Livre blanc

Clé USB sécurisée

Vous utilisez de plus en plus votre clé USB.

Maintenant que ses capacités permettent des folies, vous aimeriez emporter avec vous toutes vos données, mêmes les plus secrètes, en toute sécurité.

Voici comment vous protéger contre tous les risques.

Nous traitons en effet ici le cas difficile de la **protection des informations très sensibles** en environnement nomade (informations intimes, secrets, carnets d'adresses, référentiels de mots de passes, etc.)

En fonction de vos besoins, vous pourrez retenir une partie des recommandations ou la totalité du système de sécurité présenté.

Tous les outils utilisés sont gratuits. Vous serez en mesure de créer votre propre clé USB sécurisée.

La méthode proposée est **à la portée de tous.**

Ne vous laissez pas rebuter par le contenu très complet de ce livre blanc. Tout y est détaillé, avec le manuel d'installation et les images d'écrans. Vous allez y arriver pas à pas.

Et diffusez ce livre blanc librement.

Livre blanc

Sommaire

Livre blanc

Je vous promets que

Si vous n'êtes pas informaticien, après lecture de ce livre vous installerez votre clé en ½ heure.

Si vous êtes informaticien, vous mettrez 5 minutes.

Au bout ½ journée d'utilisation, vous ne pourrez plus vous passer de « votre coffre fort ***** ».

Il vous suffit d'appliquer la méthode point par point.

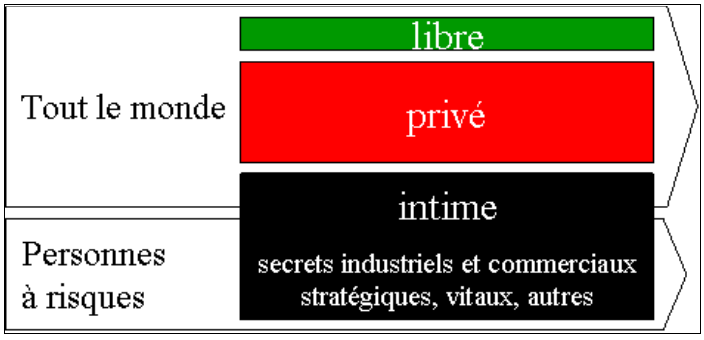
Budget à prévoir :

- le prix de votre clé
- le prix de votre temps
  - Lecture du livre, réflexion, vérifications, conseils, selon votre personnalité de 1 à 5 jours. Des passages vous paraîtront compliqués. Poursuivez jusqu'à l'installation. La pratique va tout démystifier.
  - Installation : ½ heure maxi

Autre chose, j'oubliais : la solution est compatible avec des ordinateurs équipés des systèmes d'exploitation Windows de Microsoft (toutes les versions) et Linux.

Public concerné

Tout le monde, c'est à dire vous et moi, simples citoyens
Jeunes et moins jeunes de toutes activités
Chefs d'entreprises
Professions libérales
Recherche
Armée
Police
…



Principaux risques d'une clé USB et leurs remèdes

Risques	Protections
Destruction	
Endommagement du support	Sauvegarde
Effacement	Copie
Impossibilité de lire	
Altération	Copie, test
Plus d'outil pour lire	Sauvegarde de l'outil
Mot de passe perdu	Pense bête
Dépossession du support	
Perte	Copie, coordonnées de retour
Vol	Sécurité physique, copie
Lecture sans consentement	
Par détournement de l'original ou d'une copie	Mot de passe, Chiffrement lourd, avec outil ouvert
Par l'emploi de la force	Déni plausible

Probabilités d'événements.

Le sujet que nous traitons ici va jusqu'à la protection des informations les plus vitales. Faut-il pour autant devenir paranoïaque ?

La réponse est fonction de vos activités !

Nous donnons ici quelques idées de risques. Adaptez les, complétez les. Mesurez-en les éventuelles conséquences.

Estimez votre risque global et adaptez votre organisation en fonction de celui-ci.

Destruction physique de la clé USB :

> Défaut de fabrication, fatigue de la connectique, environnement agressif (soleil, chaleur, eau, acide, égout, sable, etc.), malveillance, écrasement, destruction par un animal domestique, destruction électromagnétique, etc.
> Votre risque : 1 / 5 ans ?

Impossibilité de lire :

> Destruction ou détérioration accidentelle du contenu de la clé USB, virus, obsolescence du logiciel de lecture et/ou de déchiffrement, perte du mot de passe.
> Votre risque: 1 / 5 ans ?

Dépossession du support :

Probabilité de vol:

- Si vous faites l'objet d'un intérêt particulier : votre risque 1/ 1 an ?
- Si vous ne faites pas l'objet d'un intérêt particulier : votre risque 1 / 7 ans ?

Probabilité de perte: votre risque: 1 / 5 ans ?

Dont:

- sans possibilité de la retrouver : 30% ?
- avec possibilité de la retrouver en tombant sur une personne honnête qui vous rendra votre clé 70% x 50% = 35 % ?

Lecture sans consentement :

Après que vous soyez dépossédé de votre clé USB, ou lors de la lecture hors consentement de vos données sauvegardées

- Si vous faites l'objet d'un intérêt particulier, probabilité: sure à 100/100
- Si vous ne faites pas l'objet d'un intérêt particulier, probabilité 1/10 000 (les experts sont rares et il faut qu'ils trouvent vos supports perdus ou volé)

Autres ?

Autrement dit, on pourrait arriver aux conclusions suivantes :

<u>Vous êtes un "commun des mortels"</u>

Vous risquez d'avoir un **problème avant moins de 2 ans**, avec cependant une malchance sur 10 000 pour qu'on essaie de lire vos données. Le plus gros risque, c'est vous par mauvaise organisation.

<u>Vous êtes une personne susceptible de faire l'objet d'un intérêt particulier</u>

Vous aurez un **problème avant moins d' 1 an, avec la certitude qu'on essayera de lire vos données**. Vous avez intérêt à vous organiser avec toutes nos recommandations.

Les offres du marché

Le marché propose toutes sortes de solutions. Elles sont souvent de qualité, mais elles sont partielles. Aucune n'appréhende globalement le problème, notamment en terme d' "organisation de sécurité".

Les solutions les plus avancées, tel le chiffrement intégré à la clés, n'offrent pas l'assurance de neutralité (solution propriétaire, risque de porte dérobée, etc.).

En effet, aucun outil commercial ne peut garantir une sécurité absolue. Par ailleurs restera le problème de la dépendance aux outils propriétaires.

Nous verrons comment nous traitons ce problème.

Le paradoxe

Vous comprenez que la protection de votre information passe par un couple cadenas/clé très compliqué et très sûr.

Le cadenas sera obligatoirement un outil de notoriété mondiale, avec des principes et une construction contrôlables par le monde entier. Cet outil sera certifié par la communauté internationale comme étant exempt de trucs et astuces pour petits malins (intérêts commerciaux et d'états, etc.).

La sécurité se concentrera dans la clé, très compliquée, impossible à déduire du cadenas. Cette clé, vous la fabriquerez vous même avec le cadenas.

En fonction de la protection recherchée, le couple cadenas/clé sera conçu pour que la clé soit :

- Assez simple pour être mentalement mémorisable, mais dans ce cas la découverte de la clé (code) sera possible par une organisation puissante

Ou alors

- Extrêmement compliquée et impossible à mémoriser autrement que sur un support. Dans ce cas la découverte de la clé sera quasiment impossible.

Bien naturellement, la clé et le cadenas ne devront jamais être réunis sans votre consentement. Si la clé est sur un support, ce support ne devra jamais être mis à proximité du cadenas, sauf de façon extrêmement astucieuse !

Si vous voulez assurer la sécurité de votre information vitale, en toutes circonstances, à tout moment, en tout lieu, et en emportant votre information cadenassée sur vous, il vous faudra résoudre le paradoxe suivant :

- Avoir cadenassé votre information avec un couple cadenas clé extrêmement compliqué
- Ne pas porter sur vous le support de mémorisation de la clé
- Avoir l'usage de cette clé compliquée, en tous lieux, dès qu'il vous la faudra

Le mieux, il faut y penser, serait même en plus que personne ne puisse découvrir que vous avez de l'information très hautement cadenassée sur vous !

Eh bien voici la solution pour tout cela à la fois !

Deux types d'organisations

Comme nous venons de le voir, les risques ne sont pas les mêmes pour tous.

Votre protection doit être adaptée à la nature de votre risque.

Pour couvrir tous les niveaux possibles nous donnerons 2 modèles d'organisations :

- Pour Madame et Monsieur tout le monde

- Pour les personnes exposées à un risque élevé.

Qui peut le plus, peut le moins.

Nous ferons un exposé de la solution pour les personnes les plus exposées, et nous la réduirons pour Madame et Monsieur tout le monde. Les usages extrêmes ne seront pas détaillés ici.

Allons-y.

Choix d'une clé USB, premiers éléments de bon sens.

Choisissez une clé avec un système d'attache très solide, pour pouvoir la garder sur vous en sécurité, sur votre trousseau de clés par exemple. Le système d'attache doit être facilement amovible (anneau, mousqueton, etc.).

L'idéal est l'utilisation d'un étui de clé USB en métal (protection eau, mécanique, électromagnétique). Dans ce domaine, certains constructeurs proposent des solutions pour des usages extrêmes.

Choisissez de préférence une clé USB standard, qui n'attire pas « l'envie de possession » (trop belle, trop top, trop bijou)

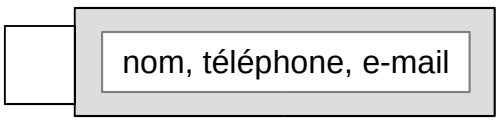
Ne transigez pas sur ses qualités techniques. La clé USB doit être à la norme USB 2.0, et son électronique doit lui permettre de bonnes vitesses en lecture et en écriture.

Par exemple :

- Lecture : 20 Mo/s pour la sauvegarde
- Ecriture :10 Mo/s

Offre du marché en 2007: 1 Go à 32 Go, USB2.0, vitesses maxi jusqu'à 25 ou 30 Mo/s

Enfin, écrivez sur le corps de la clé USB vos coordonnées, un détail très utile en cas de perte. Ça peut servir également pour retrouver votre trousseau des clés de votre maison ou de votre voiture. Les indications doivent résister aux intempéries (eau, soleil)

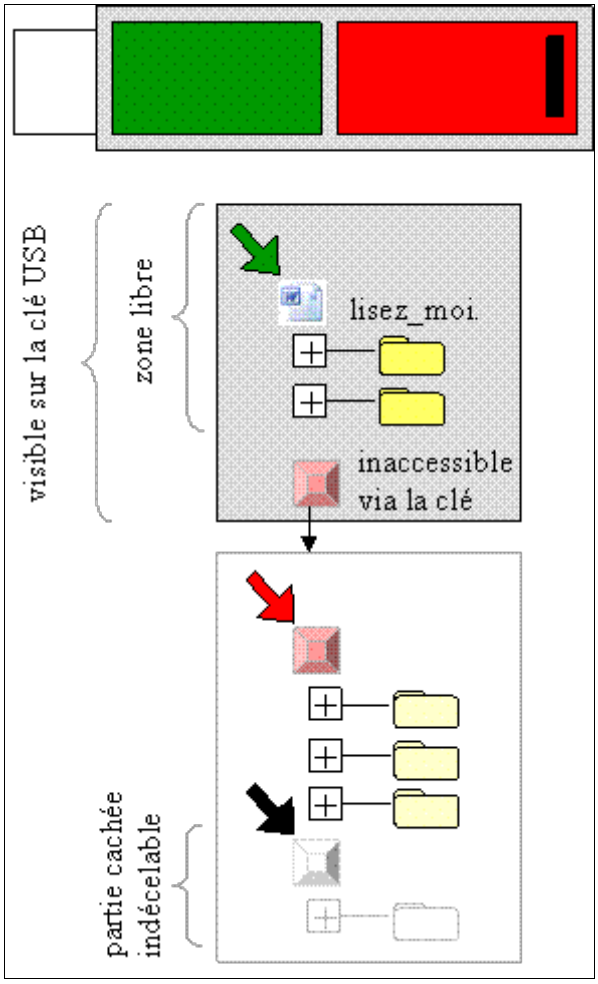


Organisation de votre clé USB

Votre clé USB sera organisée en 3 « tiroirs »: 1 vert, 1 rouge, 1 noir. Le noir sera placé dans le rouge. Nous vous indiquerons comment faire plus loin avec les précautions d'usage à prendre.

Seul le tiroir vert sera accessible. Un fichier (en rose ici), inaccessible depuis la clé USB, abritera le tiroir rouge et le tiroir noir.

Le tiroir noir n'est pas obligatoire. Mais on verra son très grand intérêt plus loin. Si vous décidez d'en avoir un, il sera dans tous les cas indécelable. Vous pourrez même nier d'en avoir un ! (valeur de "déni plausible" en cas d'usage de la force)



Expliquons l'intérêt de ces 3 tiroirs.

1) Le tiroir "vert"

Ce tiroir est libre, sans aucune protection. Il conviendra pour tout ce qui vous jugerez « non secret ».

Placez-y un petit fichier qui reprendra vos coordonnées (nom, n° tél., e-mail, etc.), avec un paragraphe sympathique à l'attention de la personne qui retrouverait votre clé perdue. Vous pourrez le baptiser "si vous avez trouvé cette clé"

Proposez une récompense représentant 1 ou 2 fois le prix de la clé USB pour que le trouveur n'ait pas intérêt à recycler votre bien. Attention : ne vous exposez pas au chantage en indiquant que votre clé contient d'éventuels secrets !

Le tiroir vert contiendra également les outils de sécurité que nous vous proposerons plus loin.

2) Le tiroir "rouge"

Ce tiroir est pour vos secrets.

Il est protégé par un **mot de passe long complexe**. Ce mot de passe est cependant mémorisable pour un usage quotidien non fastidieux.

Vous pourrez imaginer une phrase de10 à 20 caractères ou plus, accolés de façon « très particulière » en mélangeant chiffres et lettres.

Exemple : « clémaenverlan6belle » pour ma clé en verlan si belle.

Il faut savoir qu'avec ce type de protection, la sécurité est déjà très élevée. Elle est impossible à mettre en défaut par le commun des mortels.

Clin d'oeil aux Alsaciens. Un truc comme celui-là va aussi : "2zwatchgawaiafaschtenichtratzheim" c'est à dire "2 fêtes de la tarte aux quetsches à Ichtratzheim" en Français.

A vous les Bretons …et les autres.

Livre blanc

Cependant cette protection ne résistera pas à une organisation très puissante qui souhaiterait à tout prix connaître le contenu de votre clé (état, groupe secret, pirate émérite).

Par ailleurs, en cas de procédure légale vous pourrez être contraint de dévoiler votre mot de passe (le premier, car nous utiliserons également un second renforcé avec une clé de chiffrement).

L'argument « je ne m'en rappèle plus » ne sera pas valable et vous risquerez d'être poursuivit pour dissimulation de preuve.

Vous saisirez une seule fois votre mot de passe long lors du branchement de votre clé USB. Vous utiliserez son contenu normalement avec un processus qui chiffrera toutes vos données à la volée, sans que vous en rendiez compte (voir outil et installation).

Toutes vos informations seront automatiquement protégées, notamment dès que votre clé sera débranchée.

Le tiroir rouge est donc un très bon endroit pour 99% de vos données personnelles.

3) Le tiroir "noir"

Ce tiroir est ultime. Il est d'une sécurité absolue. Il pourra donc héberger en toute tranquillité le 1% de vos informations les plus stratégiques, c'est à dire vos informations vitales !

Pourquoi ? Pour 2 raisons :

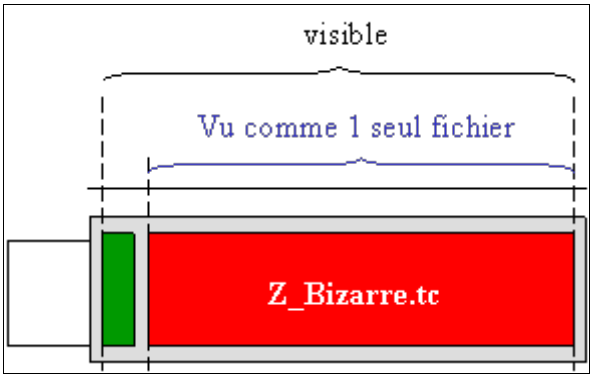
1) Ce tiroir est invisible et indécelable ! Vous pourrez même en nier l'existence !

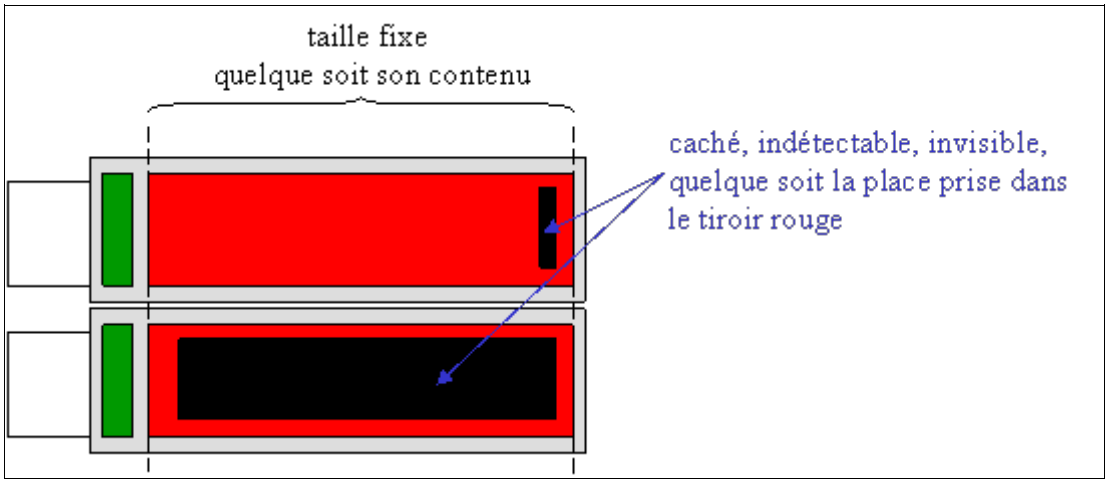
2) Ce tiroir n'est accessible que par un mot de passe long, associé c'est préférable à une clé de chiffrement très complexe, elle impossible à mémoriser. La complexité de cette clé de chiffrement est telle que vous serez obligé d'utiliser un fichier sur un support de mémorisation (voir plus loin).

Une organisation très puissante ne pourra même pas savoir, et encore moins prouver, que vous avez un tiroir noir, petit ou grand, dans votre clé USB.

Même si cette organisation vous soupçonne d'avoir un tiroir noir dans votre clé, il lui sera impossible de le trouver et de l'ouvrir.

Pour vivre heureux, vivons cachés!





Mais attention, vous devrez gérer la sécurité de ce tiroir noir de la façon que nous allons vous indiquer (voir précautions

d'écrasement, gestion des mots de passe long et de la clé de chiffrement).

Et maintenant, voudriez-vous avoir sous la main, tout le temps :

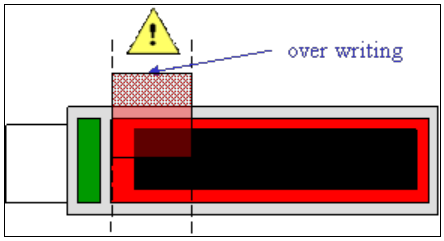
- tous vos identifiants et mots de passe de tous vos accès et outils (messageries, sites, applications, banque, etc.) ?
- votre carnet d'adresses confidentiel ?
- vos secrets ?

Moyennant quelques précautions à prendre, il vous suffit d'un seul fichier de quelque dizaines de Ko ne représentant pas plus de 1/10 000 de la capacité de votre clé USB, abrité dans le tiroir noir, lui même d'abord invisible puis ensuite indéchiffrable !

Sans votre consentement, personne ne pourra y accéder, quelque soit le sort de votre clé USB ou de ses copies, et envisageons le pire, quelque soit le contexte de coercition que vous vivrez (menace, interrogatoire, etc.)

Même si le tiroir noir est bien plus gros pour héberger des fichiers images ou de la musique, rien ne le décèlera. Vous réserverez un espace très important à votre tiroir rouge (1, 2, 4, 8, 16 Go). Votre tiroir noir, indécelable, prendra quasiment toute la place à l'intérieur du tiroir rouge, avec une capacité voisine de celle du tiroir rouge). Le tiroir rouge sera garni de quelques fichiers et paraîtra très peu rempli, c'est tout.

Attention: veillez a ne pas détruire le contenu de votre tiroir noir en cas de dépassement de capacité de votre tiroir rouge. (organisation spéciale non expliquée ici)



Ps: quelque soit son remplissage, et le fait qu'il contienne ou non un tiroir noir, votre tiroir rouge apparaîtra toujours de la même taille, c'est à dire en un seul très gros fichier cadenassé..

Alors tiroir noir ou pas, c'est vous qui déciderez.

Organisation générale de sécurité.

Vous devez résoudre un triple problème :

- faire en sorte que votre sécurité soit impossible à déjouer sans votre consentement
- ne jamais oublier vos mots de passe, ni perdre votre (ou vos) clé de chiffrement. La défaillance de l'un ou de l'autre est irrémédiable.
- disposer de vos informations partout ou vous en aurez besoin.

Voici une organisation possible. Vous pourrez l'utiliser partiellement ou totalement.

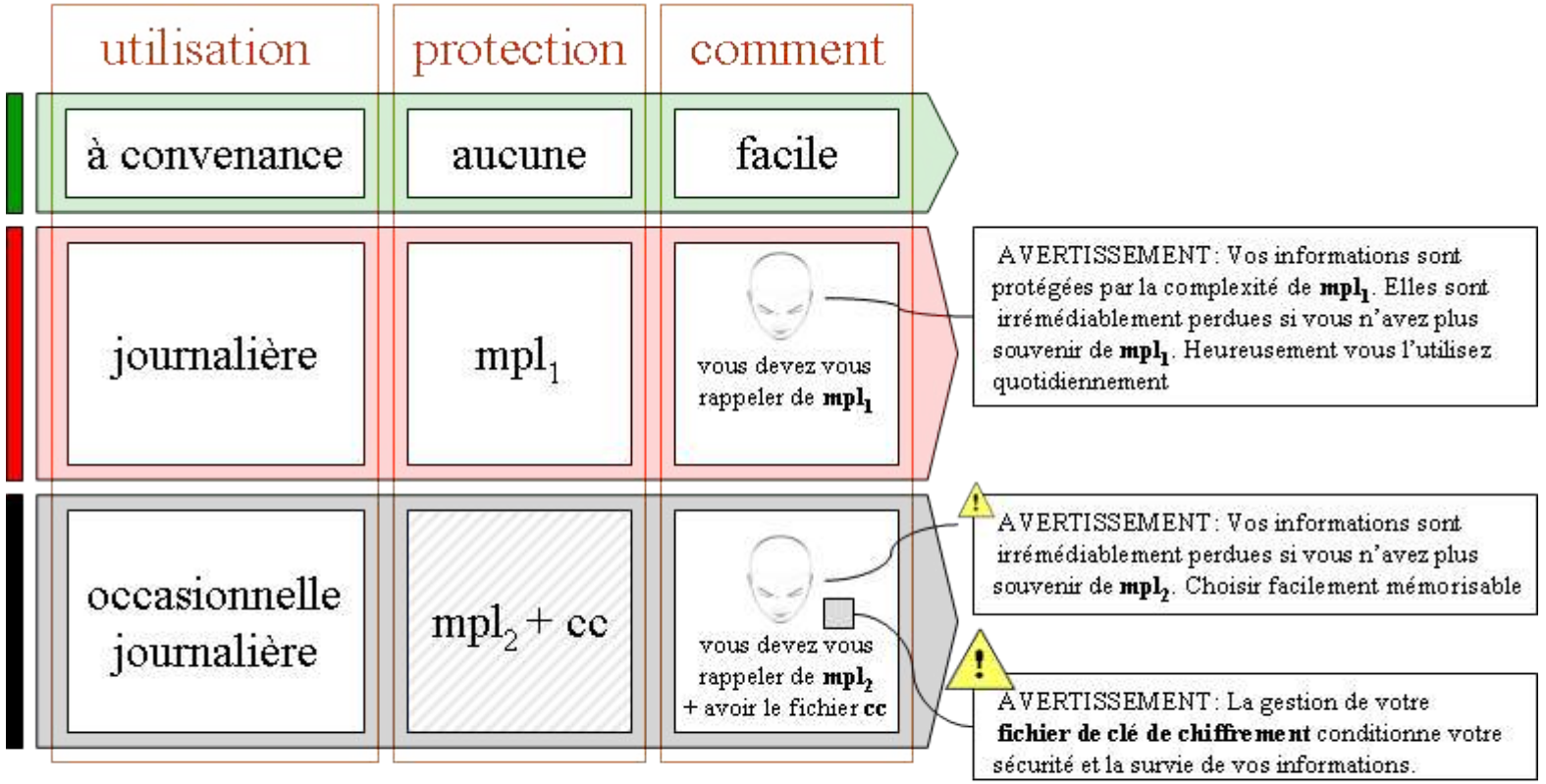
Que vous faut-il :

Notez ces définitions pour la suite de la lecture.

Pour tous	**Pour un risque très élevé**
➢ un mot de passe long, pour le tiroir rouge, **mpl_1** , obligatoirement compliqué. Vous l'utiliserez tous les jours et vous ne risquez pas de l'oublier.	➢ un second mot de passe long pour le tiroir noir **mpl_2** , plus simple que mpl_1 , plus facile à mémoriser, parce que vous ne l'utiliserez pas forcement tous les jours. ➢ une clé de chiffrement complexe réalisée par ordinateur **cc** ➢ un mot de passe de chiffrement **mpc** fait avec une variante de mpl_1. Par exemple en remplaçant certaines lettres de mpl_1 par des chiffres pour que mpc soit très compliqué. ➢ un **support ultime** et un lieu de cachette ➢ un **hébergeur** de clé anonyme
➢ un ordinateur permettant de faire les sauvegardes	
➢ votre clé USB, configurée comme nous vous l'indiquerons	

Tout ceci peut vous paraître compliqué. Mais en pratique, quand vous aurez choisi votre stratégie et quand votre organisation sera en place, vous verrez qu'il n'en est rien, même pour les risques les plus élevés.

Voici 2 schémas exemples à lire attentivement, et à garder en référence. Les couleurs Vert, Rouge et Noir correspondent aux niveaux de sécurité recherchés.

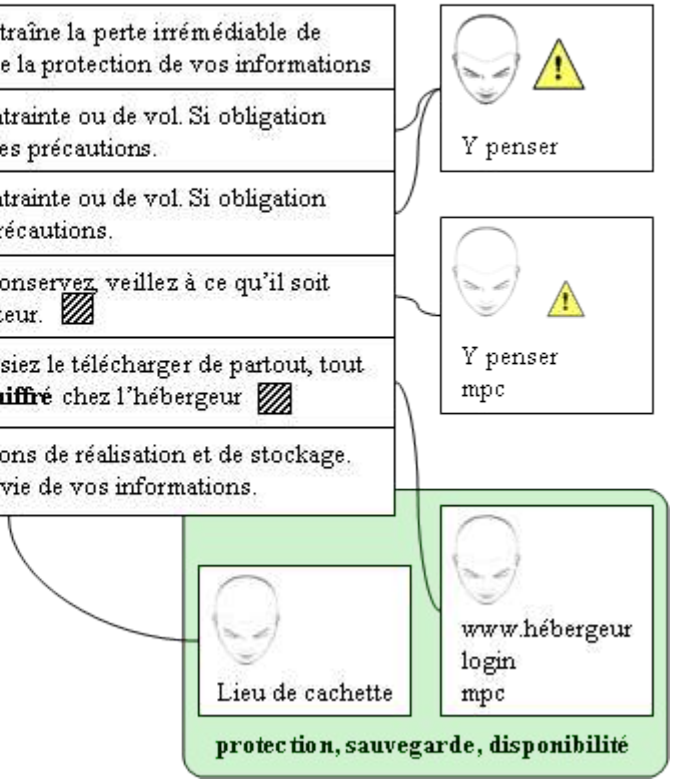


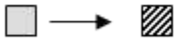
☐ : **invisible, indétectable, existence improuvable**
mpl_1 : **m**ot de **p**asse **l**ong n°**1**
mpl_2 : **m**ot de **p**asse **l**ong n°**2**
cc : **c**lé de **c**hiffrement

Gestion de votre clé de chiffrement

AVERTISSEMENT: la perte ou l'altération de votre fichier de clé de chiffrement entraîne la perte irrémédiable de toutes les informations qu'il protége ! La possession par des tiers de ce fichier fragilise la protection de vos informations

Avoir le fichier de clé de chiffrement **dans sa clé USB, même chiffré**		INTERDIT. Risque en cas de contrainte ou de vol. Si obligation temporaire, prendre de très grandes précautions.
Avoir le fichier de clé de chiffrement **sur soi, même caché, même chiffré !**		INTERDIT. Risque en cas de contrainte ou de vol. Si obligation temporaire, prendre de grandes précautions.
Avoir le fichier de clé de chiffrement **sur son ordinateur de travail**		ATTENTION. Si vous devez le conservez, veillez à ce qu'il soit **toujours chiffré** sur votre ordinateur.
Avoir le fichier de clé de chiffrement **chez un hébergeur**		NECESSITE. Pour que vous puissiez le télécharger de partout, tout le temps. Attention, **déposez le chiffré** chez l'hébergeur
Avoir le fichier de clé de chiffrement **sur un support ultime, caché**		IMPERATIF. Suivez les instructions de réalisation et de stockage. Le support ultime constitue la survie de vos informations.



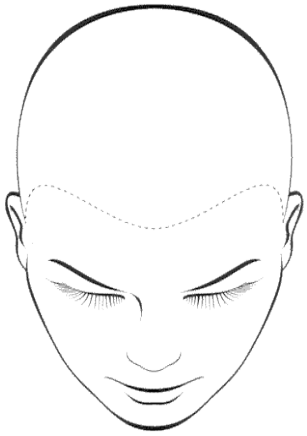


Chiffrement de votre fichier avec mpc

mpc : **m**ot de **p**asse de **c**hiffrement, variante courte de **mpl**$_1$

Autrement dit, pour le cas d'un risque très élevé :

Que devez-vous **avoir en tête** ? Réponse :



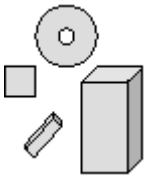
- **mpl_1** pour votre tiroir rouge. Ne jamais le transcrire, vous l'utiliserez quotidiennement
- **mpl_2** pour votre tiroir noir. Ne jamais le transcrire, vous l'utiliserez occasionnellement lors de l'accès à votre tiroir noir
- **mpc**, la variante de mpl_1 pour la protection de votre clé de chiffrement cc. Ne jamais transcrire cette variante, vous l'utiliserez occasionnellement lors de l'accès à votre tiroir noir
- La mémoire de la **cachette** de votre support ultime (voir plus loin)
- Le **www.** de votre hébergeur de clés anonymes (voir ci-après)
    - Votre **login** sur ce site
    - La réponse à votre énigme

Que devez-vous **ne jamais avoir sur vous** ? Réponse :

- Votre clé de chiffrement, même chiffrée (ou a moins d'astuces dans les cas extrêmes).

Que devez-vous **faire** ? Réponse :

- Des sauvegardes régulières de votre clé USB, tous les 1, 2, 3, mois.
- Une réactivation de votre dépôt chez votre hébergeur
- Une vérification et un rafraîchissement de votre **support ultime** tous les 10 ans.



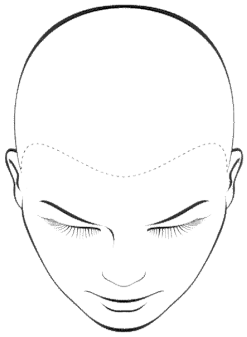
Notez sur votre calendrier préféré (pompiers, etc.) les dates de sauvegardes à faire.
Vous pouvez les multiplier sans soucis, sur tous supports de taille suffisante. Elles ne risquent rien, comme votre clé USB.

Choisissez un hébergeur de clés anonymes.
Déposez votre clé de chiffrement, après l'avoir chiffrée avec **mpc**.

Créez un **support ultime** caché dans un endroit anodin.

Ce support doit lui aussi être anodin et ne contenir comme élément de sécurité que vos outils de sécurité, le fichier de la clé de chiffrement **cc** et l'information pour accéder à l'hébergeur de clé **www.** et **login**.

AVERTISSEMENT concernant le support ultime :



- Ne jamais marquer clairement votre support ultime avec des mentions de type "sauvegarde de clé de chiffrement". Le rendre banal.
- Ne jamais l'avoir sur vous (contrainte, usage de la force)
- Ne jamais l'utiliser "sauf si" ….
- Ne jamais faire des allez retour vers lui (surveillance)
- Ne jamais mettre d'éléments permettant de remonter vers vous (nom, autres identifiants) ou vers votre clé USB.
- Ne jamais le mettre dans votre ordinateur ou en garder une copie dans votre ordinateur (dramatique).
- Ne jamais le mettre à proximité de vos sauvegardes de clés USB (dramatique)

Maintenant imaginez

Si vous avez tout le reste dans votre clé USB, il ne vous faut plus rien d'autre dans votre tête (enfin, c'est juste pour rire).

Récapitulons :

Vous avez en tête **mpl_1**, **mpl_2**, **mpc**, le lieu de **cachette** de votre support ultime, le **www**, et le **login** pour l'hébergeur. Personne ne doit les connaître.

Votre support ultime et votre hébergeur de clés abritent et sauvegardent votre clé de chiffrement **cc**.

Vous accédez à vos données secrètes avec votre seule mémoire.

- tiroir rouge > **mpl_1** ,
- tiroir noir > **mpl_2 + cc** via (**www, login, mpc**)

Si vous êtes perdu recherchez votre support ultime (**cachette**).

Vous êtes maintenant prêt pour partir avec votre clé USB, et avec vos informations les plus sensibles à votre portée, en toute sécurité.

Une précaution tout de même: faites des essais avec une clé USB et des fichiers fictifs.

Vérifiez que **mpl_1**, **mpl_2**, **mpc**, vous plaisent bien et sont très faciles pour vous à conserver en mémoire, sans Alzheimer et jusque dans votre … tombe !

Brrrr…, ce n'est pas joyeux ça ! Mais ça image bien le fait qu'avec cette organisation, vos secrets, vous pourrez les emporterez dans votre tombe, si vous le souhaitez bien entendu.

C'est bien l'organisation que vous souhaitez, n'est-ce pas ?

Livre blanc

Choix de l'hébergeur de clés anonymes de chiffrement.

Clé USB partout ! Votre activité nomade nécessite de confier à un tiers l'un des éléments de sécurité: la clé de chiffrement **cc**. Cela peut paraître curieux. Mais analysez bien le risque.

Le tiers hébergeur, ou au pire toute organisation ayant mis la main sur son service, sont dans l'impossibilité d'en faire usage si l'une au moins des 3 conditions est remplie :

- **Aucun moyen de vous connaître ou de remonter trop facilement vers vous**. Ceci par le biais d'identifiants, de comptes de messagerie ou de moyens de paiement mal appropriés. Il y a cependant un risque parce que c'est facile via votre IP, sauf si vous utilisez un ordinateur public (Cyber Café, Wifi libre, salle informatique, etc.)

- **Aucun moyen de déchiffrer votre clé de chiffrement** C'est à dire aucun moyen de connaître **mpc**

- **Aucun moyen d'associer mpl_2 avec votre clé de chiffrement cc**. Vous pouvez nier l'existence d'un tiroir noir et votre déni sera plausible. En effet, même si on découvre que vous avez une **cc** chiffrée par un **mpc** et qu'on vous force à la déchiffrer …, rien n'est possible pour démontrer l'existence de votre tiroir noir et donc de **mpl_2**, qui associé à **cc** permet d'y accéder. Vous suivez ?!

L'organisation que nous vous proposons remplit les 3 conditions à la fois !

Dans les cas d'ultimes secrets, accédez au site de l'hébergeur de clés depuis un ordinateur public (cybercafé, libre service, bornes de mairie, réseau d'entreprise, etc.)

Avant de déposer votre clé de chiffrement il vous faudra la chiffrer avec **mpc** ! Utilisez l'outil Open Source gratuit **AxCrypt** très sûr et très facile d'emploi. Il est téléchargeable depuis le site 01net.com

Ps: Un site d'hébergement personnel ou d'entreprise ne conviendrait pas pour jouer le rôle d'hébergeur puisqu'il permettrait de revenir trop vite vers vous. Le salut se trouve dans l'hébergement public, caché au milieu d'un grand nombre d'utilisateurs anonymes.

En matière d'hébergement de clés de chiffrement anonymes, le site www.cle-usb-truecrypt.org répond à notre cahier des charges.

> *Anonymat:* pas d'identification, pas d'adresse mail, pas de mémorisation d'adresse IP (c'est ce qui est promis). pas de trace de paiement.
> *Accès:* pseudo et phrases énigmes de votre composition
> *Hébergement:* votre fichier de clé est disponible pendant 1 an, renouvelable (à condition d'y retourner). Possibilité de supprimer votre fichier à tout moment.
> *Autres caractéristiques :* Limitation des dépôts de fichiers de clés de chiffrement à 1 Ko, ce qui est largement suffisant (voir plus loin)
> *Seul bémol:* pas de sécurisation de type "ssl, https", mais ça viendra peut être.

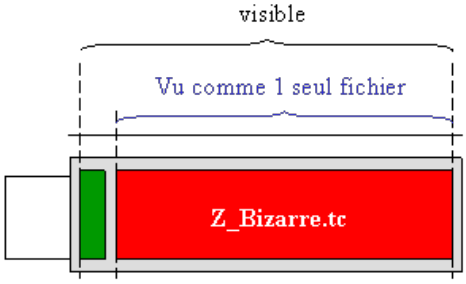
Sauvegarde de votre clé USB

Vous ferez d'assez bon cœur des sauvegardes régulières si elles sont faciles et rapides.

Cliquez déplacez, vous connaissez ! Ce simple geste vous permettra de copier tout le contenu de votre clé USB sur tout support (autre clé USB, disque dur de sauvegarde ou de votre ordinateur).

La copie sera protégée de la même manière que votre clé USB originale, sans opération supplémentaire. Si vous avez choisi une clé rapide en lecture (20 Mo/s), 1, 2 ou 4 Mo, seront sauvegardés en moins de 1, 2 ou 4 minutes. Dans ces conditions, il n'y a plus qu'à penser à faire vos sauvegardes régulièrement.

Remarque: L'outil que nous vous proposons permet d'empaqueter les fichiers de vos 2 tiroirs rouge et noir en un fichier. Ce fichier d'empaquetage est toujours vu et traité avec une taille fixe. La vitesse de sauvegarde de votre clé USB sécurisée sera donc toujours la même, quelque soit son contenu. Ce point est très avantageux en temps de sauvegarde si vous avez une grande quantité de fichiers dans vos tiroirs. Bien entendu votre clé USB doit être rapide en lecture.



Création de votre clé USB sécurisée

Passons maintenant à la phase de création de votre clé USB sécurisée.

AVERTISSEMENT: Ne confiez jamais à un tiers la mission d'organiser seul votre clé USB et d'installer l'outil de sécurité que nous allons vous indiquer. Vous pourrez cependant demander à vous faire assister par un ami, un collègue ou un prestataire pour aller plus vite.

Mais vous devrez être en mesure de comprendre ce que vous faites et **vous devrez impérativement le faire vous même**.

Nous allons vous donner toutes les explications utiles pour cela.

Le choix de l'outil est déterminant. N'installez jamais un outil commercial, propriétaire d'une entreprise, aussi prestigieuse qu'elle soit, aussi convaincants que soient ses arguments !

Utilisez un outil Open Source, entièrement transparent, garanti par la communauté mondiale contre toute « astuce » ou trou de sécurité.

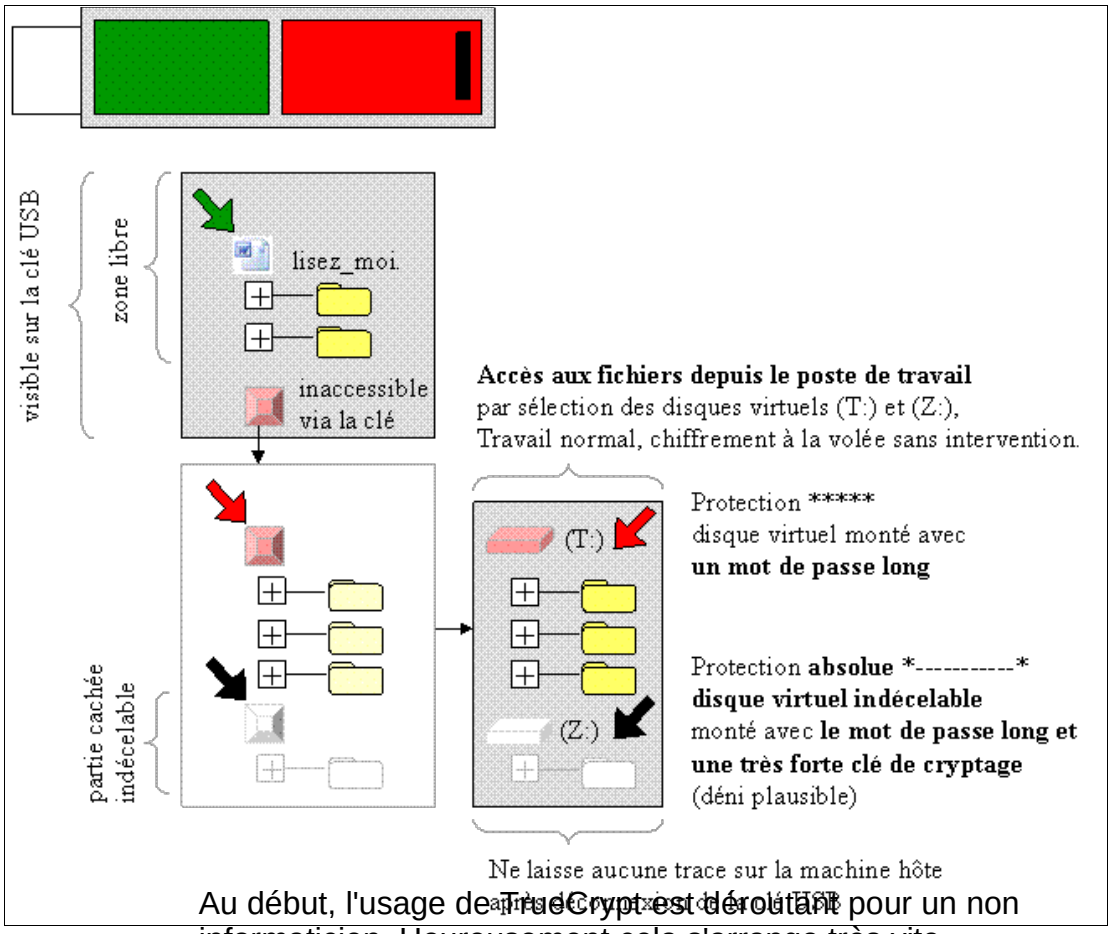
L'outil que nous vous proposons est **TrueCrypt**, l'une des plus puissantes solutions du moment. Il répond strictement à l'organisation et au cahier des charges que nous venons de vous décrire. Il est réputé inviolable avec l'utilisation d'un mode de chiffrement complexe. De plus il est totalement gratuit !

N'hésitez pas à vous renseigner sur la solidité de cet outil. Allez sur Internet, visitez les forums, questionnez votre entourage.

Il faut que vous viviez sereinement la protection de votre clé USB.

Le site officiel de TrueCrypt est www.truecrypt.org
Lisez aussi : http://fr.wikipedia.org/wiki/TrueCrypt

Fonctionnement général de TrueCrypt



Au début, l'usage de TrueCrypt est déroutant pour un non informaticien. Heureusement cela s'arrange très vite.

Voici quelques explications.

Votre clé USB comportera toutes vos données sans que vous puissiez voir, par un double-clic classique, celles qui sont protégées !

Les parties protégées, celles qui vous intéressent tant, ne seront accessibles que via 1 ou 2 disques virtuels visibles depuis le poste de travail de votre ordinateur (selon que vous aurez installé une partie rouge ou une partie rouge et une partie noire).

Ces disques virtuels seront crées par vous en quelques clics, à chaque connexion de votre clé sur l'ordinateur hôte et pour la durée de votre travail.

Livre blanc

Nous les avons notés ici (T:) pour la partie "secrète" rouge et (Z:) pour la partie "vitale" noire. Vous pourrez leur affecter les lettres qu'il vous plairont.

Dès lors qu'ils seront "montés" par vous avec **mpl$_1$** pour la partie rouge, ou avec **mplc$_1$** + **cc** pour la partie noire, ces disques virtuels seront accessibles depuis le poste de travail comme n'importe quel autre disque (C:, A:, etc.).

Dès que vous les aurez montés (par quelques clics), vous pourrez accéder à tous les fichiers qu'ils contiennent.

Vous travaillerez comme avec d'autres disques à la différence près que tous vos travaux seront protégés "à la volée", sans que vous vous en rendiez compte !

Tous les fichiers que vous aurez placés dans ces 2 disques virtuels seront physiquement dans votre clé USB, bien à l'abri en toutes circonstances. Il ne laisseront aucune trace sur l'ordinateur hôte.

Une petite précaution avant de débrancher votre clé: vous devrez "démonter" votre clé d'un simple clic sur l'icône en bas à droite de votre ordinateur + débrancher votre clé comme avant.

Installation de votre clé USB

Téléchargement des outils:

- Téléchargez la dernière version de TrueCrypt
  Vous devez récupérer 3 composants :
  - **TrueCrypt Format.exe** pour créer les "tiroirs"
  - **TrueCrypt.exe** pour monter les tiroirs en disques virtuels
  - **truecrypt.sys**, une partie logique que vous n'utiliserez pas mais qui devra impérativement être placée au même endroit que les 2 premiers composants

  Si vous ne lisez pas l'anglais, récupérez le composant de la langue française **language.fr.xml** compatible avec la version téléchargée de TrueCrypt.
  Enfin, lors de l'installation, un 4 ième composant se créera automatiquement à cote d'eux
  Configuration.xml

- Téléchargez l'outil de chiffrage AxCrypt
  Vous devez uniquement récupérer le composant
  AxCrypt-Setup.exe

- Pour les plus prudents, c'est optionnel, téléchargez enfin Eraser. Vous devez uniquement récupérer le composant
  EraserSetup584x32.exe

Sites de référence:

- Site officiel de TrueCrypt www.truecrypt.org
- Site www.cle-usb-truecrypt.org propose un kit complet d'installation en français.
- Site www.clubic.com
- Site www.01net.com
- Site www.sebsauvage.net
- Site www.commentcamarche.net

Ou tapez sur Google :

"télécharger truecrypt",
"télécharger axcrypt"
"télécharger eraser"

La communauté du Web regorge d'informations et de points de téléchargement sur ces sujets.

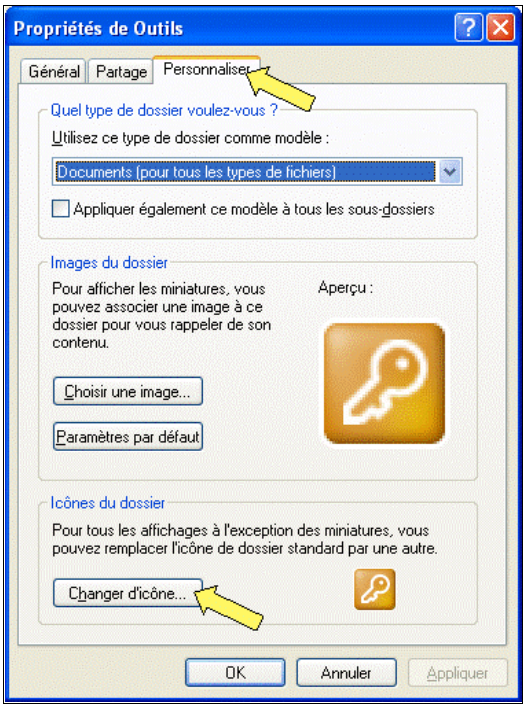
Préparation de la clé USB

Partez d'une clé USB vide (ce n'est pas une obligation, c'est juste pour faire propre au départ).

- Créez à la racine de votre clé un répertoire et un fichier.

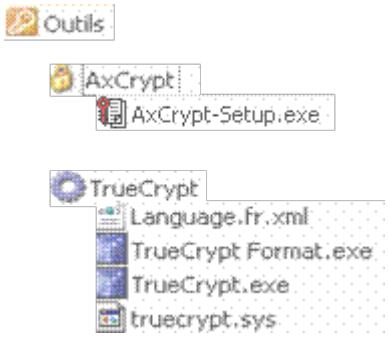
Ici nous avons utilisé la personnalisation des icônes de répertoires de Windows pour faire plus joli (mais ce n'est pas obligatoire non plus).

Si vous voulez faire cette personnalisation, cliquez sur le répertoire avec le bouton droit de la souris, choisissez "propriétés", cliquez sur l'onglet "personnaliser" et sur le bouton "changer d'icône".



Le répertoire contiendra 2 sous répertoires AxCrypt et TrueCrypt :

Dans ces 2 sous répertoires, on y placera le logiciel de chiffrage de fichier AxCrypt et surtout les 3 composants de TrueCrypt, avec l'option de la langue de la façon suivante :



Ce répertoire outil composé de ses 2 sous répertoires, vous accompagnera partout. Ce sera la boite d'outils dont vous aurez besoin pour piloter la sécurité de vos tiroirs rouge et noir.

Le fichier est créé avec le "Bloc Note" de Windows pour pouvoir être lu partout, mais vous pouvez le faire avec un autre traitement de texte.

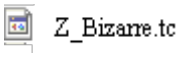
Création de la zone protégée rouge

A la racine de la clé USB apparaîtra un fichier bizarre, impossible à ouvrir de façon classique.

Nous le baptiserons Z_Bizarre.tc, mais bien naturellement vous pourrez l'appeler comme vous voulez. Conservez lui l'extension ".tc", qui voudra dire TrueCrypt.

Ce fichier contiendra les 2 fameux tiroirs rouge et noir.

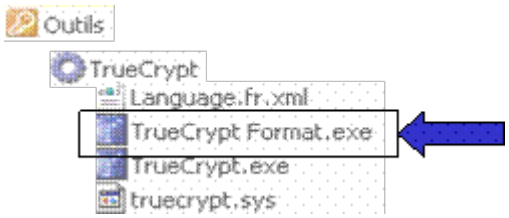
Lors de la création il apparaîtra d'abord comme ceci

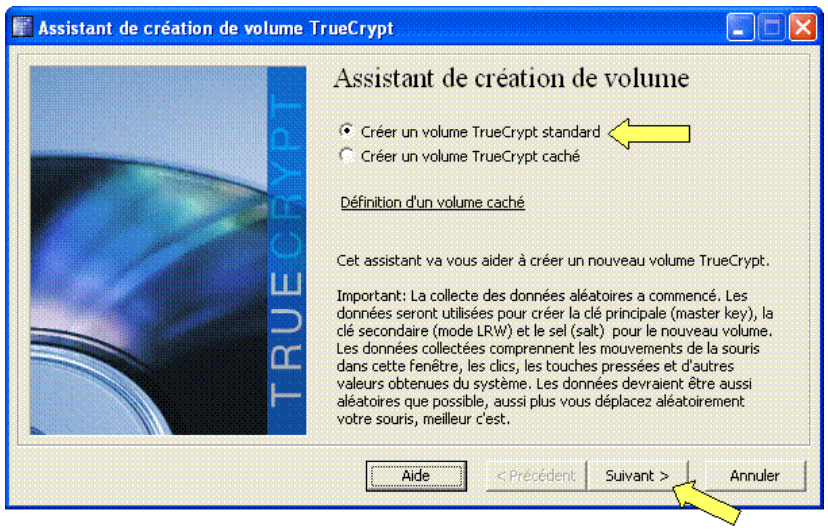


Puis ensuite comme ceci

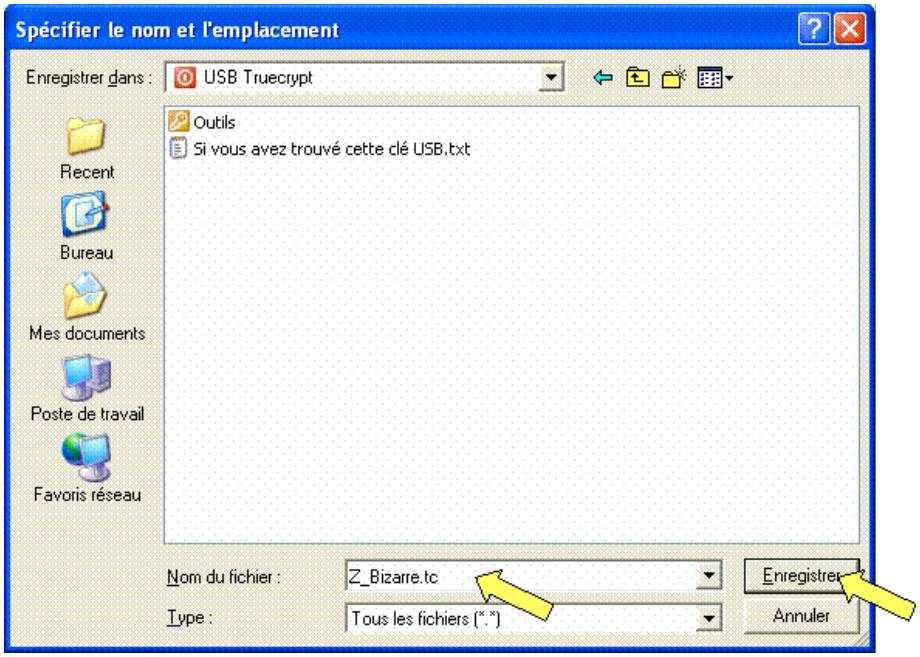
Créerons ce fichier Z_Bizarre.tc

Allez dans le sous répertoire Outils/TrueCrypt, cliquez sur le fichier exécutable TrueCrypt Format.exe

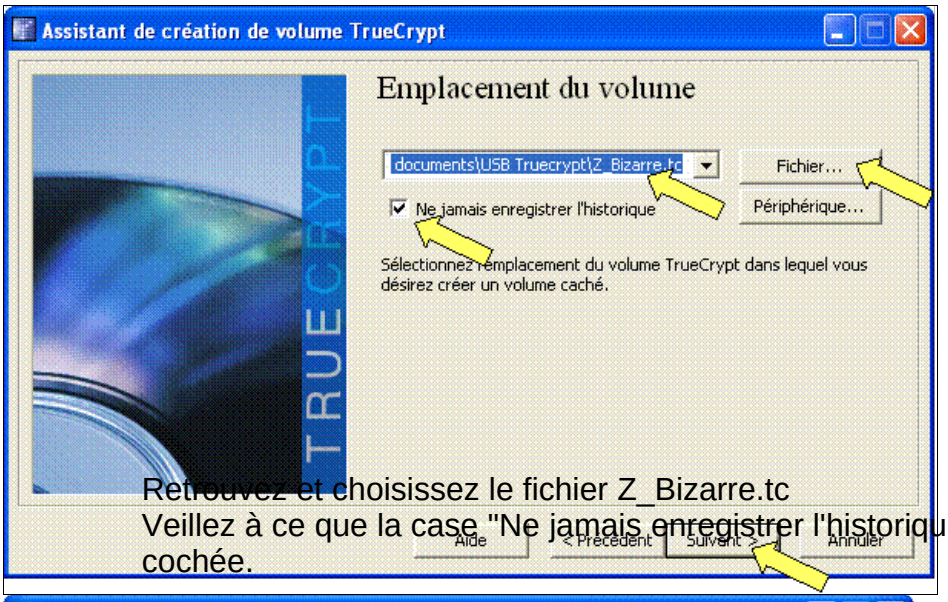




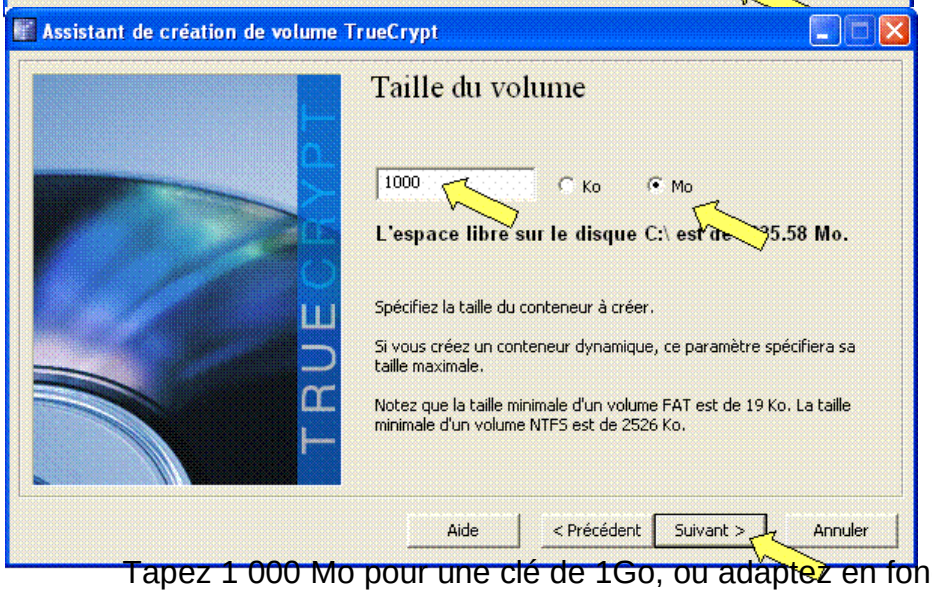
En cliquant sur "fichier", replacez vous dans votre clé USB à la racine.



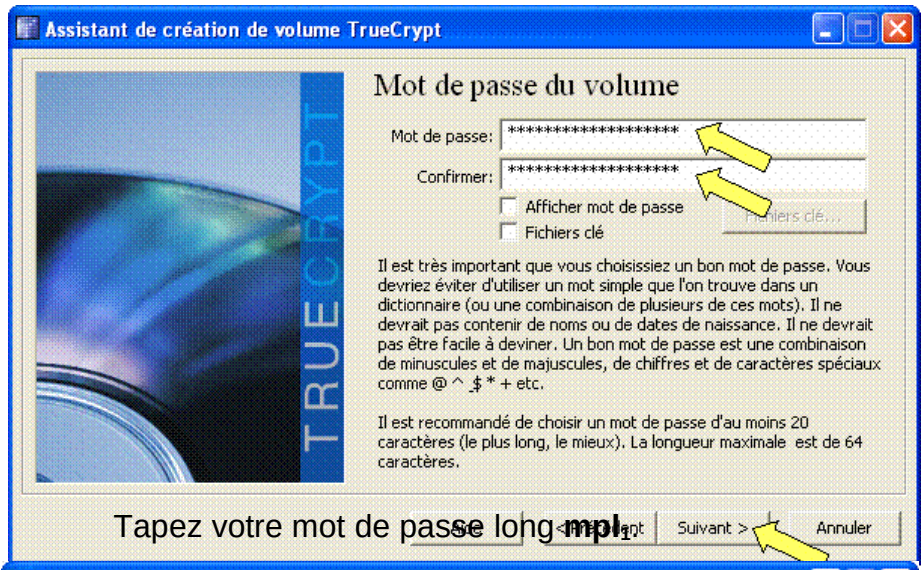
Créez le fichier "Z_Bizarre.tc" et cliquez sur « Enregistrez », puis effectuez les suites des validations suivantes :



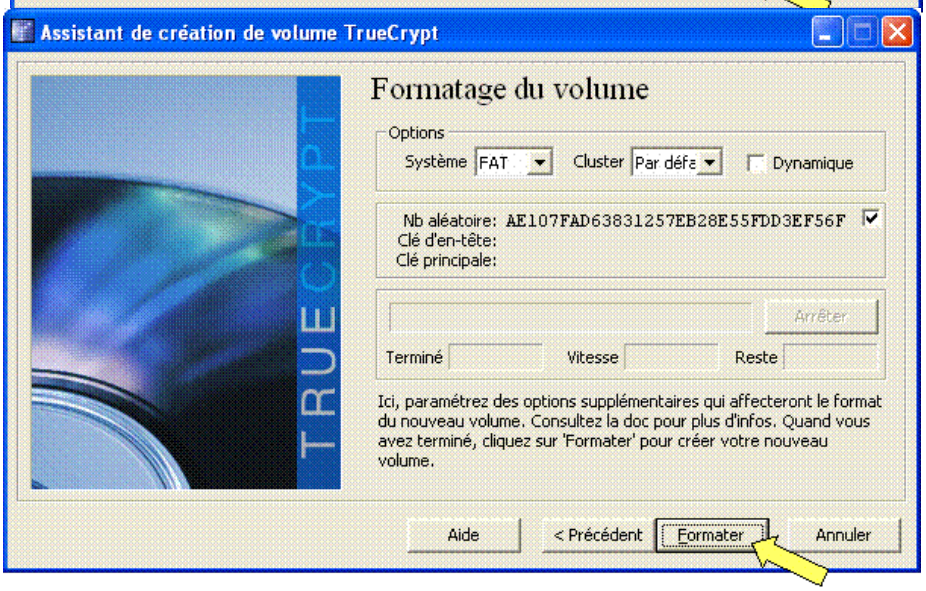
Retrouvez et choisissez le fichier Z_Bizarre.tc
Veillez à ce que la case "Ne jamais enregistrer l'historique" soit cochée.



Tapez 1 000 Mo pour une clé de 1Go, ou adaptez en fonction de votre clé, et cliquez sur suivant.

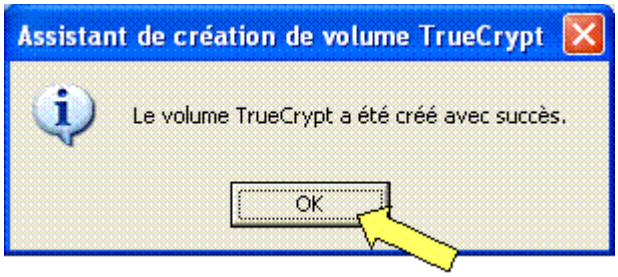


Tapez votre mot de passe long **mpl.**

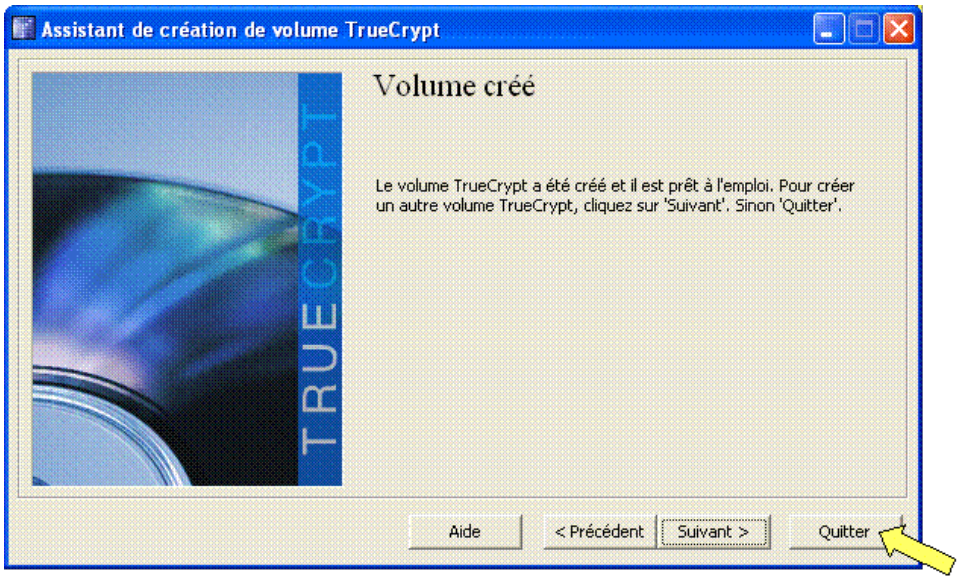


Un processus automatique de création de chiffrement aléatoire est lancé, cliquez après avoir attendu quelques secondes sur Formater.

Le processus de Formatage du fichier Z_Bizare.tc est lancé, attendre environ 1 minute pour formater 1 Go, si vous n'avez pas trop navigué sur la fenêtre au début du chiffrement aléatoire.

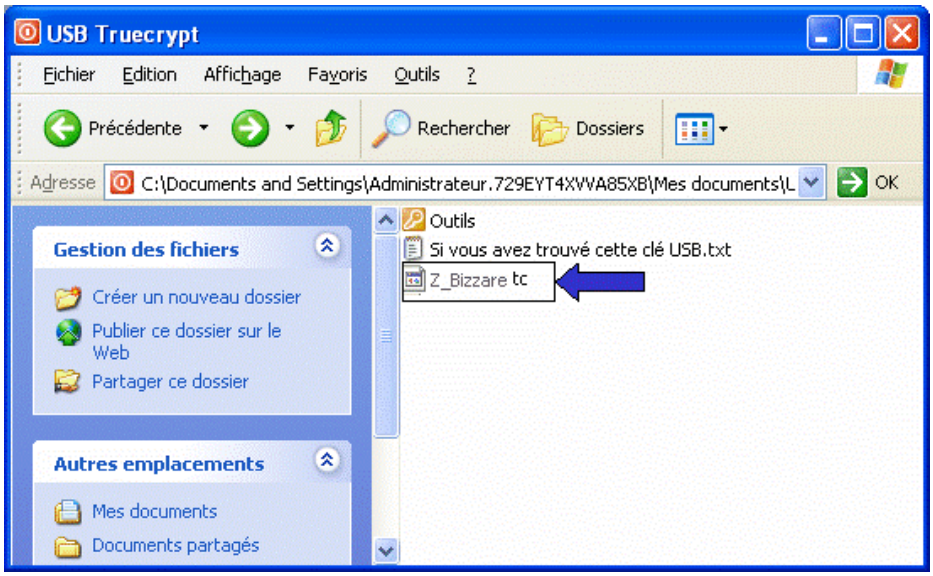


A la fin du formatage cliquez sur « OK »

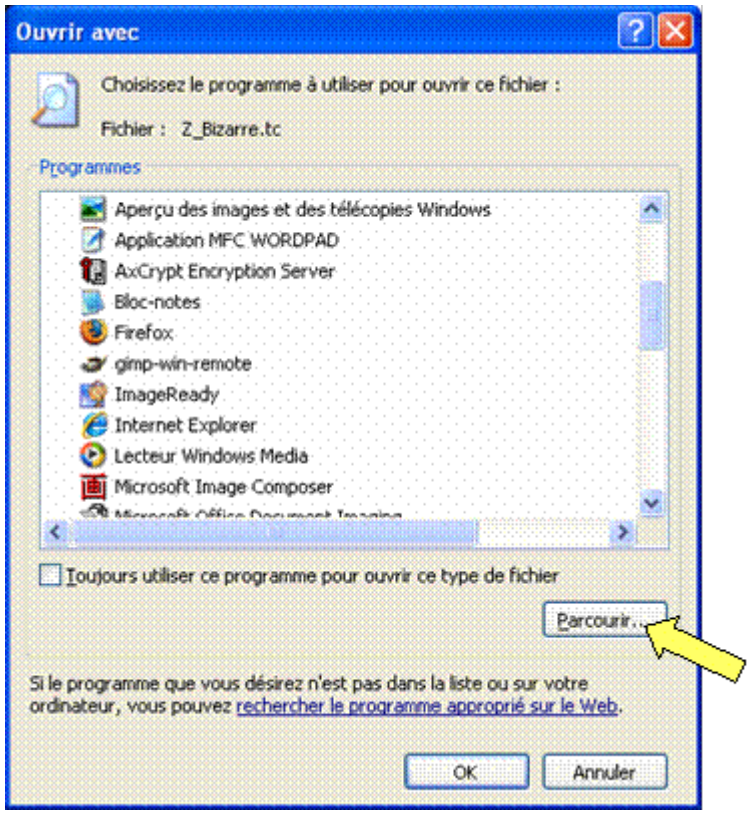


Puis cliquez sur « OK ». Le fichier Z_Bizarre.tc est créé.

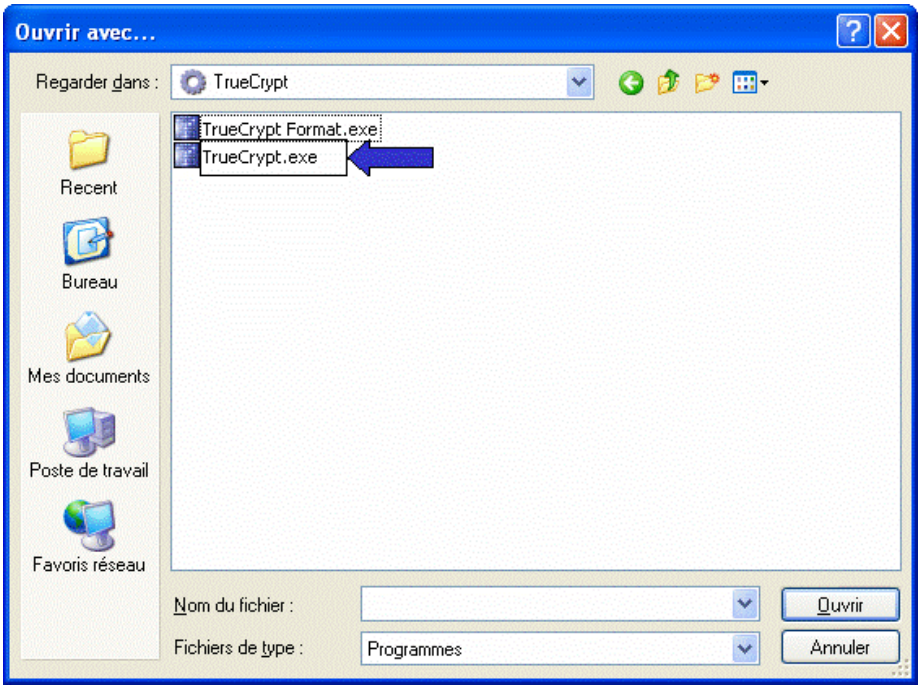
Il apparaît à la racine de votre USB ainsi



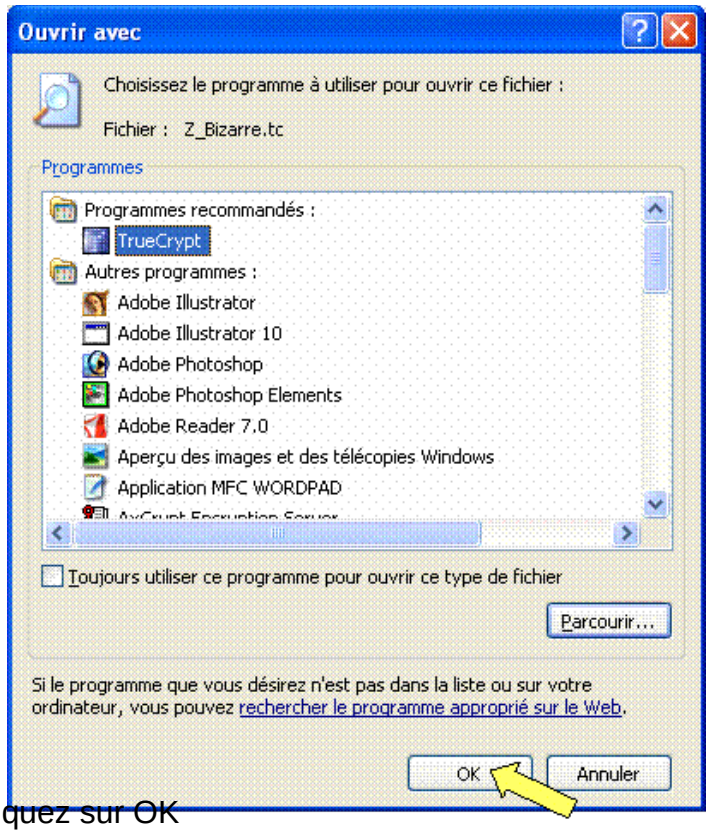
Double cliquez dessus, pour lancer la fenêtre Windows "Ouvrir avec"



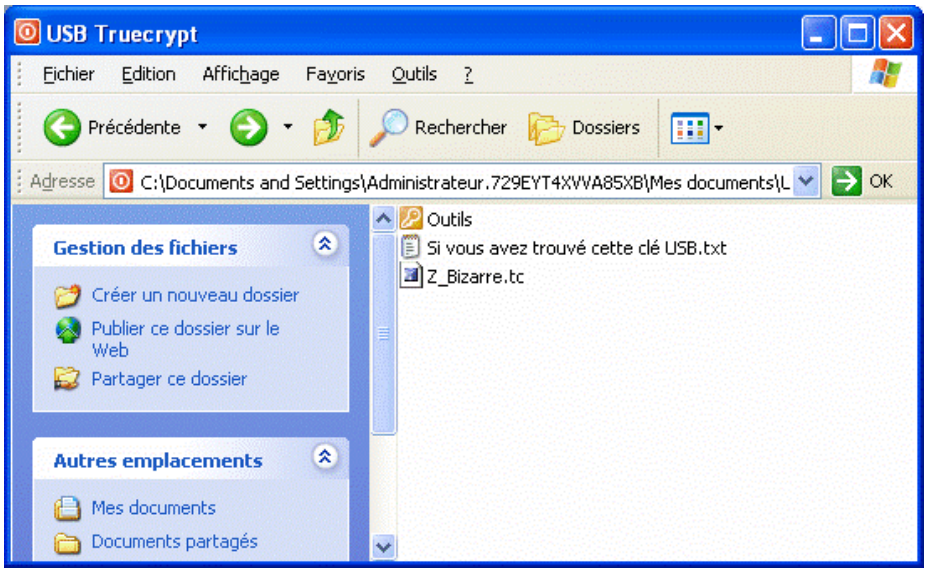
Cliquez sur « Parcourir » et revenez dans le sous répertoire TrueCrypt de votre clé USB.



Double cliquez sur le 2ième composant TrueCrypt : "TrueCrypt.exe"



Cliquez sur OK



Le fichier Z_Bizarre.tc apparaît maintenant avec l'icône de TrueCrypt. Il correspond à votre tiroir rouge.

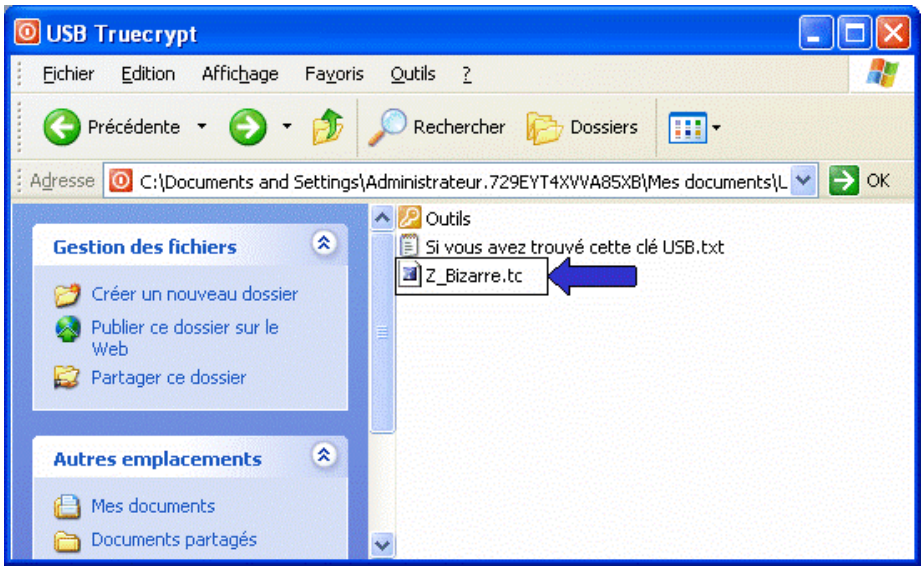
Cette procédure est à refaire éventuellement lorsque vous utiliserez un autre ordinateur. Il faut que l'ordinateur hôte puisse reconnaître l'extension « .tc » pour lancer la bonne application. Une fois qu'il le saura, il ne vous le redemandera plus.

La suite …

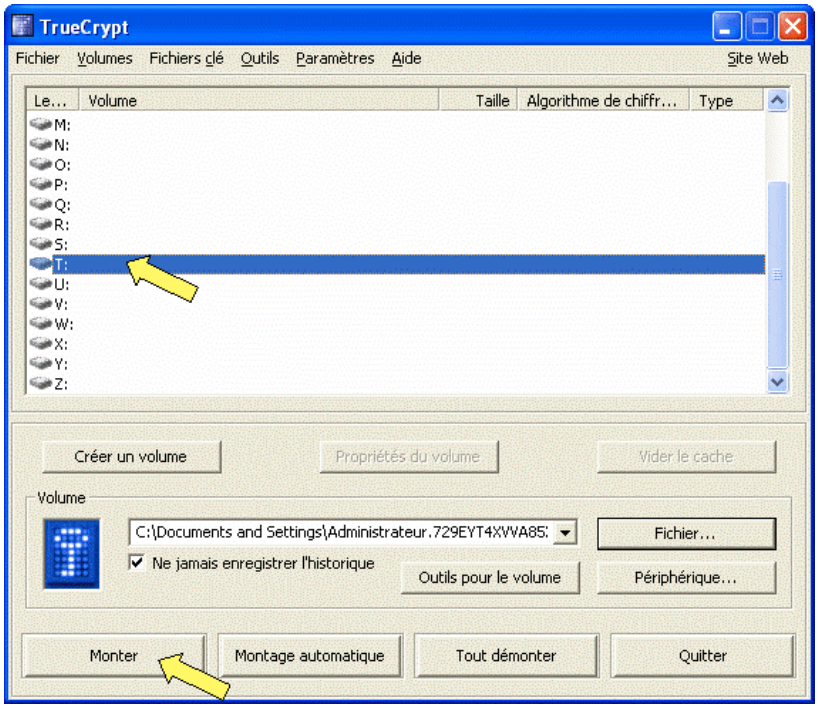
Livre blanc

Pour utiliser notre tiroir rouge nous allons faire ce que les informaticiens appellent un "montage de disque virtuel".

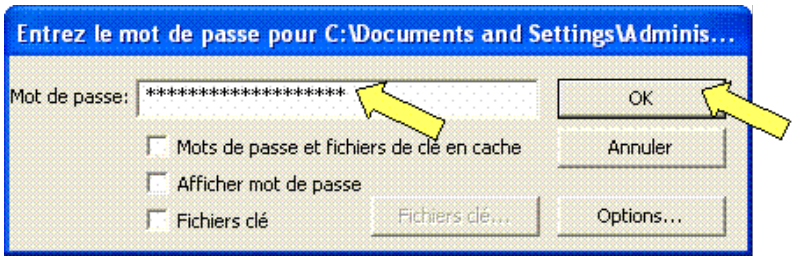
N'ayez pas peur, ça ne mord pas !



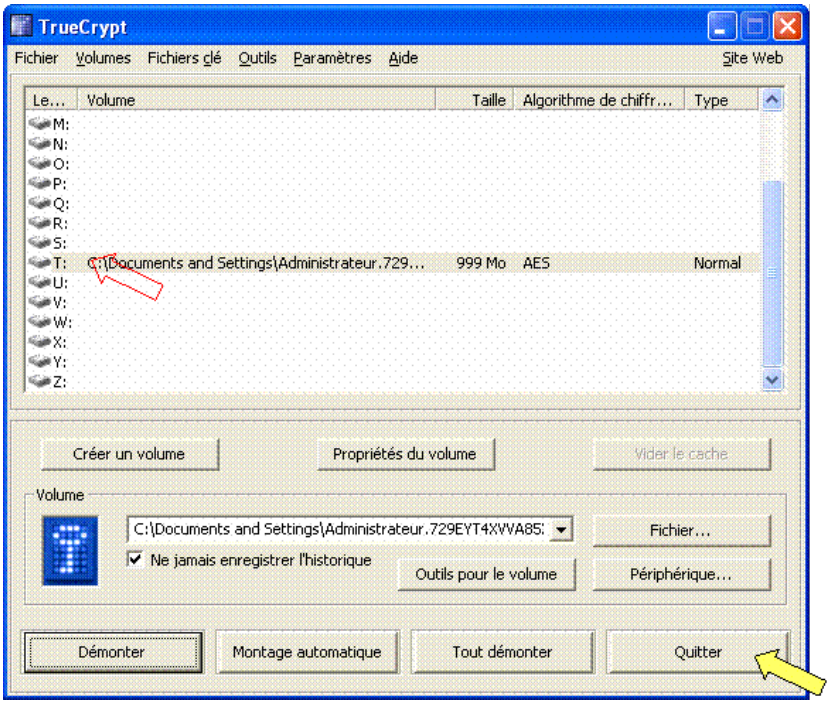
Double cliquez sur le fichier Z_Bizarre.tc



Une fenêtre TrueCript s'affiche, cliquez sur une lettre quelconque proposée, (T:) par exemple, puis sur cliquez sur "Monter"



Retaper **mpl$_1$** puis validez.



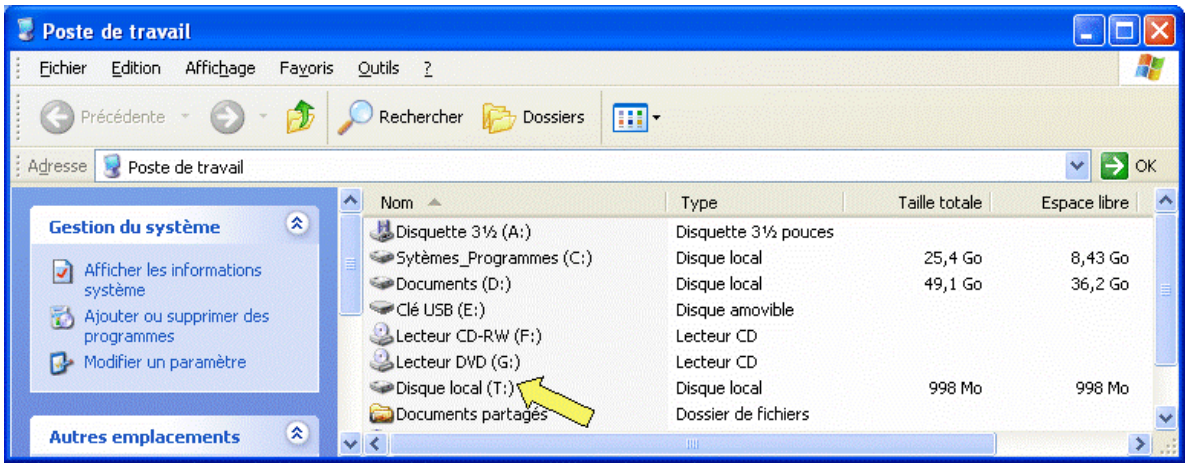
Une ligne grise apparaît, cliquez sur "Quitter".

Vous venez de monter votre tiroir rouge.

Regardez en bas à droite de votre écran, quelque chose vous indique que vous avez monté un volume TrueCrypt.

Ne cliquez pas encore dessus

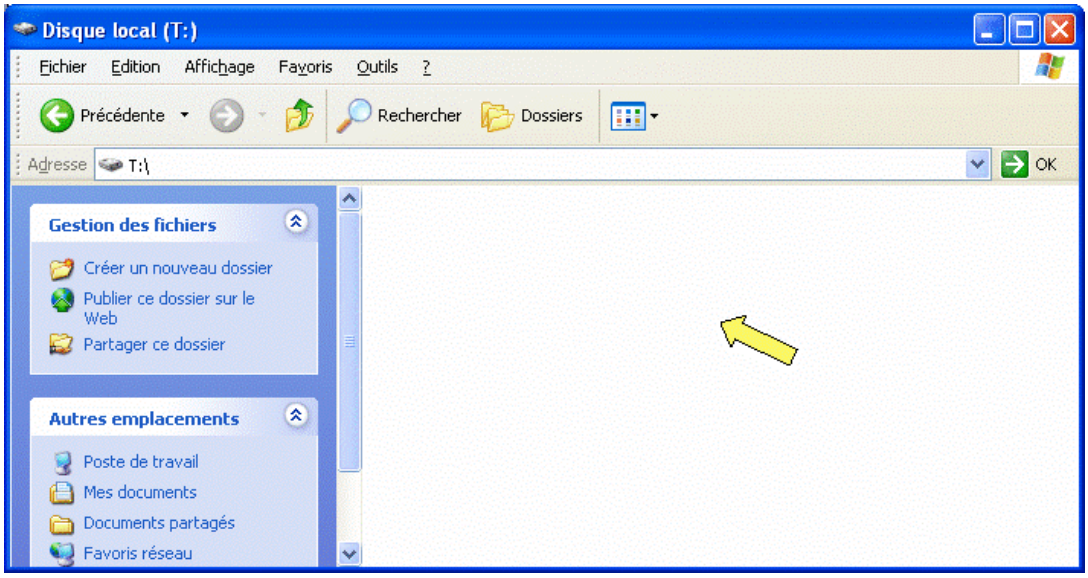
Allez le bureau de votre ordinateur et cliquez maintenant sur "Poste de travail"



Un disque local a été monté.

Il a la lettre (T:) C'est votre tiroir rouge.

Double cliquez dessus.



Vous êtes dans votre espace de travail (tiroir rouge), avec 1Go de disponible, et en toute protection grâce à votre mot de passe long **mpl$_1$**.

N'utilisez plus la fenêtre de votre clé USB.

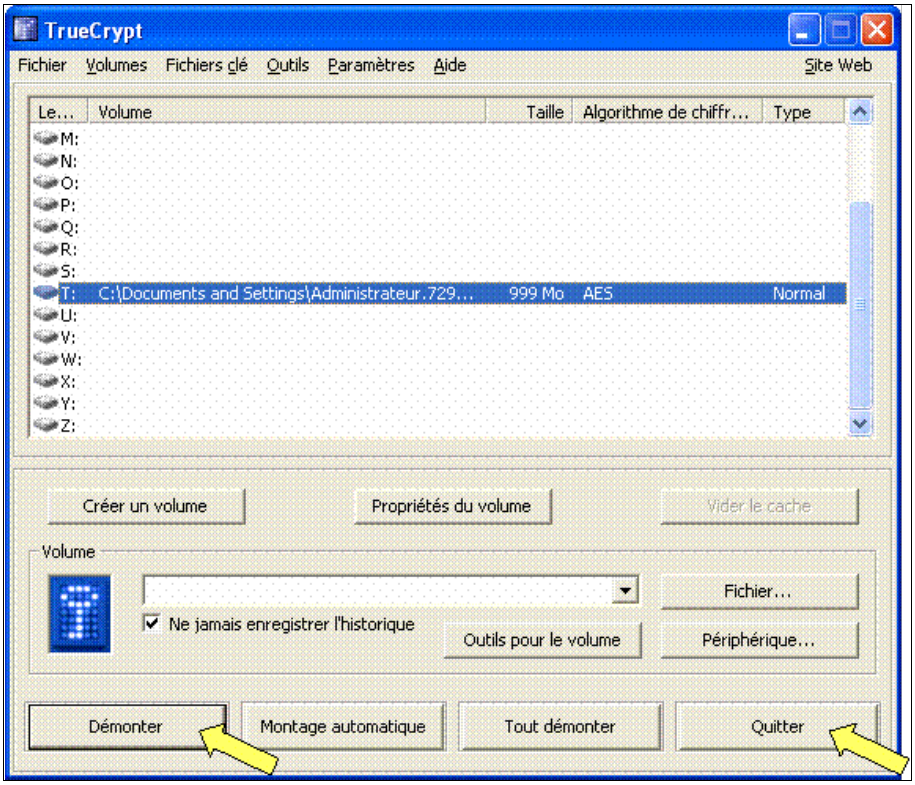
C'est par T:\ que vous allez travaillez maintenant (comme vous le faites sur un disque c:\ par exemple ou sur une a:\disquette).

La clé USB héberge le fichier Z-Bizarre.tc, qui est en fait le disque virtuel T:\.

Toutes les informations qu'il renferme sont strictement protégés par TrueCrypt.

Si vous voulez retirer votre clé, cliquez sur Sur l'icône bleu pour "démonter T:\"

Puis n'oubliez pas de débrancher votre clé USB comme auparavant, en cliquant sur l'icône vert



Cliquez sur "Démonter", puis sur "Quitter"

Un peu bizarre pour les non informaticiens n'est-ce pas !?

Au bout de 2 fois c'est compris.

En fait: une fois la clé USB branchée, et une fois monté le disque T:\, qui lui correspond, on ne s'occupe plus de la clé USB !

Mais c'est bien la clé USB qui recèle tous les contenus de T:\

Faites plusieurs essais de montage et de démontage, sans vous occuper des autres possibilités de TrueCrypt.

Procédure de travail courant

Début de travail
insérez votre clé USB, allez dans son répertoire
double cliquez sur le fichier Z_Bizarre.tc
Cliquer sur monter
Taper **mpl_1**, puis cliquez OK
Cliquez sur quitter
Allez sur votre "poste de travail" et ouvrez le disque (T:)
Laissez votre clé USB branchée mais ne vous occupez plus d'elle

En cours de travail
Travaillez normalement à partir de (T:)

Fin de travail
Cliquez sur l'icône TrueCrypt en bas à droite
Cliquez sur "démonter" puis sur "quitter"
Débranchez votre clé USB (elle est protégée)

Ça va mieux ?

Monsieur est Madame tout le monde peuvent s'arrêter là. Ils disposent d'une clé USB avec un tiroir rouge super protégé et accessible avec leur mot de passe long " mpl_1".

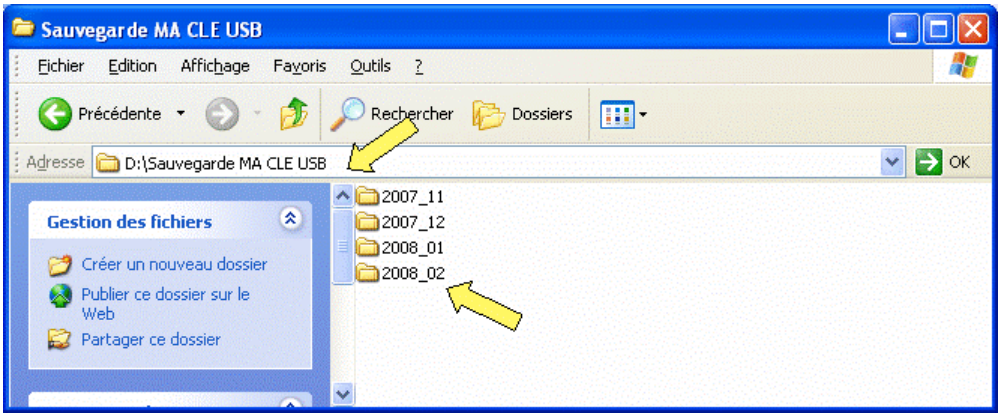
N'oubliez pas de sauvegarder votre clé USB

Procédure de sauvegarde

Préparer un répertoire de sauvegarde sur votre ordinateur ou sur une autre clé USB.

La capacité d'accueil de sauvegarde doit être égale ou supérieur à la taille de votre clé USB : 1Go, 2,4, 8, 16 Go

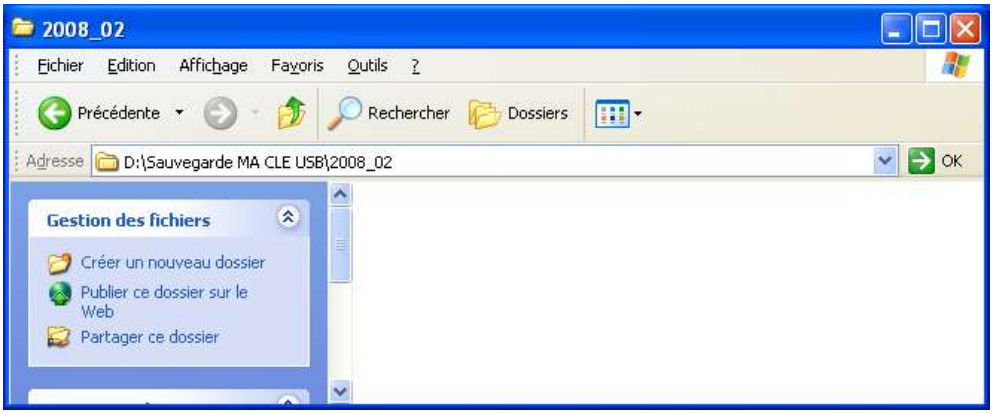
Remarque: sauf si vous avez une clé USB d'une capacité égale ou inférieur à 512 Mo, la sauvegarde sur un CD est impossible.



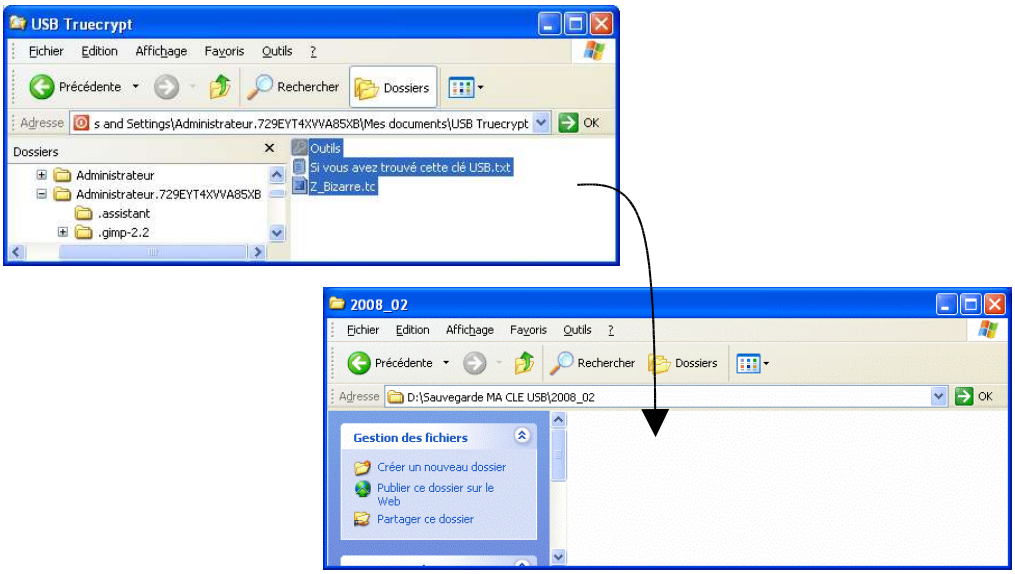
Pour chaque sauvegarde, ouvrez le répertoire de sauvegarde et créez un sous répertoire à la date de sauvegarde,
(Depuis le menu Windows, cliquez Fichier/Nouveau/Dossier).

Par exemple année_mois, ce qui vous permet d'avoir un ordre chronologique

Ouvrez ce sous répertoire.



Votre clé USB étant connectée, allez dedans et sectionnez « tout » par la double commande "touche Control"+"touche A", puis cliquez déplacez vers le sous répertoire de sauvegarde pour faire la copie. Vérifiez que vous n'avez pas fait couper/coller, mais bien seulement copier/coller.

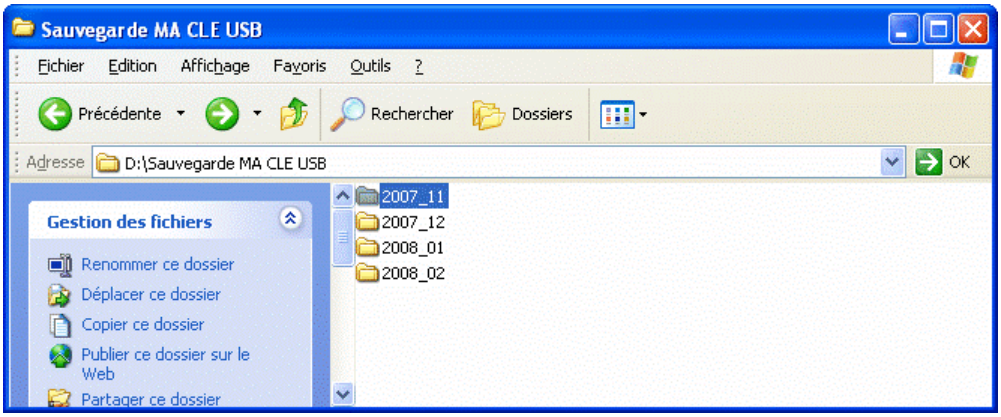


Si vous n'arrivez pas à le faire, c'est que vous avez mal "démonté" votre clé ou qu'un processus reste ouvert dans votre ordinateur. Si cela vous arrive, redémarrez votre ordinateur et recommencez.

Remarque: lors de la sauvegarde c'est tout le disque virtuel (T:) qui est sauvegardé, c'est à dire tout le fichier Z-Bizarre.tc, soit ici 1 Go, quelque soit le nombre de fichiers qu'il contient.

On aura donc tout intérêt à avoir une clé USB rapide en lecture (voir choix du départ).

En fin de sauvegarde, supprimer la plus ancienne des sauvegardes pour ne conserver que les 2 ou 3 dernières (gestion de la place sur votre ordinateur)



Voilà.

Déjà satisfait de votre clé sécurisée ?

Création de la zone critique noire

Abordons maintenant ce fameux tiroir noir, celui qui sera invisible, inviolable et qui pourra héberger vos plus intimes secrets.

Intérêt d'un fichier de clé de chiffrement

Définissons tout d'abord ce qu'est un "fichier de clé de chiffrement" **cc**

Un fichier de clé de chiffrement est un fichier dont le contenu est combiné avec un mot de passe (**cc** + **mpl_2**). Si le fichier de clé n'est pas fourni, le tiroir noir qui utilise cette combinaison ne peut être monté et toute l'information qu'il contient est irrémédiablement perdue.

L'utilisation d'un fichier de clé a de multiples avantages:

Il fournit une protection contre les enregistreurs de frappe. Ainsi, même si un mal veillant collecte votre mot de passe en utilisant un enregistreur de frappe, il ne sera pas en mesure de monter le volume sans votre clé de chiffrement.

Il renforce considérablement la protection contre les attaques par force brute, c'est à dire les tentatives de déchiffrement par l'usage de logiciels et d'ordinateurs puissants qui simulent toutes les combinaisons. Ce point est particulièrement important si votre mot de passe **mpl_2** n'est pas trop fort.

Pour qu'une attaque par force brute soit irréalisable, la taille de la clé **cc** doit être au moins de 30 octets avec une qualité aléatoire importante.

Pour ce faire nous allons utiliser le générateur de TrueCrypt. La taille du fichier résultant **cc** sera toujours de 64 octets (soit 512 bits).

Pour finir, TrueCrypt propose même la combinaison de plusieurs fichiers de clés de chiffrement !

AVERTISSEMENT:
Si vous perdez **cc** ou si votre fichier est altéré, il ne vous sera jamais plus possible de monter le tiroir noir. Son contenu sera irrémédiablement inutilisable !

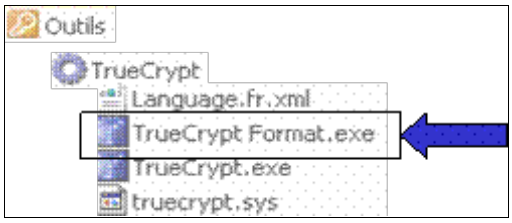
Procédure de création du tiroir noir

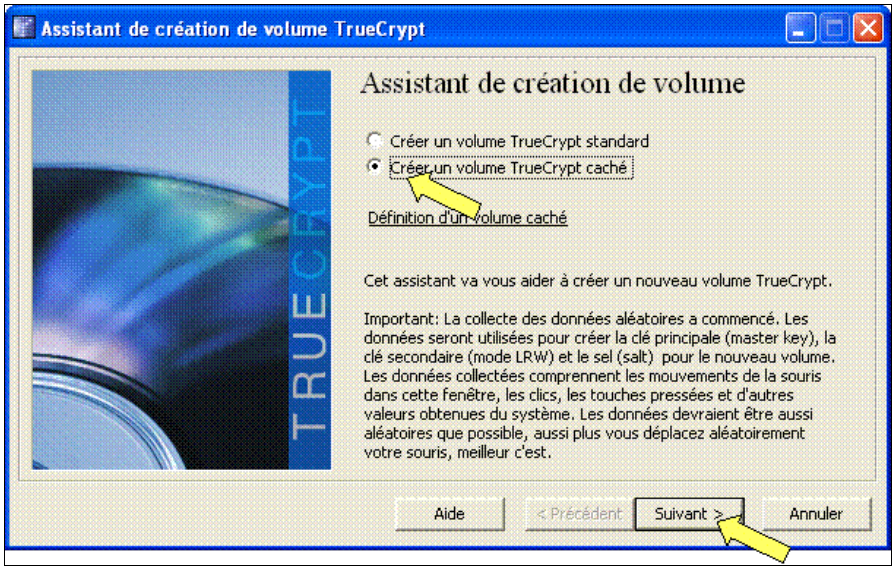
Nous allons voir que c'est finalement simple maintenant que notre tiroir rouge est créé.

Ce tiroir noir, comme nous l'avons vu, sera caché dans le tiroir rouge.

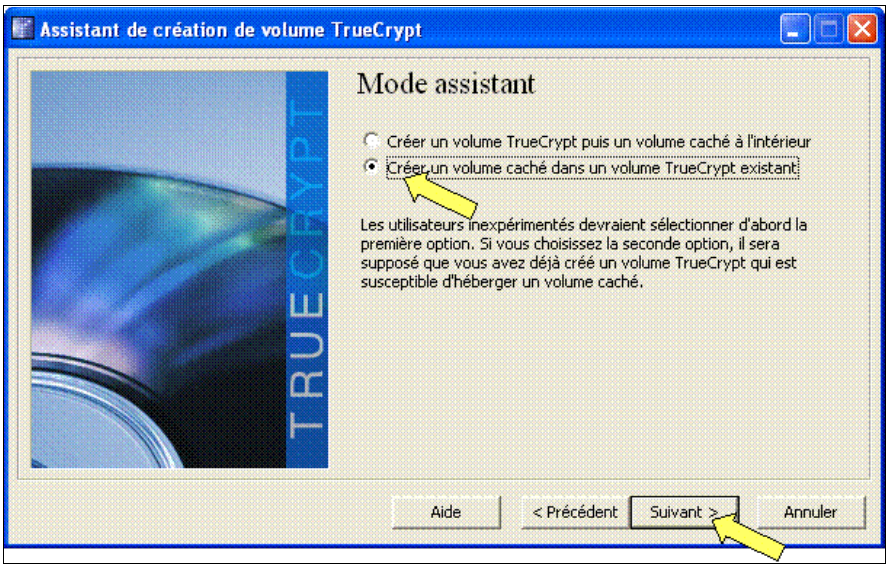
Démonter votre disque (T:) avant de faire la manipulation, pour reprendre la procédure normalement.

Laissez votre clé connectée à l'ordinateur et allez dans le répertoire outils de votre clé et double cliquez sur TrueCrypt Format.exe



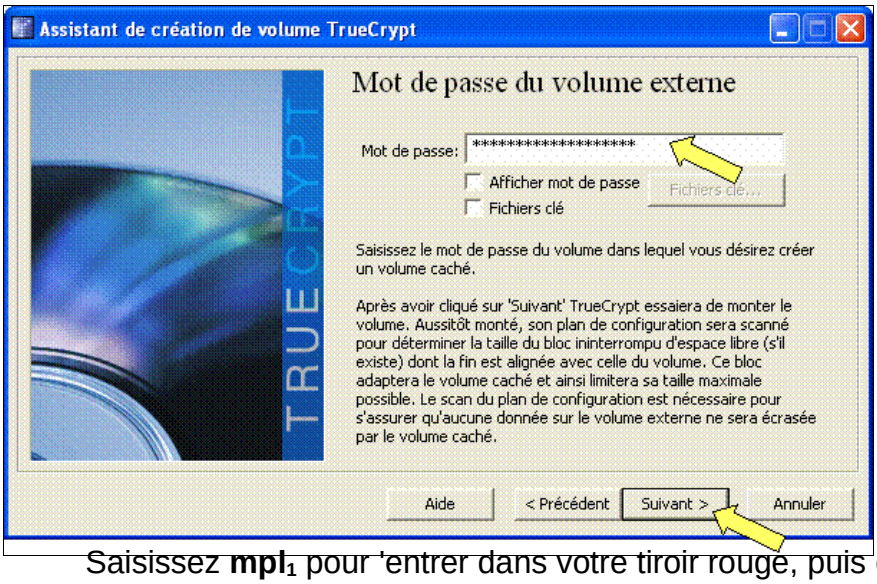


Sélectionnez le bouton "Créez un volume TrueCrypt caché", puis cliquez sur "suivant".

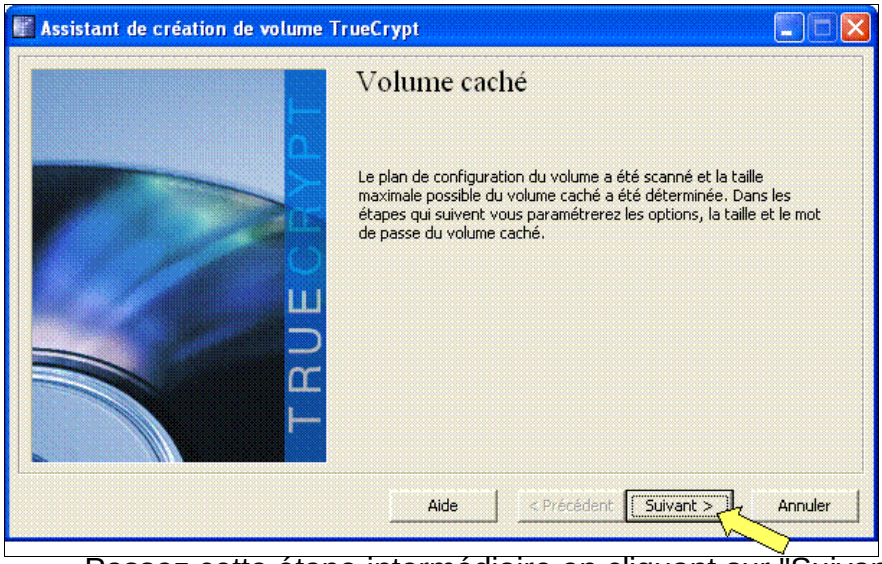


Sélectionnez le bouton "Créez un volume caché dans un volume TrueCrypt existant", puis cliquez sur "Suivant".

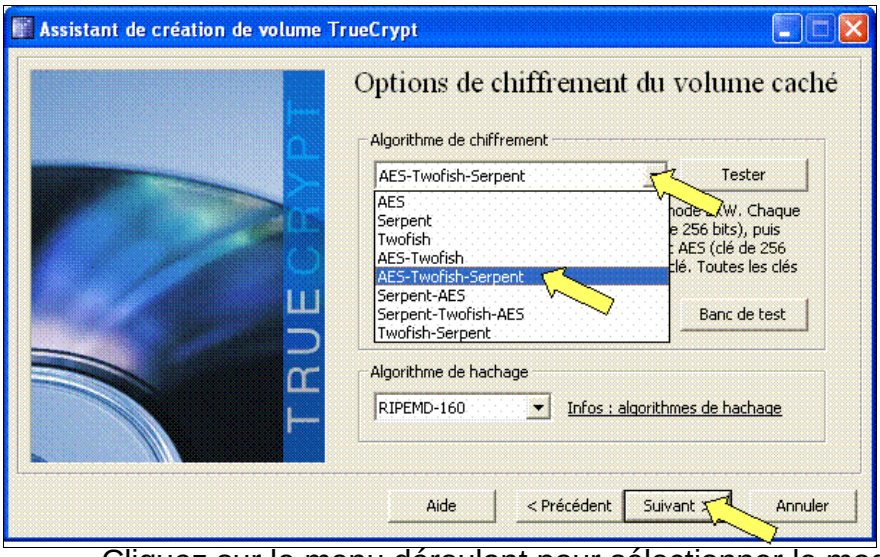
Cliquez sur "Fichier..." pour retrouvez votre fichier Z_Bizarre.tc de votre clé USB et qui correspond à votre tiroir rouge,; puis cliquez sur "suivant"



Saisissez **mpl**$_1$ pour 'entrer dans votre tiroir rouge, puis cliquez sur suivant.



Passez cette étape intermédiaire en cliquant sur "Suivant".

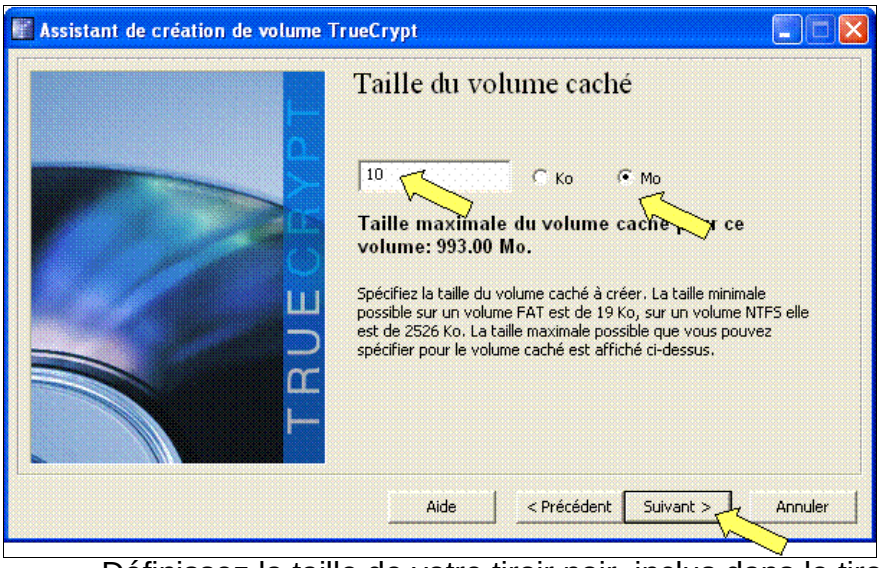


Cliquez sur le menu déroulant pour sélectionner le mode de chiffrement en triple cascade, le plus fort (3 x 258 bits)

Sélectionnez "AES-Twofish-Serpent"

Puis cliquez sur "Suivant"

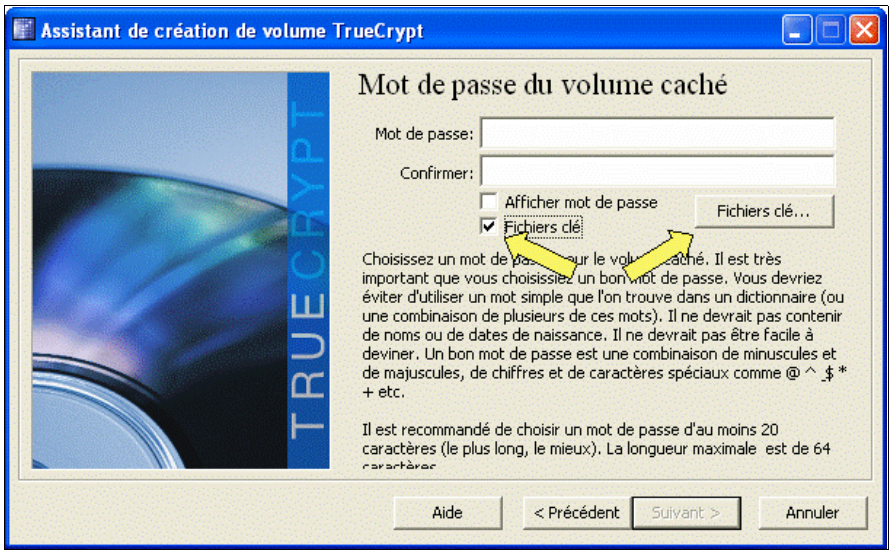
Nous ne donnons pas ici d'explications sur les différents modes de chiffrement (voir la documentation de TrueCrypt).



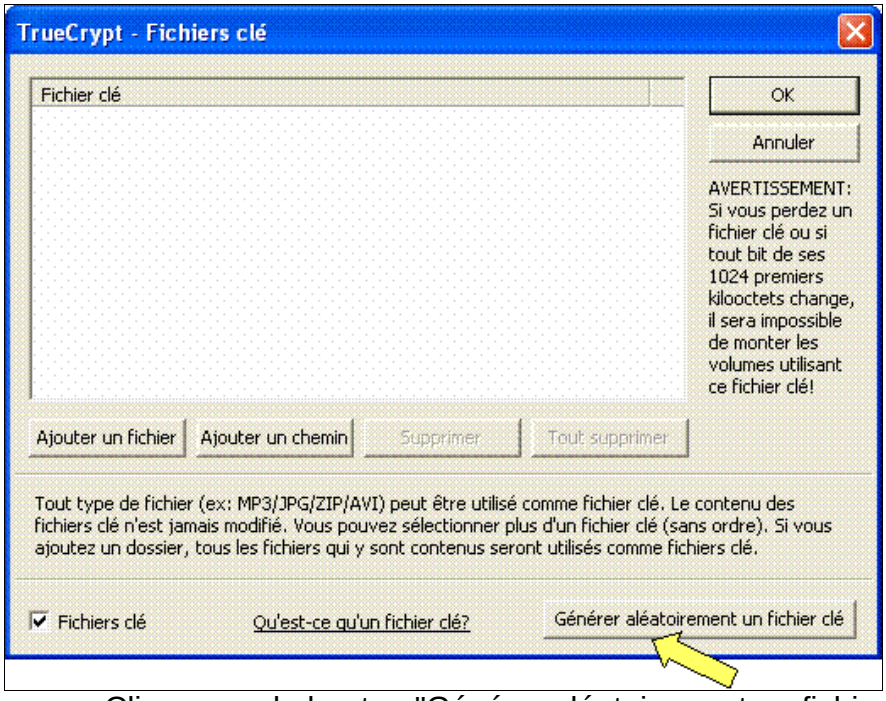
Définissez la taille de votre tiroir noir, inclus dans le tiroir rouge de 1Go. Ici nous avons choisi 10 Mo, soit 1% du tiroir rouge, mais vous pouvez prendre bien plus, ou même presque toute la place du tiroir rouge.

Nous allons créer notre fichier de clé de chiffrement **cc** (nous n'en ferons qu'un seul, car TrueCrypt permet d'en faire

plusieurs). Cette clé de chiffrement **cc** sera associée par la suite à **mpl$_2$**.

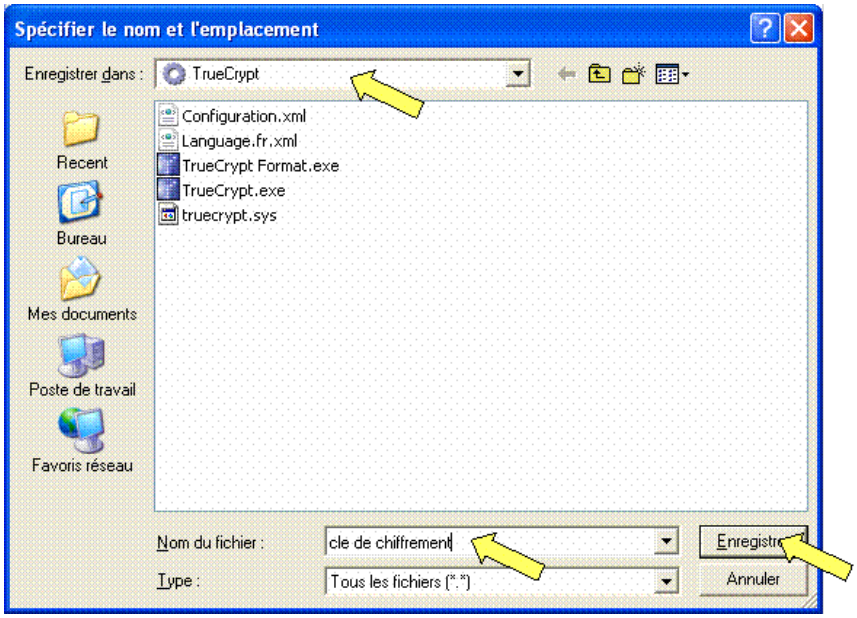


Cochez la case "Fichier clé" pour activer le bouton "Fichiers clé.." et cliquez sur le bouton.

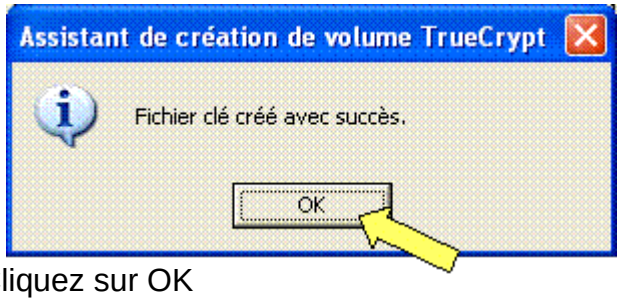


Cliquez sur le bouton "Générer aléatoirement un fichier clé"

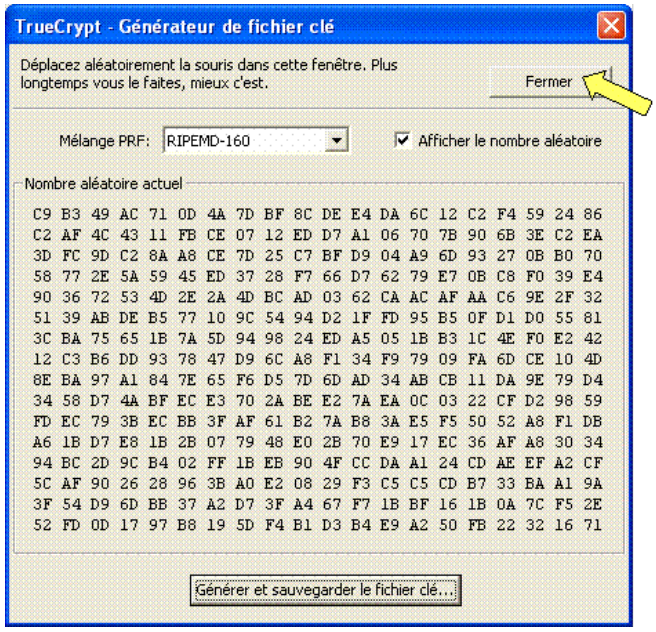
Un tableau de chiffres se met en mouvement, déplacez votre souris dans tous les sens dans cette fenêtre, puis cliquez sur "Générer et sauvegarder le fichier clé".



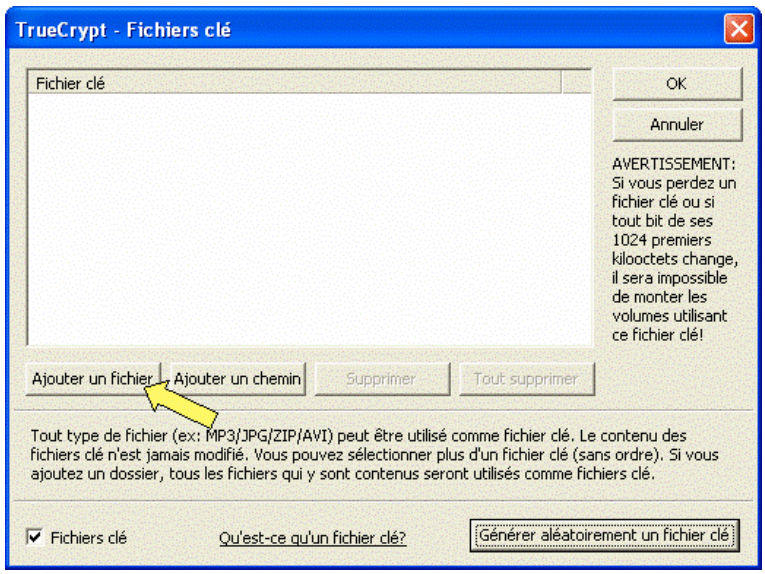
Choisissez pour l'instant le répertoire "TrueCrypt" pour stocker temporairement votre fichier de clé de chiffrement **cc** et donnez lui un nom, par exemple : "clé de chiffrement"



Cliquez sur OK

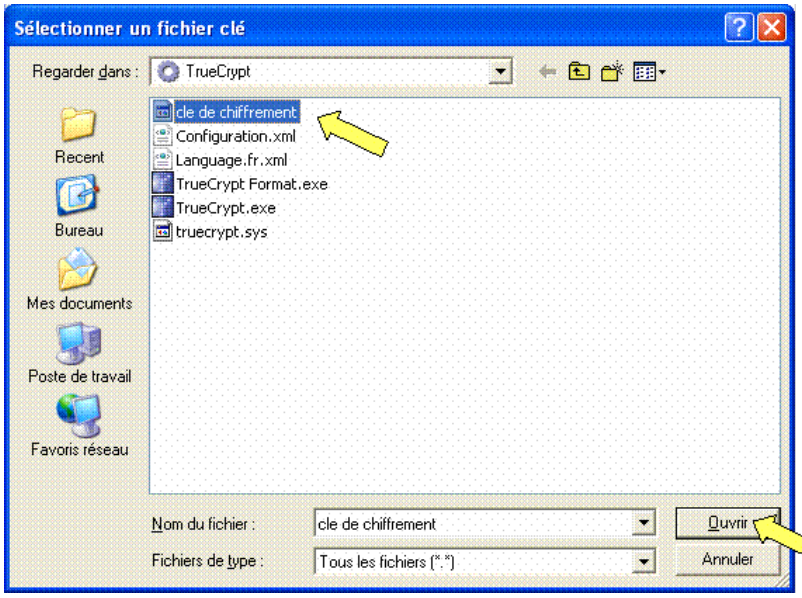


Puis fermez l'outil de création de clé de chiffrement en cliquant sur le bouton "Fermer"

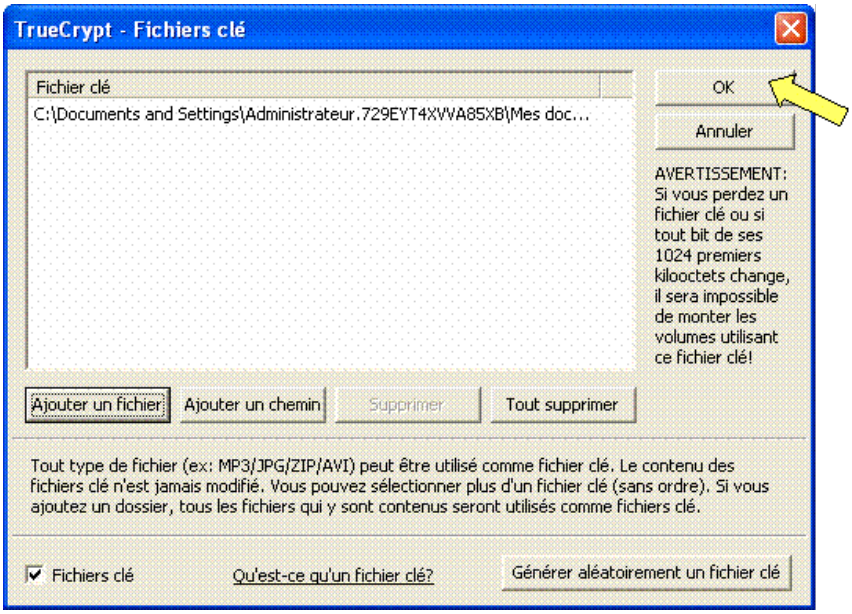


Nous allons ajouter ce fichier de clé chiffrement **cc** dans l'outil TrueCrypt pour que celui-ci puisse l'associer à **mpl$_2$** et créer un système inviolable.

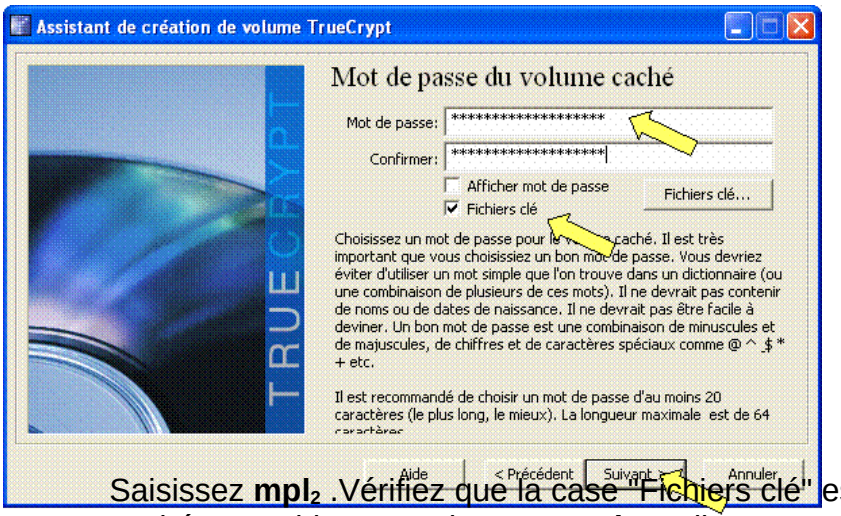
Cliquez sur le bouton "Ajouter un fichier"



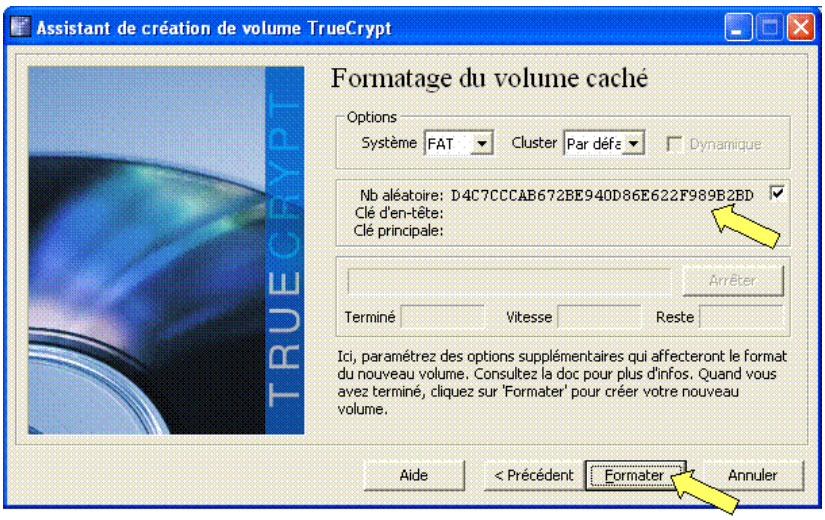
Retourner dans le répertoire TrueCrypt, là ou se trouve votre fichier de chiffrement, sélectionnez le et cliquez sur le bouton "Ouvrir"



Le fichier de clé de chiffrement **cc** est placé dans l'outil de TrueCrypt prêt à effectuer l'association avec le mot de passe **mpl_1**. Cliquez sur le bouton "OK"

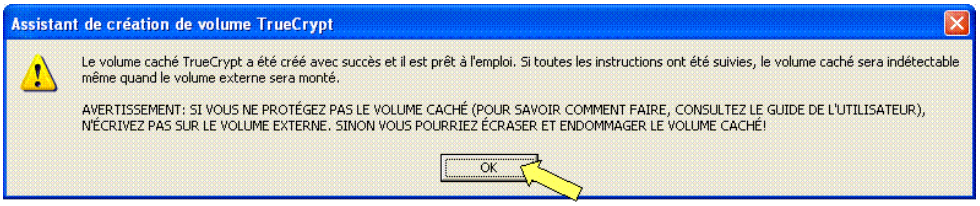


Saisissez **mpl₂** .Vérifiez que la case "Fichiers clé" est restée cochée pour bien associer **cc** + **mpl₂** et cliquez sur le bouton "Suivant".

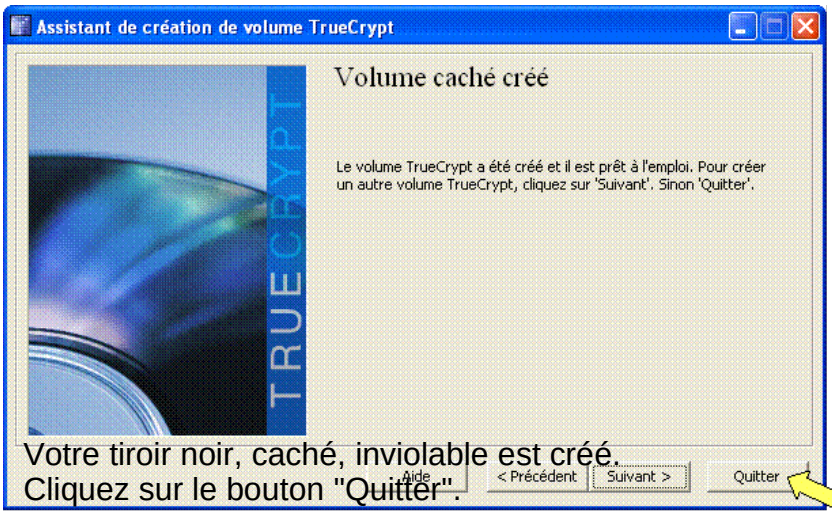


Des nombres aléatoires sont en mouvement, attendez quelques secondes et cliquez sur le bouton "Formater".

Le formatage est lancé, attendre en fonction de la taille du tiroir noir caché.



Puis cliquez sur le bouton "OK du message d'avertissement que vous ignorerez si vous utilisez un très petit tiroir noir. Cet avertissement veut dire que vous devez prendre des précautions si votre tiroir rouge commence à être aux limites de recouvrement de votre tiroir noir, trop grand (dans ce cas prévoir une organisation spéciale non expliquée ici pour des raisons de déontologie d'usage des tiroirs noirs)



Votre tiroir noir, caché, inviolable est créé.
Cliquez sur le bouton "Quitter".

Nous allons maintenant voir comment faire apparaître ce fameux tiroir noir caché et inviolable.

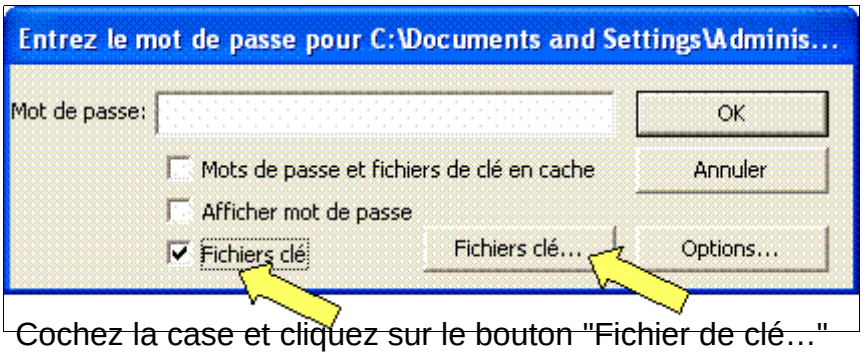
Attention: notez que votre clé de chiffrement **cc** est dans votre répertoire TrueCrypt, dans votre clé USB. Il ne faut pas la laisser en l'état. Nous verrons comment la mettre en protection plus loin.

Apparition du tiroir noir

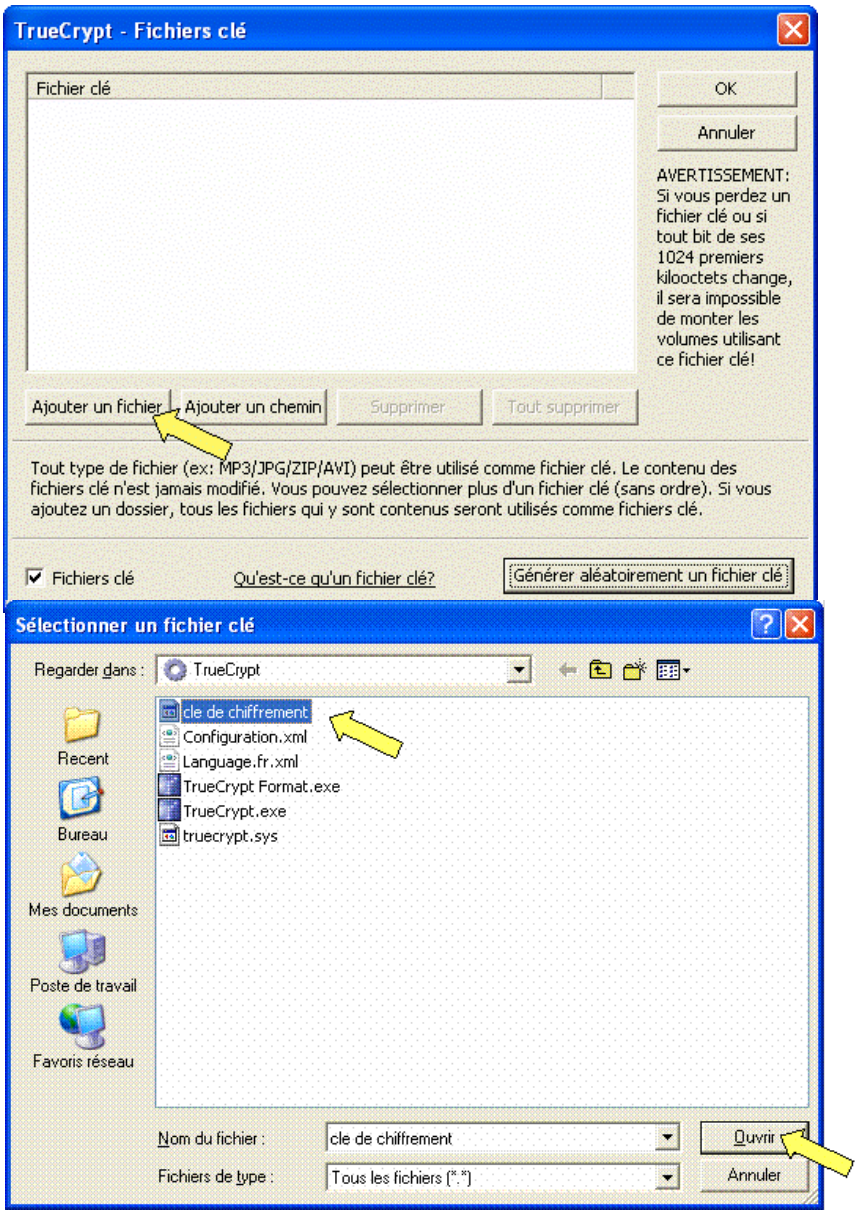
Allez sur votre clé USB, et sélectionner le fichier Z_Bizarre.tc, Comme auparavant, double-cliquez dessus pour le monter.

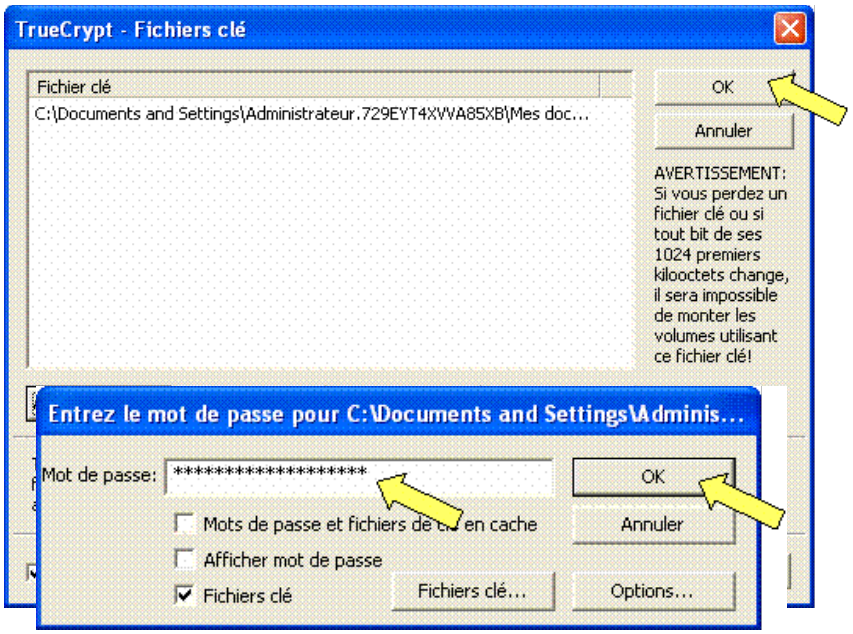
Si vous tapez **mpl$_1$** , il se monte en tiroir rouge, rien de surprenant vous l'avez déjà fait.

Démontez-le et remontez le en prenant la peine cette fois de faire ceci:



Cochez la case et cliquez sur le bouton "Fichier de clé…"

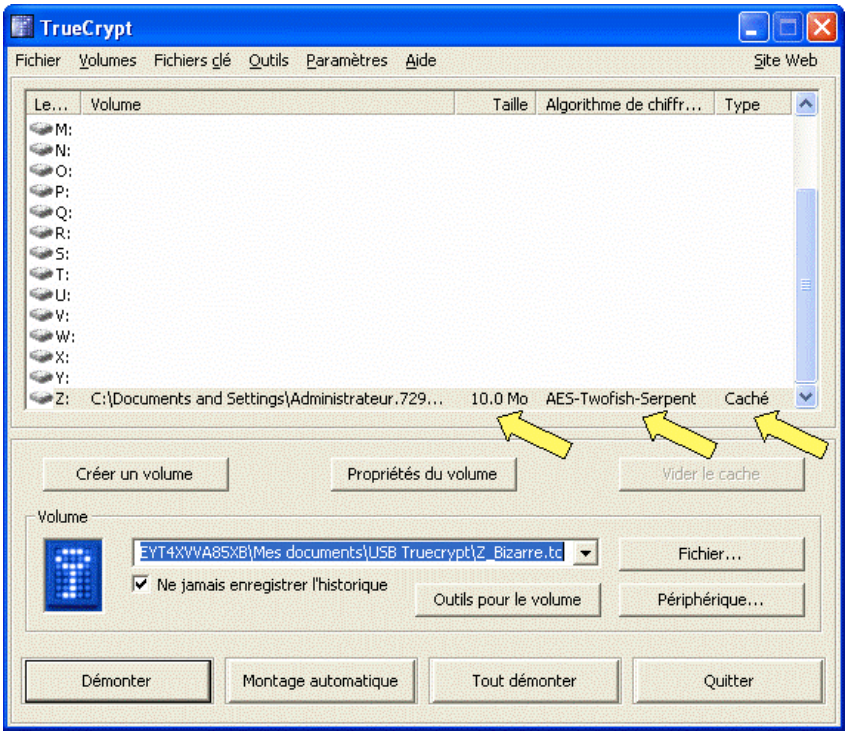

TrueCrypt - Fichiers clé
Fichier clé
OK
Annuler
AVERTISSEMENT: Si vous perdez un fichier clé ou si tout bit de ses 1024 premiers kilooctets change, il sera impossible de monter les volumes utilisant ce fichier clé!
Ajouter un fichier
Ajouter un chemin
Supprimer
Tout supprimer
Tout type de fichier (ex: MP3/JPG/ZIP/AVI) peut être utilisé comme fichier clé. Le contenu des fichiers clé n'est jamais modifié. Vous pouvez sélectionner plus d'un fichier clé (sans ordre). Si vous ajoutez un dossier, tous les fichiers qui y sont contenus seront utilisés comme fichiers clé.
Fichiers clé
Qu'est-ce qu'un fichier clé?
Générer aléatoirement un fichier clé
Sélectionner un fichier clé
Regarder dans :
TrueCrypt
Recent
Bureau
Mes documents
Poste de travail
Favoris réseau
cle de chiffrement
Configuration.xml
Language.fr.xml
TrueCrypt Format.exe
TrueCrypt.exe
truecrypt.sys
Nom du fichier :
cle de chiffrement
Ouvrir
Fichiers de type :
Tous les fichiers (*.*)
Annuler



Entrez cette fois **mpl₂**

Cliquez sur "OK".

mpl₂ et **cc** sont associés et c'est le tiroir noir qui apparaît !



Refaites plusieurs fois la manipulation.

Pour des raisons de sécurité, pour chaque montage de votre tiroir noir, il vous faut remettre votre fichier de clé de chiffrement **cc** dans l'outil d'association avec **mpl₂**.

A partir de là, le tiroir noir s'utilise comme le tiroir rouge.

Remarque : il semble que l'on ne puisse pas monter le tiroir rouge et le tiroir noir en même temps. C'est soit l'un soit l'autre. Attendons les nouvelles versions de TrueCrypt.

Procédure de protection de la clé de chiffrement

Vous venez de le constater, votre fichier de clé de chiffrement **cc** joue bien son rôle. Mais si vous le perdez ou si il est altéré, votre tiroir noir et son contenu sont perdus!

Alors respectez strictement l'organisation décrite dans les pages précédentes.

Vous sortirez dès que possible ce fichier **cc** de votre clé USB et vous le copierez sur votre **support ultime**, un CD ou une disquette. Ne mettez jamais **cc** à proximité de vos sauvegardes et encore moins dans votre ordinateur. Ne le conservez jamais sur vous !

Vous le rechercherez selon vos besoins depuis un dispositif d'hébergement. Voir le paragraphe précédent "Choix de l'hébergeur de clés anonymes de chiffrement".

Constatez que la taille de **cc** est très petite. Et pourtant c'est une très puissante clé de chiffrement. Si vous essayez de l'ouvrir avec votre traitement de texte, vous verrez apparaître de drôles de caractères.

Avant de le confier à un tiers qui ne vous connaîtra jamais, nous allons le protéger et le transformer.

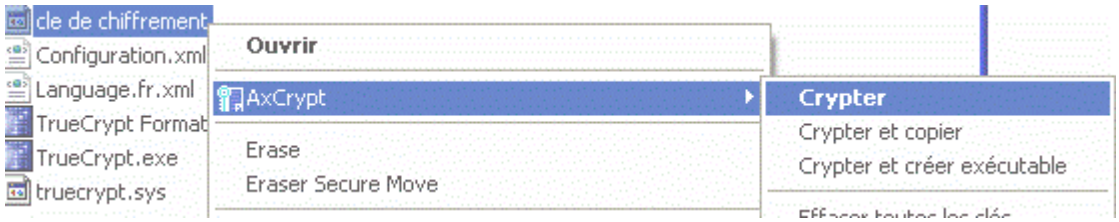
Nous allons le chiffrer avec l'outil AxCrypt et **mpc**.

Allez sur votre répertoire AxCrypt et double-cliquez sur le fichier exécutable.

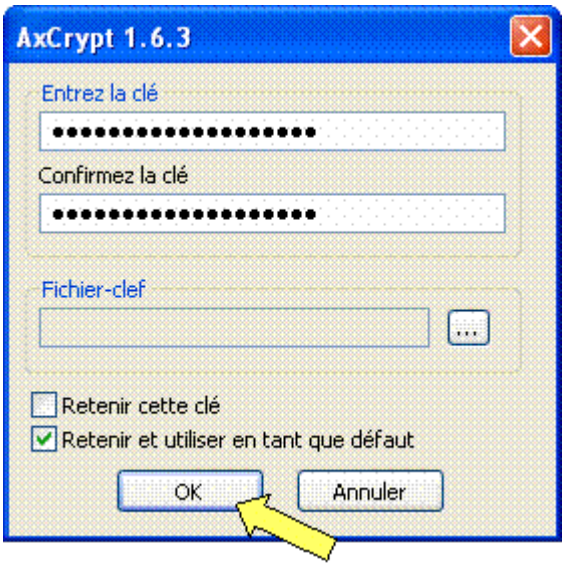
AxCrypt s'installe sur votre ordinateur, suivez les instructions simples.

A la fin de l'installation, revenez sur votre fichier de clé de chiffrement **cc** dans votre répertoire "TrueCrypt" sélectionnez le en cliquant sur le bouton droit de votre souris.

Et choisissez crypter comme suit :

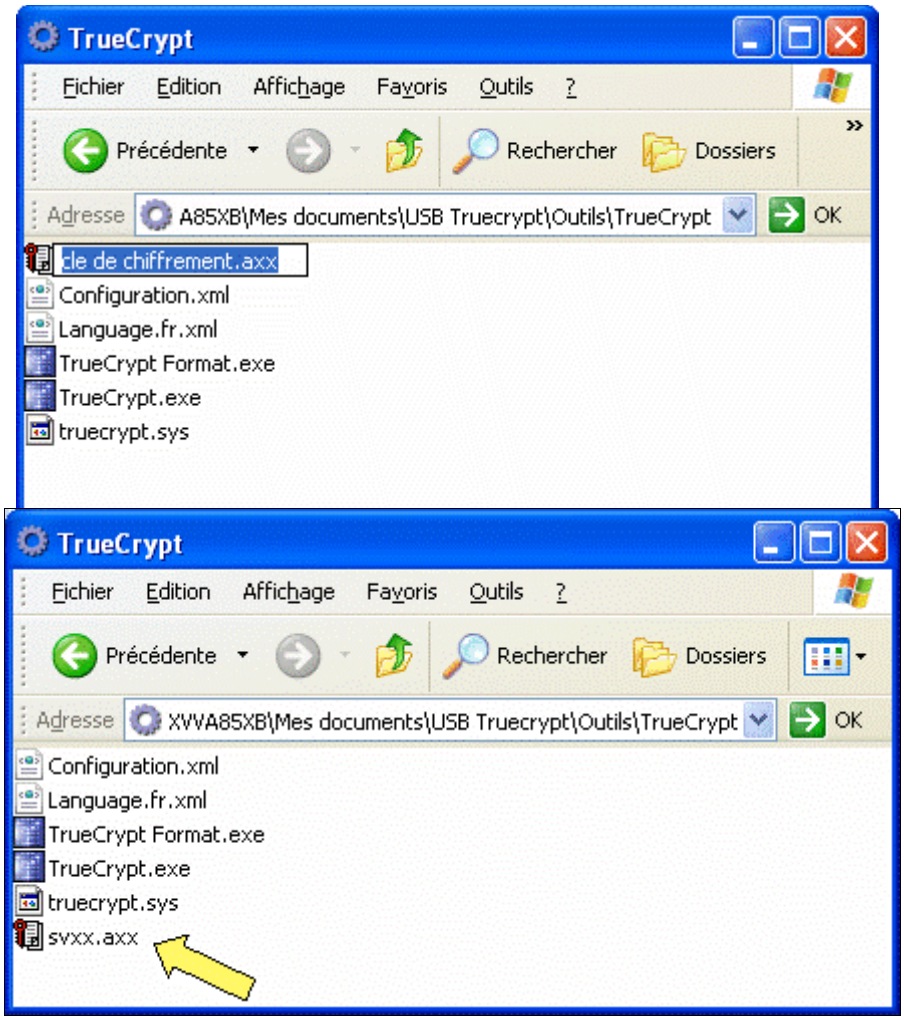


Chiffrez votre clé de chiffrement avec **mpc**

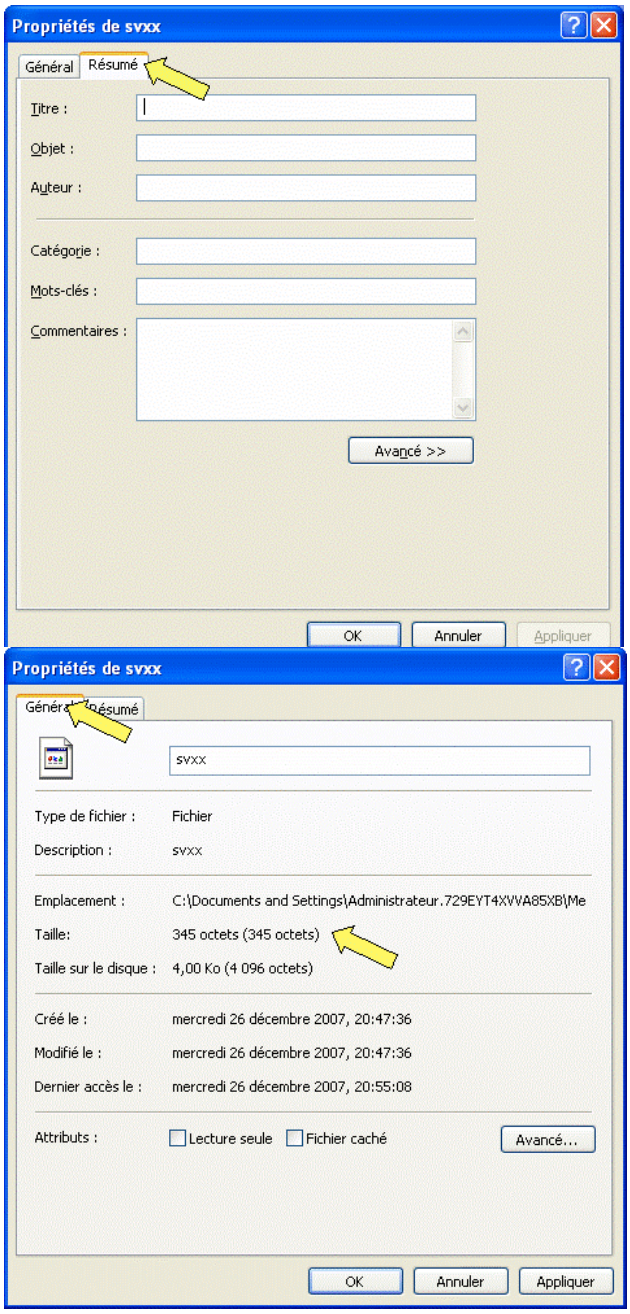


Puis cliquez sur "OK".

Pensez à rendre **cc** anodin, et renommez le en conservant l'extension (vous pouvez écraser l'extension pour masquer le fait que c'est un fichier chiffré avec AxCrypt, mais dans ce cas il vous faudra remettre l'extension pour de déchiffrement).



Vérifiez que **cc** ne porte pas le nom de son auteur. Sélectionnez le fichier en cliquant sur le bouton droit de votre souris pour choisir "propriété".



Notez au passage la taille de **cc** chiffré (345 octets)

Voilà **cc** est prêt pour être hébergé chez l'hébergeur de clés anonymes de chiffrement.

Nous rappelons qu'il est impensable d'avoir **cc** sur soi ou sur son ordinateur, sous quelque forme que ce soit, même chiffré et aussi caché soit-il.

Une fois **cc** mis en sauvegarde (support ultime et hébergeur de clé de chiffrement), et une fois les sauvegardes testées pour vérifier qu'elles sont bien en ordre de fonctionnement, pensez à détruire toute trace de **cc** dans votre ordinateur de création ou de récupération.

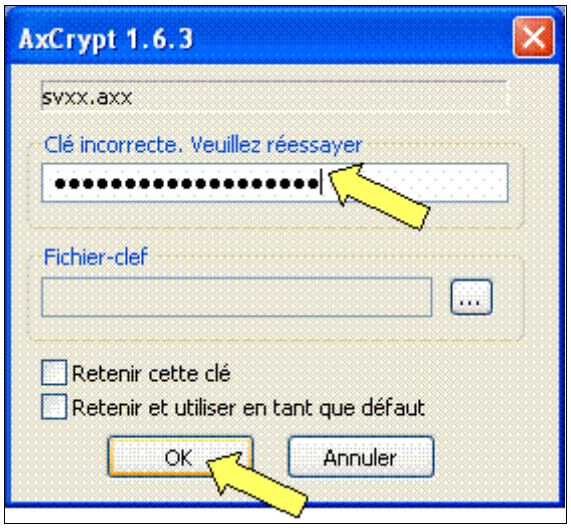
Supprimez **cc** et supprimez ensuite la corbeille de votre ordinateur. Pour les plus précautionneux utilisez un effaceur définitif de type "Eraser" que vous pouvez télécharger sur Internet et installer sur votre ordinateur.

Pour l'utiliser par la suite **cc**, il vous faudra bien naturellement le récupérer et le décrypter avec AxCrypt et **mpc**, puis le mettre dans l'outil d'association de TrueCrypt pour l'associer à **mpl₂**.

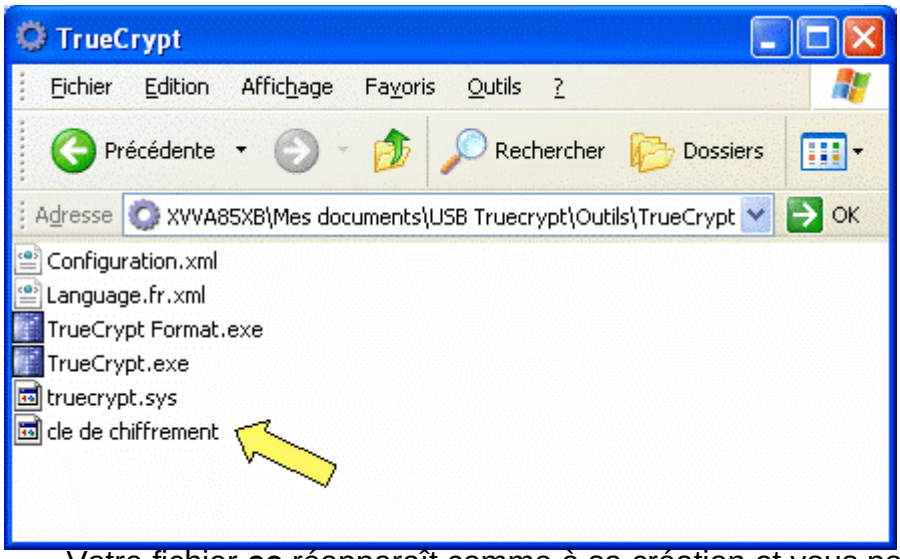
Faisons ensemble cette manipulation.

Nous supposons que vous venez de télécharger **cc** depuis le site de votre hébergeur et que vous l'avez placé dans votre répertoire Outil/TrueCrypt. Rappel: n'utiliser le **support ultime** qu'en cas de force majeure.

Vous n'avez plus qu'à faire l'opération de décryptage avec AxCrypt et **mpc**



Utilisez **mpc**, veillez à ce que les cases "retenir cette clé" et "retenir et utiliser en tant que défaut" ne soient pas cochées.



Votre fichier **cc** réapparaît comme à sa création et vous pouvez l'associer à **mpl₂** pour monter votre tiroir noir et le faire apparaître. (voir procédure précédente)

Une fois votre tiroir noir monté, n'oubliez pas de faire disparaître **cc** de votre ordinateur ou de votre clé USB !

Création du support ultime

Comme précédemment expliqué dans l'organisation de sécurité, il vous faut créer un **support ultime**. Vous le cacherez dans un endroit de votre choix, mais jamais, ni dans (ou à proximité de) votre ordinateur, ni dans (ou avec) vos sauvegardes !

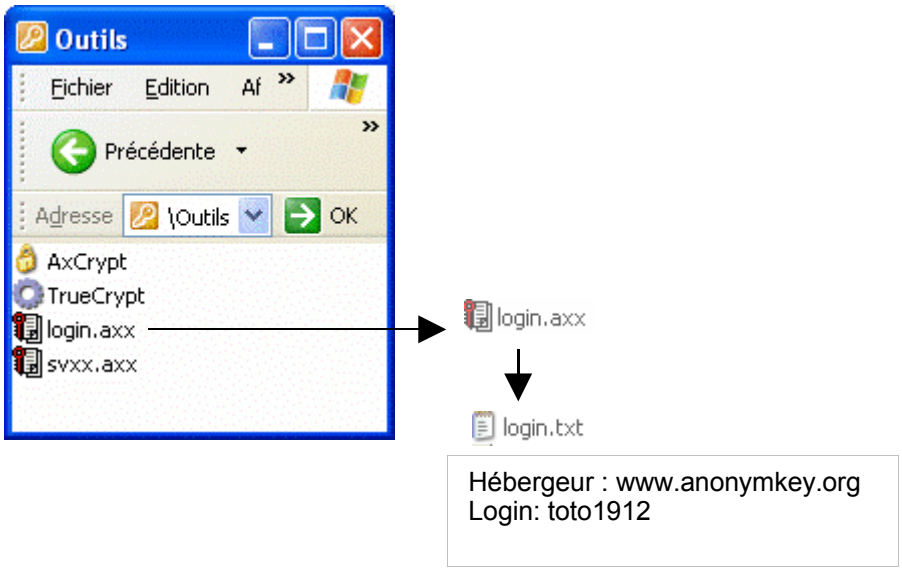
Vous n'utiliserez jamais ce support, sauf si …

Ce support ultime comprendra :

- Votre boite à outils, AxCrypt et TrueCrypt (dans les versions de votre installation)
- Le fichier de clé de chiffrement **cc** au choix non chiffré ou chiffré avec AxCrypt + **mpc**. S'agissant de votre support ultime vous pouvez le laisser non chiffré
- Un texte créé avec votre traitement de texte qui reprendra: le **www** de l'hébergeur de clé de chiffrement et votre **login** pour y accéder. Ce texte sera non chiffré, ou chiffré avec AxCrypt + **mpc**. Même remarque que précédemment, s'agissant de votre support ultime vous pouvez le laisser non chiffré

Votre support ultime ne portera jamais votre nom, ou d'autres éléments permettant de remonter vers vous ou vers votre clé et ses sauvegardes.

Contenu du support ultime (moins de 3 Mo) avec option de chiffrement



Que faire si

La solution proposée est ce qui se fait de mieux actuellement par la communauté Open Source.

Les logiciels proposés sont des grands classiques largement diffusés. Ils sont repris dans des distributions commerciales de clés USB. On peux donc avoir l'assurance d'une maintenance et d'une pérennité.

En cas de problèmes, une vaste communauté de techniciens et utilisateurs est accessible sur Internet. Elle est efficace au travers d'un nombre important de forums.

Soyez cependant en mesure de pouvoir revenir à vos outils initiaux et à faire des réinstallations comme vous venez de l'apprendre.

Prenez la précaution de sauvegarder toute votre clé USB, avec sa boite à outils.

Vous aurez toujours ainsi la possibilité de monter vos tiroirs et de migrer leurs contenus sur d'autres solutions.

Attention:

Veillez à ce que votre tiroir rouge ne soit pas trop rempli au risque d'écraser le contenu de votre éventuel tiroir noir. L'utilisation intensive d'un tiroir noir important et sa protection contre le risque d'écrasement n'est pas expliquée ici (déontologie à l'usage intensif de tiroirs noirs)

Livre blanc

Livre blanc

Conclusion

Configuration de base

Pour Madame et Monsieur tout le monde, sans secrets intimes

Clé USB rapide 1 Go, vitesse 20 Mo/s, prix 20 € environ

Tiroir Vert OUI
Tiroir Rouge OUI utilisée régulièrement et massivement
Tiroir Noir NON

mpl₁ de 10 à 20 caractères à mémoriser.
support ultime NON, si bonne mémoire, utilisation des sauvegardes en secours.
www de l'hébergeur et ***login*** NON si bonne mémoire, OUI pour ***mpl₁*** en sécurité pour la mémoire.

Sauvegarde sur ordinateur personnel.

Configuration élaborée

Pour les personnes exposées à un risque élevé, et pour les secrets intimes

Clé USB rapide 4 à 8 Go, voire 16 Go, vitesse 25 à 30 Mo/s, prix selon les configurations.

Tiroir Vert OUI
Tiroir Rouge OUI utilisée régulièrement et massivement
Tiroir Noir OUI avec précaution, pour stockage d'informations en très petit volume..

mpl₁ de 15 à 30 caractères à mémoriser
mpl₂ de 10 à 20 caractères à mémoriser
mpc de 10 à 20 caractères à mémoriser
support ultime OUI obligatoire
cachette du support ultime OUI
www de l'hébergeur et ***login*** OUI indispensable pour le fichier de chiffrement.

Sauvegarde sur ordinateur personnel, ou sur autre clé USB.

Configuration paranoïaque

Pour les paranoïaques, ou les absolus de la sécurité, pour toutes les bonnes et mauvaises raisons du monde

Méthode non expliquée (à peine dévoilée ici, voir éthique page suivante).

Une clé USB de sécurité rapide 4 à 8 Go, voire 16 Go, vitesse 25 à 30 Mo/s, prix selon les configurations.

Tiroir Vert OUI remplie de plus de 1 000 fichiers divers, beaucoup de petits, quelques gros, petits textes, quelques musiques légales, etc.
Tiroir Rouge OUI apparemment utilisée, mais non utilisée en réalité (leurre) !
Tiroir Noir OUI utilisation intensive et masquée

mpl₁ de 15 à 30 caractères à ne pas mémoriser fortement et à placer chez un hébergeur (leurre) pour présentation si nécessaire.
mpl₂ de 10 à 20 caractères à mémoriser + combinaison de plusieurs fichiers de clé, à choisir parmi les 1 000 fichiers du tiroir vert + clé de chiffrement chiffrée cryptée
mpc de 10 à 20 caractères à mémoriser
support ultime OUI obligatoire, complété des fichiers clés
cachette du support ultime OUI
www de l'hébergeur et ***login*** OUI, pour ***mpl₁*** en leurre.

Sauvegarde sur ordinateur personnel, ou sur autre clé USB.

Loi française et éthique

L'auteur de ce livre blanc souhaite que son travail de vulgarisation d'éléments disponibles sur Internet serve à la vie privée de chacun, sans qu'il soit détourné à d'autres fins.

Référence légale en France, voir site DCSSI www.ssi.gouv.fr

"**En vertu de l'article 30-I de la loi 2004-575 du 21 juin 2004, l'utilisation des moyens de cryptologie est libre**" (lire ici)

L'auteur n'est pas un spécialiste du droit français concernant les moyens de cryptologie. Ce droit, difficile à comprendre, s'interprète de multiples façons sur les forums.

La loi en France interdisait le chiffrement avec des clés de plus de 128 bits (16 caractères). Cette loi était justifiée pour la lutte contre le terrorisme ou d'autres calamites comme la pédophilie, notamment en cas de transmissions d' informations entre personnes.

Sauf éléments inconnus, TrueCrypt ne souffre d'aucune interdiction en France.

Ses algorithmes conduisent à des chiffrements supérieurs à 128 bits (256 bits pour la partie rouge et 768 bits pour la partie noire dans cet exemple d'utilisation).

Les autorités, sous mandat de loi, pourront cependant exiger d'un utilisateur de TrueCrypt qu'il fournisse son long mot de passe **mpl$_1$** de la zone rouge. Et vous aurez intérêt à vous soumettre, au risque d'être inculpé de rétention de preuves.

Mais dans sa partie la plus sécurisé, l'outil est conçu sur le principe du "déni plausible".

Ne jamais pouvoir faire la preuve technique et juridique que ce que l'on cherche existe, c'est ennuyeux. Cherchez ce qui n'existe pas est absurde.

Ainsi aucune autorité ne pourra démontrer que vous employez ou non un tiroir noir. Elle ne pourra jamais faire la preuve que vous avez utilisé une clé impossible à casser (**mpl$_2$** + **cc**). En présupposant que la partie noire existe, le seul moyen pour la dite autorité sera d'essayer de casser la clé, ce qui est impossible à ce jour.

Livre blanc

L'auteur de ce livre blanc

L'auteur est un utilisateur de clé USB, qui à l'usage, a compris que la sécurité n'était pas à la portée de tous, surtout sans réflexion, sans aide, et sans éthique.

Merci à la communauté Open Source. Ma contribution est un juste retour.

Jean-Luc LEMOINE

e mail : 1@1bu1.fr

Si vous voulez en savoir un peu plus sur moi.

Je suis un chercheur et un professionnel de l'organisation et des systèmes d'information. De par mon métier d'intervenant auprès de différentes structures, je suis un utilisateur "nomade" de l'informatique.

La Clé USB évolue vers un usage universel. On peut y mettre actuellement de l'information en quantité plus que suffisante et bientôt des outils qui traitent cette information.

En quelque sorte cela devient un conteneur d'utilités personnelles dont on ne pourra plus se passer (je ne peux plus m'en passer). Je prédis que les appareils numériques portables : téléphones; appareils de photos; portables; PDA; etc.; seront compatibles un jour, via le sans fil, avec les clés USB pour que celles ci jouent pleinement leur rôle de stockage d'informations portatif universel.

J'ai fait l'effort de rédiger ce document pour partager mon expérience (5 jours).

Pour moi la sécurité est d'abord une affaire d'organisation. La sécurité à 100% n'existe pas, et il existe une infinité de façons de la mettre en œuvre.

Votre sécurité doit être proportionnelle à vos risques, et doit vous permettre une vie sereine. C'est dans cette intention que je vous présente modestement quelques solutions (il y en a bien d'autres).

Si ce document vous plait et si il vous apporte une valeur d'usage, merci de le transmettre à vos amis.

Ma clé USB

4 Go
Solution pour 55 € TTC.

Le corps se fixe par un anneau à mon trousseau de clés. La clé USB se dévisse de son conteneur pour être utilisée sans décrocher le conteneur.

Retour d'expérience:.fabuleux, avec un sentiment de tranquillité dont je comprends bien la teneur.

Je vais y mettre également ma messagerie et tous mes contacts, via Thunderbird, un autre logiciel Open Source.

Et rapidement aussi toutes mes applications portables.

Livre blanc

Foire aux questions

Extraits du site TrueCrypt

_____

Q: Est-ce que je pourrai monter TrueCrypt sur n'importe quel ordinateur?

R: Les tiroirs TrueCrypt sont indépendants du système d'exploitation. Vous aurez la possibilité de monter vos tiroirs TrueCrypt sur n'importe quel ordinateur sur lequel vous pouvez exécuter TrueCrypt (Windows, linux).

_____

Q: J'ai oublié mon mot de passe, y a-t-il moyen de récupérer les fichiers de mon tiroir TrueCrypt?

R: TrueCrypt ne contient pas de mécanisme ou d'installation qui permettrait une récupération partielle ou totale de vos données cryptées sans connaître le mot de passe ou la clé utilisée pour chiffrer les données. Le seul moyen de récupérer vos fichiers est d'essayer de "craquer" le mot de passe ou le fichier de clé, mais ceci peut prendre des milliers ou des millions d'années, selon la durée et la qualité du mot de passe ou de la clé de chiffrement, du logiciel de craquage et du matériel utilisé et d'autres facteurs .

_____

Q: Est-il possible d'installer une application dans un tiroir TrueCrypt et de l'exécuter à partir de là ?

R: Oui.

_____

Q: Puis-je directement lire une vidéo (. AVI,. Le mpg, etc ...) stockée dans un tiroir TrueCrypt?

R: Oui, les tiroirs TrueCrypt sont cryptés comme des disques normaux. Vous fournissez le mot de passe (et / ou la clé de chiffrement) pour monter les tiroirs TrueCrypt. Lorsque vous double-cliquez sur un fichier vidéo, le système d'exploitation lance l'application associée au type de fichier, généralement un lecteur multimédia. Le logiciel commence alors à charger une première partie de la vidéo en RAM (mémoire), afin de le jouer. Pendant que cette partie est en cours de chargement, TrueCrypt déchiffre automatiquement en RAM. La partie déchiffrée de la vidéo, stockées dans la mémoire RAM, est ensuite jouée par le lecteur multimédia. Pendant que cette partie est jouée, le lecteur multimédia commence le chargement de la prochaine partie et le processus se répète. Il en va de même pour l'enregistrement vidéo.

Ce processus est appelé à chiffrement à la volée et est valable pour tous les types de fichiers.

Livre blanc

_____

Q: TrueCrypt est-il Open-Source et gratuit pour toujours?

R: Oui. Nous nous engageons à ne créer aucune version commerciale de TrueCrypt. Nous croyons au code source ouvert et libre des logiciels de sécurité.

_____

Q: Est-il possible de faire un don projet TrueCrypt?

R: Oui. Pour de plus amples renseignements, veuillez visiter http://www.truecrypt.org/donations/

_____

Q: TrueCrypt crypte-t-il également les noms de fichiers et des noms de dossiers?

R: Oui. L'ensemble du système de fichiers dans un volume de TrueCrypt est crypté (y compris les noms de fichiers, noms de dossiers, et le contenu de chaque fichier).

_____

Q: Puis-je débrancher une clé USB (ou un disque dur USB) lorsqu'un tiroir TrueCrypt est monté?

R: Avant de débrancher ou d'éteindre l'appareil, vous devez toujours démonter d'abord le tiroir TrueCrypt, puis effectuer l'opération de déconnexion de la clé. Sinon, la perte de données peut se produire.

-&-