WinSesame

www.aragon-technologies.com

www.aragonsoft.com

Sommaire :

Présentation :

WinSesame est un logiciel permettant de protéger les dossiers et les fichiers par un mot de passe sur un ordinateur, un support mobile, en réseau. D'autre part les données contenues dans un dossier ou un fichier verrouillé par WinSesame sont codées par un des 6 protocoles disponibles : 3 protocoles de cryptage spécifiques à WinSesame absolument inviolables, sans limitation de longueur de clé et à clé perdue (WNS910, WNS915, WNS1020) plus 3 protocoles standards reconnus (DES, TripleDES, AES). Il ne s'agit donc pas d'un simple système de masquage des dossiers et fichiers, les dossiers et fichiers restent protégés et cryptés même s'ils sont transférés sur un autre ordinateur que ce soit par l'intermédiaire d'un disque dur portable, d'une clé usb, d'un accès par le réseau ou envoyés par email. Ceci constitue une protection absolue contre l'accès à vos données en cas de vol du support (disque dur externe, clé usb, cdrom, disque de sauvegarde, ordinateur portable) ou intrusion sur les réseaux, logiciels espions, etc... . Les dossiers ou fichiers verrouillés par WinSesame peuvent être envoyés par email sous forme de pièce jointe. A la suite d'un verrouillage WinSesame professionnel effectue plusieurs passes de nettoyage du disque et de la mémoire dans le but de supprimer toutes traces résiduelles de données en clair sur les supports et interdire toute tentative de récupération de données par lecture directe des secteurs ou même par analyse magnétique des disques. WinSesame est aussi un très bon système de contrôle parental d'accès aux documents. Dans ce cas ce n'est pas les documents qui sont protégés mais les personnes susceptibles d'y accéder. La désinstallation du logiciel ne supprime pas la protection des documents qui restent cryptés avec le même niveau de sécurité.

WinSesame existe en 3 versions Free, Classic et Pro.

Logiciel compatible Windows XP / Vista / 8 / 8,1 / 10

Langages disponibles : Anglais, Français, Espagnol, Portugais.

La souplesse d'emploi du programme vous permet de configurer votre mode d'accès aux données en fonction de vos besoins ou désirs.

Par exemple le protocole de cryptage WNS1020 permet la protection de l'accès aux données de 3 manières différentes :

Protection de l'accès aux données par mot de passe.

Protection de l'accès aux données par détection de la présence d'une clé matérielle (présence d'un fichier de signature sur une clé usb, une carte mémoire etc..).

Protection de l'accès aux données par détection de la présence d'une clé matérielle plus fourniture d'un mot de passe.

Sur un parc informatique important vous pouvez configurer un canal de cryptage pour faire en sorte que certaines données ne soit accessibles que sur les ordinateurs utilisant le même canal de cryptage et ainsi créer un cloisonnement de l'accès aux données importantes,

WinSesame est compatible avec tous les systèmes de sauvegarde de sorte que les données sauvegardées le soient tout en conservant leur haut niveau de cryptage. Grâce à WinSesame la réticence à effectuer des sauvegardes multiples de données sensibles disparaît ce qui est un point important pour la sécurité des vos données. Nous vous conseillons d'utiliser le logiciel WinSauvegarde pour vos sauvegardes car ce logiciel et en mesure de commander WinSesame pour fermer automatiquement tous les dossiers et fichiers protégés ouverts avant d'effectuer la sauvegarde.

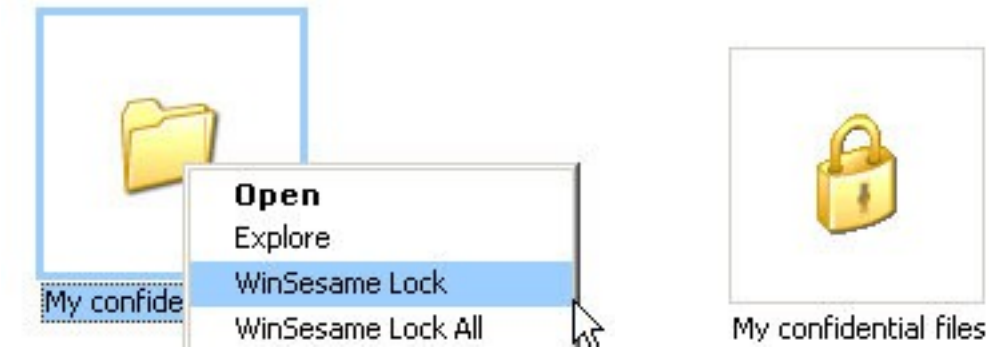
WinSesame satisfait à l'article 226-17 du Code Pénal dont voici le rappel :
Le manquement à l'obligation de sécuriser un traitement informatique comportant des données personnelles est sanctionné pénalement par une peine de 5 ans d'emprisonnement et 300 000 euros d'amende.

Retour au sommaire.

Utilisation du programme :

Le programme est utilisable à partir de sa fenêtre principale : sorte de tableau de bord ou toutes les fonctions sont disponibles:

Le programme est utilisable à partir de menus contextuels apparaissant à l'aide de clics droits sur les dossiers dans Windows et permettant de gérer vos dossiers comme autant de coffres-forts virtuels:



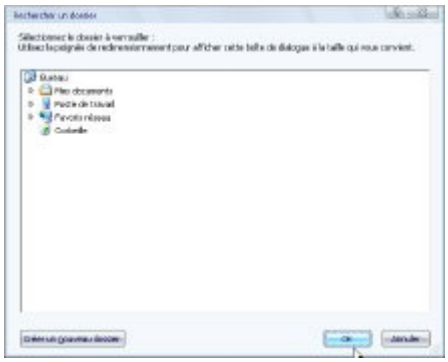
Les utilisateurs expérimentés pourront utiliser WinSesame à partir de lignes de commande qu'ils créeront eux-mêmes.

Retour au sommaire.

Verrouiller un dossier ou un fichier:

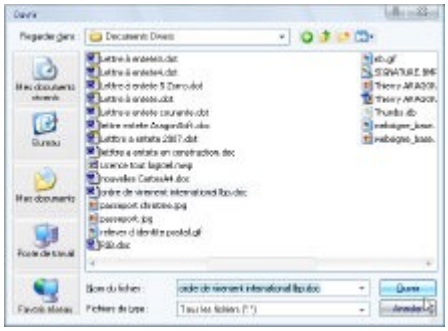
Dossiers :

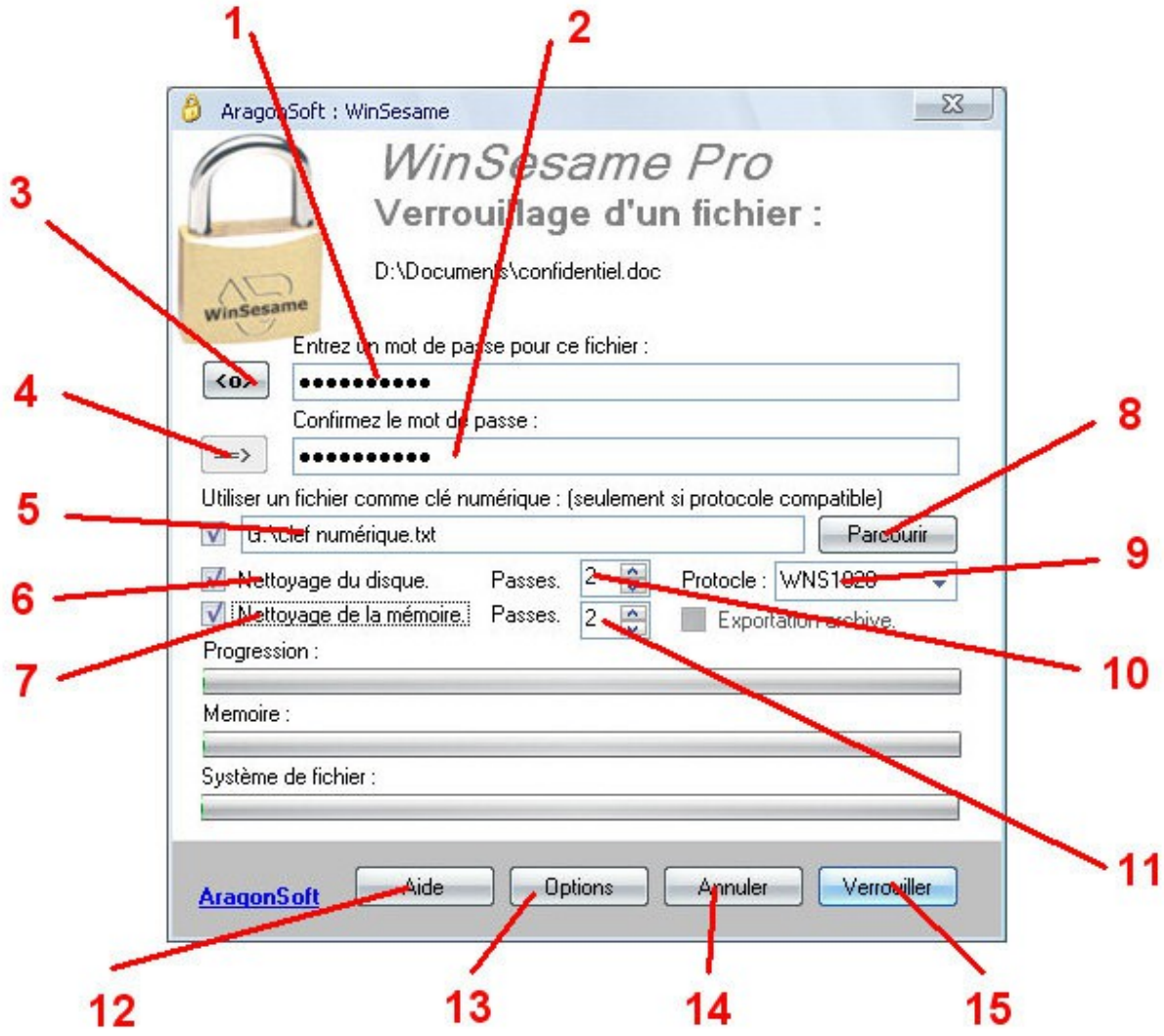
A partir de la fenêtre de menu cliquez sur l'icône Verrouillez un dossier.



Fichiers :

A partir de la fenêtre de menu cliquez sur l'icône Verrouillez un fichier.





1 :

Entrez le mot de passe à utiliser pour protéger ce dossier dans ce champ. Quelque soit le protocole de cryptage utilisé la longueur du mot de passe n'est pas limité mais doit être supérieure ou égale à 8 caratères. Voir les informations sur la longueur du mot de passe.

2 :

Champ de confirmation du mot de passe.

3 :

Ce bouton permet d'afficher le mot de passe en clair pendant la saisie si cet aspect ne présente pas de risque. A utiliser en fonction de la configuration des lieux ou de votre utilisation du programme.

4 :

Si vous affichez les mots de passe en clair, à moins d'utiliser des mots de passe longs il n'est pas nécessaire de confirmer le mot de passe. Ce bouton permet d'activer la confirmation automatique du mot de passe.

5:

Chemin d'accès du fichier de signature numérique utilisé avec les protocoles compatibles avec cette fonction. Si vous avez sélectionné un fichier par défaut dans les options du programme ce champ est rempli.

6 :

Activation / désactivation de la fonction de nettoyage des données résiduelles sur le disque. (Version Pro uniquement).

7 :

Activation / désactivation de la fonction de nettoyage des données résiduelles en mémoire. (Version Pro uniquement).

8 :

Ce bouton permet de sélectionner le fichier que sera utilisé comme signature numérique.

9 :

Sélection de l'algorithme de cryptage à utiliser.

10 :

Nombre de passe utilisé pour le nettoyage du disque.

11 :

Nombre de passe utilisé pour le nettoyage de la mémoire.

12 :

Accès à l'aide en ligne du logiciel.

13 :

Accès aux option du programme permettant notamment la configuration des réglages par défaut que vous voulez retrouver à chaque ouverture de cette fenêtre.

14 :

Bouton annulation permettant de fermer cette fenêtre sans effectuer de cryptage.

15 :

Ce bouton lance le verrouillage du fichier ou dossier. Ce bouton est inactif tant que tous les éléments nécessaires au verrouillage n'ont pas été fournis comme par exemple non concordance du mot de passe et de sa confirmation.

Retour au sommaire.

Verrouillage de tous les fichiers et dossiers protégés ouverts :

Lors du déverrouillage d'un dossier ou fichier celui-ci est enregistré dans une liste de documents déverrouillés. En utilisant cette fonction tous les fichiers ou dossiers de la liste seront reverrouillés automatiquement sans avoir à fournir d'informations (mots de passe etc) à moins que vous ayez refusé l'enregistrement des mots de passe au déverrouillage de certains dossiers ou dans les options du programme. Les fichiers de signatures numériques éventuellement utilisés doivent être accessibles. Cette fonction peut être désactivée pour certains documents au moment de l'ouverture ou pour tous les documents à partir des options.

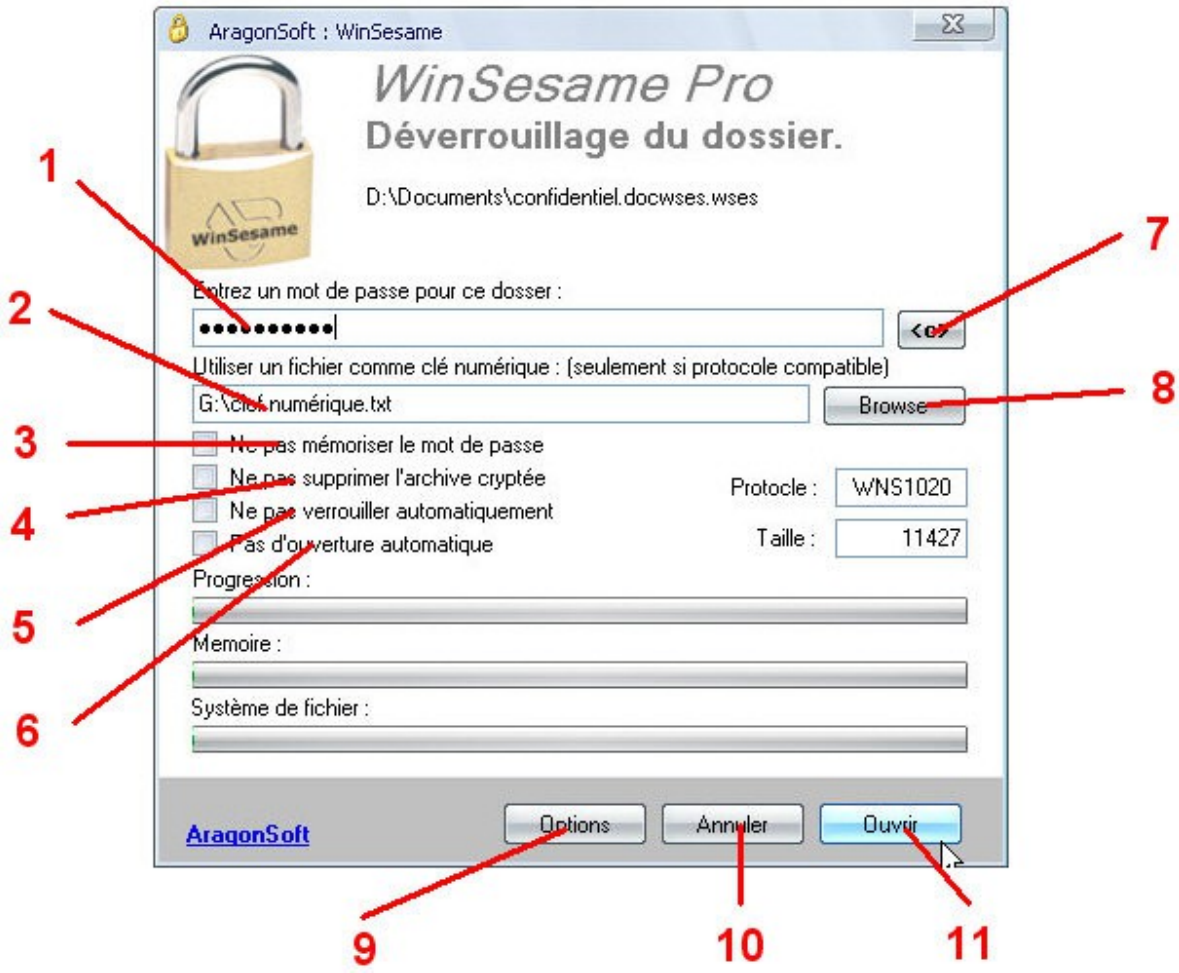
Retour au sommaire.

Déverrouillage et ouverture d'un dossier ou d'un fichier protégé :

Il n'y a pas de différence entre l'ouverture d'un dossier ou fichier protégé par WinSesame. Il s'agit du même type de document qui peut contenir indifféremment un fichier isolé ou un dossier de fichiers.

Double cliquez sur le document protégé :

Ou cliquez sur Déverrouillez un dossier ou un fichier :



1 :

Entrez le mot de passe de ce dossier ou fichier dans ce champ.

2 :

Si vous avez utilisé un fichier de signature numérique pour verrouiller ce dossier ce champ affiche le fichier que vous avez sélectionné après recherche par l'utilisation du bouton 8.

3 :

Ne pas mémoriser le mot de passe : Par défaut à l'ouverture d'un dossier ou fichier protégé, WinSesame mémorise dans le registre (de manière protégée) le mot de passe, le protocole de cryptage, et le fichier de signature numérique de celui-ci pour permettre de reverrouiller celui-ci sans avoir à fournir à nouveau le mot de passe. Ceci n'a pas qu'une utilité pratique mais permet aussi d'éviter des erreurs au niveau de l'entrée des mots de passe d'où des risques de perte de données. Dans ces conditions le mot de passe reste associé à ce document et ne change jamais. L'entrée du registre est supprimée dès que vous refermez le dossier ou fichier protégé. Cette fonction est donc sure et ne présente aucun risque. Si vous cochez cette case le mot de passe n'est pas mémorisé et vous devrez le fournir à nouveau pour refermer ce document.

4 :

Si vous choisissez cette option en fin de déverrouillage le dossier ou fichier verrouillé n'est pas supprimé et vous obtenez 2 dossiers ou fichiers. Cette configuration n'est pas très utile en tant que configuration par défaut mais peut être intéressante pour accéder rapidement au contenu d'un gros dossier verrouillé dans le but d'y extraire un fichier que vous n'avez pas besoin de modifier.

5 :

Ne pas verrouiller automatiquement :

WinSesame possède une fonction qui permet de verrouiller automatiquement tous les dossier ou fichiers protégés ayant été ouverts. Si vous cochez cette case le fichier ou dossier ne sera pas ajouté à la liste de dossiers ou fichiers à verrouiller et ne sera pas refermé automatiquement par la fonction de verrouillage automatique.

6 :

Pas d'ouverture automatique :

Par défaut lorsque vous déverrouillez un dossier protégé, celui-ci s'ouvre automatiquement et lorsque vous déverrouillez un fichier protégé celui-ci s'ouvre automatiquement dans l'application prévue pour ce type de fichier. Si vous cochez cette case le dossier ou le fichier ne s'ouvrira pas automatiquement mais sera simplement déverrouillé.

7 :

Ce bouton permet d'afficher le mot de passe en clair pendant la saisie si cet aspect ne présente pas de risque. A utiliser en fonction de la configuration des lieux ou de votre utilisation du programme

8 :

Ce bouton permet de sélectionner le fichier que sera utilisé comme signature numérique.

9 :

Accès aux options du programme permettant notamment la configuration des réglages par défaut que vous voulez retrouver à chaque ouverture de cette fenêtre.

10 :

Bouton annulation permettant de fermer cette fenêtre sans effectuer le déverrouillage.

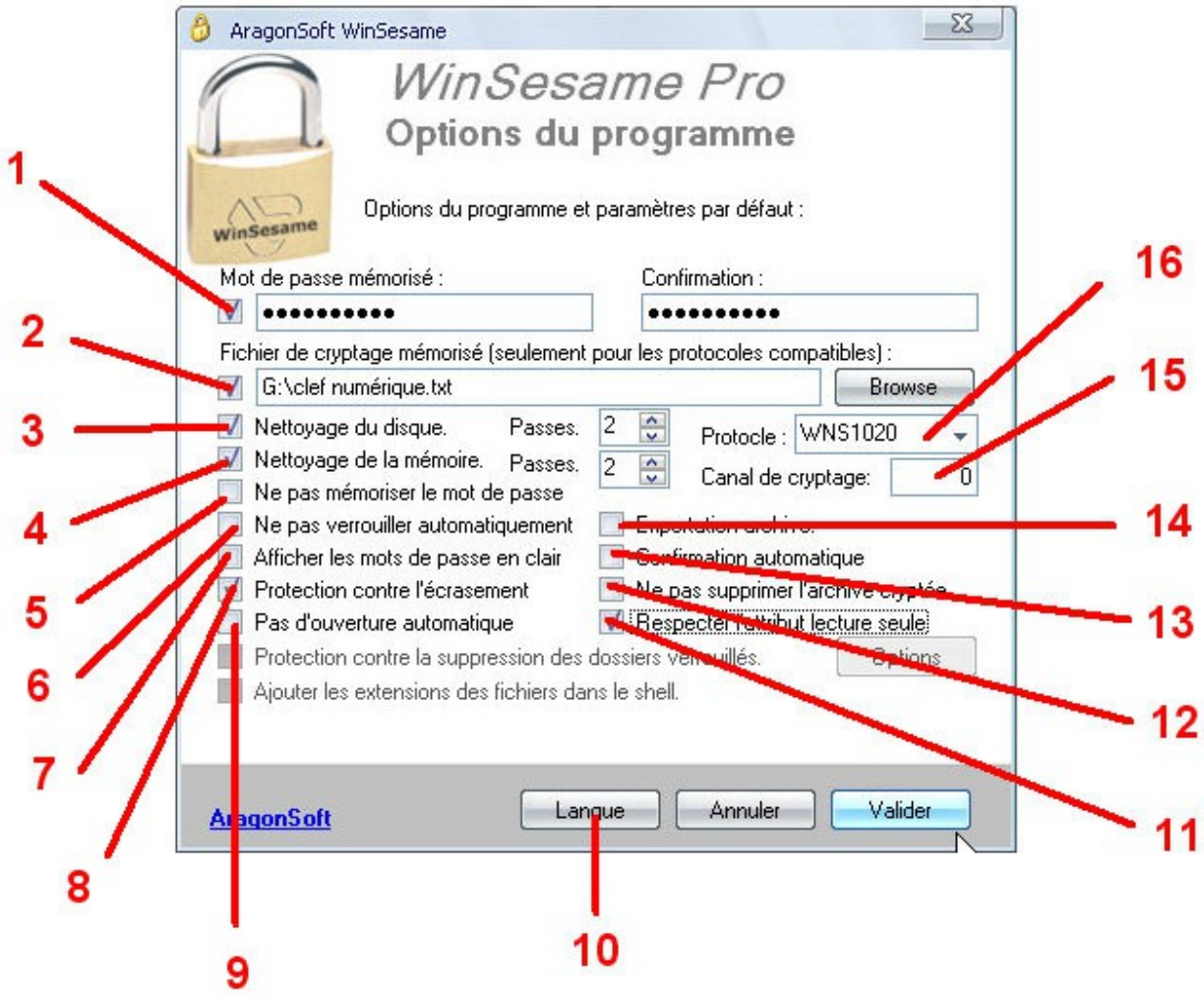
11 :

Ce bouton lance le déverrouillage du fichier ou dossier.

Retour au sommaire.

Les options du programme et réglages par défaut :

Dès l'installation du programme, celui-ci est utilisable sans aucune configuration pour verrouiller vos documents mais il est probable que vous vouliez configurer le programme pour l'adapter plus précisément à vos besoins et profiter de sa souplesse d'utilisation. La plupart des réglages disponibles au niveau des options sont disponibles sur les fenêtres de verrouillage ou déverrouillage mais permettent de créer une configuration par défaut que vous retrouverez à chaque verrouillage ou déverrouillage sans toutefois vous empêcher de les modifier dans les fenêtres de verrouillage ou déverrouillage pour un cas particulier.



1 :

Enregistrement d'un mot de passe mémorisé :

Même si cette option ne représente pas le maximum de sécurité, celle-ci se justifie dans certaines utilisations. Par exemple vous ne craignez pas le vol de données sur votre ordinateur mais vous transportez souvent des données importantes de votre bureau à votre domicile en utilisant des supports mobiles comme des clés usb ou des disques durs portables. En cas de vol de ces supports, vous ne voulez pas que ces données soient utilisables. Cette option vous permet de ne pas avoir à entrer vos mots de passe à chaque ouverture d'un dossier mais vos documents sont parfaitement protégés lors des transports. Cette option de protection sera aussi suffisante s'il s'agit de protéger des données contre des accès non autorisés par le réseau etc.. Le mot de passe n'est mémorisé que sur l'ordinateur et seulement pour le profil utilisateur.

2 : (version Pro uniquement)

Ce champ permet de mémoriser le chemin d'accès du fichier qui vous sert de signature numérique pour l'ouverture des fichiers et dossiers protégés à l'aide des protocoles offrant cette possibilité (WNS1020). (voir : Utilisation des fichiers de signature numérique)

3 : (version Pro uniquement)

Cette case à cocher permet d'activer la fonction de nettoyage des disques et le champ numérique situé en regard de configurer le nombre de passe de nettoyage :

Lorsque vous effectuez le cryptage d'un fichier ou d'un dossier, le programme crée un nouveau fichier représentant le document crypté puis efface du disque le ou les fichiers en clair. Malheureusement la simple suppression d'un fichier sur un disque dur supprime son entrée dans la table d'allocation du disque de sorte que si vous regardez le contenu du disque, le fichier n'apparait plus bien que toutes les données soient encore présentes dans les secteurs du disque tant que ceux-ci n'ont pas été utilisés par un autre fichier. Ces données peuvent être récupérées par l'utilisation de logiciels spécialisés ou par la lecture du disque secteur par secteur. La fonction de nettoyage du disque va remplacer tous les octets des fichiers en clair par une alternance de valeur de masque (FF et 00) avant de supprimer les fichiers ce qui reviendra à laisser à la place des fichiers des espaces équivalents à un espace de disque formaté. Le champ numérique associé à cette case à cocher permet de choisir le nombre de passe et pour chaque passe les valeurs FF et 00 seront inversées de manière à effectuer des modifications magnétiques maximales sur la surface du disque ; car il existe des techniques permettant encore de récupérer des données par scan de la surface de disques formatés sur les bordures de pistes en raison de la différence de positionnement des têtes sur le disque selon le sens de déplacement de celles-ci et les petits défauts mécaniques. Dans la pratique il est inutile de sélectionner plus de 2 passes pour des raisons de temps d'exécution. Des études ont été faites sur ce sujet et il apparaît qu'à partir de 2 passes de masquage il est extrêmement difficile de récupérer quoi que ce soit sur un disque dur. Les moyens à mettre en œuvre deviennent très lourds et sont donc réservés à des recherches dans des domaines très spéciaux. ATTENTION : Le nettoyage du disque n'est pas garanti si vous verrouillez par le réseau des dossiers ou fichiers situés sur un autre ordinateur.

4 : (version Pro uniquement)

Si vous utilisez de la mémoire virtuelle sur votre ordinateur (configuration par défaut) Windows maintient une copie du contenu de la mémoire dans un gros fichier situé par défaut à la racine de votre disque système. Une autre copie de votre mémoire est disponible sur le disque si vous avez activé la veille prolongée sur votre système. En cas de récupération d'un disque dur sur un PC éteint il devient donc possible de récupérer des données ayant été utilisées en mémoire. Cette fonction va donc procéder de la même manière que pour le masquage des secteurs du disque dur mais avec tout l'espace mémoire utilisé par le programme pour crypter les données. Dans la pratique utilisez le même nombre de passe que pour le nettoyage du disque. Si vous utilisez WinSesame uniquement pour protéger des données contre le vol des disque durs portables mais ne craignez pas pour les disque situés sur votre PC, il est inutile d'activer cette fonction.

5 :

Ne pas mémoriser le mot de passe : Par défaut à l'ouverture d'un dossier ou fichier protégé, WinSesame mémorise dans le registre (de manière protégée) le mot de passe, le protocole de cryptage et le fichier de signature numérique de celui-ci pour permettre de reverrouiller celui-ci sans avoir à fournir à nouveau le mot de passe. Ceci n'a pas qu'une utilité pratique mais permet aussi d'éviter des erreurs au niveau de l'entrée des mots de passe d'où des risques de perte de données. Dans ces conditions le mot de passe reste associé à ce document et ne change jamais. L'entrée du registre est supprimée dès que vous refermez le dossier ou fichier protégé. Cette fonction est donc sure et ne présente aucun risque. Elle pourra par contre être inhibée de manière ponctuelle à partir de la fenêtre de déverrouillage si vous souhaitez changer le mot de passe, le canal de cryptage ou le fichier de signature d'un dossier ou fichier protégé ou si vous voulez ne plus protéger un fichier ou dossier.

6 :

Ne pas verrouiller automatiquement :

WinSesame possède une fonction qui permet de verrouiller automatiquement tous les dossiers ou fichiers protégés ayant été ouverts. Si vous cochez cette case les fichiers ou dossiers que vous déverrouillés ne seront pas ajoutés à la liste de dossiers ou fichiers à verrouiller et ne seront pas refermés automatiquement par la fonction. Il n'est pas conseillé de cocher cette case car vous risquez d'oublier de refermer des documents important par contre si le besoin s'en fait sentir vous pourrez le faire de manière ponctuelle à partir de la fenêtre de déverrouillage.

7 :

Afficher les mots de passe en clair :

Si vous travaillez seul dans votre bureau ou utilisez le programme pour protéger vos données en cas de vol de vos supports, il n'est pas forcement utile de masquer vos mots de passe puisque personne ne regarde par dessus votre épaule. Vous pouvez donc afficher les mots de passe en clair ce qui est plus pratique et peu parfois éviter des erreurs de saisie. Si vous avez choisi d'afficher les mots de passe en clair par défaut et que vous avez besoin d'entrer un mot de passe alors que vous n'êtes pas seul dans votre bureau, il suffit de cliquer sur le bouton en regard du champ du mot de passe pour que celui-ci soit masqué.

Note : dans le cas de la fonction de verrouillage automatique d'un dossier ou fichier sans nécessité de ressaisir le mot de passe, celui-ci sera toujours masqué.

8 :

Protection contre l'écrasement :

Si vous avez déjà un dossier verrouillé nommé Mon Dossier, rien ne vous empêche de créer un nouveau dossier normal nommé lui aussi Mon Dossier. Par contre la protection contre l'écrasement vous empêchera d'écraser votre dossier verrouillé en verrouillant le dossier normal ou l'inverse. Nous déconseillons fortement de cocher cette case car il existerait alors un risque de perte de données.

9 :

Pas d'ouverture automatique :

Par défaut lorsque vous déverrouillez un dossier protégé, celui-ci s'ouvre automatiquement et lorsque vous déverrouillez un fichier protégé celui-ci s'ouvre automatiquement dans l'application prévue pour ce type de fichier. Si ce comportement vous dérange, vous pouvez cocher cette case. Les dossiers ou les fichiers ne s'ouvrent plus automatiquement mais sont simplement déverrouillés.

10 :

Bouton Langue :

En cliquant sur ce bouton une petite boite de dialogue s'affiche pour vous permettre de choisir la langue dans laquelle s'affiche le programme : Anglais, Français, Espagnol, Portugais.

Note : La boîte de dialogue du choix de la langue s'affiche au premier lancement du programme.

11 :

Respecter l'attribut lecture seule :

En principe un fichier marqué en lecture seule ne devrait pas pouvoir être verrouillé puisque ceci revient à le supprimer en fin de verrouillage et à le recréer au déverrouillage C'est pourquoi WinSesame supprime l'attribut lecture seule des fichiers qu'il doit protéger. Si ceci vous pose un problème, cochez cette case pour forcer WinSesame à respecter cet attribut ; par contre vous ne pouvez plus verrouiller de fichiers marqués en lecture seule.

12 :

Ne pas supprimer l'archive cryptée :

Si vous choisissez cette option en fin de déverrouillage, le dossier ou fichier verrouillé n'est pas supprimé et vous obtenez 2 dossiers ou fichiers. Cette configuration n'est pas très utile en tant que configuration par défaut mais peut être intéressante pour accéder rapidement au contenu d'un gros dossier verrouillé dans le but d'y extraire un fichier que vous n'avez pas besoin de modifier. Vous supprimez ensuite simplement le dossier déverrouillé sans avoir besoin de le reverrouiller puisque l'original est toujours présent. ATTENTION : dans le cas où vous supprimez des fichiers de votre disque dur, leur emplacement ne sera pas masqué. Veuillez prendre par ailleurs toutes les précautions nécessaires si cet aspect peut être gênant pour vous. (la défragmentation assure un assez bon masquage pour des données courantes)

13 :

Confirmation automatique :

Si vous affichez les mots de passe en clair il ne vous apparaît peut être pas indispensable d'avoir à confirmer le mot de passe (à moins que vous n'utilisiez des mots de passe très longs). Si cette case est cochée le mot de passe entré est automatiquement recopié dans le champ de confirmation. La confirmation automatique n'est disponible que si l'affichage des mots de passe en clair est activé.

14 :

Exportation archive :

Si cette case est cochée, WinSesame crée des dossiers ou fichiers verrouillés, ne supprime pas les fichiers et dossiers en clair et vous demande où enregistrer l'archive. Cette fonction est rarement utilisée en tant que configuration par défaut mais peut être utilisée ponctuellement à partir de la fenêtre de verrouillage pour vous permettre de faire une copie protégée d'un fichier ou dossier dans le but de l'envoyer par email ou de l'enregistrer sur un disque portable ou clé usb dans le but de son transfert en toute sécurité.

15 :

Canal de brouillage :

Vous pouvez choisir un canal de 1 à 99999. Les dossiers ne peuvent être ouverts que sur un ordinateur et par un utilisateur utilisant le même canal de brouillage que celui ayant servi au cryptage même si le mot de passe est connu. Le canal par défaut est le 0 (pas de canal). Le canal de brouillage agit à différents niveaux du cryptage selon le protocole. Il ne renforce pas le niveau cryptage sauf contre des attaques par force brute ou application de dictionnaires au niveau des mots de passe. Il permet de mettre en place un cloisonnement de l'accès aux données.

16 :

Protocole de cryptage :

Permet de choisir le protocole de cryptage par défaut que vous pouvez bien sur changé au niveau de la fenêtre de verrouillage. WinSesame utilise 6 protocoles différents :

3 protocoles propriétaires AragonSoft :

WNS910

WNS915

WNS1020

3 protocoles standards du domaine public :

DES

TripleDES (3DES)

AES

Informations sur les protocoles de cryptage

Retour au sommaire.

Les protocoles de cryptage (ou algorithmes) utilisés par WinSesame :

Les protocoles WNS :

Tous les protocoles WNS utilisent un canal de cryptage de 0 à 99999 (canal par défaut 0).

WNS910 : Protocole de cryptage symétrique à clé perdue sans limitation de longueur de clé. Ce protocole est compatible avec les dossiers verrouillés crées par toutes les versions antérieures de WinSesame.

WNS915 : Protocole de cryptage symétrique à clé perdue sans limitation de longueur de clé. Ce protocole utilise le nouveau système de hachage de clé WHA915 permettant le hachage de clé de longueur quelconque par des calculs logarithmiques multiples. Ce protocole de hachage n'utilise aucune donnée fixée par le programme.

WNS1020 : Protocole de cryptage symétrique double à clé perdue sans limitation de longueur de clé. Ce protocole est en fait un double WNS915 dont le deuxième cryptage est effectué en utilisant le contenu d'un fichier de signature. Ce qui revient à utiliser pour ce second cryptage un second mot de passe d'une longueur telle qu'il ne serait pas possible de l'enter manuellement. Pour ouvrir un document crypté avec le protocole WNS1020 vous devez fournir le mot de passe, le fichier de signature et être sur le bon canal de cryptage. CE PROTOCOLE EST LE PROCEDE DE CRYPTAGE LE PLUS PUISSANT EXISTANT À CE JOUR.

Les protocoles standards :

Il s'agit de protocoles standards (non conçus par AragonSoft) disponibles dans le domaine public et ayant fait leurs preuves. Ces protocoles sont tous à longueur de clé limitée et procèdent à un cryptage par bloc de longueur définie. Ils sont fournis dans WinSesame si par exemple la législation de votre pays ne vous permet pas l'utilisation de protocoles de cryptage sans limitation de longueur de clé. Les clés sont créées à partir du mot de passe fourni par hachage WHA915. Ils sont compatibles avec le canal de cryptage utilisé au niveau du vecteur d'initialisation.

DES : (Data Encryption Standard) algorithme de chiffrement par bloc utilisant des clés de 64 bits.

Triple DES (3DES) : Algorithme de chiffrement symétrique enchaînant 3 applications successives de l'algorithme DES et fonctionnant avec une clé de 192 bits.

AES : (Advanced Encryption Standard) est un processus de standardisation lancé par le NIST en 1997 pour demander aux cryptologues de concevoir un nouvel algorithme de chiffrement par bloc destiné au gouvernement des États-Unis. Le but était de remplacer les protocoles DES et Triple DES.

Comme la spécification de AES n'est pas secrète et qu'elle ne se limite pas aux États-Unis (tout comme DES et 3DES), ce chiffrement est destiné à diverses utilisations, entre autres :
- applications militaires / gouvernementales
- produits commerciaux
- logiciels libres
- matériel dédié au chiffrement (routeurs, etc.)

Ce protocole utilise une longueur de clé de 256 bits.

Note :
Relation entre la longueur d'un mot de passe et la longueur de clé pour les protocoles standards dont la longueur de clé est fixe :

Par l'utilisation du système de hachage WHA915, la longueur de la clé utilisée par les protocoles de cryptage à longueur de clé limitée est constante et ne dépend pas de la longueur du mot de passe fourni mais l'utilise dans sa totalité. Le système de hachage va procéder à un calcul permettant de fournir à partir d'un mot de passe de longueur quelconque une clé de longueur définie en faisant en sorte que tous les bits du mot de passe fournis agissent sur le résultat final. Par exemple la fourniture d'un mot de passe de 192 caractères (1536 bits) à la fonction de cryptage AES par l'intermédiaire du hachage WHA915 aboutira à la création d'une clé de 256 bits (équivalente en longueur à 32 caractères) mais en utilisant les 200 caractères du mot de passe. De sorte que vous deviez bien fournir le mot de passe de 200 caractères dans son intégralité pour décrypter et ouvrir le fichier ou dossier (dans ce cas il existera cependant 6 mots de passe différents qui donneront la même clé de 256 bits). Par contre dans le cas d'une tentative de cassage de ce fichier le pirate recherchera directement une clé de 256 bits pour l'appliquer aux données plutôt que de rechercher le mot de passe utilisé pour créer celle-ci. Le niveau de cryptage d'un protocole à longueur de clé limitée dépend donc bien de la longueur de la clé et non pas de la longueur du mot de passe ayant servi à la création de la clé. POUR CETTE RAISON IL EST TOUJOURS PREFERABLE D'UTILISER DES PROTOCOLES DE CRYPTAGE SANS LIMITATION DE LONGUEUR DE CLE CAR LA DIFFICULTE A CASSER UN CRYPTAGE VARIE DE MANIERE EXPONENTIELLE A LA LONGUEUR DE LA CLE UTILISEE. Les protocoles WNS915 et WNS1020 rendent même impossible la simple détection de cette longueur de clé (même sur un fichier

peu bruyant*) ce qui est pourtant la première chose qu'un pirate cherchera à obtenir pour tenter de casser un fichier crypté dont la longueur de clé n'est pas connue.

Il ressort que pour un protocole standard à longueur de clé fixe, il existe une longueur de mot de passe conseillé minimum dépendant du nombre de bits. Cette longueur minimum de mot de passe permettra d'obtenir les performances maximum du protocole.

64 bits : 8 caractères

192 bits : 24 caractères

256 bits : 32 caractères

*Un fichier texte contenant par exemple une succession de 1000 caractères identiques est très peu bruyant et dans le cas de l'utilisation d'une clé courte avec un système de hachage insuffisant et un cryptage faible, il existerait un risque de détecter la longueur de la clé utilisée. Un fichier jpg ou un dossier compressé sont des fichiers bruyants rendant l'opération plus difficile.

Retour au sommaire.

Pour changer le mot de passe, le protocole de cryptage ou le fichier de signature d'un dossier ou fichier :

Déverrouillez le document en cochant la case Ne pas mémoriser le mot de passe. Puis reverrouillez le document. Vous pouvez alors choisir un autre mot de passe ou signature numérique ou protocole de cryptage.

Retour au sommaire.

Création de raccourcis et lignes de commande :

Lignes de commande valables dans le cas d'une installation de WinSesame dans le dossier C:\Program Files\ WinSesame\

Verrouillage d'un fichier ou dossier :

"C:\Program Files\WinSesame\winsesame.exe" "path du fichier ou dossier"

Déverrouillage d'un dossier ou fichier verrouillé :

"C:\Program Files\WinSesame\winsesame.exe" "path du fichier ou dossier verrouillé avec extension .wses"

Verrouillage de tous les fichiers et dossiers verrouillés ouverts :

C:\Program Files\WinSesame\fermses.exe

Accès aux Options du programme :

'C:\Program Files\WinSesame\winsesame.exe" "|options|"

Pour créer un raccourci de verrouillage de tous les fichiers et dossiers verrouillés ouverts créez un raccourci vers C:\Program Files\WinSesame\fermses.exe

Il est possible de lancer l'exécutable fermses.exe par des tâches planifiées de manière à pouvoir programmer cette action à l'aide de tous les paramètres disponibles avec le planificateur de tâches de Windows.

Retour au sommaire.

Utilisation conjointe de WinSesame WinSauvegarde :

Si vous utilisez WinSauvegarde version 4 et que vous voulez que ce programme commande à WinSesame la fermeture automatique de tous les dossiers et fichiers protégés ouverts avant de commencer la sauvegarde, vous devez activer un pont de compatibilité avec le format des paramètres d'activation de la version 9 de WinSesame. Pour ce faire rendez vous dans le dossier où est installé le programme WinSesame et lancez le fichier Pont de compatibilité 910 101.exe. Ceci n'est valable qu'avec les versions Classic ou Pro.

Retour au sommaire.

Affichage des mots de passe en clair et répétition automatique :

Si vous travaillez seul dans votre bureau ou utilisez le programme pour protéger vos données en cas de vol de vos supports, il n'est pas forcement utile de masquer vos mots de passe puisque personne ne regarde par dessus votre épaule. Vous pouvez donc afficher les mots de passe en clair en cliquant sur le bouton en regard du champ de saisie de mot de passe ce qui est plus pratique et peu parfois éviter des erreurs de saisie.

Dans la mesure où vous affichez les mots de passe en clair, il ne vous apparaît peut être pas indispensable d'avoir à confirmer le mot de passe (à moins que vous n'utilisiez des mots de passe très longs). Dans ce cas en cliquant sur le bouton en regard du champ de confirmation le mot de passe est automatiquement recopié dans le champ de confirmation.

Ces choix peuvent être faits au niveau des fenêtres verrouillage et déverrouillage ou être choisis comme choix par défaut au niveau des options du programme.

Note : dans le cas de la fonction de verrouillage automatique d'un dossier ou fichier sans nécessité de ressaisir le mot de passe celui-ci sera toujours masqué.

Si vous avez choisi d'afficher les mots de passe en clair par défaut et que vous avez besoin d'entrer un mot de passe alors que vous n'êtes pas seul dans votre bureau, il suffit de cliquer sur le bouton en regard du champ du mot de passe pour que celui-ci soit masqué.

Retour au sommaire.

Utilisation d'un mot de passe mémorisé :

Vous pouvez mémoriser votre mot de passe si vous voulez utiliser toujours le même pour tous vos dossiers et fichiers verrouillés. Ce mot de passe n'est mémorisé que pour le profil utilisateur l'ayant enregistré. Bien que n'offrant pas le niveau de protection maximum sur la machine, cette méthode peut être utilisée si vous ne désirez protéger que des données sur des supports amovibles ou cdrom ou protéger les données lors d'accès par le réseau ou par les autres utilisateurs de l'ordinateur (contrôle parental par exemple).

Retour au sommaire.

Utilisation des fichiers de signature numérique :

Le protocole WNS1020 est en fait un double WNS915 dont le deuxième cryptage est effectué en utilisant le contenu d'un fichier de signature. Ce qui revient à utiliser pour ce second cryptage un second mot de passe d'une longueur telle qu'il ne serait pas possible de l'enter manuellement. Ce protocole ne subissant pas de limitation de longueur de clé, ceci rend possible le cryptage de certains fichiers par une clé dont la longueur est égale (ou supérieure) à celle des données à crypter. Le contenu du fichier de signature est haché par la protocole WHA915 permettant le hachage de clé de longueur quelconque par des calculs logarithmiques multiples. Ce protocole de hachage n'utilise aucune données fixée par le programme.

Il est recommandé de placer ce fichier sur un support mobile (clé usb, carte mémoire etc..) et d'avoir une sauvegarde de celui-ci quelque part. Pour une sécurité maximale cette sauvegarde sera elle-même cryptée mais avec un autre protocole ne nécessitant pas son utilisation pour le décryptage (WNS915). Il sera dans ce cas impossible d'ouvrir un document protégé par ce protocole si le support mobile où est enregistré la clé numérique n'est pas connecté à l'ordinateur. Si vous utilisez cette option conjointement avec l'option de mémorisation du mot de passe tous les documents protégés avec ce protocole pourront être ouverts sans avoir à fournir aucun mot de passe ni chemin d'accès à un fichier de signature numérique à condition que le support contenant cette clé soit connecté à l'ordinateur. Emmenez le support de votre clé lorsque vous quittez votre bureau.

Si vous n'avez pas mémorisé de mot de passe, votre protection est optimale puisque pour ouvrir un document il faut connaître le mot de passe et posséder la clé numérique. Si quelqu'un connait votre mot de passe il n'a pas la clé. Si quelqu'un vous vole la clé, il n'a pas le mot de passe. Le chemin d'accès à votre clé numérique ne doit pas être considéré comme un élément de protection. Le fait que celui-ci apparaisse dans la boîte des options du programme et soit mémorisé sur l'ordinateur (seulement dans le profil de l'utilisateur) n'est pas une faiblesse.

Il existe même une possibilité de triple protection : Votre fichier de clé numérique situé sur un support mobile est protégé par un mot de passe sous le protocole WNS915. Les documents sont protégés sous le protocole WNS1020 par la clé numérique et un mot de passe différent de celui utilisé pour protéger la clé. Vous devez donc fournir le support de la clé, déverrouillez la clé à l'aide de son propre mot de passe puis l'utiliser pour ouvrir vos documents conjointement au mot de passe des documents. Ce type de protection est en fait exagérée, lourd à utiliser et ne peut se justifier que dans des cas rares de la nécessité de l'autorisation de 2 ou 3 personnes pour accéder à un document ou dans des cas de protection de données très sensibles et subissant des attaques fréquentes.

Type de fichier à utiliser : tout type de fichier est utilisable en clé numérique : un texte aléatoire, une photo, une chanson etc.. ATTENTION : n'utilisez jamais un fichier susceptible d'être modifié par un programme ou une mise à jour de programme, jamais d'exécutable ou de fichier système. En fait nous vous conseillons d'utiliser une photo au format jpg car même si tout le monde sait ce qu'il y a sur cette photo personne ne pourra reconstituer le fichier ce qui n'est pas le cas d'un texte connu (poème par exemple).

Retour au sommaire.

Verrouillage des données à l'aide d'une clef usb carte à puce etc...

Utilisation d'une clé pour autoriser l'accès aux documents protégés : enregistrez le fichier de signature sur un support mobile clé usb, carte mémoire etc.. Si vous ne voulez pas avoir à entrer le mot de passe mémorisez le. Mémorisez le chemin d'accès au fichier de signature. Sélectionnez WNS1020 comme protocole par défaut. Le support de la clé numérique doit simplement être connectée à l'ordinateur pour pouvoir ouvrir les dossiers verrouillés.

Retour au sommaire.

Informations sur les mots de passe :

Un mot de passe de sécurité doit obéir aux règles minimales suivantes:

1. Contenir un nombre non nul et non égal de lettres minuscules, lettres majuscules et chiffres.
2. Ne pas être prononçable sous forme de mot et donc ne figurant pas dans un dictionnaire. Une personne ayant un accès fugitif à un mot de passe devra souvent le mémoriser quelque temps avant de pouvoir le noter il aura donc plus de peine a mémoriser H2uTyf4lP1 que 253 rue du PARC qui pourtant obéi à la règle N°1.
3. Posséder au moins 8 caractères.

Le choix d'un mot de passe et sa préservation sont des choses qui ne doivent pas être prise à la légère.

D'une enquête effectuée par Ciao Surveys à la demande de McAfee, il apparaît que les utilisateurs d'un ordinateur ne s'en font pas trop à propos des mots de passe. Un utilisateur européen sur quatre court ainsi le risque d'être la victime d'une fraude ou d'un vol d'identité en ligne. Le mot de passe le plus souvent utilisé semble être le nom du chien de l'utilisateur.

Un peu moins d'un quart des personnes interrogées utilisent simplement le même mot de passe pour tous leurs comptes en ligne, et 42% ne modifient jamais leur mot de passe. Quasiment un tiers des participants à l'enquête choisissent encore et toujours des mots de passe de six signes maximum, et quasiment un quart (22%) n'utilise que des lettres. Ce sont là des réponses inquiétantes dans la mesure où les cyber-délinquants spécialisés dans le vol de l'identité d'autrui, se voient ainsi grandement faciliter la tâche et ne doivent souvent mettre la main que sur un seul mot de passe.

Le mot de passe le plus fréquent semble être celui de son animal domestique, suivi par celui d'un hobby ou du nom de jeune fille de la maman. Et c'est précisément ce type d'information que l'on trouve souvent publiquement sur des sites de réseaux sociaux. Il serait donc utile d'envisager l'utilisation de mots de passe plus originaux et moins aisément identifiables.

Le top 10 des mots de passe les plus choisis en Europe:
1. Nom de l'animal domestique
2. Un hobby
3. Le nom de jeune fille de la mère
4. La date de naissance d'un membre de la famille
5. Sa propre date de naissance
6. Le nom du/de la partenaire
7. Son propre nom
8. Le club de football préféré
9. La couleur préférée
10. Le nom de la première école

(source 17 octobre 2007 -- Kristof Van der Stadt)

Retour au sommaire.

Générer des mots de passe fiables et facilement mémorisables :

Si vous ne pouvez vraiment pas retenir un mot de passe correspondant aux critères de sécurité recommandés vous pouvez par contre surement retenir une méthode pour le générer. Vous allez de cette manière créer un "couple" constitué d'une méthode que vous ne donnerez à personne et d'une phrase clé que vous garderez aussi pour vous et qui peut quant à elle avoir un bas niveau de sécurité (poème, parole de chanson etc...). La combinaison de la méthode et de la phrase clé vous permettront de retrouver votre mot de passe. Voici à titre d'exemple une méthode. Il n'est pas très difficile d'inventer la votre et de la garder pour vous.

La méthode de la phrase clé :

La phrase clé : Choisir un proverbe, un dicton, un titre de film ou de livre, suffisamment long et utiliser cette phrase comme clé pour la génération du mot de passe. Celui-ci se déduit de la phrase clé par une méthode de votre choix, dont voici un exemple : ne conserver que les premières lettres de chaque mot formant la phrase code, et mélanger les lettres obtenues avec le nombre de caractères formant chaque mot. Illustration: la phrase clé est "La vie en rose". Les premières lettres de chacun des mots sont Lver (respect des majuscules !), et les quatre mots sont respectivement constitués de 2, 3, 2 et 4 lettres. Le mot de passe choisi est "Lver2324". Une autre convention donnerait une préférence à l'alternance lettre/chiffre et fournirait "L2v3e2r4". Cette méthode présente l'avantage de générer des mots de passe relativement aléatoires, qui sont une "compression" d'une phrase clé qu'il est difficile de retrouver dans sa totalité afin de découvrir le mot de passe.

Si cette méthode ne génère pas un mot de passe au niveau maximum de sécurité c'est de toute façon mieux qu'un mot de passe très sur écrit sur bout de papier ou un agenda. De plus cette méthode permet de générer des mots de passe longs permettant de profiter de la sécurité des protocoles ne possédant pas de limitation de longueur de clé sans risquer de perte de données provoquée par la perte d'un mot de passe.

Retour au sommaire.

Activation du logiciel :

A la première utilisation du logiciel en version Classic ou Pro, vous devez activer le logiciel (la version gratuite limitée ne nécessite pas d'activation). La boîte de dialogue suivante s'ouvre :

Le programme vérifie d'abord votre connectivité à Internet. En cas d'échec, vérifiez votre connexion internet et cliquez sur le bouton Connecter. Dès que votre ordinateur est connecté au serveur, le champ de saisie de votre jeton d'activation s'active. Entrez le jeton d'activation qui vous a été fourni lors de l'achat du logiciel et cliquez sur le bouton Envoyer. Le serveur va renvoyer automatiquement la clé de débridage valable sur cet ordinateur et celle-ci sera enregistrée sur votre compte. Patientez quelques instants et relancez le programme. Le programme est maintenant disponible. Dans le cas de l'utilisation du logiciel sur un ordinateur qui n'est jamais connecté à Internet, vous devez prendre contact avec AragonSoft par email en transmettant l'identifiant qui s'affiche dans la partie haute de cette boîte de dialogue. Votre clef de débridage vous sera transmise par retour. Lorsque vous êtes en possession de votre clef de débridage, entrez celle-ci dans le champ correspondant et cliquez sur le bouton Enregistrer.

La procédure d'activation en ligne est simple, rapide et ne transmet aucune autre information que l'identifiant de votre ordinateur. L'identifiant de votre ordinateur est crée à partir de paramètres logiciels et matériels dont le choix dépend de la disponibilité au niveau de votre machine puis subit un hachage de sorte qu'il soit impossible de reconstituer les paramètres ayant servi à générer l'identifiant. Les paramètres matériels choisis ne dépendent jamais de matériels susceptibles d'être remplacés couramment sur les ordinateurs de sorte qu'une réparation de votre ordinateur ne modifiera pas son identification. Le seul paramètres logiciel utilisé est votre licence Microsoft Windows. Donc si vous réinstallez votre système d'exploitation veillez simplement à utiliser toujours la même licence Windows. Dans ces conditions vous êtes assuré de toujours pouvoir réinstaller et réactiver vos logiciels rapidement.

Retour au sommaire.

Les différentes versions de WinSesame :

Pro :

Version professionnelle du programme possédant toutes les fonctions avancées disponibles.

Classic :

Version destinée à une utilisation courante du logiciel pour les particuliers. Ce qui n'est pas disponible dans la version Classic par rapport à la version Pro :

Pas de nettoyage des données résiduelles sur le disque et en mémoire.

Pas de canal de cryptage.

Pas de cryptage par fichier de signature numérique.

Free :

Il s'agit d'une version gratuite du programme destinée à une utilisation sur de petits volumes de données ou pour découvrir le système avant l'achat d'une version complète. Par rapport à la version Classic la version Free subit les limitations suivantes :

Limitation des dossiers : 50Ko ou 5 fichiers maxi

Limitation des fichiers : 20 Ko maxi

Pas de limitation quant à la durée d'utilisation du logiciel. Il s'agit d'une version gratuite limitée et non pas d'une demo ou version d'essai.

La taille limite des dossiers que vous pouvez verrouiller avec la version gratuite vous permettra de protéger dans chaque dossier quelques fichiers Word ou Exel mais ne vous permettra pas de protéger des dossiers de photos ou la comptabilité d'une entreprise. Utilisations type de la version gratuite : un gestionnaire de mot de passe parfaitement sécurisé qui vous permettra de retrouver tous vos mots de passe utilisés par ailleurs ou un dossier ultra confidentiel contenant les numéros de la carte bancaire que vous utilisez pour vos achats sur internet.

IMPORTANT : La version gratuite n'est limitée que pour le verrouillage des dossiers mais pas pour l'ouverture de sorte qu'il est toujours possible d'ouvrir un dossier WinSesame avec la version gratuite quelque soit son volume c'est une sécurité contre la perte de données en cas d'indisponibilité d'une version enregistrée. Vous pourrez toujours récupérer vos données avec une version gratuite du logiciel (qu'il est donc conseillé de sauvegarder quelque part).

Retour au sommaire.

Résolution des problèmes :

Nom des dossiers et fichiers :

Certains caractères accentués bien qu'acceptés par Windows dans les noms de dossiers et de fichiers ne sont pas acceptés par WinSesame (par exemple le caractère €). En cas de présence d'un fichier ou dossier contenant un caractère non autorisé, le programme fermera sur un message d'erreur. Il n'y a aucun risque de perte de données puisqu'à ce stade aucune opération n'a encore été effectuée. Renommez simplement le dossier ou fichier en cause et procédez à nouveau au verrouillage.

Blocage du programme pendant une opération de verrouillage :

Si pour une raison accidentelle le programme subit un blocage pendant une opération de verrouillage d'un fichier, vous retrouverez toujours le fichier dans un dossier qui porte le même nom que le fichier. Il suffit donc dans ce cas de replacer le fichier à son emplacement et de supprimer le dossier qui ne contient plus alors qu'un fichier témoin utilisé temporairement par WinSesame et qui n'est plus utile. Toutes les mesures sont prises pour qu'aucun incident ne puisse nuire à la sécurité des données. La suppression des données est toujours effectuée en dernier et seulement à la condition que les opération précédentes se soit déroulées avec succès.

Retour au sommaire.

Limites d'utilisation :

WinSesame peut verrouiller des dossiers dont le volume dépend à la fois de la taille des plus gros fichiers, du nombre de fichiers contenus dans le dossier et de la quantité de mémoire contiguë que Windows peu allouer au programme à cet instant sans excéder 2 Go. WinSesame peut verrouiller et crypter des dossiers contenant jusqu'à 5000 fichiers. Dans la pratique ces limites ne doivent pas empêcher de protéger la totalité des documents présents sur un ordinateur puisque pour des raisons de compatibilité avec les différents systèmes de fichier, un logiciel ne crée pas de fichier supérieur à 2 Go. S'il est nécessaire de verrouiller des dossiers contenant plus de 2Go de données, celles-ci sont donc contenues dans plusieurs fichiers de taille compatible qu'il suffit de verrouiller indépendamment ou de classer dans des sous-dossiers qui pourront être verrouillés sans problème. Ceci présente en outre l'avantage d'un accès plus rapide aux données protégées et d'une sécurité accrue en évitant de déverrouiller inutilement la totalité d'un gros dossier. Dans la pratique lorsqu'un dossier contient un grand nombre de fichiers, vous verrouillerez directement le dossier et lorsqu'un dossier contient quelques gros fichiers, vous verrouillerez les fichiers indépendamment.

Retour au sommaire.