**PROCEDURE D’EXPLOITATION VERACRYPT**

**MAIRIE DE SIGNES**



**Table des matières**

[**Préambule** - 3 -](#_Toc67203470)

[**1)** **Télécharger VeraCrypt** - 4 -](#_Toc67203471)

[**2)** **Installer l’application** - 5 -](#_Toc67203472)

[**3)** **Démarrer l’application** - 6 -](#_Toc67203473)

[**3.1.** **Créer un volume pour crypter les données à protéger** - 6 -](#_Toc67203477)

[**3.2.** **Afficher le volume** - 12 -](#_Toc67203482)

[**3.3.** **Ajouter des fichiers au volume crypté** - 13 -](#_Toc67203488)

[**3.4.** **Monter le lecteur à l’ouverture de session Windows** - 13 -](#_Toc67203489)

# **Préambule**

**VeraCrypt** est un programme gratuit de chiffrement de partition qui fonctionne sous GNU/Linux, MacOS et Windows. Il est sous double licence Apache v2.0 et collective TrueCrypt v3.1.

Veracrypt chiffre des volumes (fichiers, partitions) ou des systèmes d'exploitation entiers, à la volée.

C'est à dire qu'il monte un volume chiffré, dans lequel vous mettez ce que vous voulez. Il est possible de cacher ces fichiers/partitions/OS chiffrés.

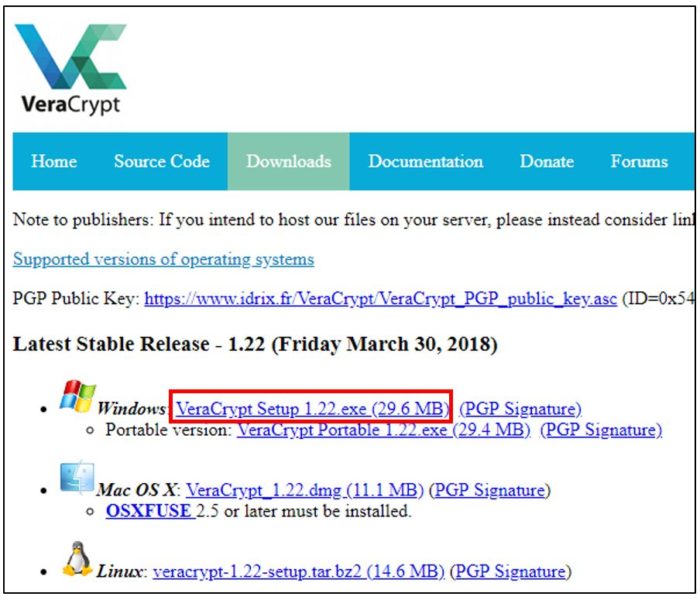
Les algorithmes de chiffrement proposés sont nombreux et utilisables en cascade. Évidemment, Veracrypt est open-source, multi-plateforme et utilisable en mode portable (sur une clef-usb).

La société FUTURZO recommande fortement l’utilisation de ce logiciel car en plus d’être OpenSOurce, il est également recommandé par la CNIL pour protéger les données.

# **Télécharger VeraCrypt**

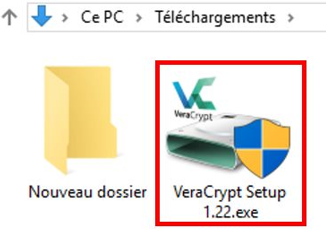
Accédez à la page de téléchargement de VeraCrypt et téléchargez la version appropriée à votre système d’exploitation :

* [**https://www.veracrypt.fr/en/Downloads.html**](https://www.veracrypt.fr/en/Downloads.html)**.**

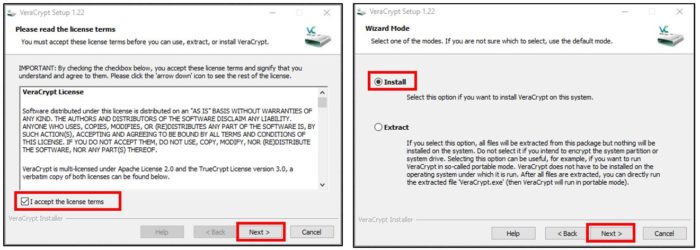


# **Installer l’application**

Ouvrez **l’explorateur Windows** et accédez au répertoire **Téléchargement** pour exécuter le fichier téléchargé et installer l’application.

****

* **Cochez la case** pour accepter les termes de la licence,
* Cliquez sur **Next**,
* Conservez l’option **Install**,
* Validez par **Next**.



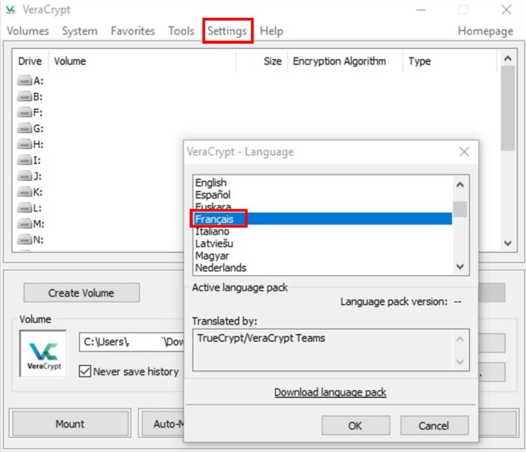
* Laissez ensuite les cases cochées et validez par **Install**.



* Cliquez enfin sur **Finish**.

# **Démarrer l’application**

* **Double cliquez** sur l’icône créée sur le bureau,
* Commencez ensuite par paramétrer le logiciel en français :
  + cliquez sur le menu **Settings** puis sur **Language** et choisissez enfin **Français**.





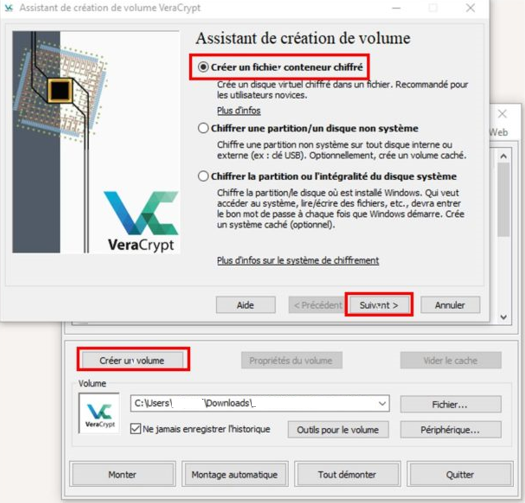
## **Créer un volume pour crypter les données à protéger**

La première étape consiste à créer un volume chiffré qui contiendra les données protégées.

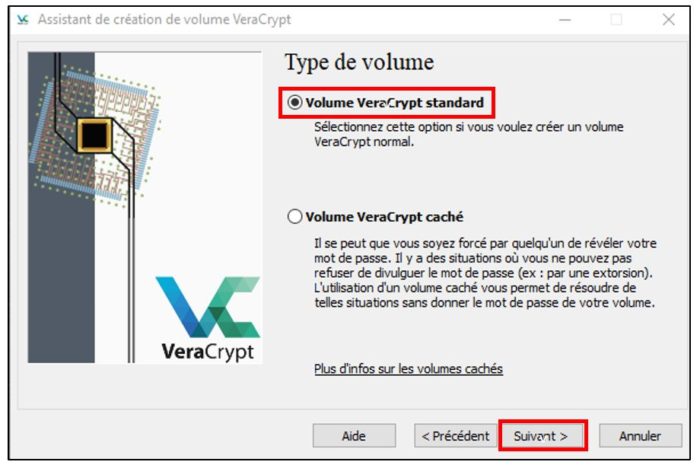
Cliquez sur **Créer un volume**. Trois possibilités sont proposées :

* **Créer un fichier conteneur chiffré** : créer un volume chiffrant les fichiers et dossiers choisis
* **Chiffrer une partition non système** : un second disque dur, un disque dur externe, une clé USB…
* **Chiffrer la partition système** : le disque ou est installé le système d’exploitation Windows.

Dans notre exemple, nous sélectionnons l’option permettant de **créer un fichier conteneur chiffré** puis cliquons sur **Suivant**.



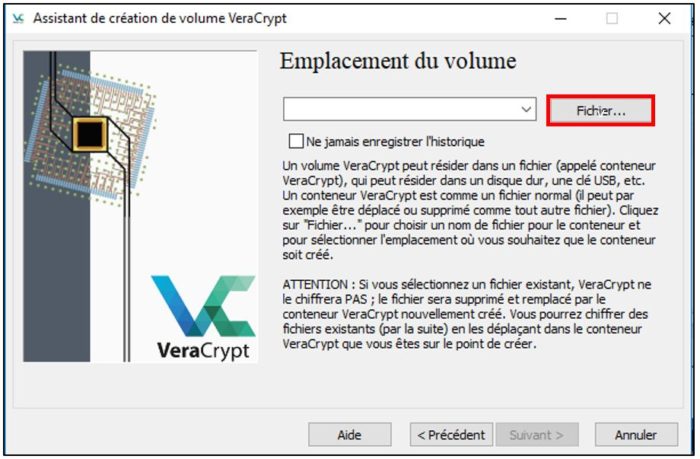
Dans le type de volume, nous **conservons la première option**.



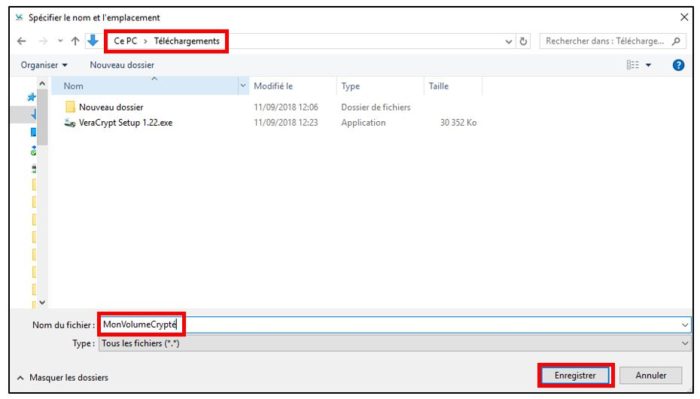
Sélectionnez enfin **l’emplacement ou sera stocké ce volume**.

Le fichier créé peut se situer sur un disque local ou externe.

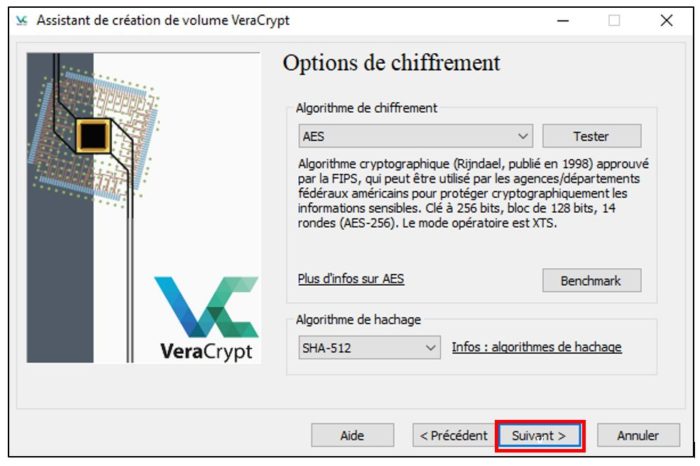
* Cliquez sur **Fichier**.



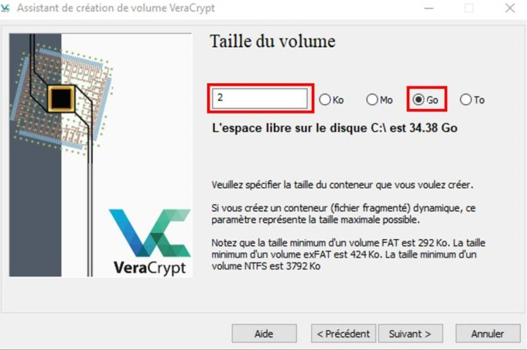
Choisissez un emplacement sur votre ordinateur, indiquez un **nom** pour celui-ci et validez enfin par **Enregistrer**.



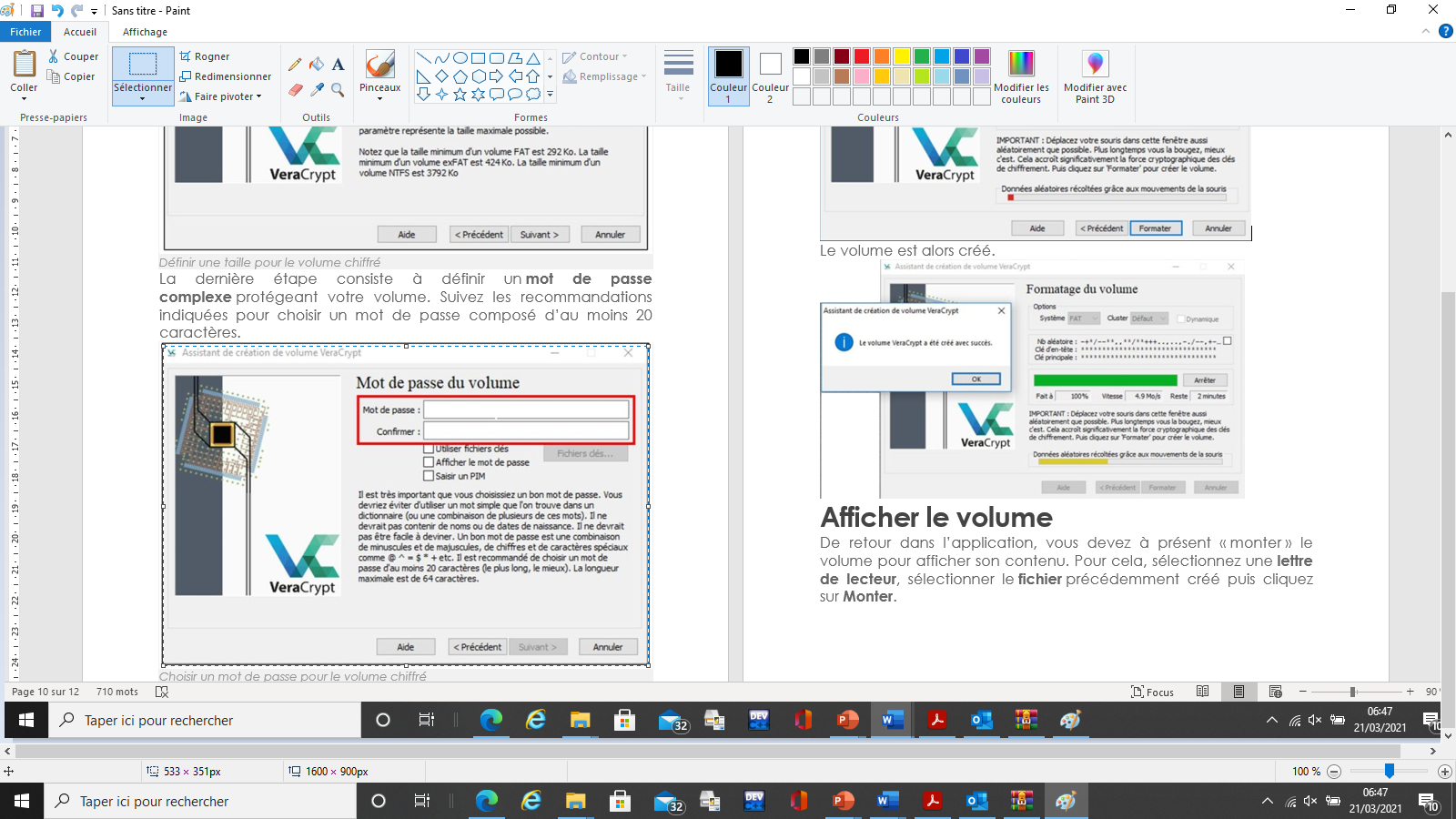
Sélectionnez le **type de chiffrement**. Nous conservons les paramètres indiqués dans notre exemple, à savoir « **AES**».



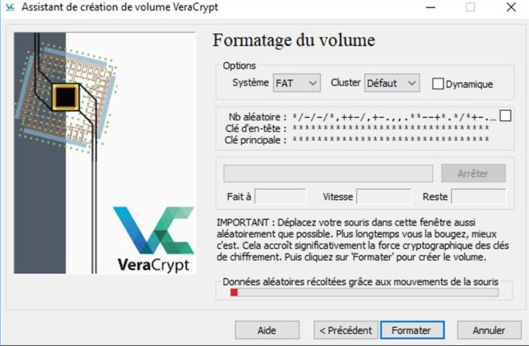
Indiquez ensuite une **taille maximale** pour le volume que vous créez. Celle-ci dépend du nombre de fichiers stockés.



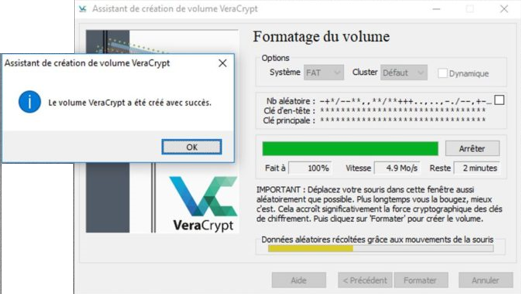
La dernière étape consiste à définir un **mot de passe complexe** protégeant votre volume. Suivez les recommandations indiquées pour choisir un mot de passe composé d’au moins 20 caractères.



Après avoir validé le choix du mot de passe, cliquez sur **Formater** pour créer le volume.



Le volume est alors créé.

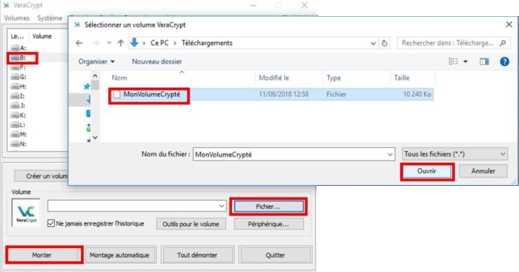




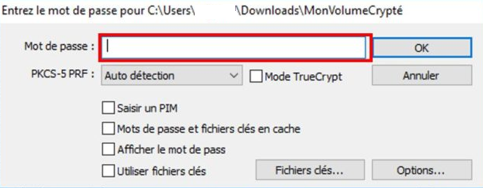
## **Afficher le volume**

De retour dans l’application, vous devez à présent « **monter** » le volume pour afficher son contenu.

Pour cela, sélectionnez une **lettre de lecteur**, sélectionner le **fichier** précédemment créé puis cliquez sur **Monter**.



Saisissez votre **mot de passe**.

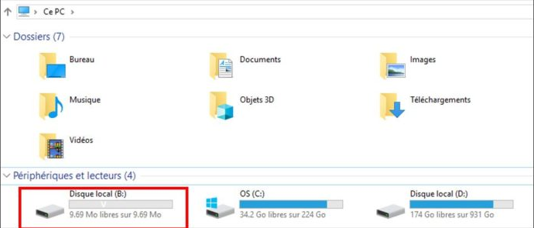




## **Ajouter des fichiers au volume crypté**

Vous retrouvez à présent votre volume sécurisé sous forme de lecteur dans **l’explorateur Windows**.

Double cliquez sur celui-ci **(B:)** pour l’ouvrir et y **ajouter autant de fichiers** **que souhaités**.



## **Monter le lecteur à l’ouverture de session Windows**

Le menu **Favoris** de l’application permet d’ajouter le volume automatiquement à l’explorateur à l’ouverture de session Windows.

Lors du prochain redémarrage, l’application **se** **lancera automatiquement**et **demandera le mot de passe** lié au volume pour en afficher le contenu.

