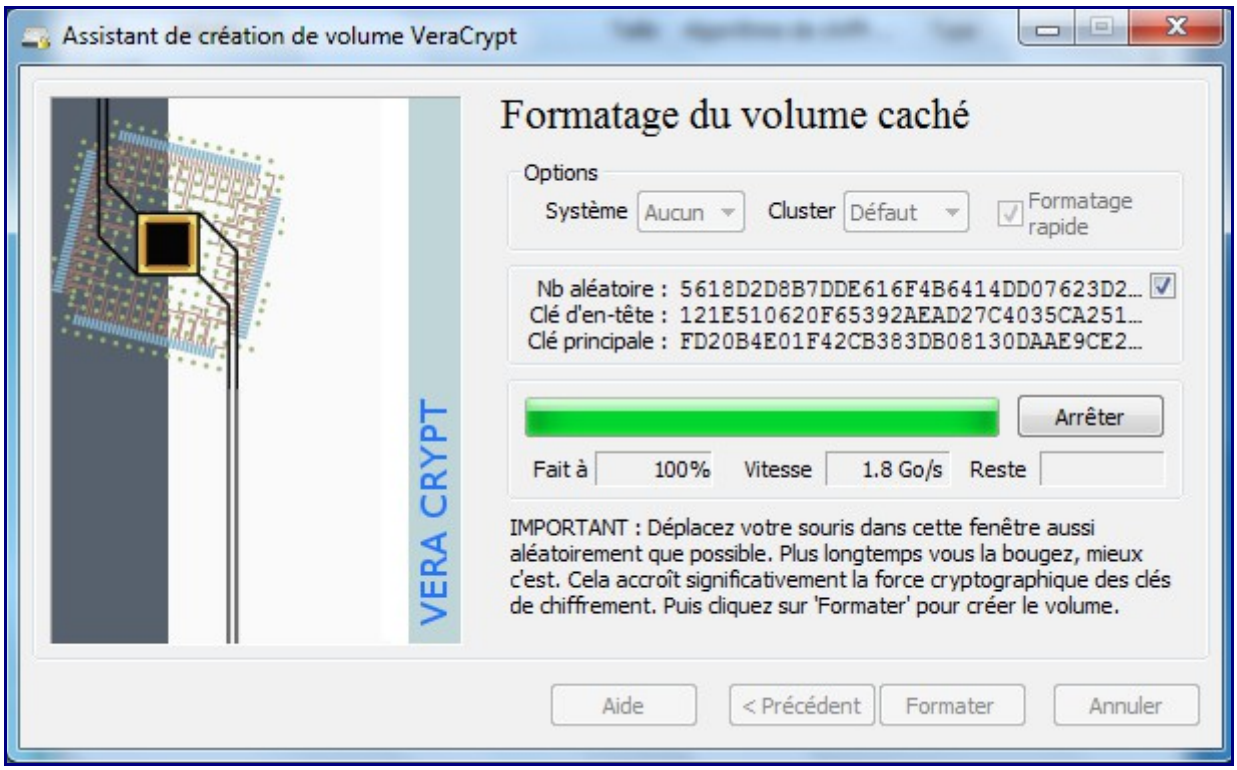


Attention : l'algorithme de cryptage de la partition 2 devra être le même que celui de la partition 1.

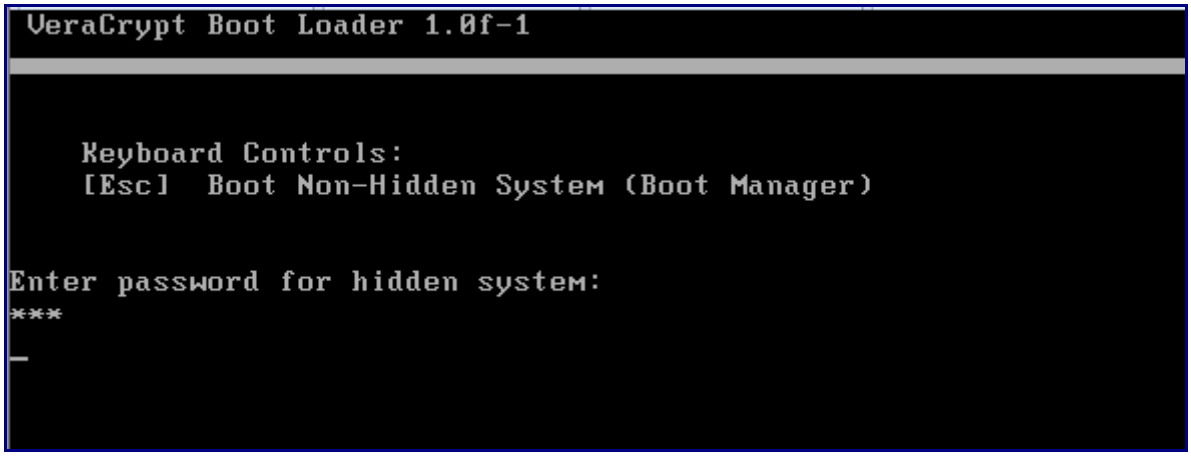


Spécifiez un mot de passe (un3ème) disctinct des 2 autres.

Formattage de la partition 2.

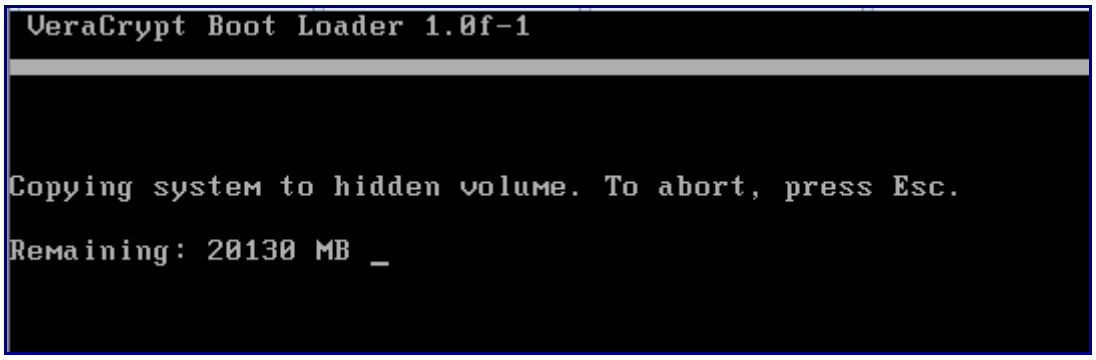


Reboot du système.



Saisissez le **dernier mot de passe saisi** (celui fourni pour la mise en œuvre du système caché)

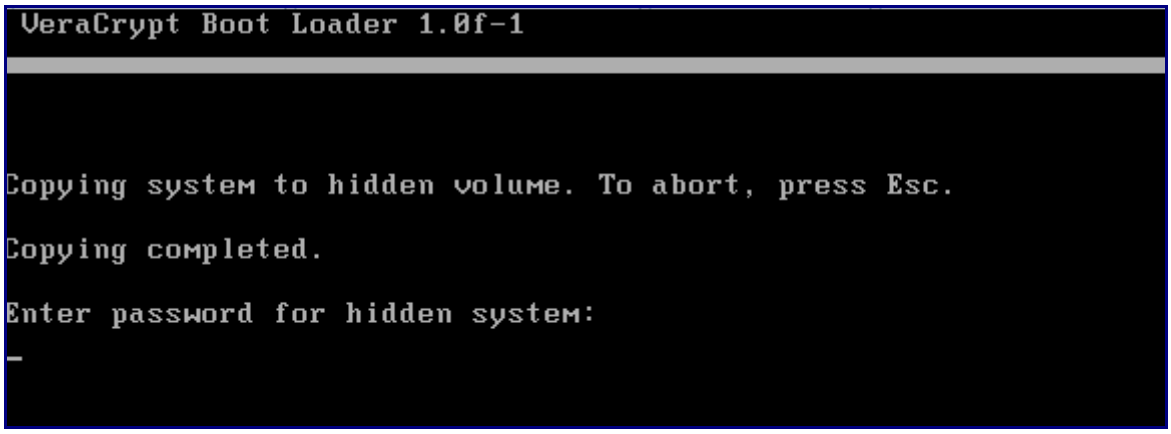
L'opération de recopie du premier système vers le second système en version cachée commence. (clonage de la partition 1 vers Partition 2.)



Et là, il faut s'armer de patience….

…

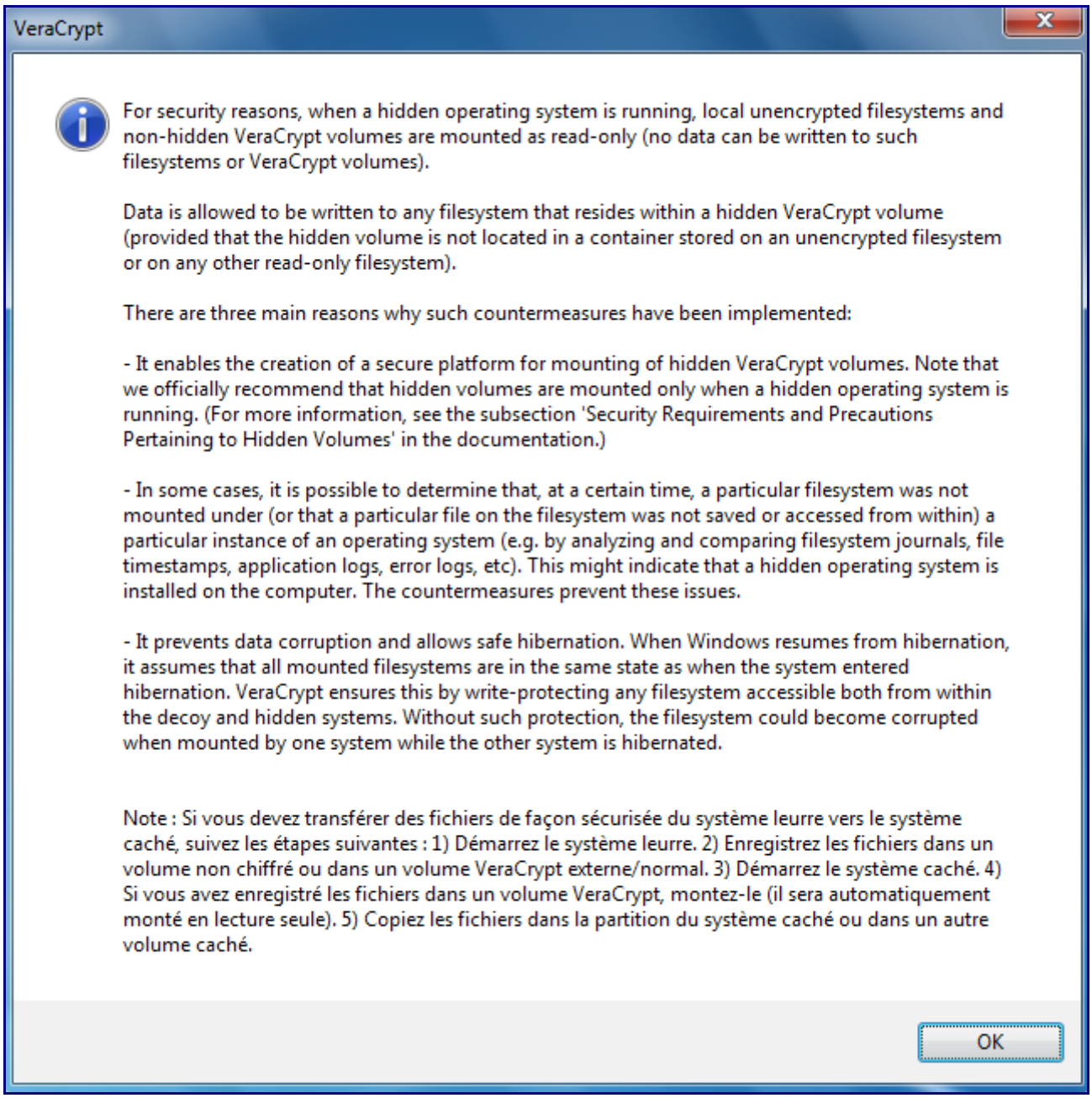
…



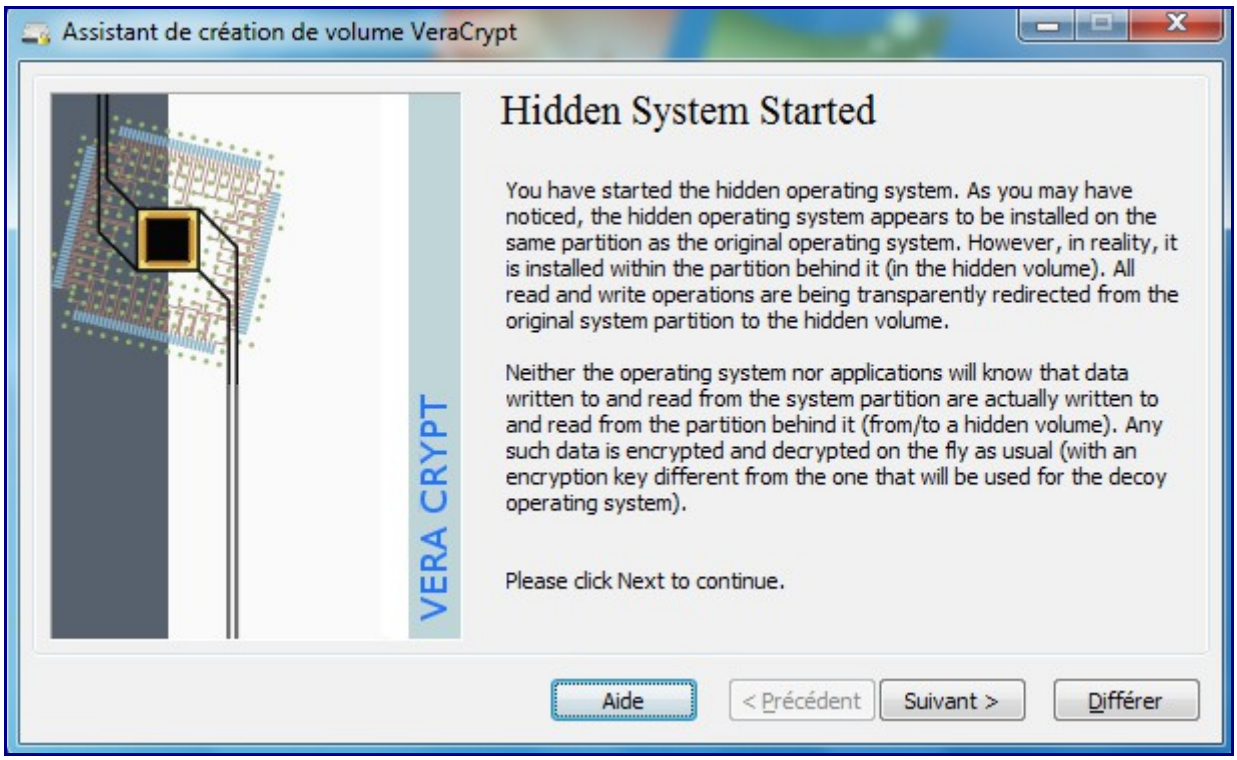
Quand la copie est terminée, ressaisissez à nouveau votre mot de passe (le dernier créé, celui de votre partition cachée).

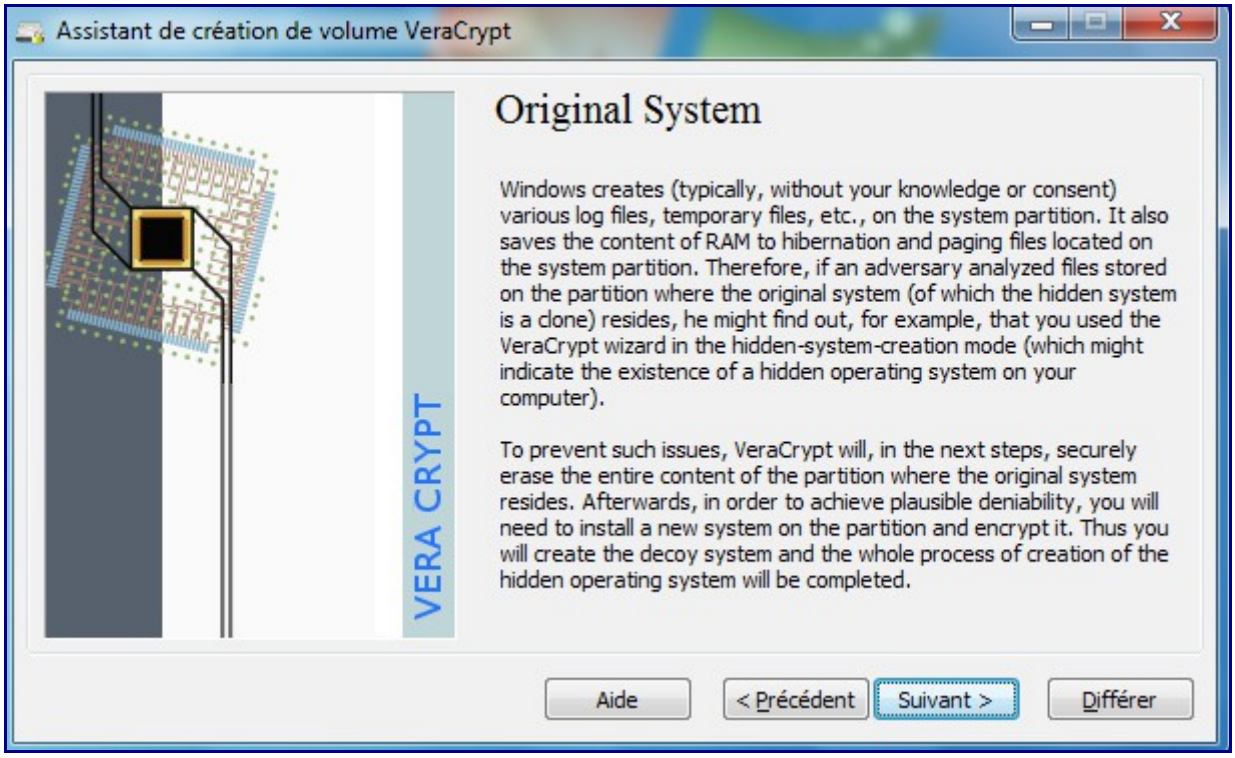
Votre système caché démarre.

A l’ouverture de session Windows, un nouvel avertissement fort sur les recommandations :

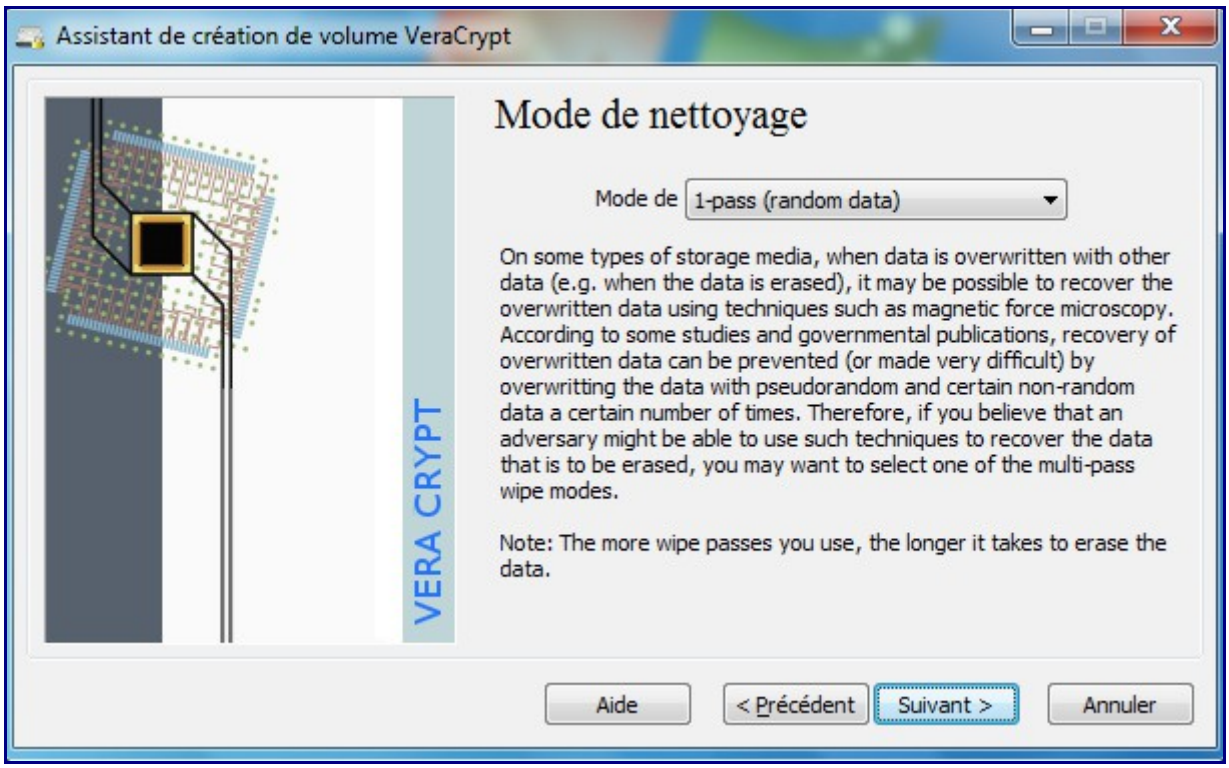


Ensuite démarre la procédure d’effacement de l’OS1 :

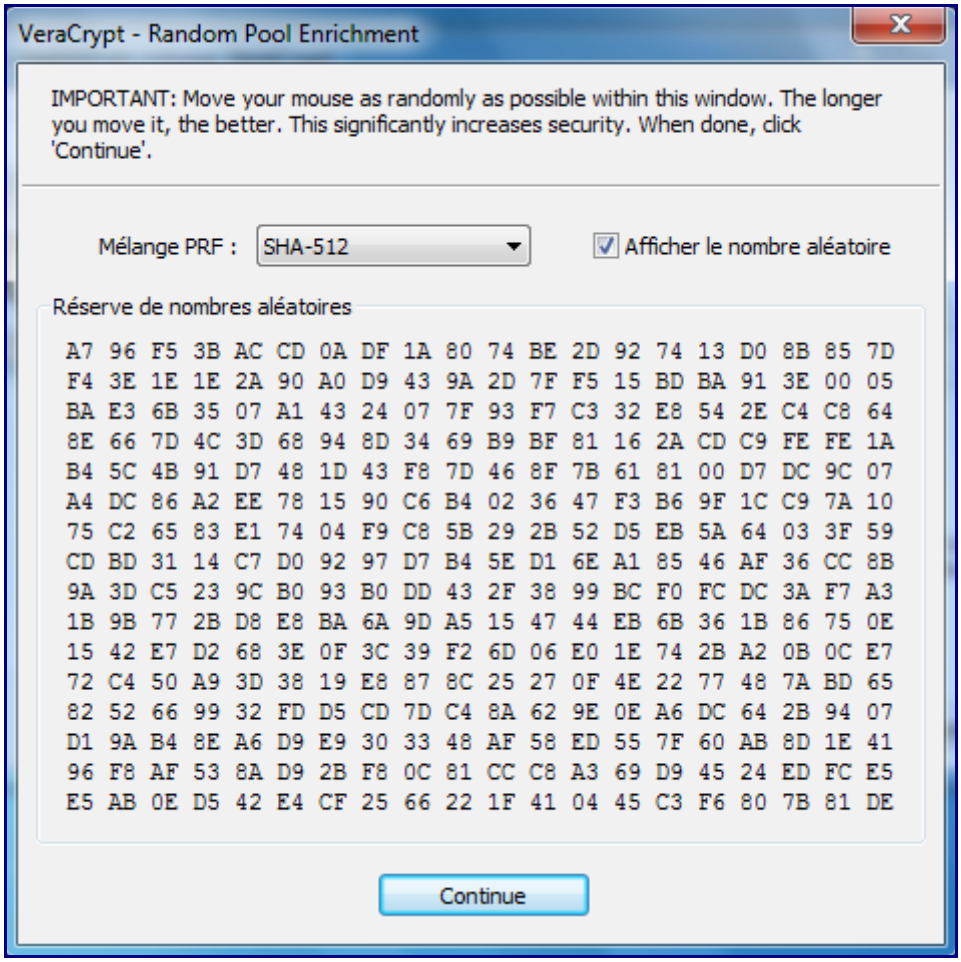




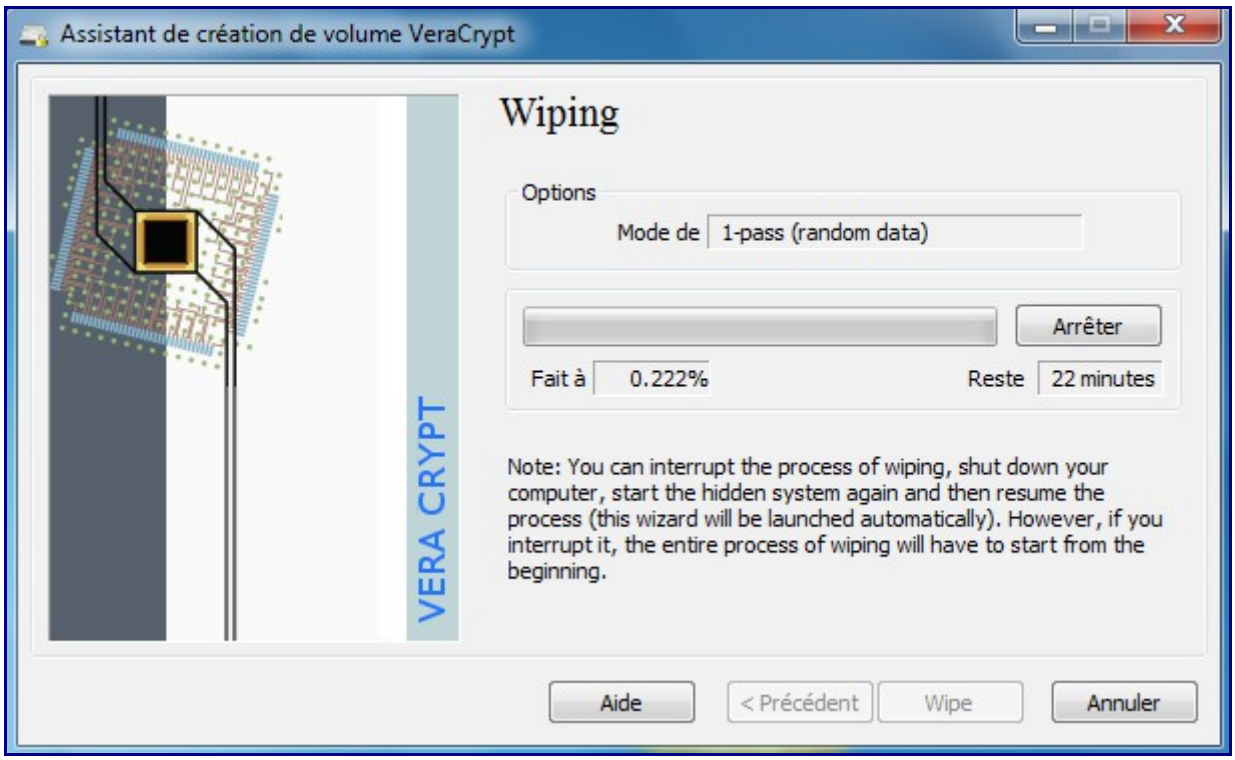
Une fois démarré, TrueCrypt va vous proposer d'effacer le plus efficacement possible le contenu de la partition 1.



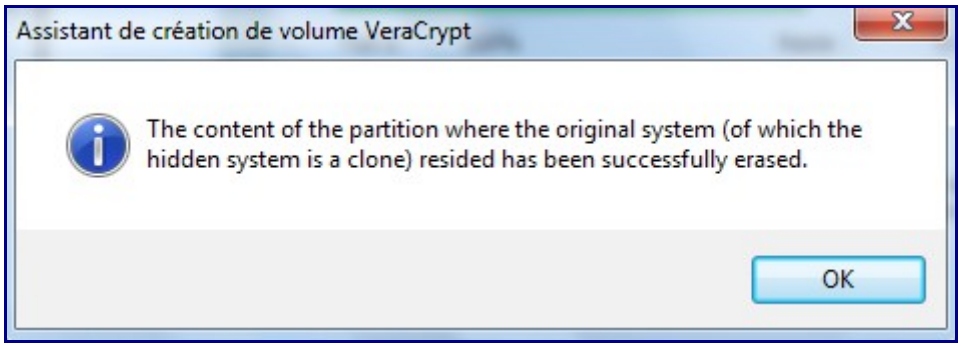
Générer une clé supplémentaire aléatoire pour renforcer l'effacement :



Attention, toutes les données de la partition 1 seront effacées (sachant que c'est une copie de cette première partition qui actuellement sur la partition 2).



Quand c'est terminé :



Vous devez éteindre vos ordinateur (histoire de vider autant que possible toute rémanence de mémoire).

Redémarrez votre ordinateur et installez votre OS : ne bootez pas sur le disque contenant le système caché = donc démarrez sur votre média d'installation (DVD/USB/WDS).

…

…

…

Installation de votre OS

…

…

…

Une fois votre OS installé, bien sûr vous ne pouvez plus booter sur votre système caché.

Installez VeraCrypt sur le système fraichement réinstallé et lancez la fonction de cryptage de votre

partition système (comme au chapitre 7 précédent), c'est-à-dire :

– menu Système / Chiffrer la partition, le disque système,

– Choisissez « Normal » et non « Caché »

– Choisissez « Chiffrer la partition Sysème Windows »

– Si votre PC n'a qu'un seul système (hors celui est caché), choisissez Amorçage (simple),

– Dans l'étape Options de Chiffrement : choisissez impérativement le même cryptage que celui utilisé pour votre système crypté ET caché.

– Spécifiez un mot de passe (différent de celui qui vous permet de booter sur votre OS cyrpté et caché)

– Laissez VeraCrypt vous graver un CD de récupération d'urgence (si vous en avez déjà, mettez le CD pour que VeraCrypt en fasse la vérification)

– Sélectionnez le mode de nettoyage qui vous convienne,

– Lancez le pré-test de chiffrement du système => un reboot sera proposé.

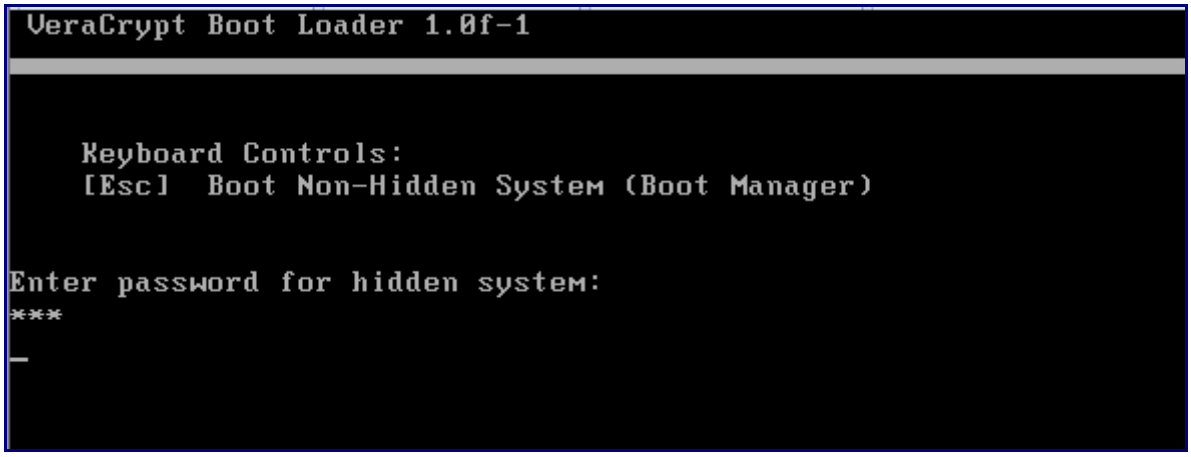
– Au reboot, saissez votre password créé dernièrement (pas encore celui de la partition chiffrée/cachée)

– Lancement de votre OS crypté (non caché), VeraCrypt vous propose vous confirme que le prétest est terminé et lance le chiffrage de votre partition.

– Quand c'est terminé, rebootez votre OS.

<u>Maintenant, le process est terminé :</u>

– Au boot de votre PC, le loader VeraCrypt vous demande un mot de passe



Si vous mettez le password de votre partition système cryptée ET cachée, vous booterez sur cet OS (l'OS2).

Si vous mettez le password de votre partition système chiffrée (la partition leurre), vous booterez sur l'OS normal .

Le troisième password vous permet d'accès à la partition externe.

10 – Détecter la présence de Conteneurs TrueCrypt

(partie non mise à jour pour VeraCrypt)

Utiliser TrueCrypt est sans doute indispensable lorsqu'on manipule des données confidentielles mais lorsqu'il s'agit à l'inverse de détecter si une personne ~~abuse~~ utilise TrueCrypt. Il existe à minima quelques pistes, outils et traces laissées par TrueCrypt.

TCHunt (TC pour TrueCrypt et Hunt pour…) : cet outil permet de détecter les fichiers TrueCrypt sur un ordinateur, pas seulement si ils ont l'extension .TC => http://16s.us/TCHunt A cette heure, TCHunt ne détectait pas encore les partitions. La dernière version était la 1.6, voici son usage :

TCHUNT –d C:\temp –v

-d pour Detect

C:\temp ou autre répertoire

-v pour mode verbeux.

Si vous lancez cette commande (surtout à la racine d'une partition), tous les fichiers seront analysés à la chaine, avec un résultat difficile à exploiter.

Préférez alors : tchunt –d c:\ 2>nul

TChunt vous renverra alors les éventuels fichiers ayant 1 conteneur TrueCrypt.

Attention : TChunt permet de suspecter la présence d'un fichier TrueCrypt. Le taux de faux négatifs et faux positifs peut être déroutant.

Traces locales :

Dans le cadre de conteneurs cachés (de second niveau), il reste deux arguments systématiques pour détecter la présence de ces conteneurs : 1 – le conteneur premier ne pourra jamais contenir ou stocker la totalité de l'espace qui lui est alloué, 2 – les fichiers leurres du premier conteneur sont rarement mis à jour et donc souvent obsolètes.

Le système d'exploitation laisse apparaitre également la présence de fichiers tels que truecrypt (-x64).sys dans system32\drivers

Le registre laisse entrevoir quelques associations de fichiers : .TC par défaut

Etc …