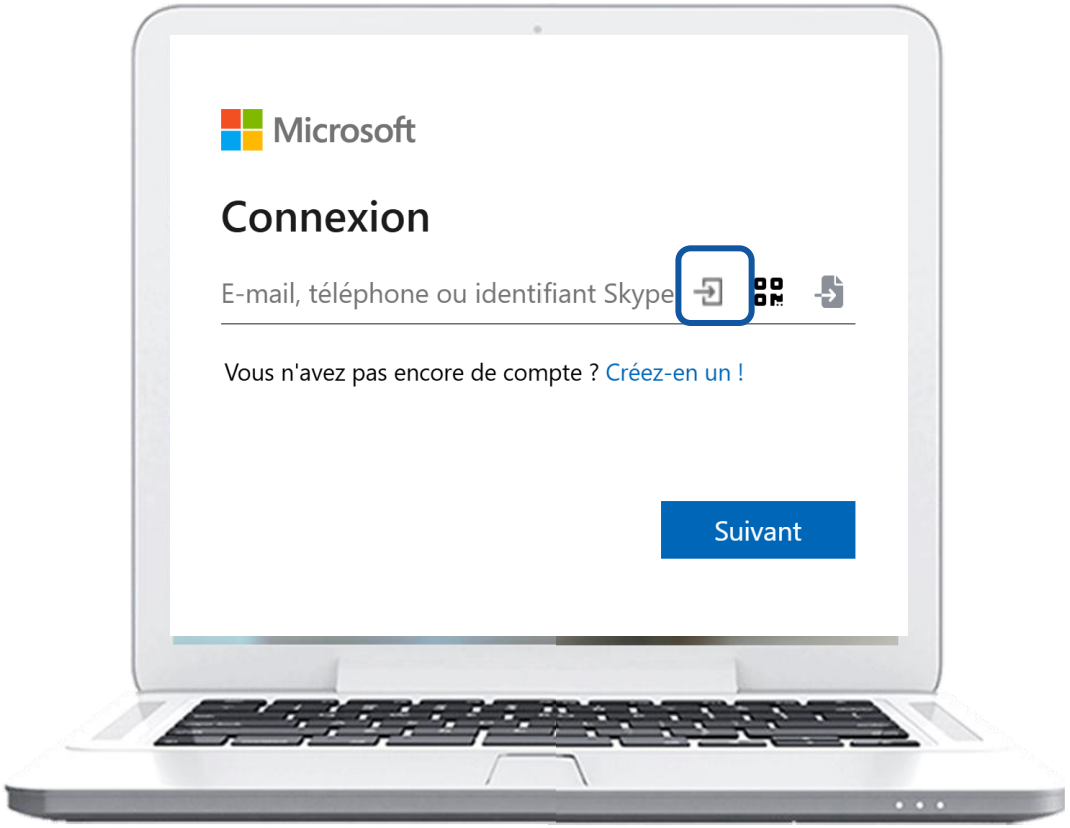
TUTORIEL EXTENSION PASSCYPHER HSM PGP Licence

By Freemindtronic Andorra

Gestionnaire de mots de passe sécurisé

Sans serveur, sans base de données, sans identification
« Zéro Trust & Zéro Knowledge »

CONNEXION AUTOMATIQUE INSTANTANÉE

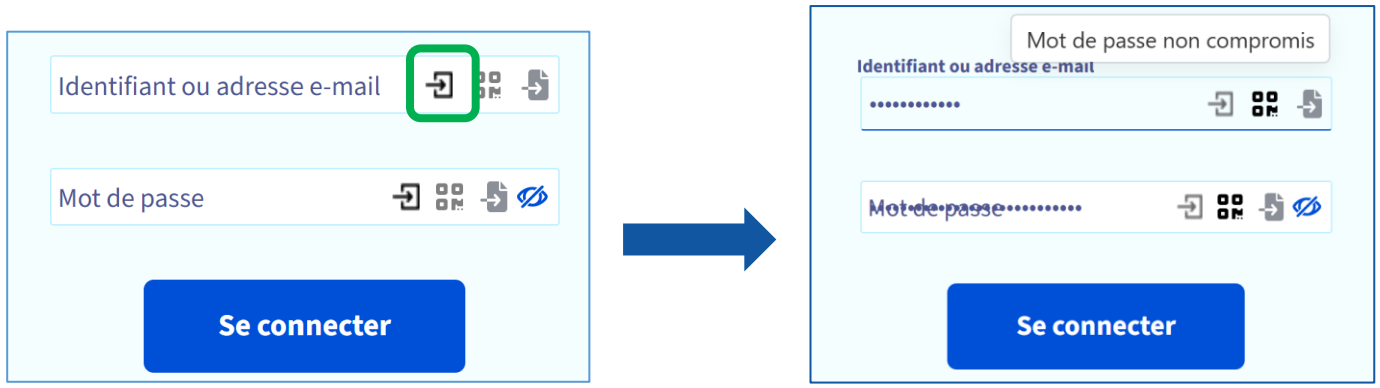


Un seul clic *sur l'icône indiquée, les champs se remplissent et la* ***connexion est établie.***

SOMMAIRE

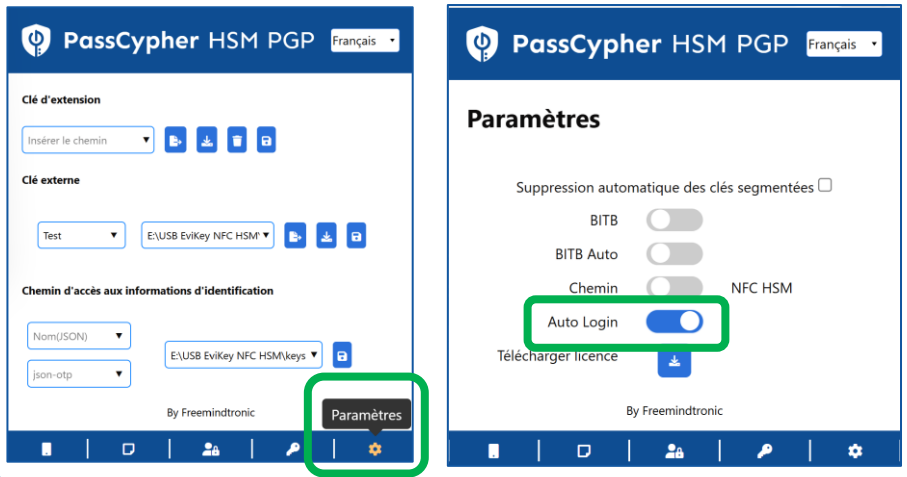
COMMENT CELA FONCTIONNE ?

- **PassCypher HSM PGP** est une extension pour navigateurs Web qui permet une **connexion automatique instantanée**
- Un **système breveté d'authentification par clés segmentées** est implémenté
- Vous bénéficiez d'une **sécurité maximale** ainsi que d'une **rapidité d'exécution inégalable**
- **Cliquez sur l'icône** indiquée ci-dessous dans le champ « **Identifiant** »
- Les champs sont remplis et la connexion est réalisée
- **Pensez à activer l'Auto Login dans les Paramètres de l'extension***



(*) Activer l'Auto Login

Cliquez sur l'icône « **Paramètres** » puis glissez le bouton « **Auto Login** » vers la droite.



INSTALLATION DE L'EXTENSION

Téléchargez & installez l'extension PassCypher HSM PGP

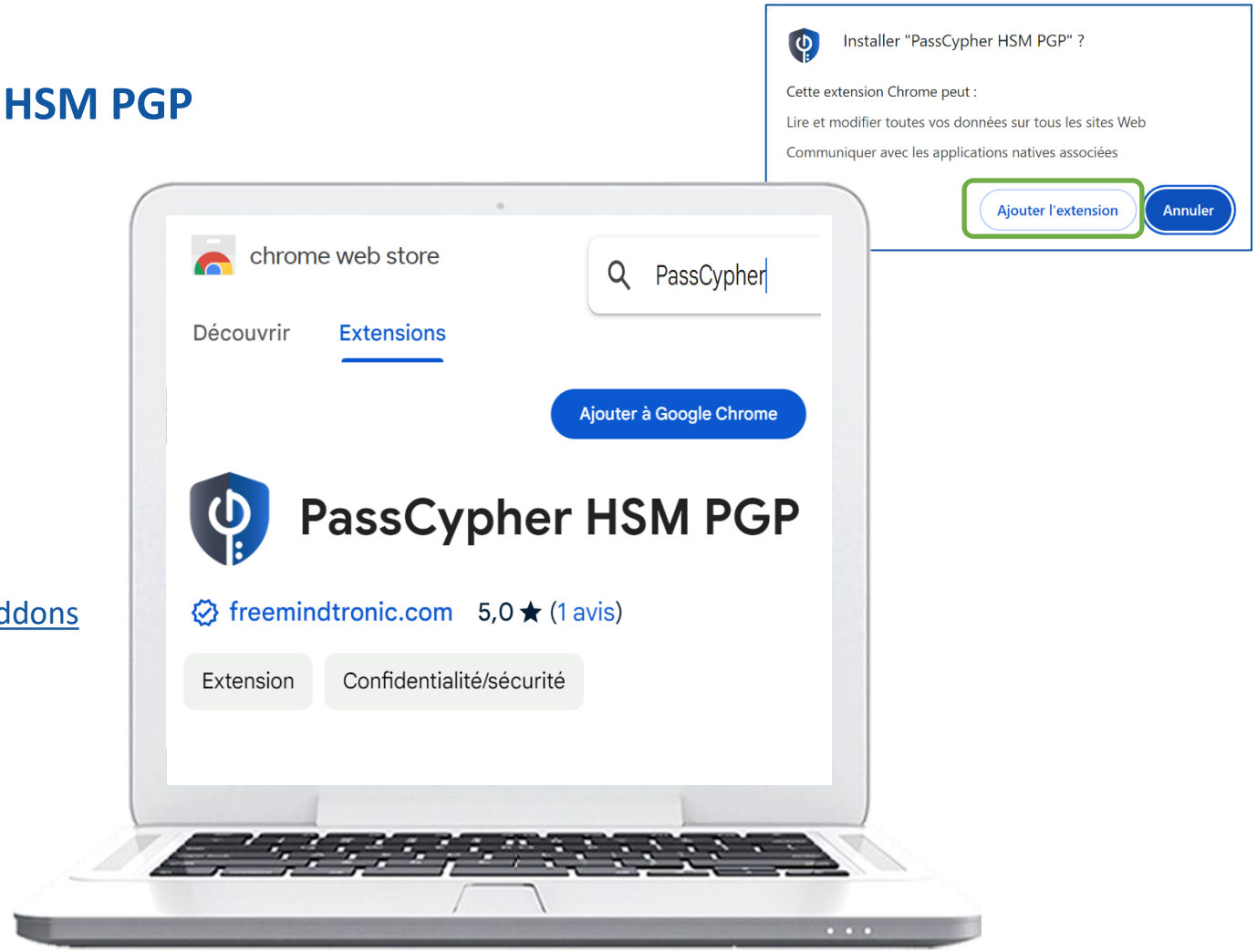
CHROME : chrome web store

BRAVE : chrome web store

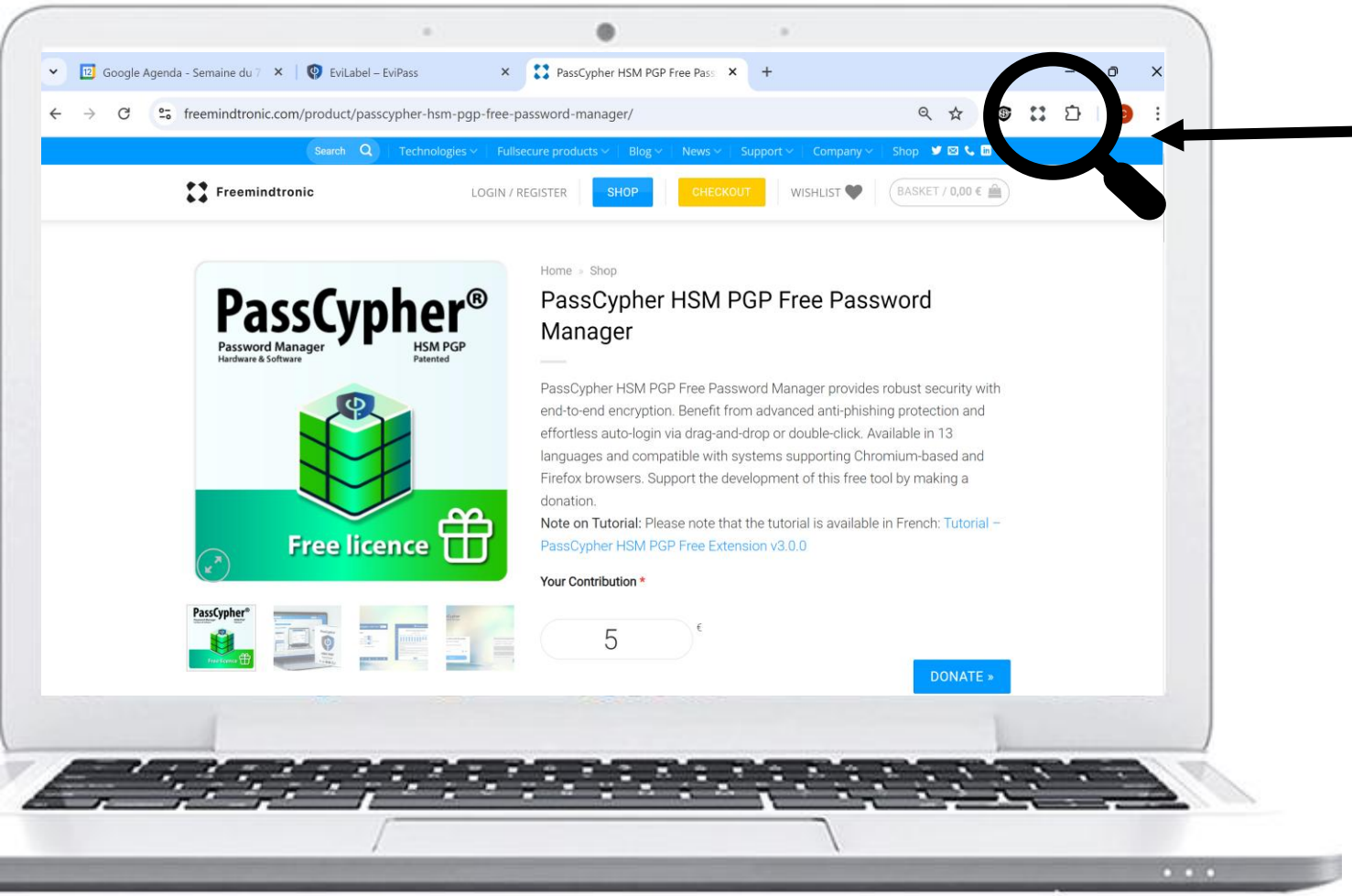
OPERA : chrome web store

MICROSOFT EDGE : PassCypher HSM PGP - Microsoft Edge Addons

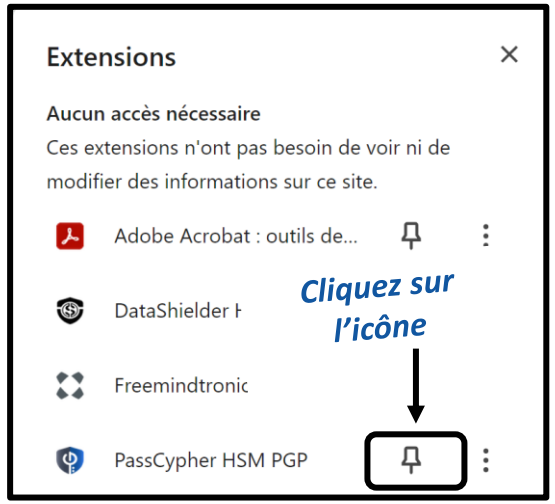
FIREFOX : en cours



FINALISATION DE L'INSTALLATION



Cliquez sur cette icône pour accéder aux extensions



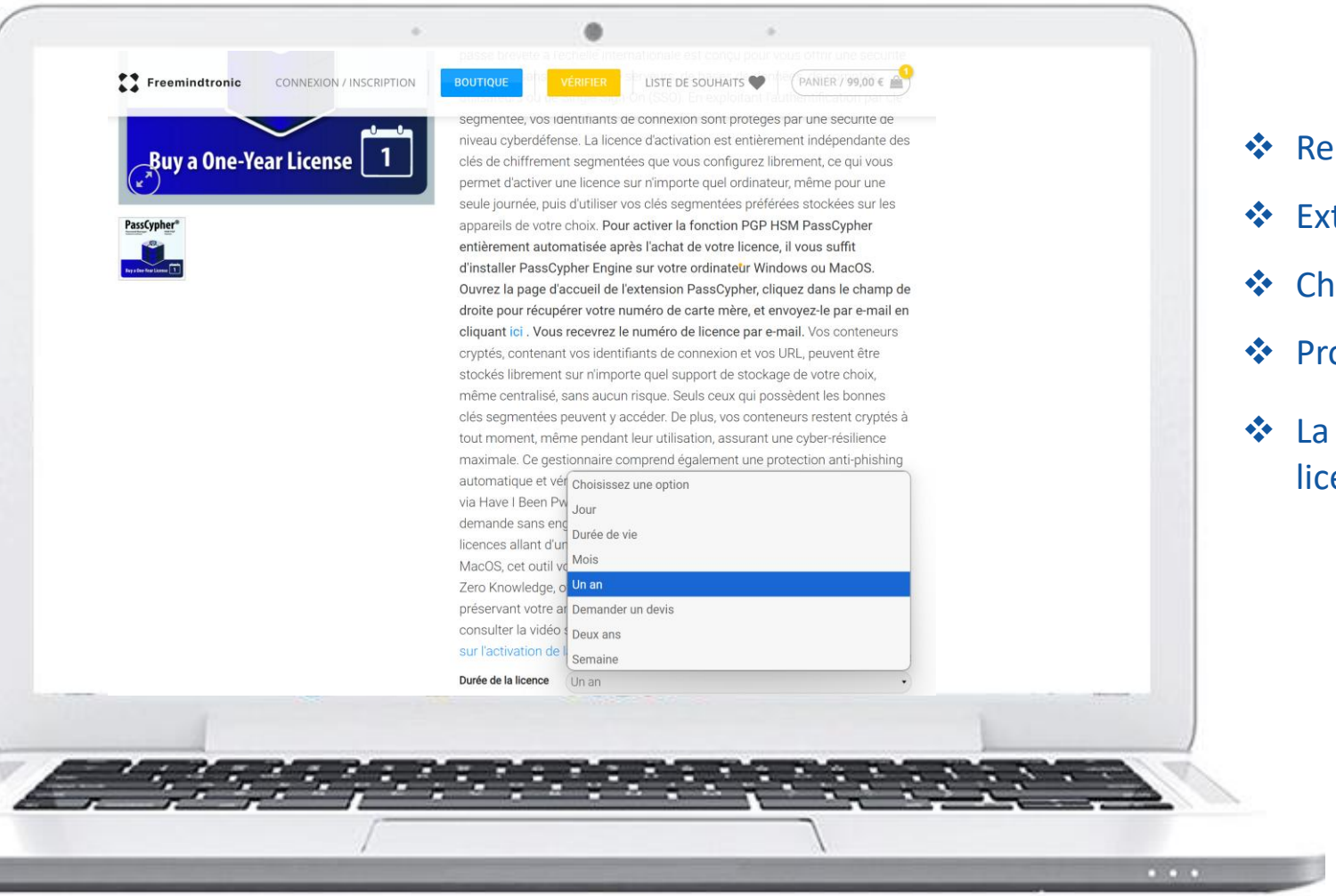
Cliquez sur l'icône PassCypher en haut à droite de l'écran de votre ordinateur pour ouvrir l'extension

EXTENSION MULTILANGUES

L'extension PassCypher HSM PGP est traduite en 13 langues : Arabe, Allemand, Anglais, Catalan, Chinois, Espagnol, Français, Hindi, Italien, Japonais, Portugais, Roumain et Russe.

Vous pouvez choisir dans quelle langue afficher l'extension.

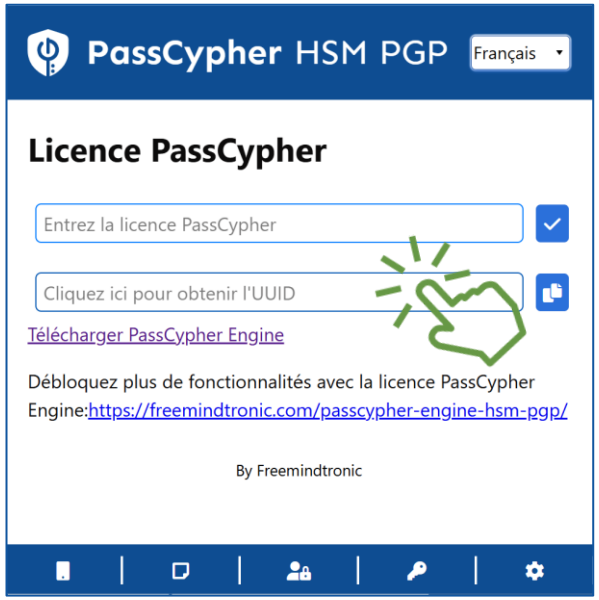
ACHAT DE LA LICENCE



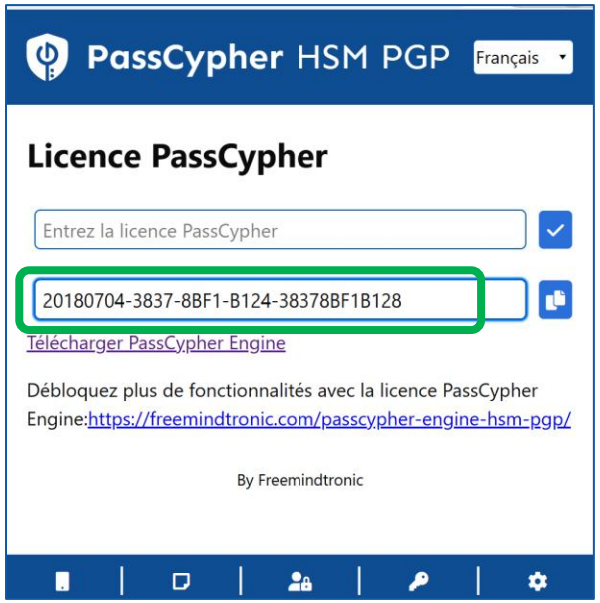
- Rendez-vous sur la boutique FREEMINDTRONIC
- Extension « **PassCypher HSM PGP Password Manager** »
- Choisissez l'option qui vous convient le mieux
- Procédez au paiement
- La page suivante vous explique comment activer votre licence

(*) Note: Il y a plusieurs abonnements disponibles : à la journée, à la semaine, au mois ou à l'année

ACTIVATION DE LA LICENCE

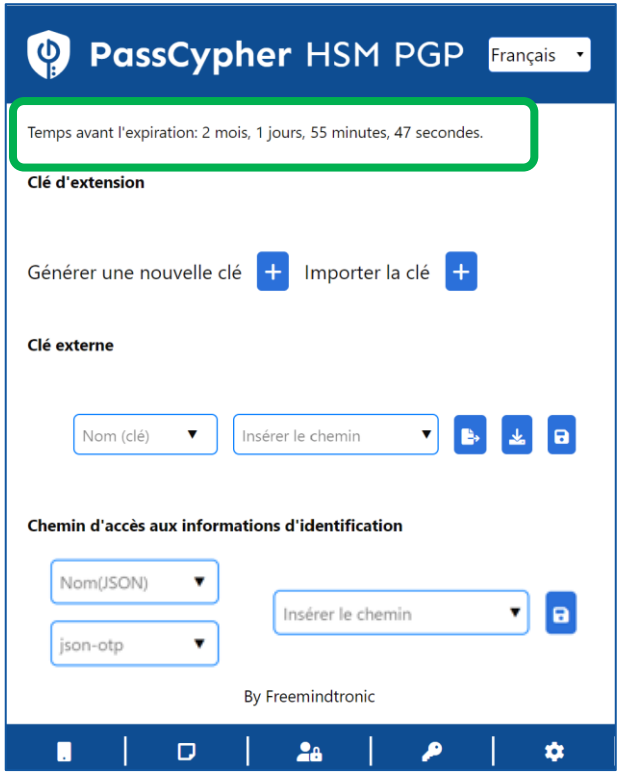


Cliquez sur « **Télécharger PassCypher Engine** *» et installez le logiciel (**Windows ou MacOS**). **Cliquez** ensuite pour obtenir **l'UUID de votre ordinateur**



Envoyez ce numéro par mail à **fullsecure [at] freemindtronic.com**

Copiez/collez le numéro de licence reçu en retour. Puis cliquez sur l'icône indiquée pour **activer la licence**



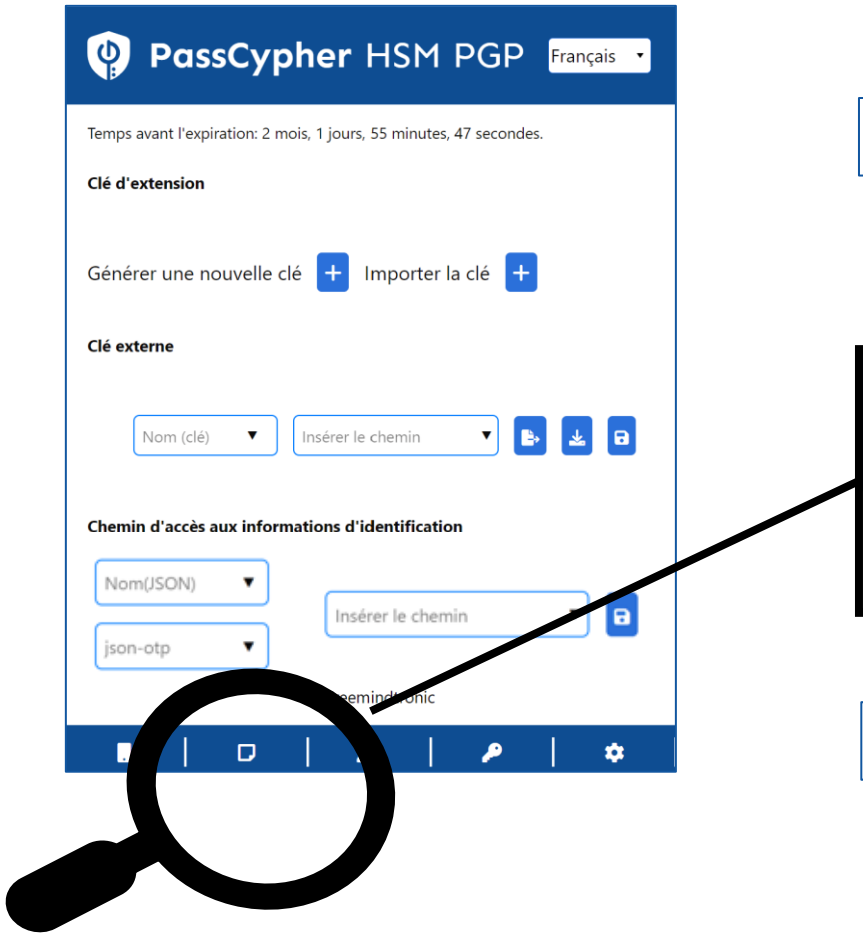
La licence est activée. La validité est indiquée en temps réel en haut de la page*

(*) Après avoir téléchargé le logiciel, **allez** dans « **Téléchargements** » et cliquez sur le fichier

PassCypherEngine_1.3.0_x64 (3).exe

YouTube **Installer PassCypher Engine**

LA PAGE D'ACCUEIL EN DÉTAIL



Par défaut, l'extension s'ouvre sur la fenêtre « clés »

Téléphones * Fonction NFC	Récupérer un libellé	EviPass Gestion MDP	Clés Création/Gestion	Paramètres

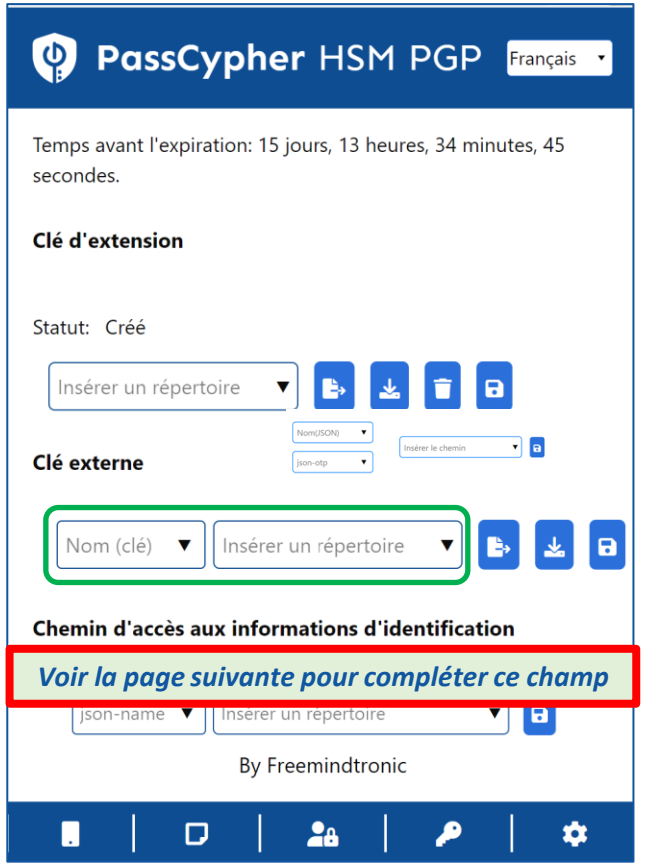
Retrouvez toutes les fonctionnalités expliquées dans ce tutoriel

(*) Consultez le tutoriel spécifique fonction NFC : https://freemindtronic.com/how-it-works-products-in-depth-guide-to-fullsecure/

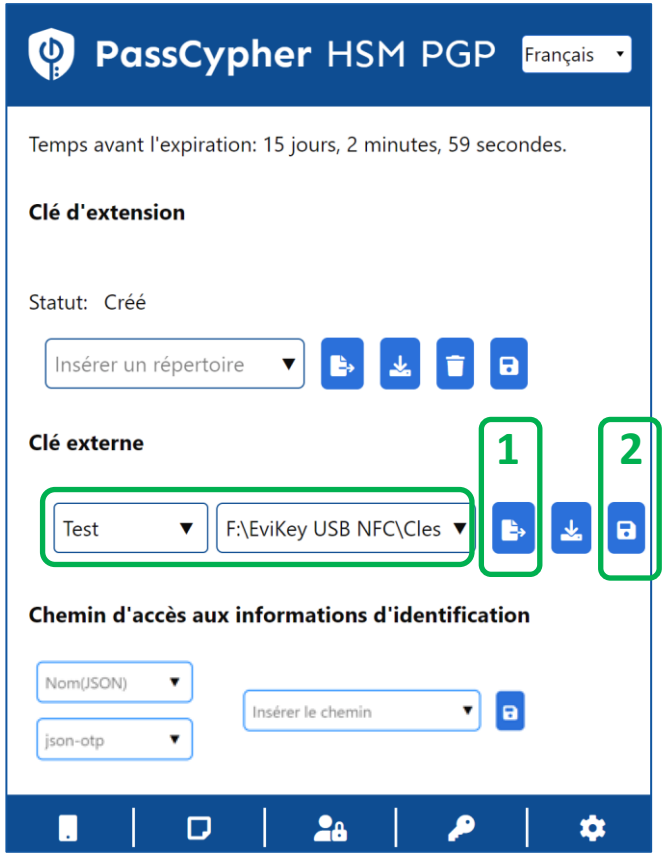
CRÉEZ* VOS CLÉS SEGMENTÉES

(*) Si une clé segmentée existe déjà (clé d'extension et clé externe) se référer aux pages 14 à 16

Cliquez sur le symbole « **+** » pour générer une **clé d'extension**. Cette clé est enregistrée dans le « local storage » de votre navigateur web.



La clé d'extension est créée. Vous devez maintenant créer la **clé externe**. Donnez un nom à la clé et Insérez le chemin d'accès*. **Il est conseillé d'utiliser un moyen de stockage externe (clé USB, SSD…)**



Cliquez ensuite sur l'icône « **EXPORTER** » **[1]** puis sur l'icône « **SAUVEGARDER** » **[2].** La clé externe « **Test** » est créée et enregistrée.

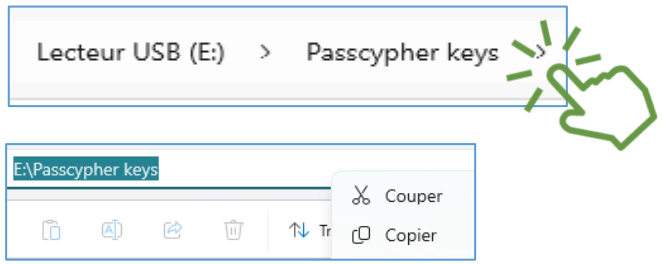
insérez le chemin d'accès* : explications détaillées dans la page suivante

INSÉREZ LE CHEMIN D'ACCÈS

- **Choisissez** l'endroit où vous allez **sauvegarder votre clé externe** (un dossier dans un disque dur interne ou externe, une clé USB ….)
- Indiquez ensuite le chemin d'accès exact de cet emplacement
- Vous trouverez ci-dessous comment faire si vous utilisez un ordinateur sous système d'exploitation **Windows** ou **macOS**
- **Suivez scrupuleusement les instructions mentionnées.**

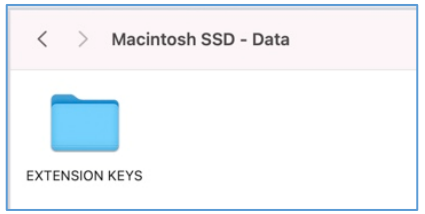
Pour garantir une sécurité optimale, si le support externe n'est pas disponible ou connecté à l'ordinateur, il ne sera pas possible d'accéder à la clé externe.

Windows

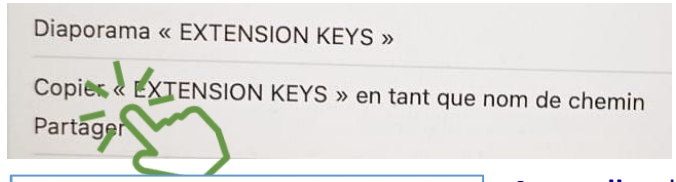


1. Créez un dossier [**ici « PassCypher keys**] dans votre support externe
2. L'emplacement de ce dossier est affiché
3. Cliquez dans la fenêtre
4. Le chemin d'accès est sélectionné
5. Cliquez sur « **Copier** » et **collez** dans l'extension **sans ajouter aucun autre caractère**

macOS



1. Créez un dossier [**ici « EXTENSION KEYS**] dans votre support externe
2. L'emplacement est affiché
3. Maintenez la **touche « alt ou option »** enfoncée et faites un clic droit sur la souris

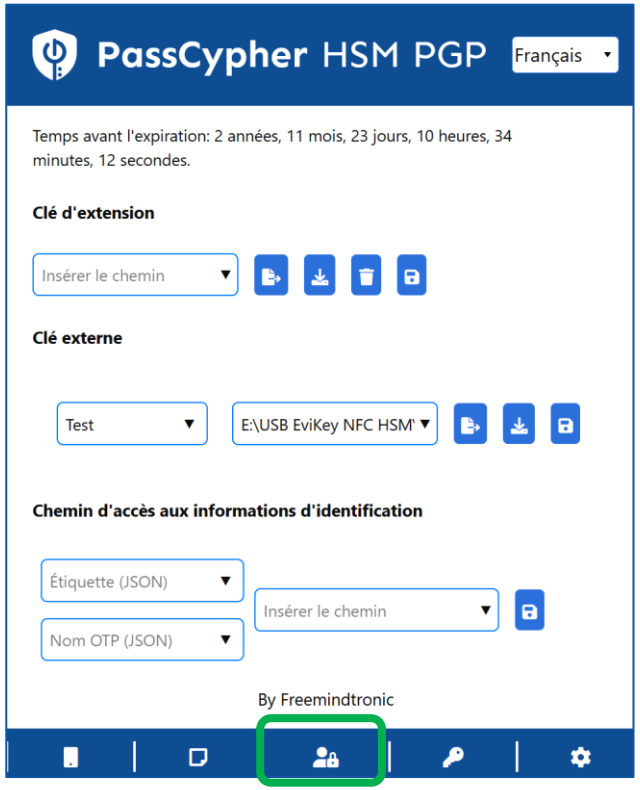


3. Cliquez sur « **Copier** »

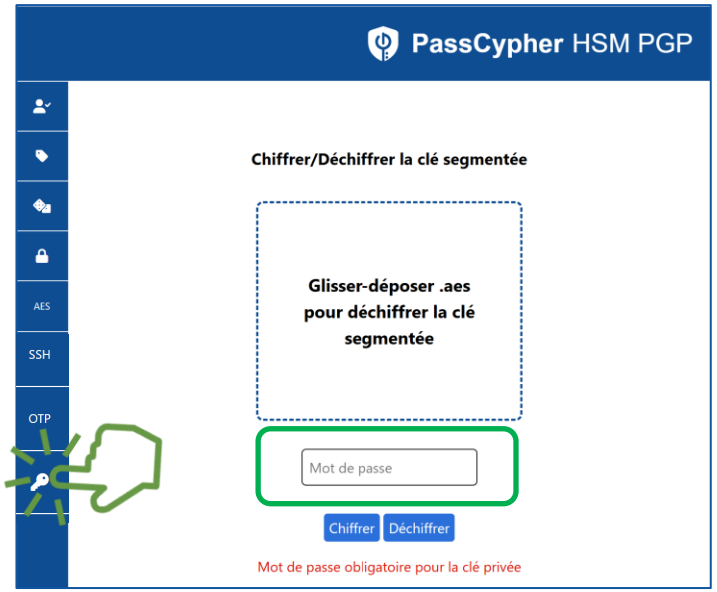
4. et **collez** dans l'extension **sans ajouter aucun autre caractère**

Vérifiez lors du collage que le caractère " ne s'ajoute pas au début des caractères collés. Si c'est le cas, supprimez-le

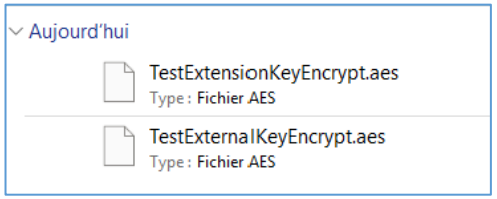
PARTAGEZ VOS CLÉS DE CHIFFREMENT SEGMENTÉES



Pour partager les clés avec un correspondant, vous devez les **chiffrer. Cliquez sur l'icône « EviPass ».** Une nouvelle fenêtre s'ouvre.



Cliquez sur l'icône « **Clés** » puis saisissez un **mot de passe** de 12 caractères minimum et cliquez sur l'icône « **Chiffrer** »

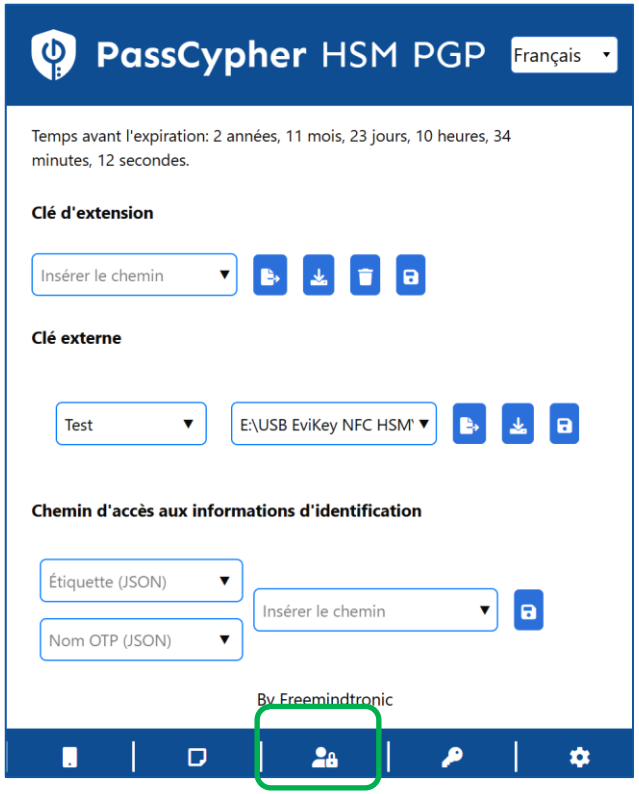


Automatiquement la clé externe et la clé d'extension sont **chiffrées**. Vous pouvez les récupérer dans le dossier « **Téléchargements** »

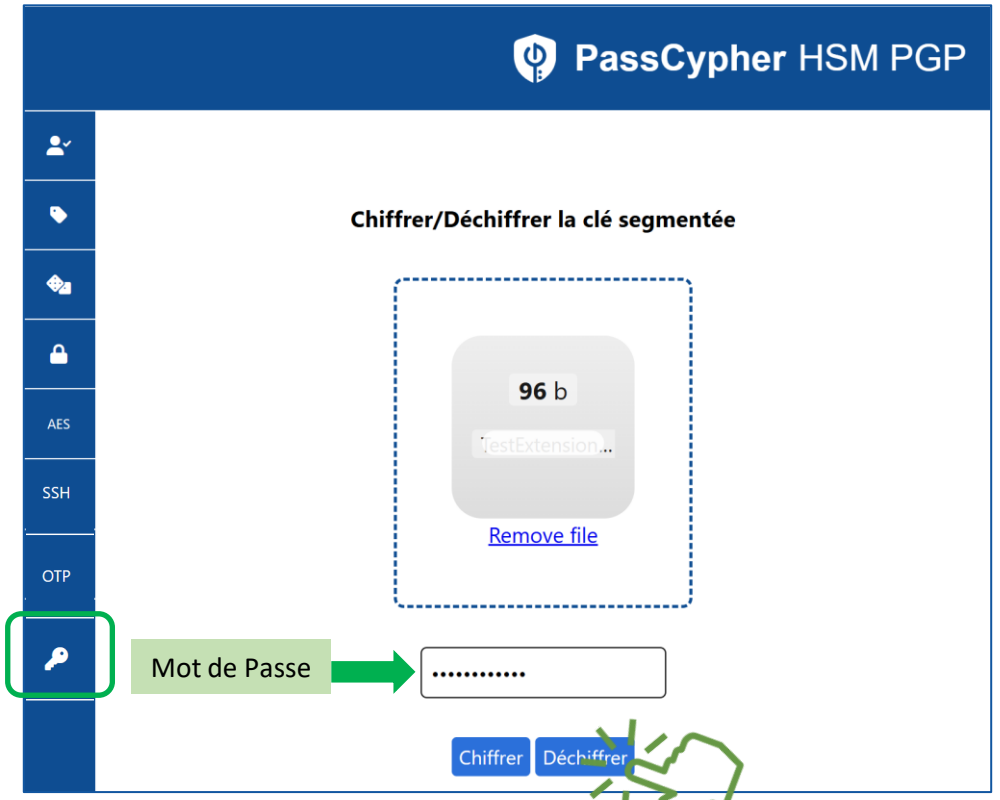
Envoyez ces 2 fichiers par **mail** (ou autre) à votre correspondant et indiquez-lui le mot de passe par un autre canal (**SMS** par exemple).

IMPORTEZ UNE CLÉ DE CHIFFREMENT SEGMENTÉE 1/3

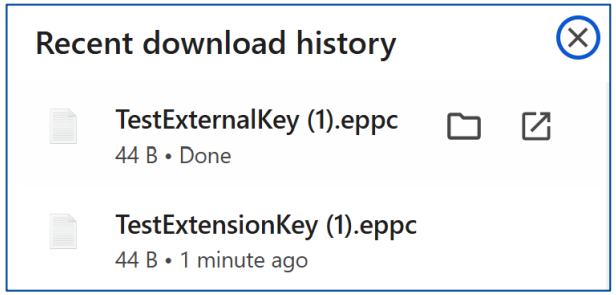
Commencez par déchiffrer les segments de clé



Pour déchiffrer les clés envoyées par un correspondant, cliquez sur l'icône « **EviPass** » et cliquez sur l'icône « **clés** »



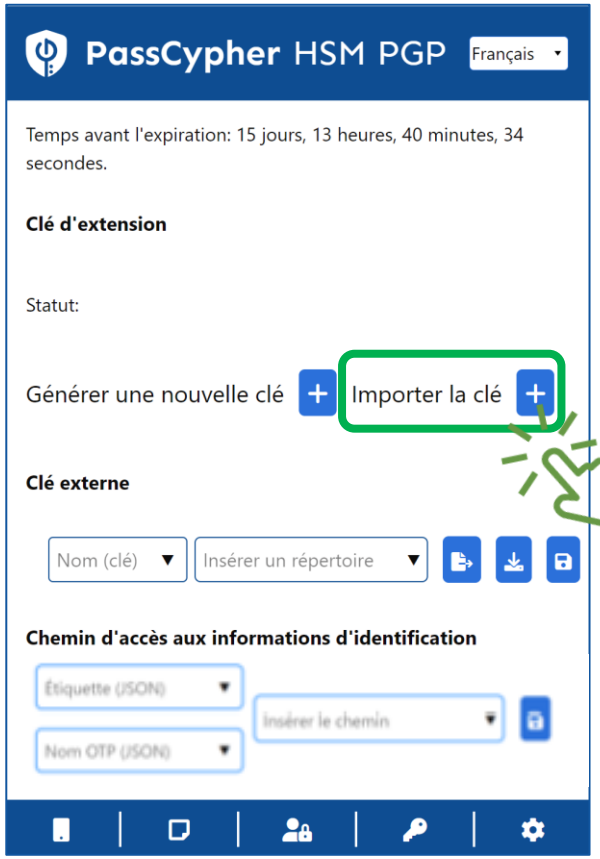
Insérez la **clé d'extension** chiffrée (Copier/coller ou Glissez le fichier). Saisissez ensuite le mot de passe à l'endroit indiqué et cliquez sur « **Déchiffrer** »



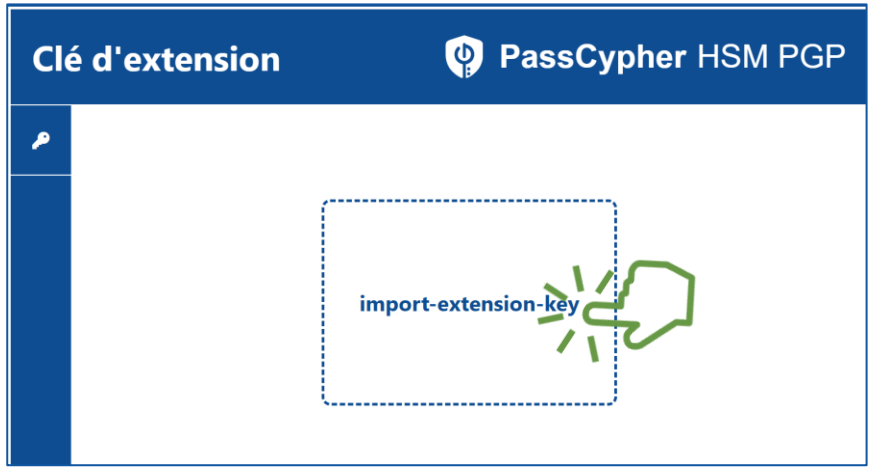
Procédez de la même façon pour déchiffrer la clé externe. Les **2 fichiers déchiffrés** sont dans le dossier « **Téléchargements** »

IMPORTEZ UNE CLÉ DE CHIFFREMENT SEGMENTÉE 2/3

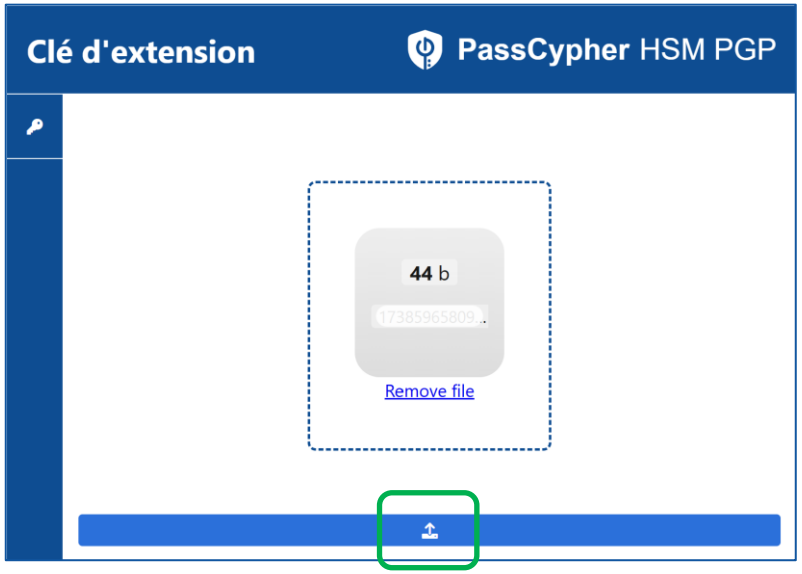
Importez d'abord la clé d'extension



La clé d'extension envoyée par votre correspondant est déchiffrée. Cliquez sur l'icône « **Importer la clé** »



Cliquez dans la fenêtre et importer la **clé d'extension déchiffrée**



Quand la clé est insérée, cliquez sur la flèche. Un message « **succès** » apparaîtra. Fermez cette fenêtre et réouvrez l'extension.

IMPORTEZ UNE CLÉ DE CHIFFREMENT SEGMENTÉE

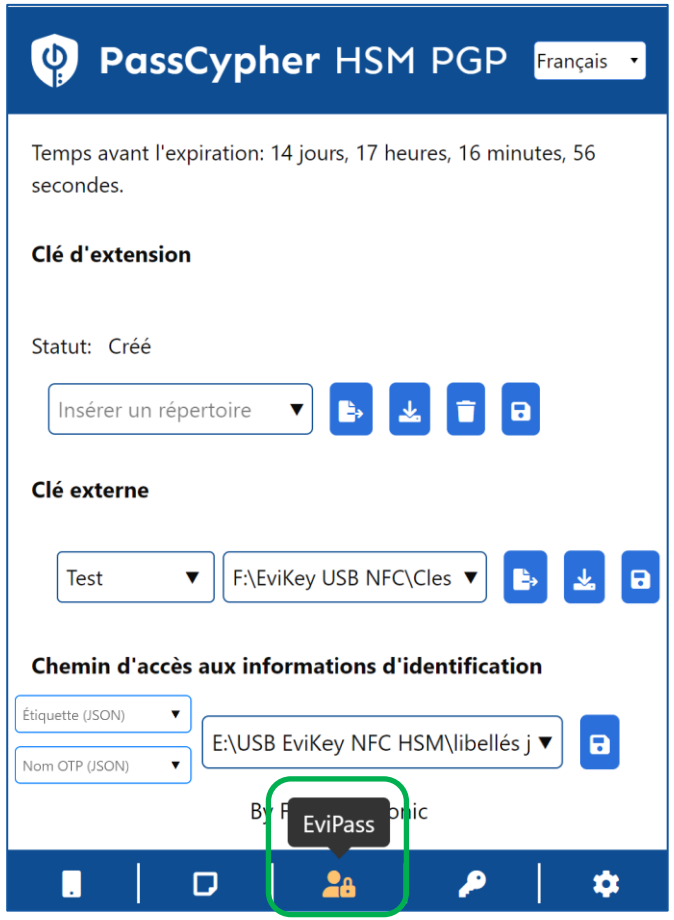
Indiquez le chemin où est stockée la clé externe

Stockez la clé externe « **TestExternalKey.eppc** » à l'endroit de votre choix* (ici une **clé USB EviKey**). Pour que l'extension puisse accéder à la clé externe, écrivez le nom de la clé (**Test**) et entrez le **chemin d'accès à la clé.** Cliquez ensuite sur l'icône « **Sauvegarder** ».

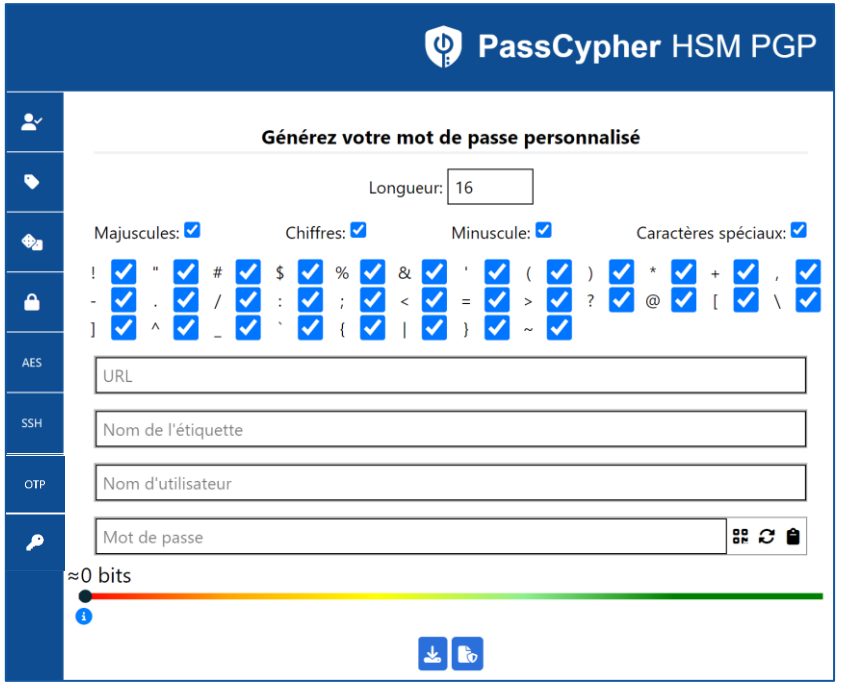
L'importation des clés est terminée. Vous pouvez commencer à constituer votre répertoire de conteneurs d'identifiants de connexion. Pour cela, cliquez sur **l'icône « EviPass »**

(*) Nous vous recommandons de stocker la clé externe dans un support amovible

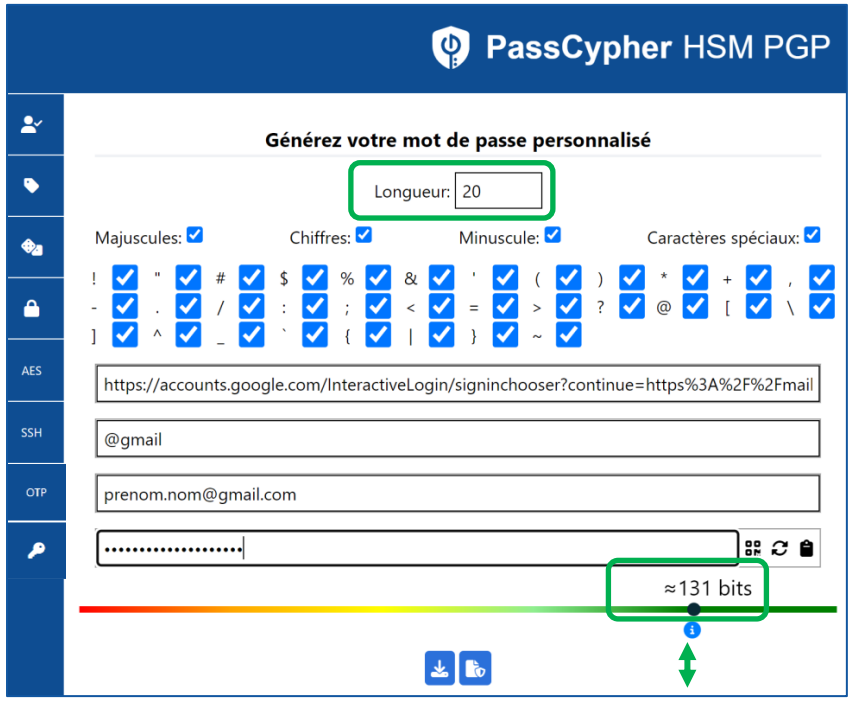
CRÉEZ VOS IDENTIFIANTS DE CONNEXION



Ouvrez l'extension puis **cliquez sur l'icône indiquée** pour créer vos identifiants de connexion



Complétez les informations demandées. **Pour compléter l'URL,** copier les informations affichées dans la barre de navigation (***cf exemple ci-dessous***)

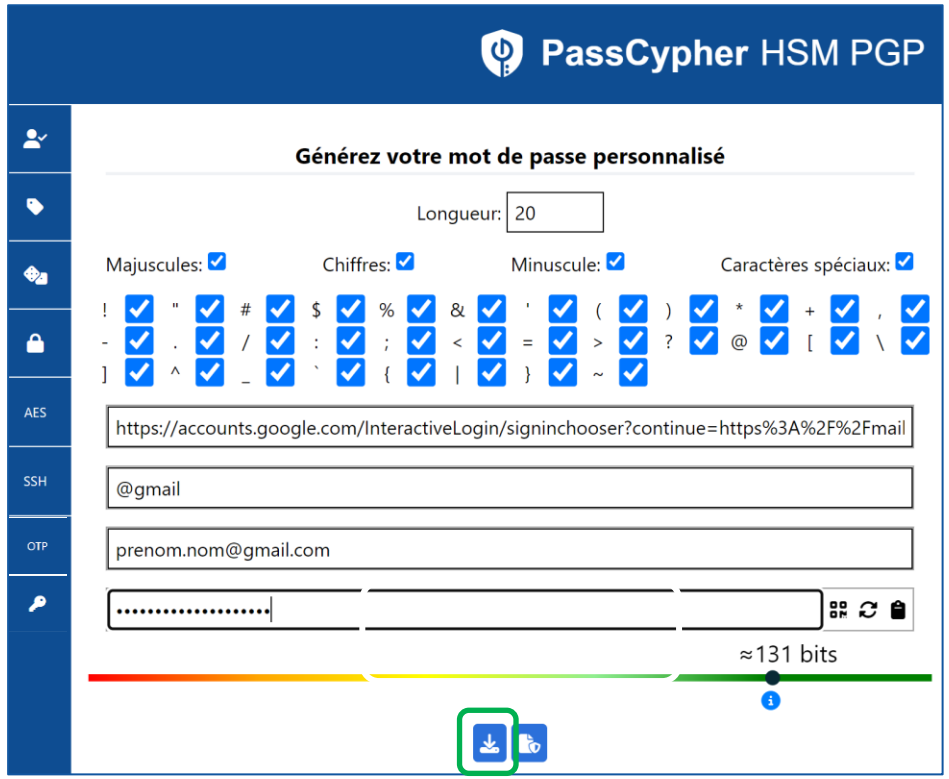


L'entropie du mot de passe est calculée et s'affiche sous forme de code couleur

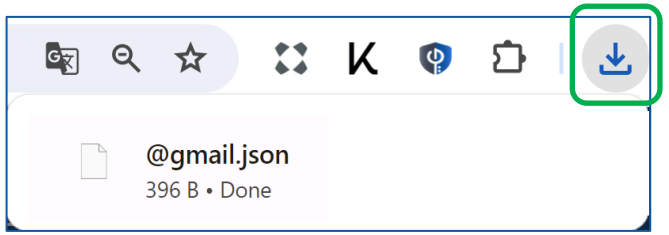
La force de votre mot de passe est calculée en fonction de la taille de l'alphabet qu'il utilise et de sa longueur. Plus la taille de l'alphabet et la longueur du mot de passe sont grandes, plus il sera sécurisé.

URL = https://accounts.google.com/InteractiveLogin/signinchooser?continue=https%3A%2F%2Fmail.google.c...

SAUVEGARDEZ VOS IDENTIFIANTS DE CONNEXION



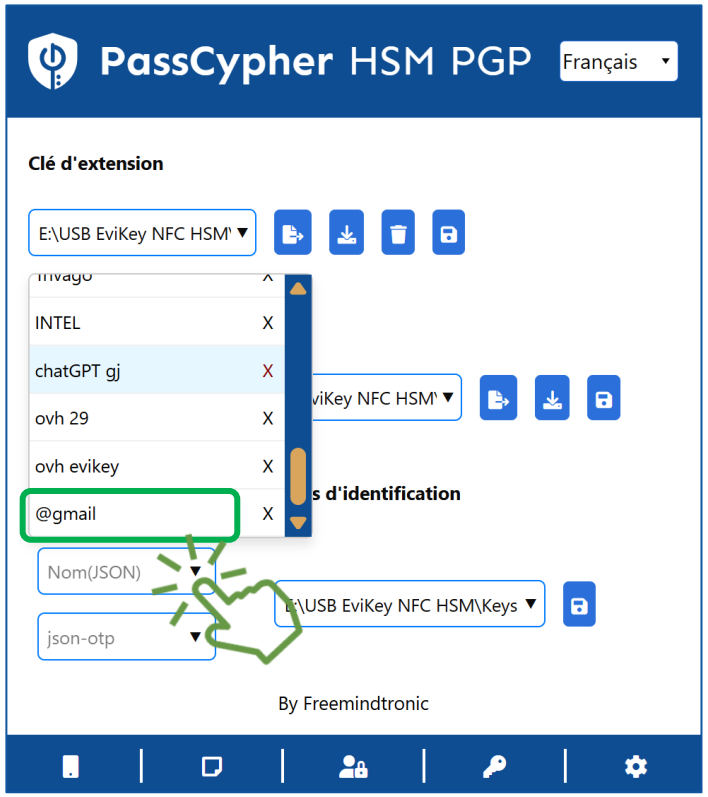
Cliquez ensuite sur l'icône indiquée afin de générer cet identifiant



Le fichier **@gmail.json** est disponible dans le dossier « **Téléchargements** » de votre ordinateur

Choisissez un dossier pour sauvegarder vos containers chiffrés (fichiers .json). Il est conseillé d'utiliser un support externe pour des raisons de sécurité.

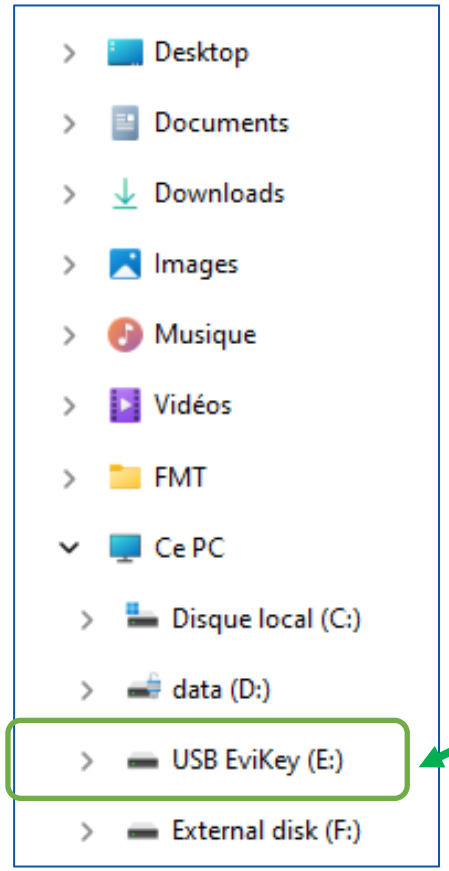
Voir page suivante



Le fichier « **.json** » créé est automatiquement ajouté dans l'extension à la liste de tous les identifiants créés.

Pensez à faire des sauvegardes régulières dans différents supports, y compris dans le cloud puisque vos containers sont chiffrés.

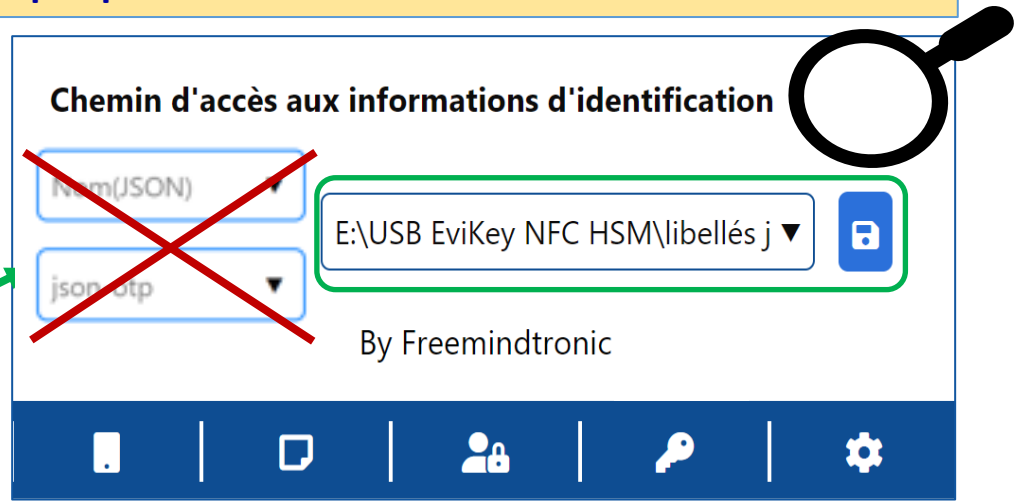
DÉTERMINEZ LE CHEMIN D'ACCÈS À VOS IDENTIFIANTS DE CONNEXION & OTP

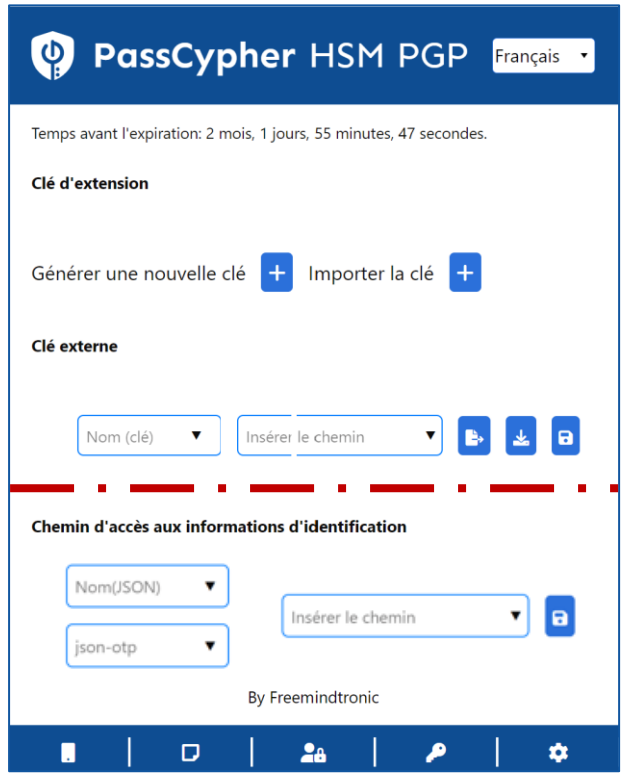


Il est **indispensable** d'indiquer **très précisément le chemin d'accès** à vos containers chiffrés (fichiers .json) pour la connexion automatique aux sites internet et messageries.

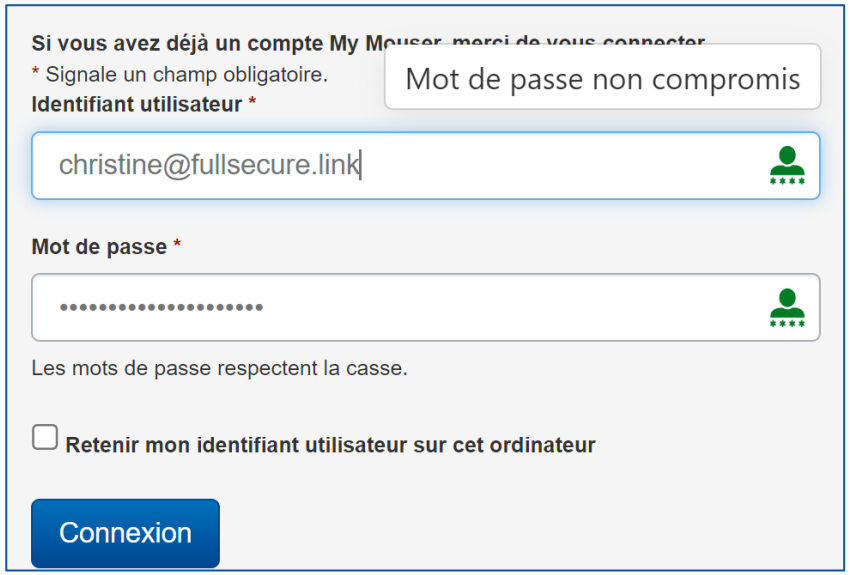
Cliquez ensuite sur l'icône « **Sauvegarder** »

Pour garantir une sécurité optimale, si le support externe n'est pas disponible ou connecté à l'ordinateur, il ne sera pas possible d'utiliser les containers chiffrés.

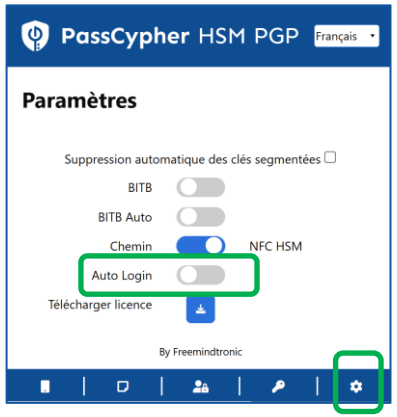




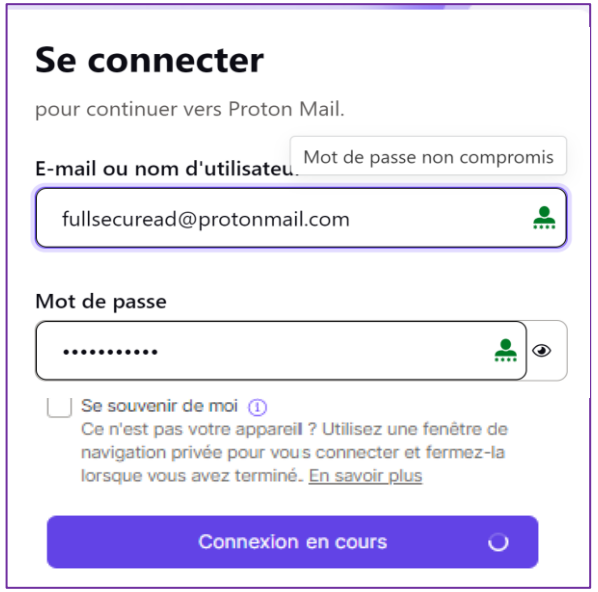
REMPLISSAGE AUTOMATIQUE VS CONNEXION AUTOMATIQUE



Les champs « Nom d'utilisateur » et « Mot de passe » sont remplis automatiquement. **Il vous reste à cliquer sur « CONNEXION »**



Pour une connexion automatique, glissez le bouton « **Autologin** » vers la droite. **Vous n'aurez plus besoin de cliquer sur « Connexion »**



Exemple d'Autologin ici. Les champs ont été remplis et la connexion est en cours sans intervention de votre part.

ACTIVEZ LA FONCTIONNALITÉ AUTOLOGIN DANS LES PARAMÈTRES DE L'EXTENSION

(tous les sites ne sont pas compatibles)

CONNECTEZ-VOUS DÈS MAINTENANT

1. Sur votre ordinateur, ouvrez le site web ou la messagerie auxquels vous souhaitez vous connecter
2. Allez sur la page de connexion [*Identifiant & mot de passe*]
3. Cliquez sur l'icône visible dans le champ de connexion
4. Les champs sont remplis automatiquement et la connexion est réalisée (**si vous avez activé l'Autologin dans les Paramètres de l'extension**)

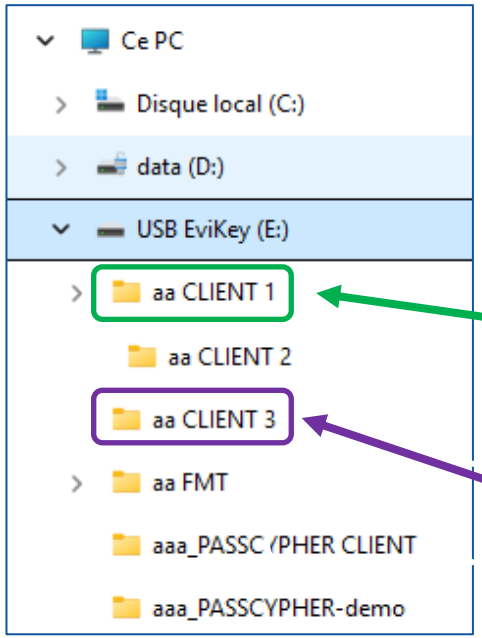
Votre mot de passe est vérifié. Le symbole vert indique que celui-ci n'a pas été compromis

Si ce symbole apparaît, cela indique que votre mot de passe est compromis. Changez-le !

CONNECTEZ-VOUS EN UN CLIC !

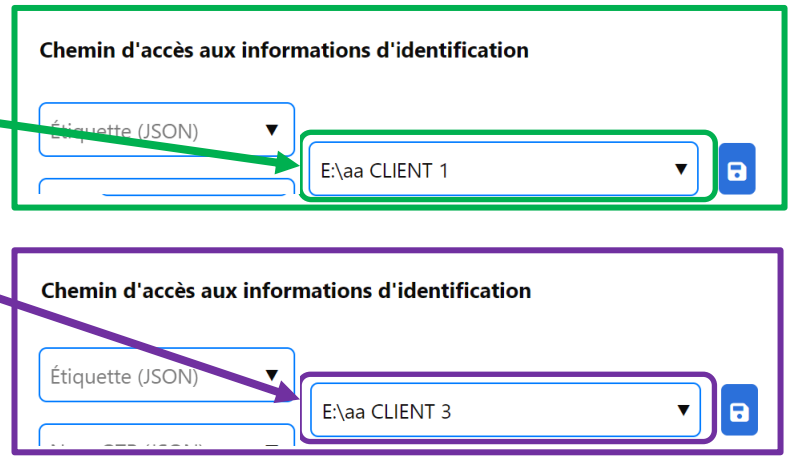
GÉREZ PLUSIEURS COMPTES

Exemple : Cabinet comptable ou juridique gérant des clients avec des comptes dans la même Banque

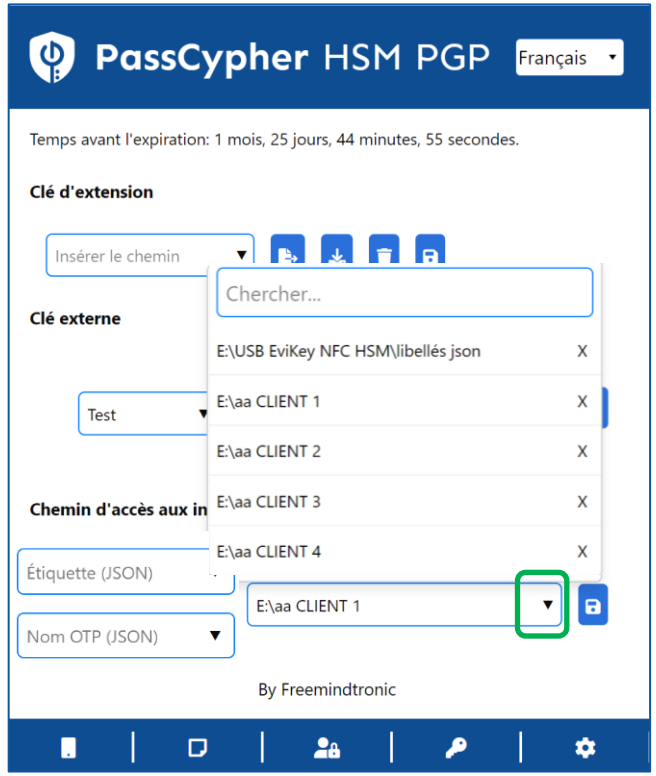


Dans chaque « **dossier client** » enregistrez les différents identifiants de connexion spécifiques à ce client.

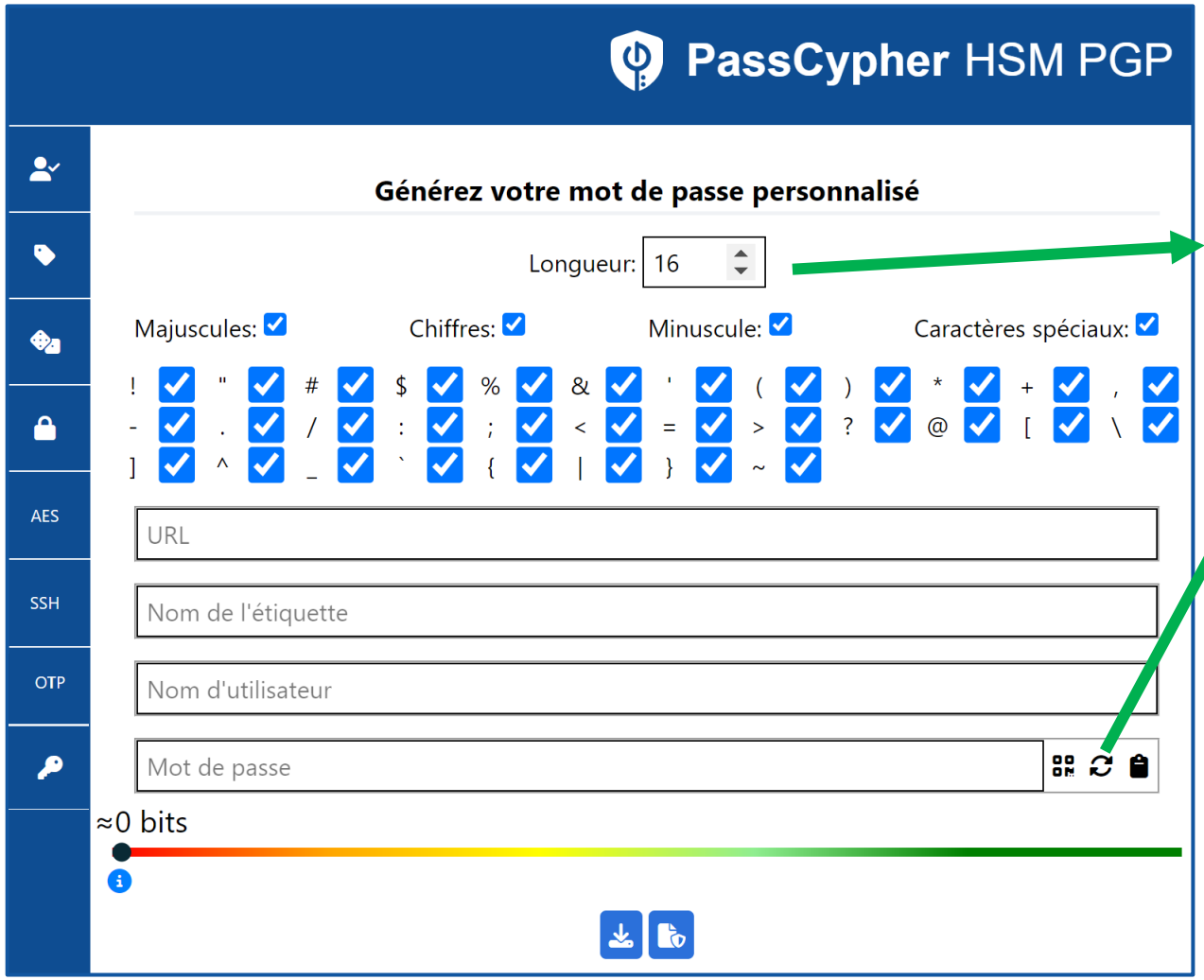
Lors de la connexion automatique, **spécifiez le chemin d'accès** dans lequel se trouvent **les identifiants du client**.



Cliquez sur le symbole indiqué pour accéder à tous les **chemins CLIENTS**. Vous pouvez **utiliser la fenêtre « Chercher »** pour aller plus vite. Cliquez sur le chemin souhaité

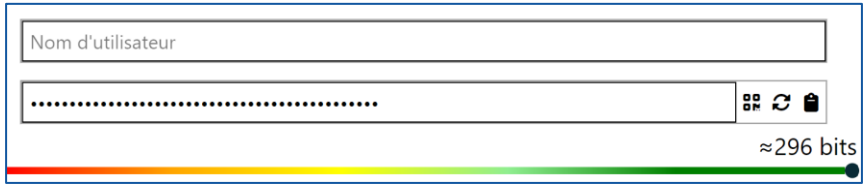


UTILISEZ LE GÉNÉRATEUR DE MOTS DE PASSE

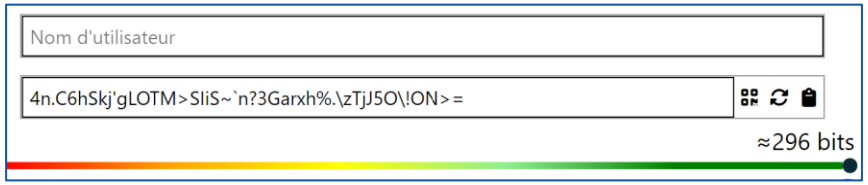


Par défaut la longueur du mot de passe est de 16 caractères, vous pouvez la modifier depuis la fenêtre.

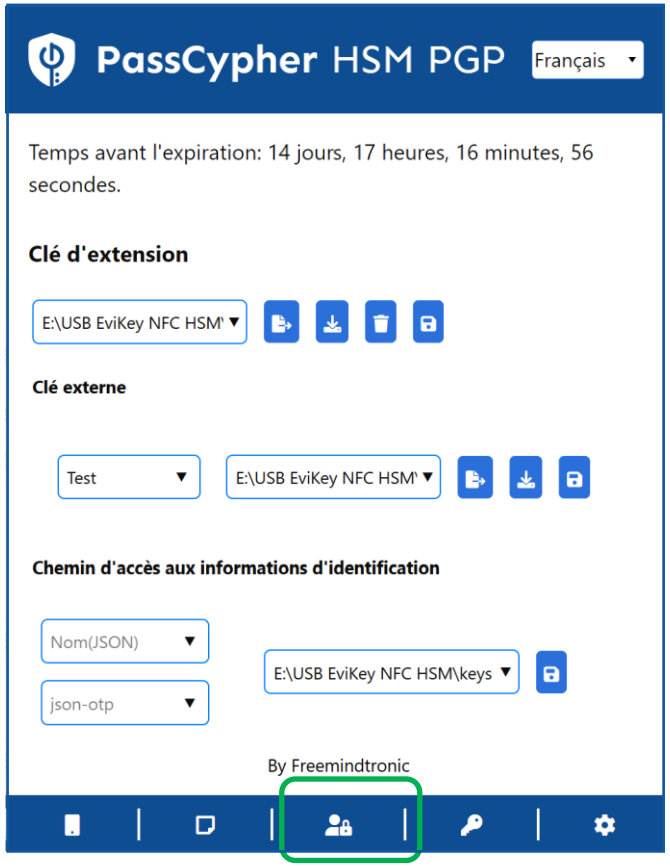
Cliquez ensuite pour générer le mot de passe (ici 45 caractères)



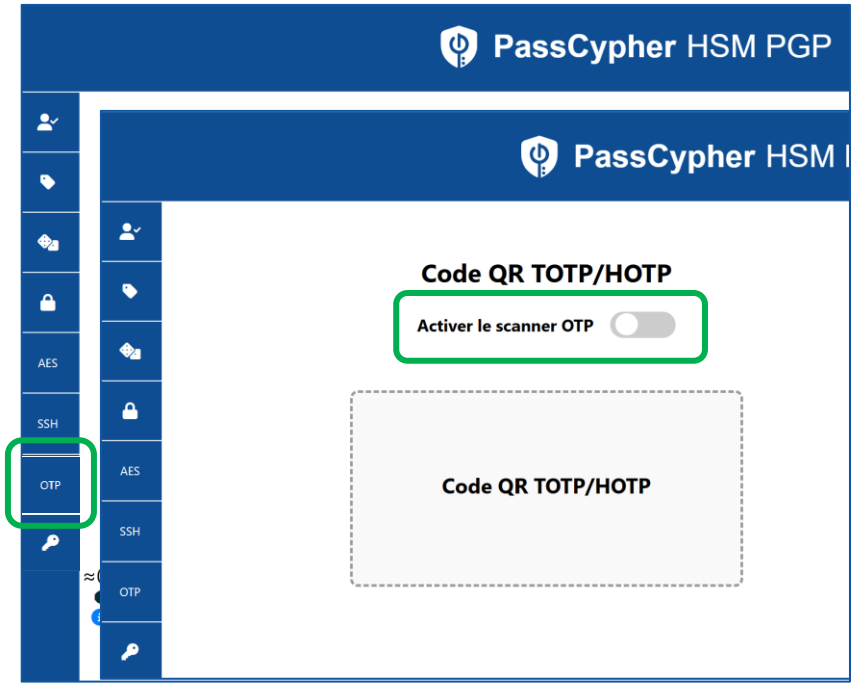
En passant votre souris sur le champ, vous verrez le mot de passe affiché en clair.



GÉREZ VOS TOTP/HOTP (2FA)



Ouvrez l'extension puis **cliquez sur l'icône indiquée** pour gérez vos OTP



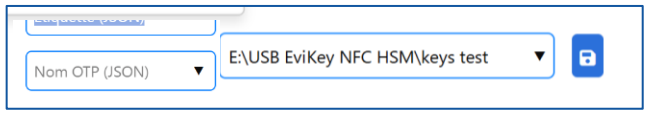
Cliquez sur « **OTP** ». Une nouvelle fenêtre s'ouvre. **Glissez/Déposez** le fichier ou activez le **scanner OTP**

Positionnez le **QR code à scanner** dans le champ de la caméra

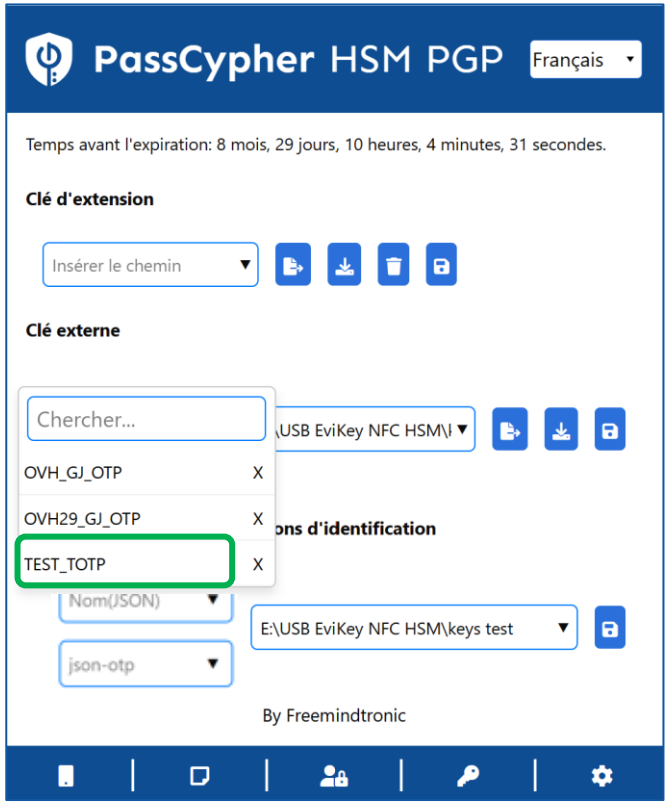
GÉREZ VOS TOTP/HOTP (2FA) 2/2

Le type d'OTP est détecté. Donnez un nom à ce code OTP, inscrivez l'URL associée et **cliquez sur l'icône** pour générer un fichier .json

Récupérez le fichier dans vos **Téléchargements** et placez-le dans le **dossier adéquat (voir page 19)**.

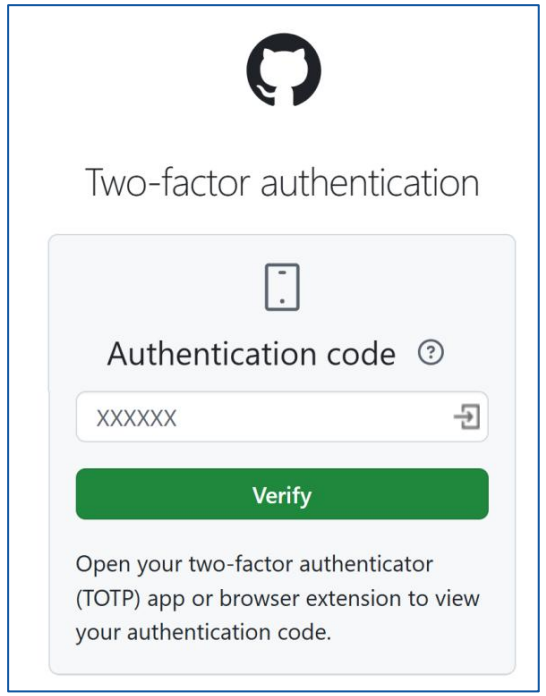


Dans cet exemple, le fichier est **sauvegardé dans une clé USB**

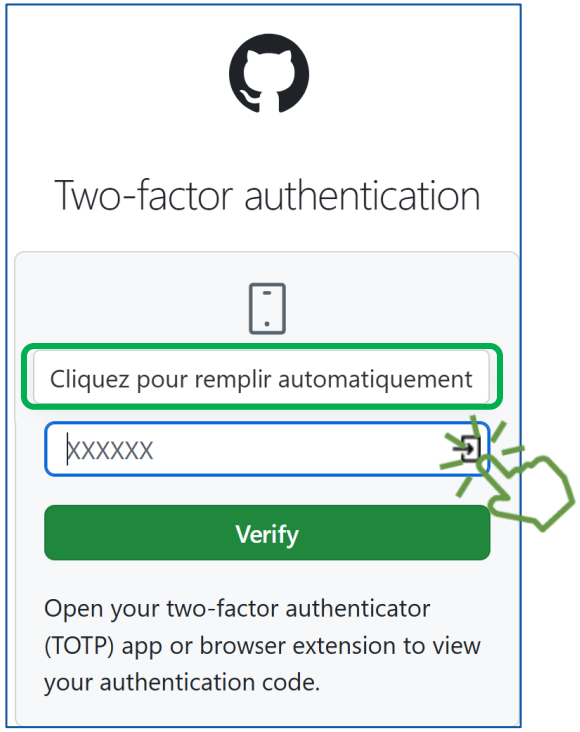


Le fichier « **.json** » créé est automatiquement ajouté dans l'extension à la liste de tous les OTP créés.

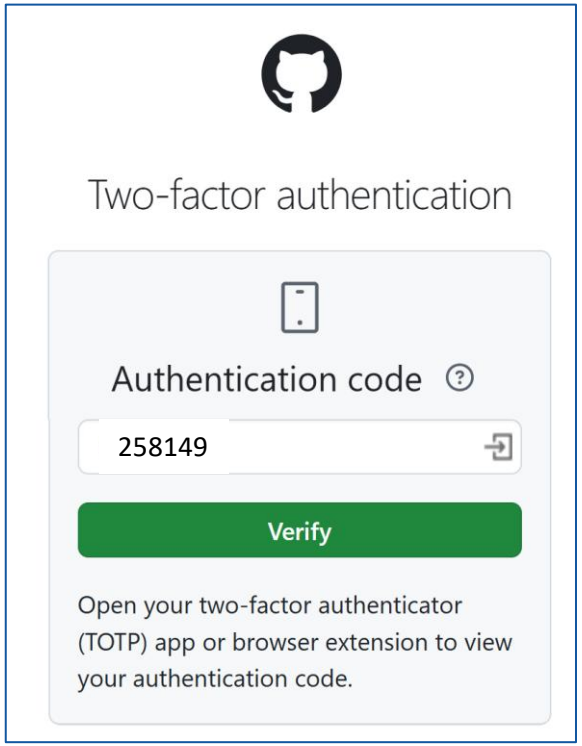
AUTHENTIFIEZ-VOUS AVEC L'OTP



Si vous avez activé la double authentification sur un site voilà le type de page qui s'affiche

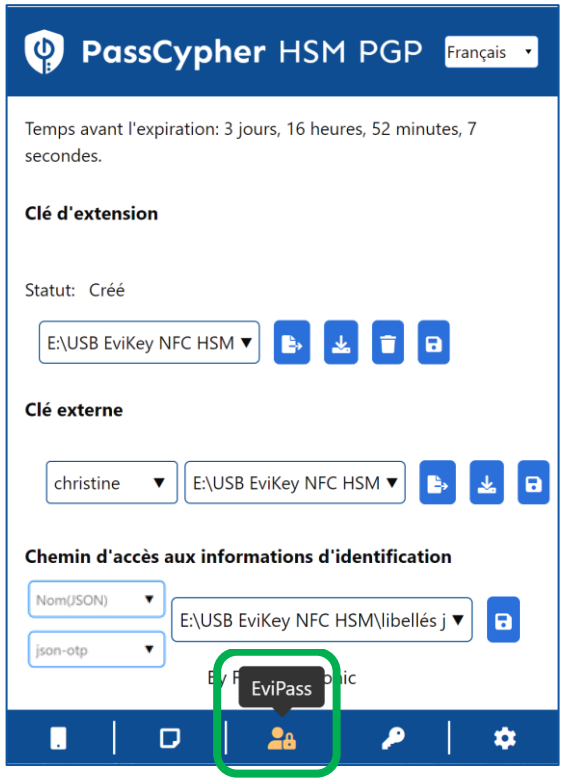


Cliquez sur l'icône indiquée, automatiquement le code sera inséré dans le champ…

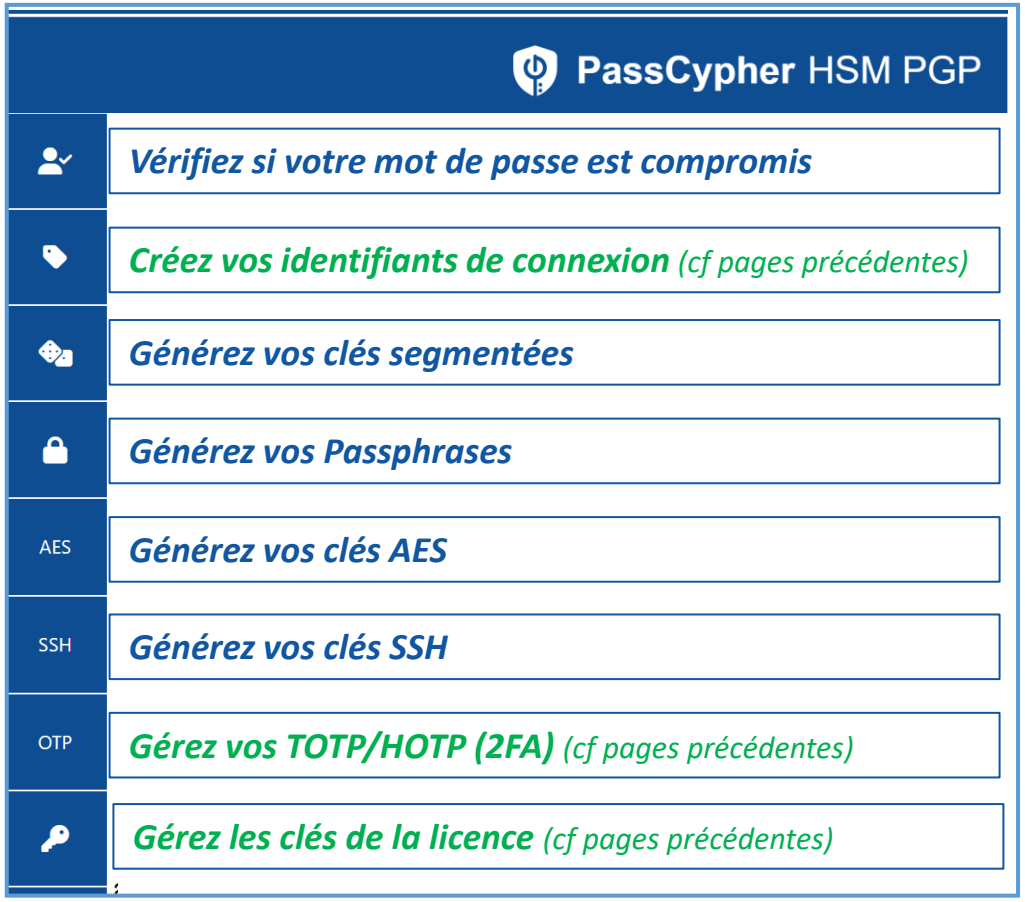


… et la connexion sera réalisée

FONCTIONNALITÉS EVIPASS

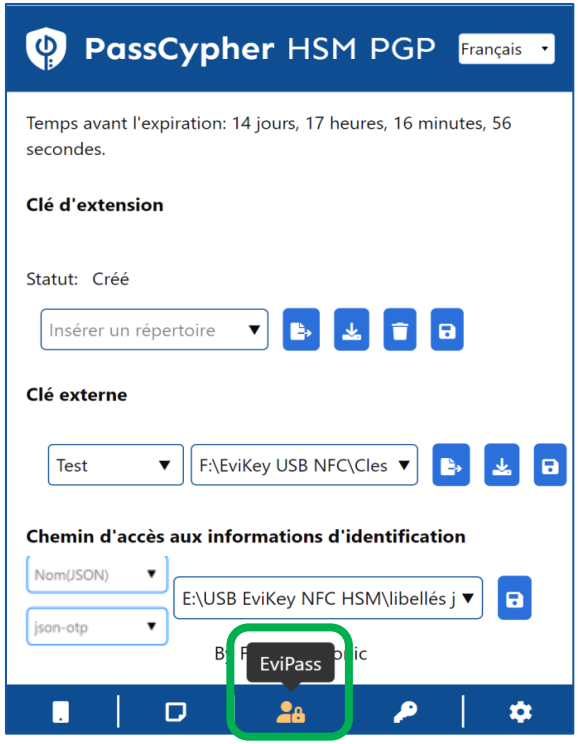


Cliquez sur l'icône indiquée pour accéder à toutes les fonctionnalités disponibles

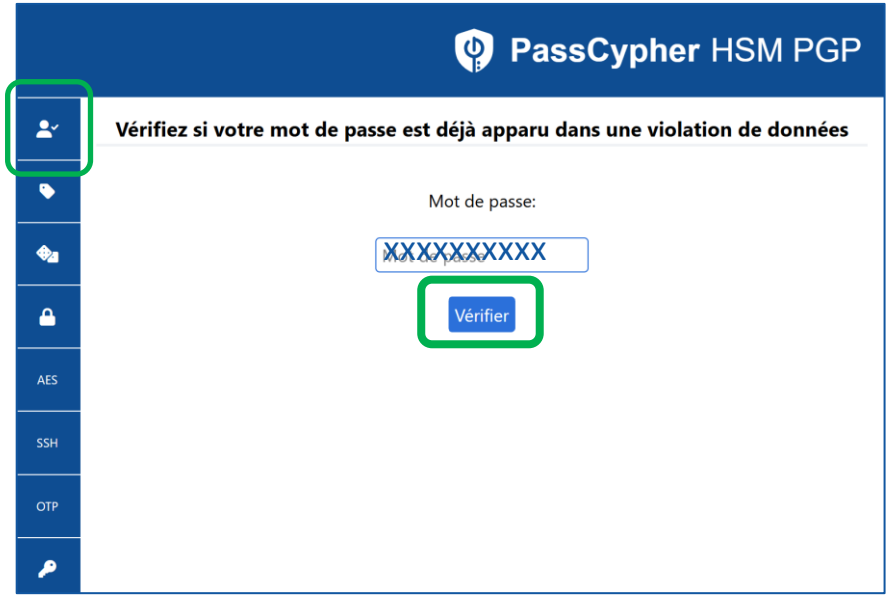


Les fonctionnalités écrites en bleu sont expliquées dans les pages suivantes.

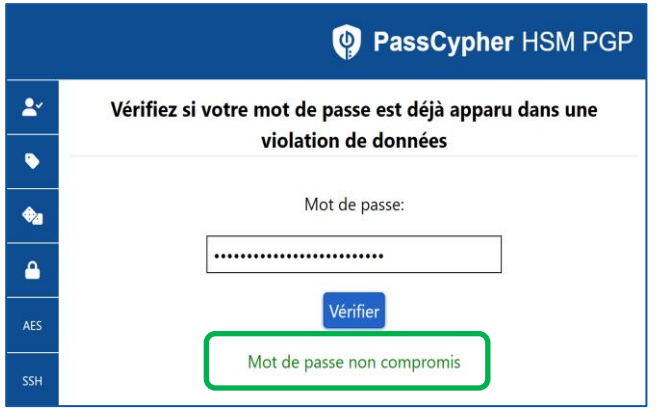
EVIPASS (VÉRIFICATION MOT DE PASSE) 1/5



Cliquez sur l'icône indiquée pour accéder à la vérification de vos mots de passe

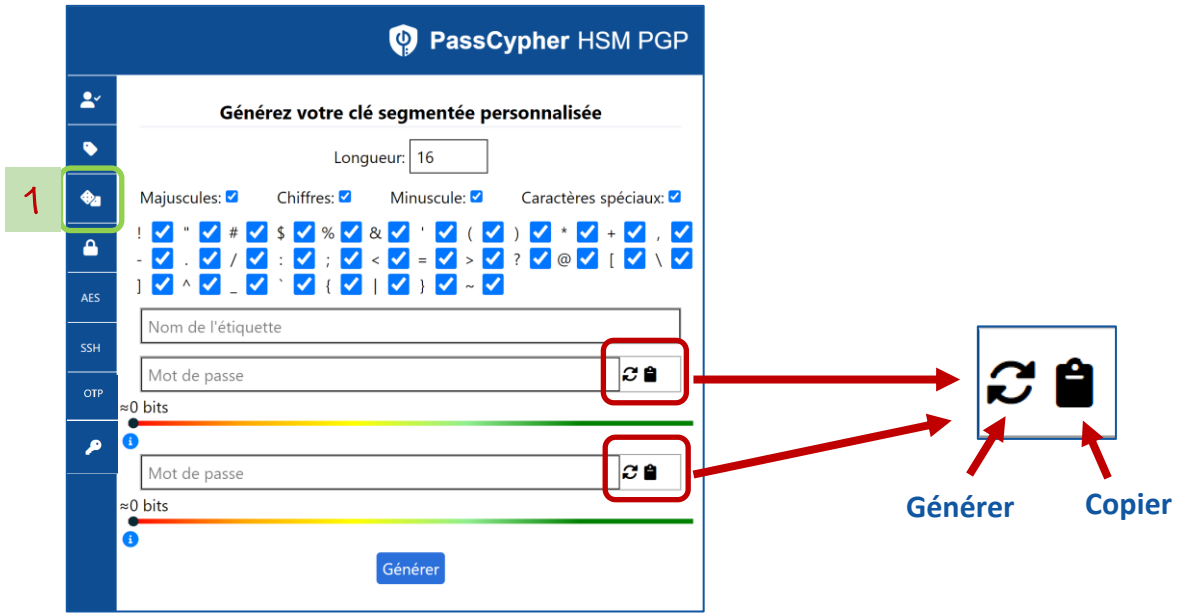


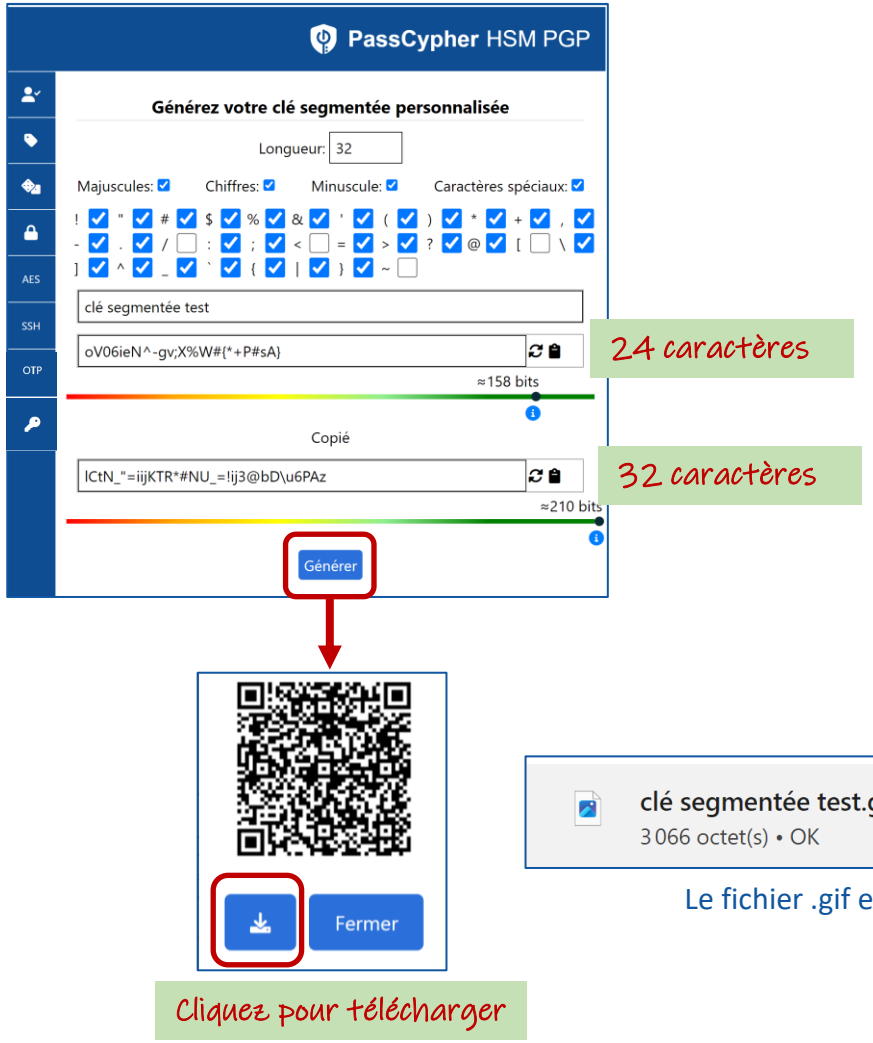
Cliquez sur l'icône indiquée pour vérifier si votre **mot de passe est corrompu**. Ecrivez votre mot de passe dans le champ indiqué et cliquez sur « **Vérifier** ». Le résultat s'affiche.



EVIPASS (CLÉ SEGMENTÉE) 2/5

Fonctionnalité réservée aux entités régaliennes et Sécurité IoT



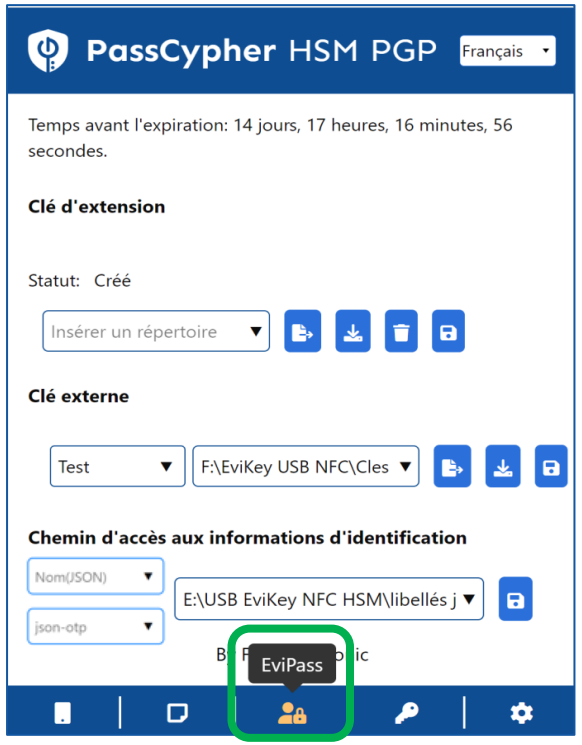


1. **Cliquez sur l'icône indiquée (1).** Une fenêtre apparaît
2. Donnez un nom à la clé segmentée
3. Choisissez la longueur d'un segment (nombre de caractères). Cette longueur peut être différente pour les deux segments
4. Choisissez les caractères : décochez certains caractères si besoin. Cliquez ensuite sur l'icône pour **générer** le segment.

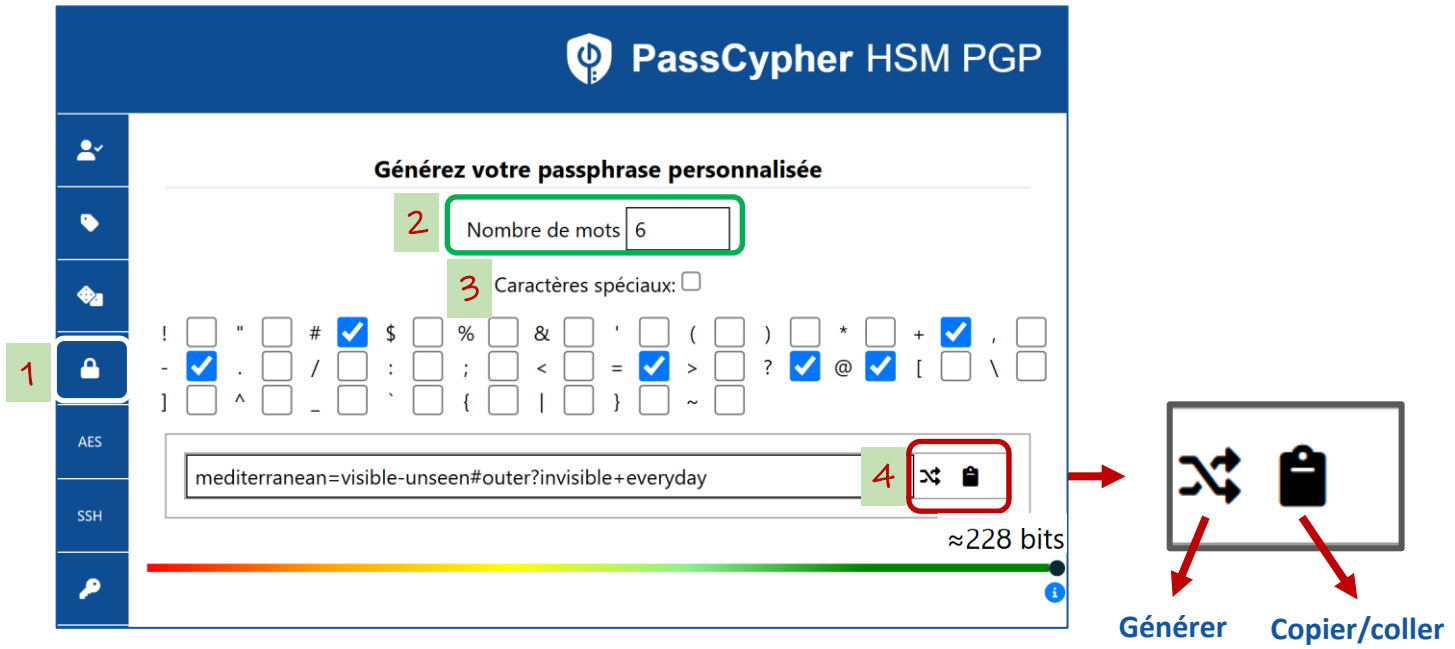
Vous pouvez **copier** ce segment dans le presse papiers.

Cliquez sur l'icône pour **générer** la clé segmentée aléatoirement.

EVIPASS (PASSPHRASE)

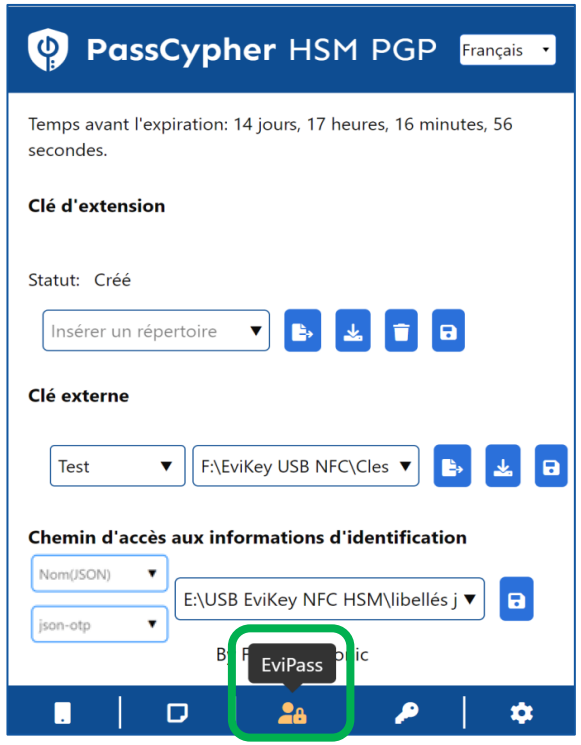


Cliquez sur l'icône indiquée pour accéder aux fonctionnalités de création de Passphrase

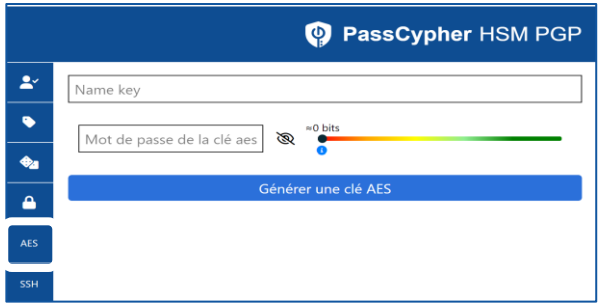


1. Cliquez sur l'icône indiquée pour générer une passphrase
2. Choisissez le nombre de mots de la passphrase
3. Choisissez les caractères qui vont séparer les mots
4. Cliquez sur l'icône pour générer la passphrase. Vous pouvez copier/coller cette passphrase.

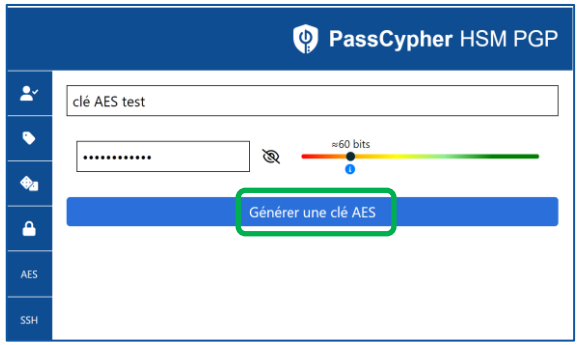
EVIPASS (CLÉ AES)



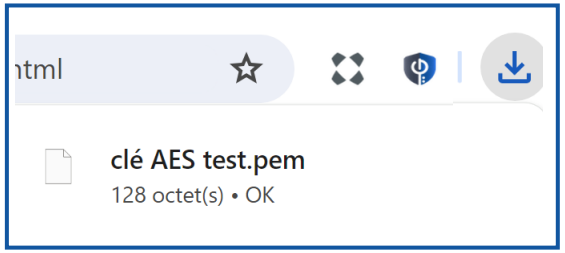
Cliquez sur l'icône indiquée



Cliquez sur l'icône indiquée pour accéder à la génération de clé AES

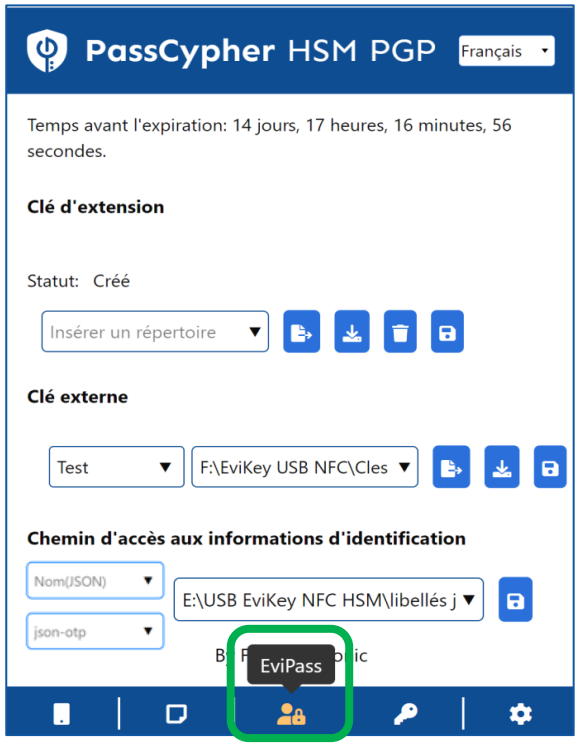


Donnez un nom à la clé, saisissez un mot de passe puis cliquez sur « **Générer une clé AES** »

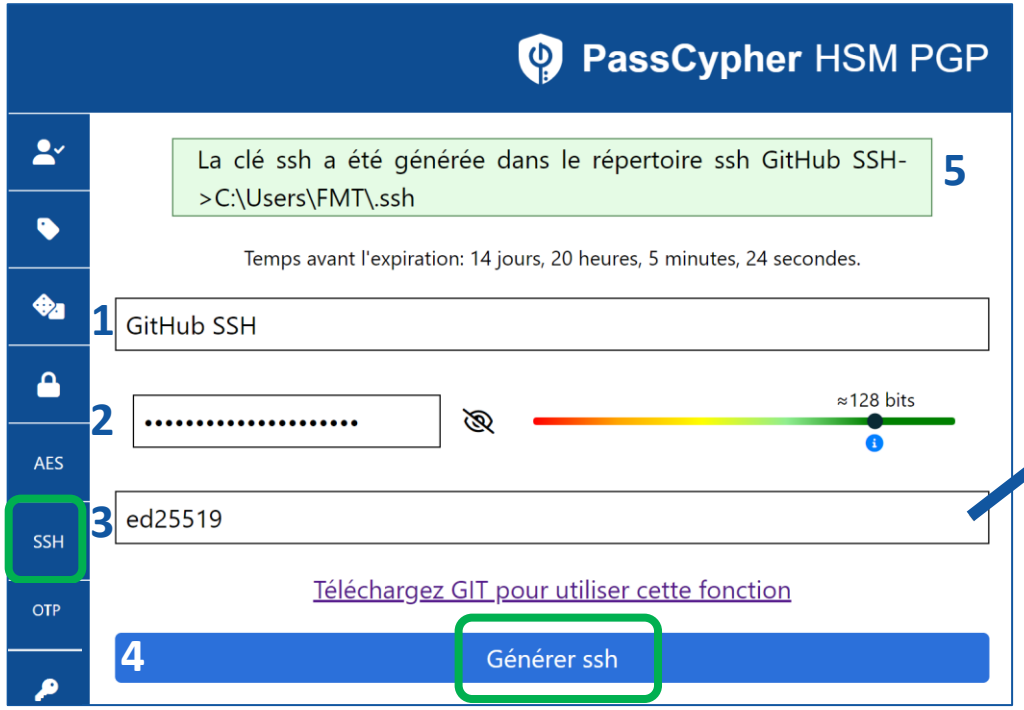


Le fichier .pem est généré. Vous pouvez le sauvegarder où vous voulez

EVIPASS (CLÉ SSH)



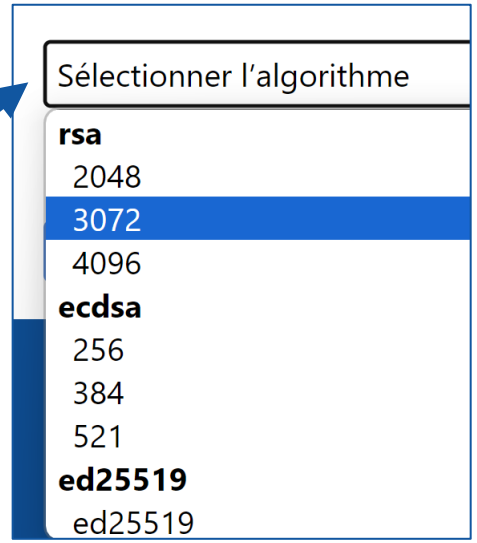
Cliquez sur l'icône indiquée pour accéder aux fonctionnalités de création de clé SSH



Cliquez sur l'icône « **SSH** » et compléter les différents champs :

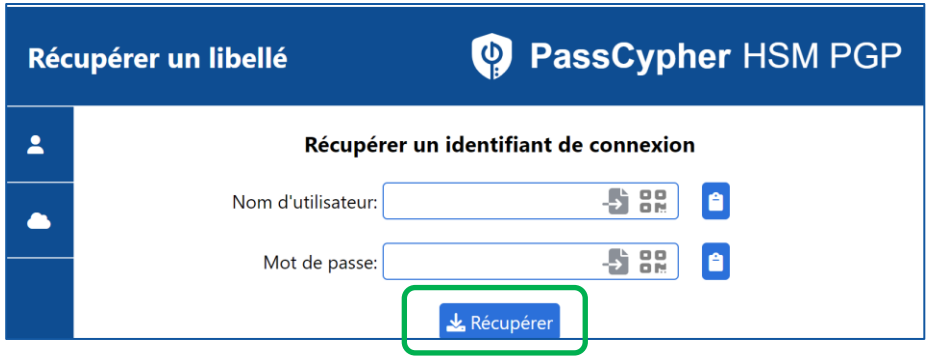
1. **Nom** de la clé
2. **Mot de passe** associé à la clé
3. Sélectionnez **l'algorithme**
4. Cliquez enfin sur « **Générer ssh** »
5. L'emplacement où est **stockée** la clé apparaît en haut de la fenêtre

3. Algorithmes disponibles

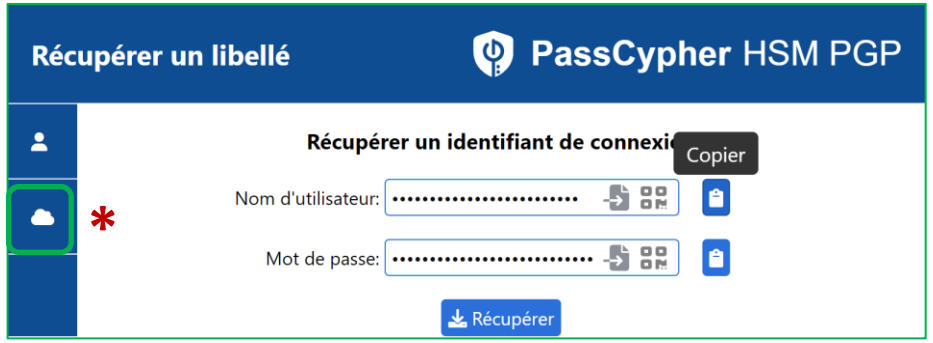


RÉCUPÉRER UN LIBELLÉ

Sur la page d'accueil de l'extension, **écrivez le nom du libellé** concerné puis cliquer sur l'icône « **Sauvegarder** ». Cliquez ensuite sur l'icône indiquée pour accéder à la récupération d'un libellé



Une fenêtre s'ouvre, cliquez sur « **Récupérer** »



Les informations s'affichent à l'écran : nom d'utilisateur et mot de passe. Cliquez pour copier les informations utiles

(*) La récupération d'une clé Cloud se fait uniquement à partir d'un dispositif NFC

LA CLÉ D'EXTENSION EN DÉTAIL

Lorsque la clé d'extension est générée, la fenêtre ci-dessous s'affiche.

Par défaut, cette clé est sauvegardée dans le local storage de votre navigateur web.
Vous pouvez ne rien faire de plus, tout fonctionne. Cependant, plusieurs options sont disponibles.

1. Vous pouvez définir et insérer un chemin pour enregistrer cette clé. Vous pouvez définir plusieurs chemins

2. En cliquant sur cette icône, la clé sera enregistrée dans le chemin indiqué

3. Vous pouvez importer la clé (fichier.eppc) et l'enregistrer à l'endroit de votre choix comme sauvegarde de sécurité

4. En cliquant sur cette icône vous supprimez la clé du local storage

5. N'oubliez pas de cliquer pour sauvegarder le chemin défini

LA CLÉ EXTERNE EN DÉTAIL

Vous pouvez créer plusieurs clés externes en lien avec une même clé d'extension

Cela permet à plusieurs personnes d'utiliser PassCypher sur le même ordinateur en utilisant chacun sa propre clé.

1. Définissez un nom pour la clé externe qui va être créée. Vous pourrez définir plusieurs clés différentes

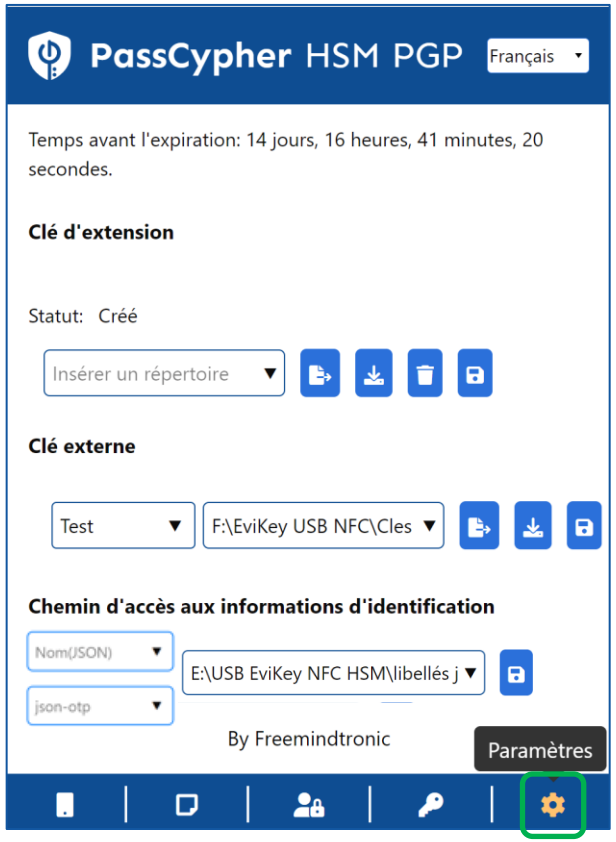
2. Insérez le chemin où sera stockée la clé externe. Vous pouvez définir plusieurs chemins

3. Cliquez pour créer et exporter la clé

4. En cliquant sur cette icône vous pouvez télécharger la clé et la sauvegarder à l'endroit de votre choix

5. N'oubliez pas de cliquer pour sauvegarder le chemin défini

PARAMÈTRES & FONCTIONNALITÉS



Cliquez sur l'icône « **Paramètres** »

Une fenêtre s'ouvre avec différentes options que vous pouvez activer

(*) Fonctionnement explicité dans ce tuto : enregistrement des clés segmentées dans des chemins spécifiques

(**) lorsque la licence expire, il y a effacement automatique de la clé pour des mesures de cybersécurité surtout s'il s'agit d'un usage temporaire sur un ordinateur qui n'est pas celui de l'utilisateur.

(***) Consultez le Tutoriel Extension PassCypher avec dispositif NFC https://freemindtronic.com/how-it-works-products-in-depth-guide-to-fullsecure/

Take back control, Take back power

EviPass Technology

By Freemindtronic Andorra

En savoir plus : https://www.freemindtronic.com

Freemindtronic **Chaine Freemindtronic**