

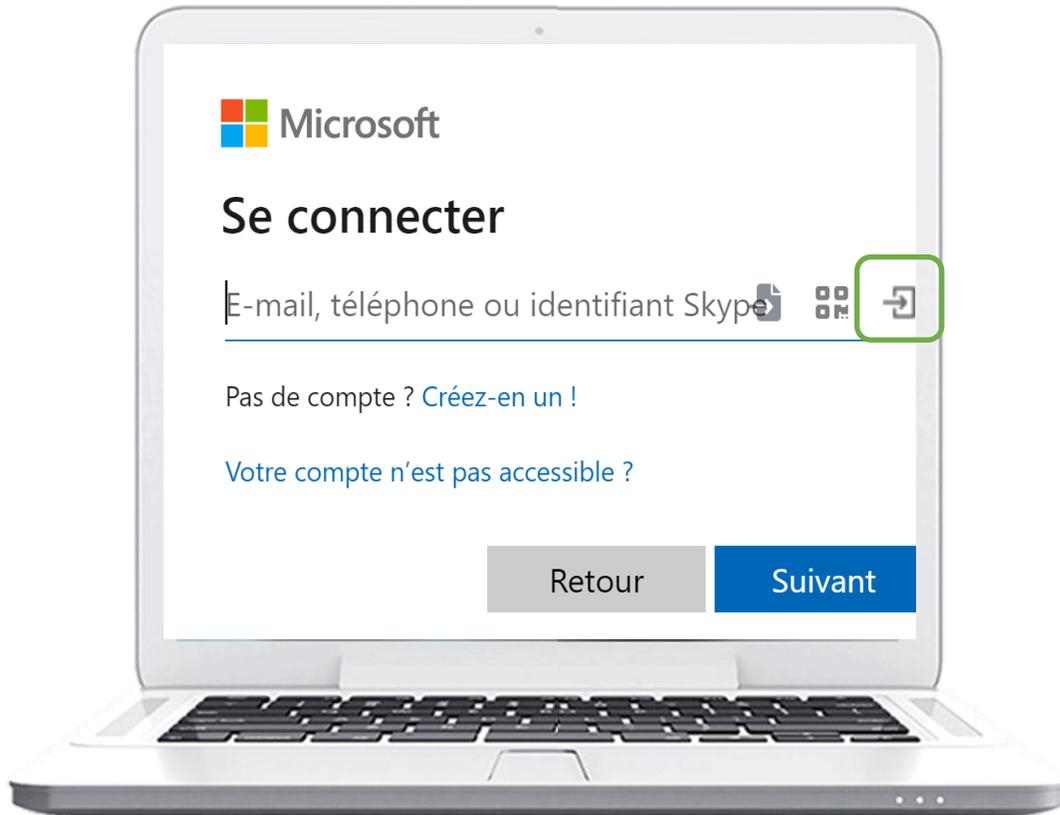
TUTORIEL EXTENSION PASSCYPHER HSM PGP

By Freemindtronic Andorra

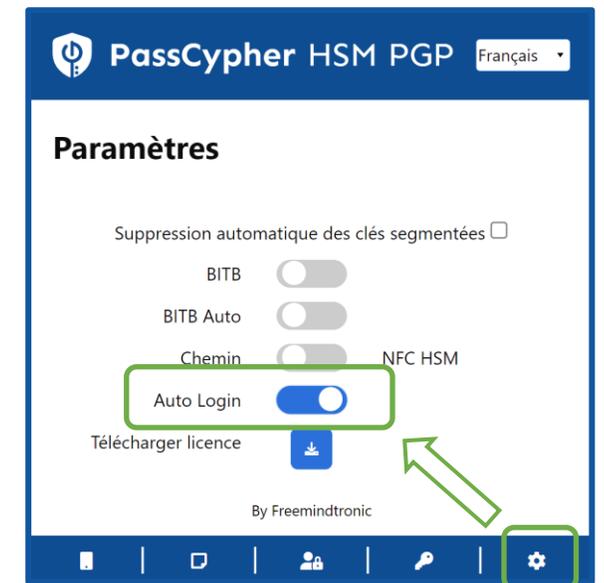
Sans serveur, sans base de données, sans identification
« Zero Trust & Zero Knowledge »



Connexion automatique instantanée



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



() Activez la fonction « Auto Login » dans les Paramètres de l'extension*

SOMMAIRE

- Installation de l'extension PassCypher HSM PGP
- Activation de la licence
- Principes de fonctionnement
- Page d'accueil en détail
- Création des clés segmentées
- Clé d'extension et clé externe en détail
- Connexion automatique aux sites internet et messageries
- Création et sauvegarde des identifiants de connexion
- Fonctionnalités EviPass
- Génération d'une clé SSH
- Récupération d'un libellé
- Paramètres et fonctionnalités



INSTALLATION DE L'EXTENSION

Téléchargez et installez l'extension PassCypher HSM PGP

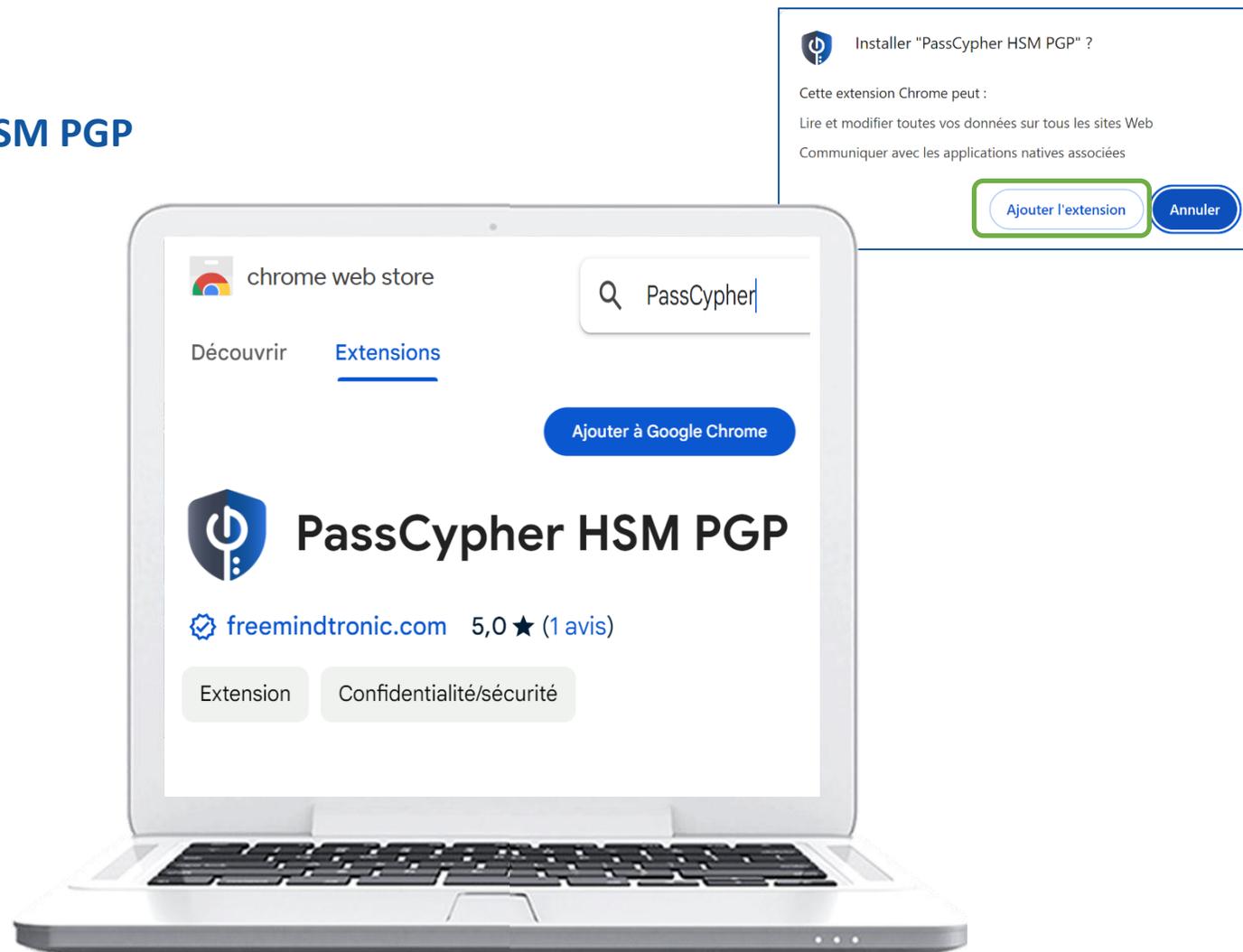
CHROME : [chrome web store](#)

BRAVE : [chrome web store](#)

OPERA : [chrome web store](#)

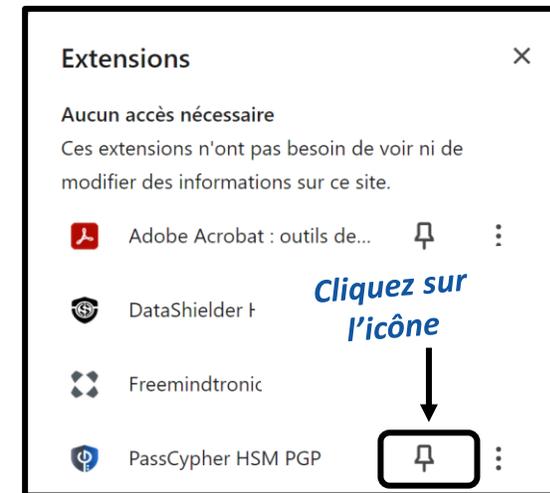
MICROSOFT EDGE : [PassCypher HSM PGP - Microsoft Edge Addons](#)

FIREFOX : en cours



FINALISATION DE L'INSTALLATION

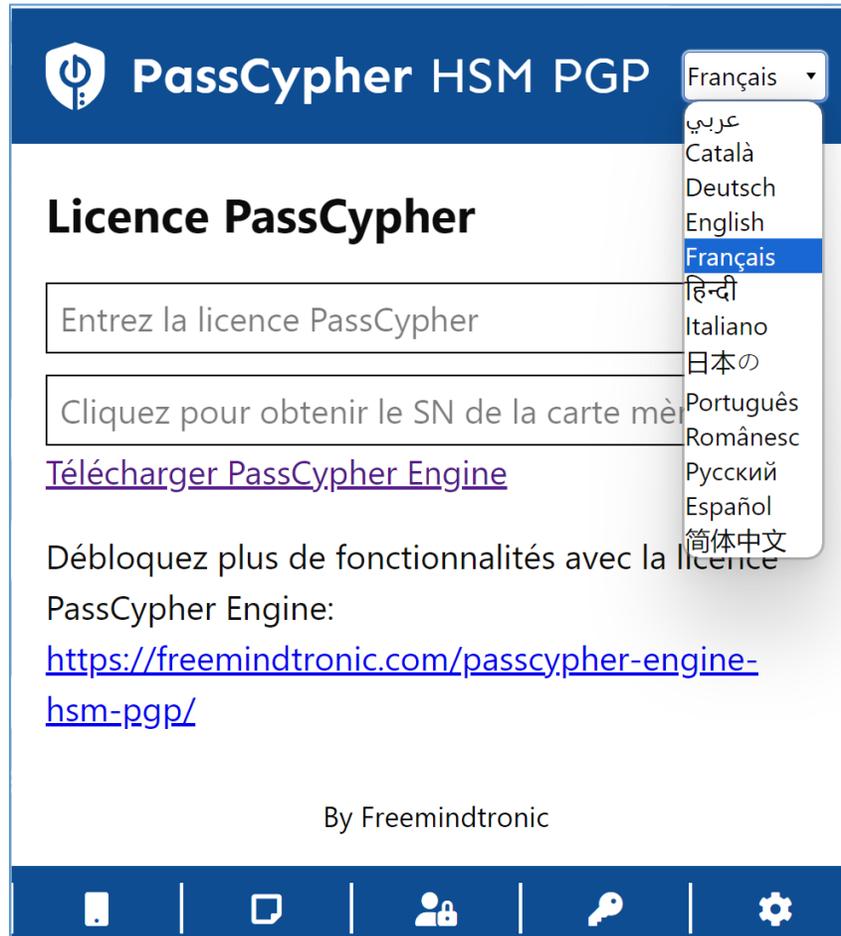
Cliquez sur cette icône pour accéder aux extensions



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



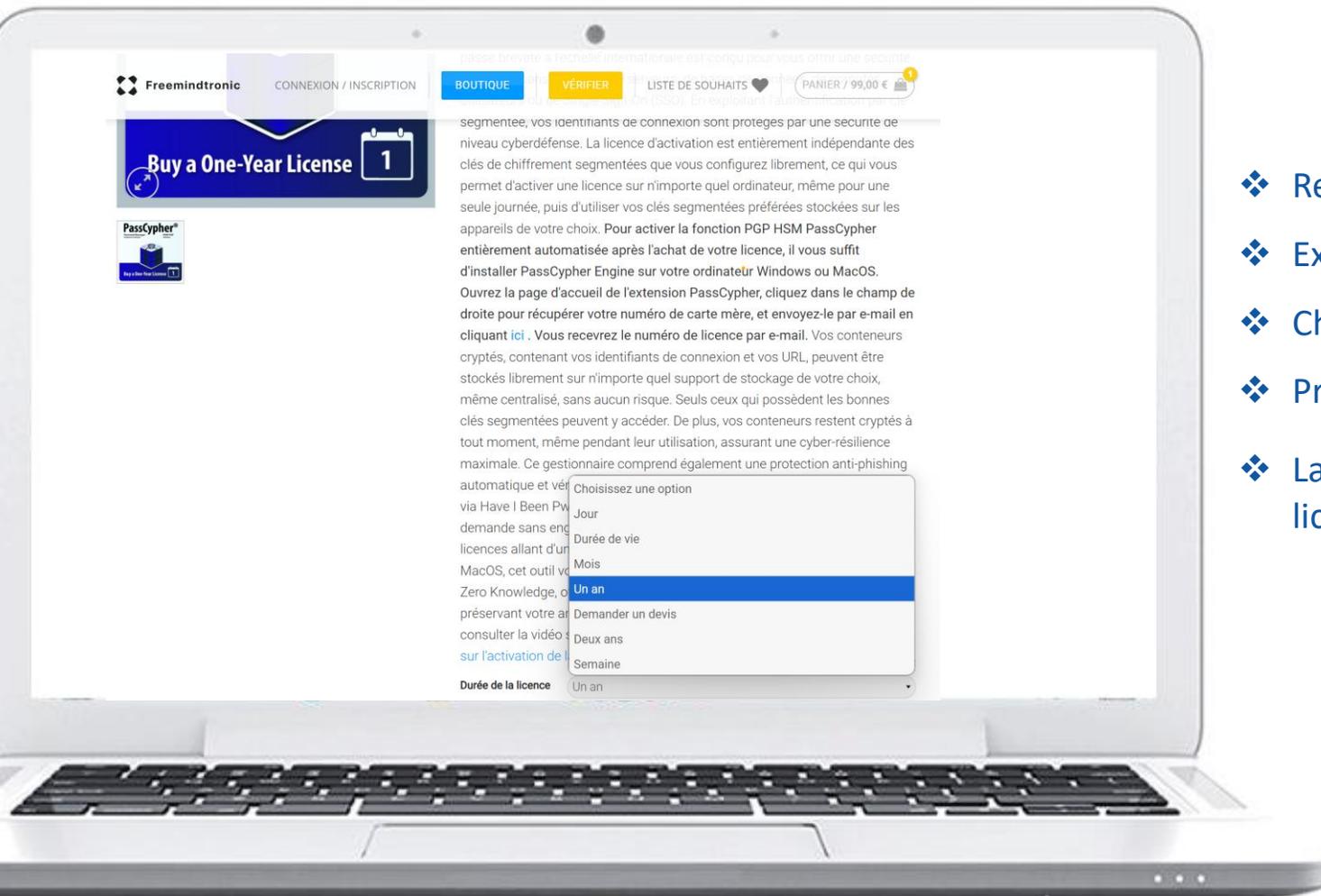
EXTENSION MULTILANGUES



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

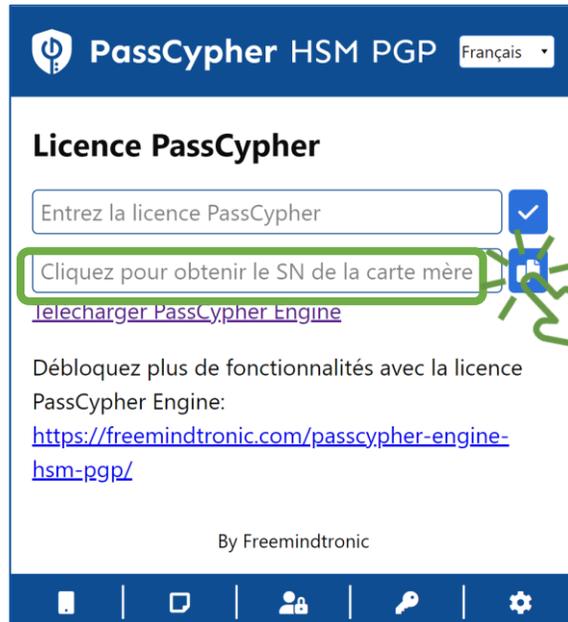
Vous pouvez choisir dans quelle langue afficher l'extension.

ACHAT DE LA LICENCE

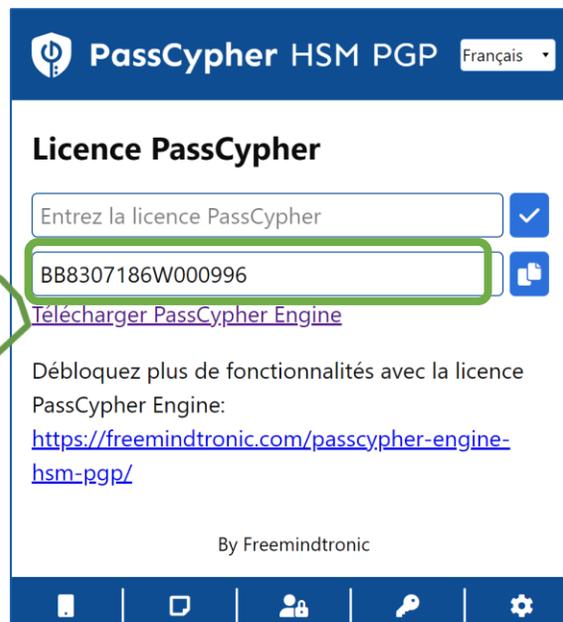


- ❖ Rendez-vous sur la boutique [FREEMINDTRONIC](#)
- ❖ Extension « **PassCypher HSM PGP Password Manager** »
- ❖ Choisissez l'option qui vous convient le mieux
- ❖ Procédez au paiement
- ❖ La slide suivante vous explique comment activer votre licence

ACTIVATION DE LA LICENCE



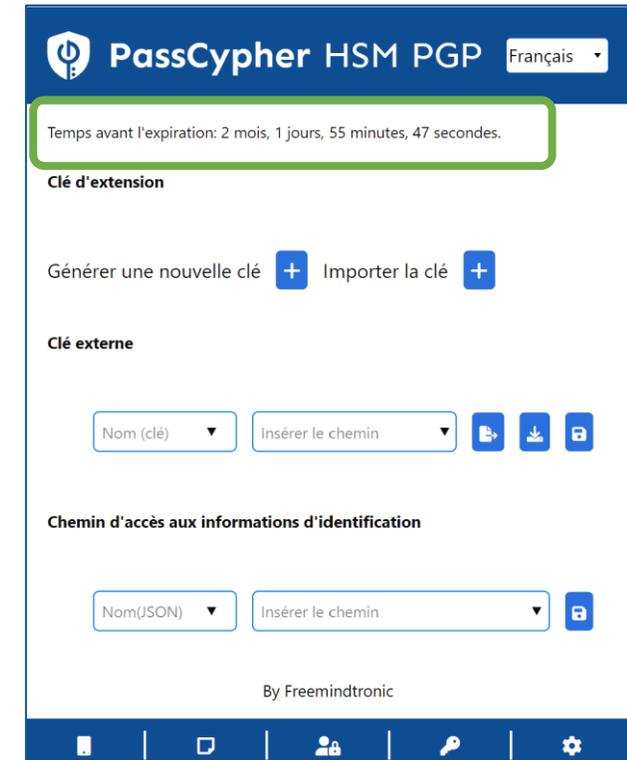
Cliquez sur « [Télécharger Engine](#) » et installez le logiciel (Windows ou MacOS). Cliquez ensuite pour obtenir le **n° de série de la carte mère** de votre ordinateur



Envoyez ce numéro par mail à **fullsecure [a] 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*

Allez dans « [Téléchargements](#) » et cliquez sur le fichier

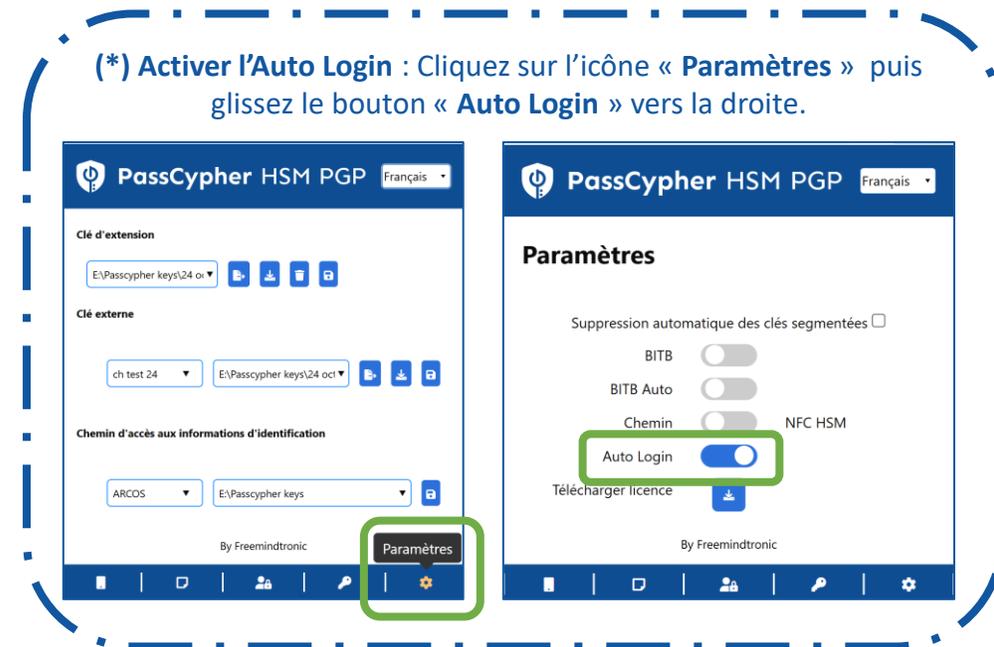
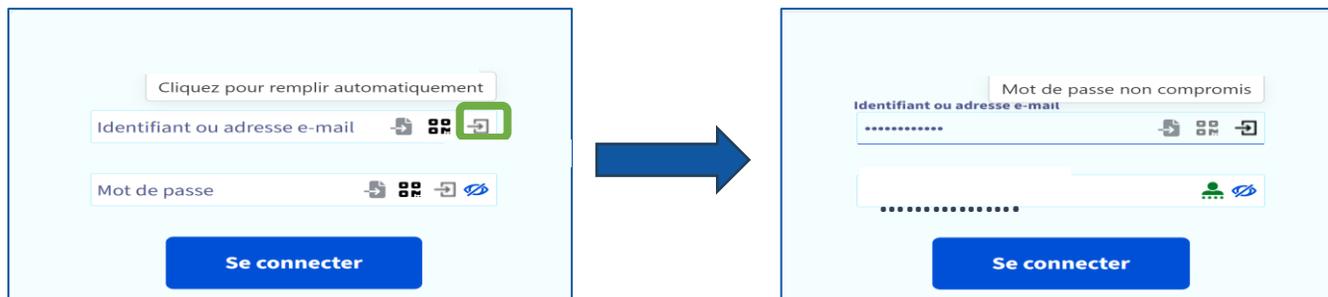
 [PassCypherEngine_1.3.0_x64 \(3\).exe](#)

 [YouTube](#) [Installer PassCypher Engine](#)

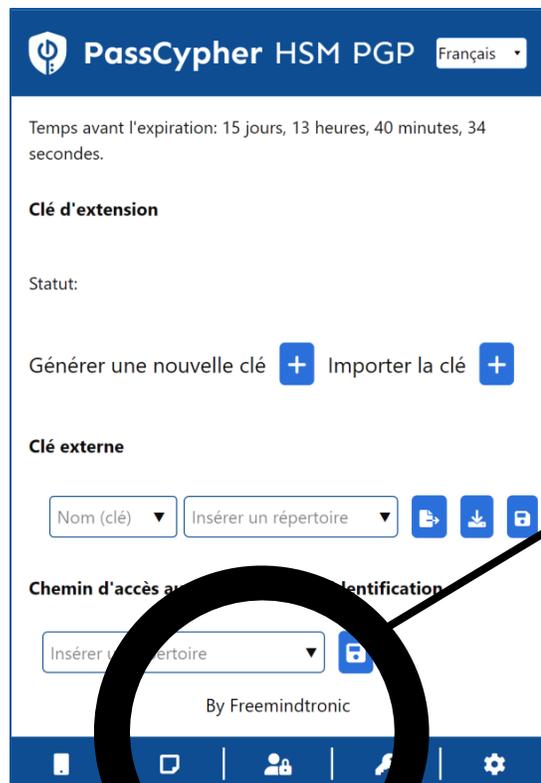
(*) Il existe plusieurs abonnements disponibles : au jour, à la semaine, au mois ou à l'année

Comment cela fonctionne ?

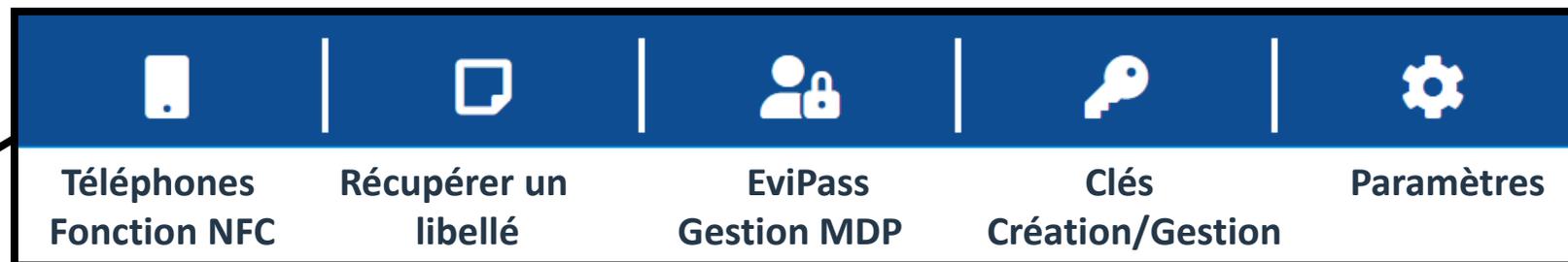
- **PassCypher HSM PGP** est une extension pour navigateurs Web qui permet une **connexion automatique instantanée**
- Un **système breveté d'authentification par clés segmentées** est implémenté
- Vous bénéficiez d'une **sécurité maximale** ainsi que d'une **rapidité d'exécution inégalable**
- **Cliquez 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***)



La page d'accueil en détail



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



Retrouvez toutes les fonctionnalités expliquées dans ce tutoriel

Créez vos clés segmentées

PassCypher HSM PGP Français

Temps avant l'expiration: 15 jours, 13 heures, 40 minutes, 34 secondes.

Clé d'extension

Statut:

Générer une nouvelle clé **+** Importer la clé **+** *

Clé externe

Nom (clé) ▼ Insérer un répertoire ▼

Chemin d'accès aux informations d'identification

json-name ▼ Insérer un répertoire ▼

By Freemindtronic

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

PassCypher HSM PGP Français

Temps avant l'expiration: 15 jours, 13 heures, 34 minutes, 45 secondes.

Clé d'extension

Statut: Créé

Insérer un répertoire ▼

Clé externe

Nom (clé) ▼ Insérer un répertoire ▼

Chemin d'accès aux informations d'identification

json-name ▼ Insérer un répertoire ▼

By Freemindtronic

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...)**

PassCypher HSM PGP Français

Temps avant l'expiration: 15 jours, 2 minutes, 59 secondes.

Clé d'extension

Statut: Créé

Insérer un répertoire ▼

Clé externe

Test ▼ F:\EviKey USB NFC\Cles ▼

Chemin d'accès aux informations d'identification

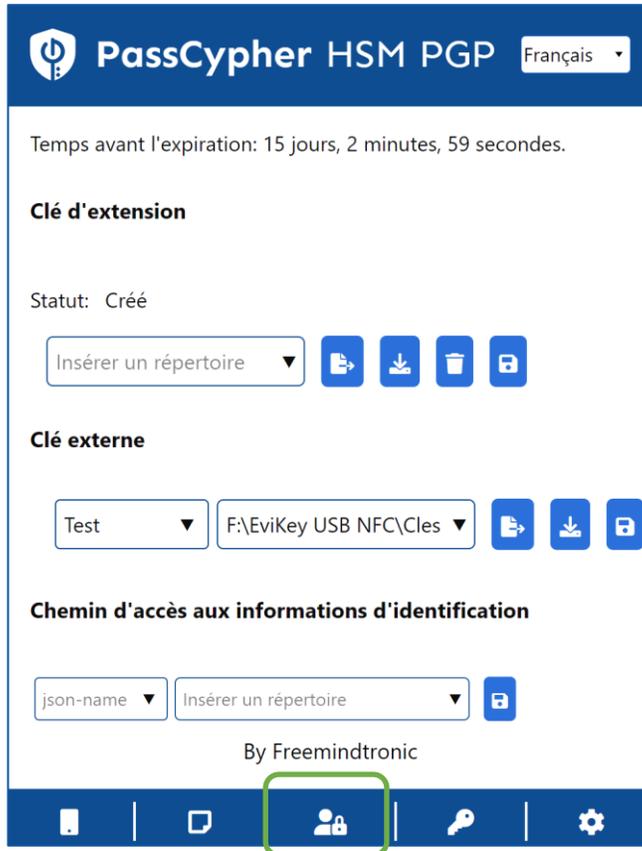
json-name ▼ Insérer un répertoire ▼

By Freemindtronic

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

(*) Si une clé segmentée (clé d'extension et clé externe) existe déjà, voir le processus d'installation dans slides suivantes

Partagez vos clés de chiffrement segmentées



PassCypher HSM PGP Français

Temps avant l'expiration: 15 jours, 2 minutes, 59 secondes.

Clé d'extension

Statut: Créé

Insérer un répertoire [icônes]

Clé externe

Test F:\EviKey USB NFC\Cles [icônes]

Chemin d'accès aux informations d'identification

json-name Insérer un répertoire [icône]

By Freemindtronic

[icône] [icône] [icône] [icône]

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



PassCypher HSM PGP

Chiffrer/Déchiffrer la clé segmentée

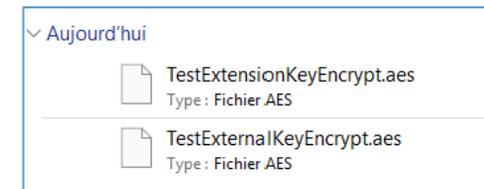
Glisser-déposer .aes pour déchiffrer la clé segmentée

Mot de passe

Chiffrer Déchiffrer

Mot de passe obligatoire pour la clé privée

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



Aujourd'hui

- TestExtensionKeyEncrypt.aes
Type : Fichier AES
- TestExternalKeyEncrypt.aes
Type : Fichier AES

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

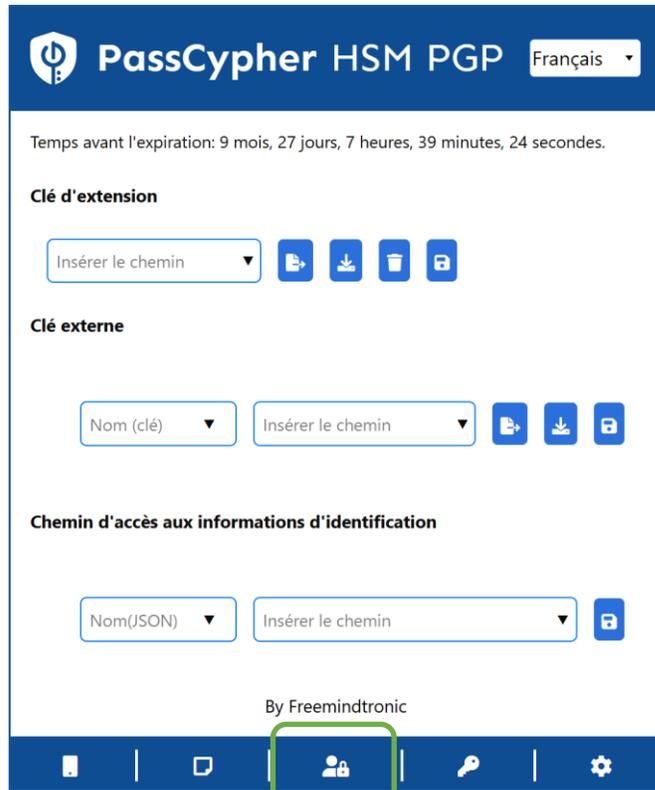


Envoyez ces 2 fichiers par **mail** (ou autre) à votre correspondant et indiquez-lui le mot de passe par un autre canal (**SMS** par exemple).

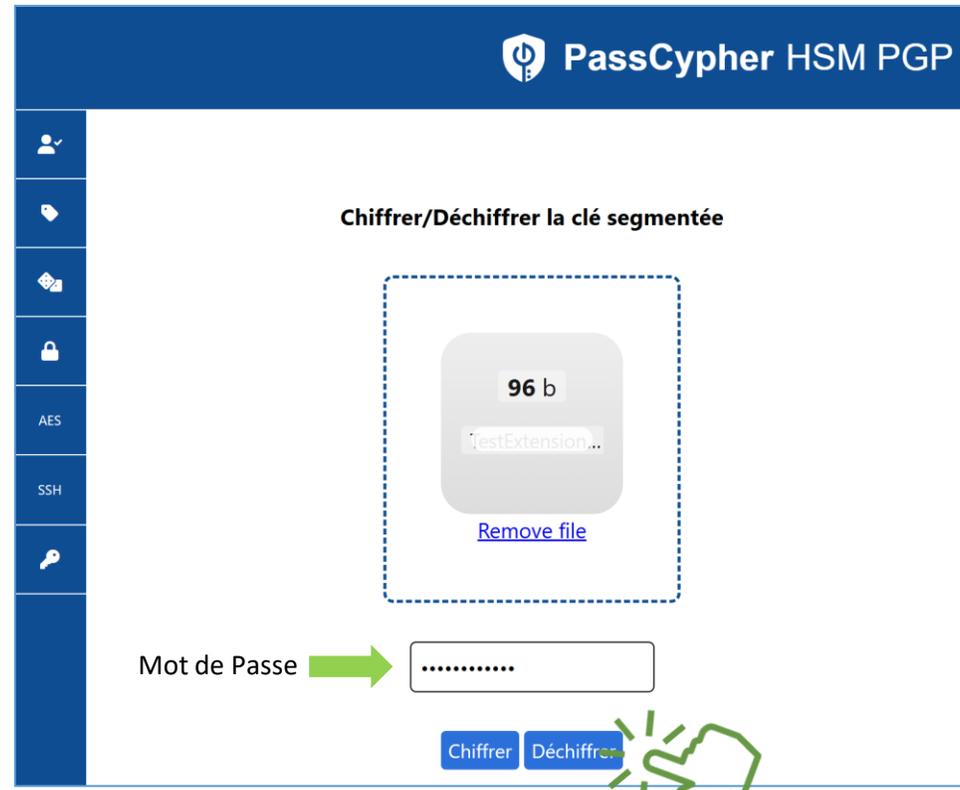
Importez une clé de chiffrement segmentée

Commencez par déchiffrer les segments de clé

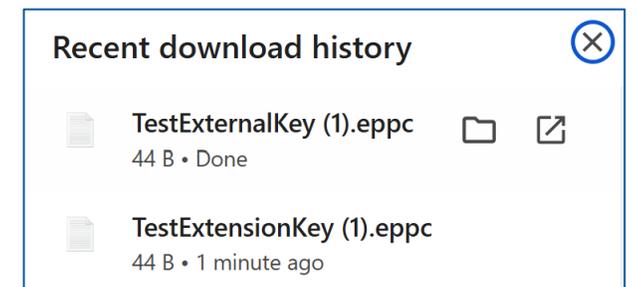
1/3



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



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

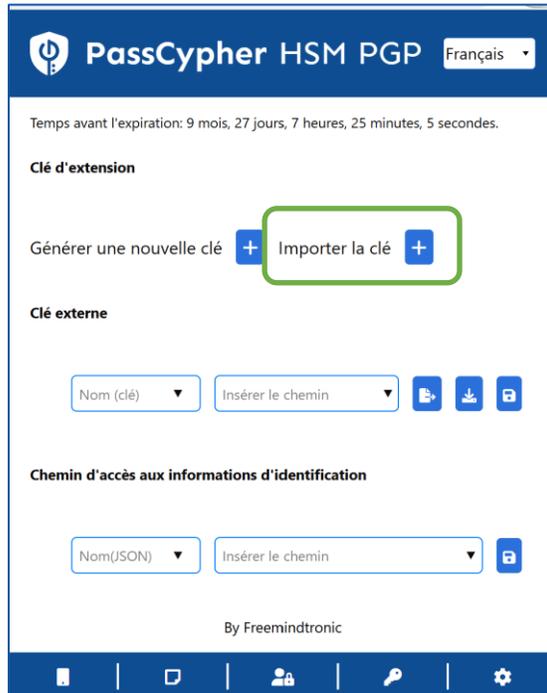


Procédez de la même façon pour déchiffrer la clé externe. Les **2 fichiers déchiffrés** sont dans le dossier « **Téléchargements** »

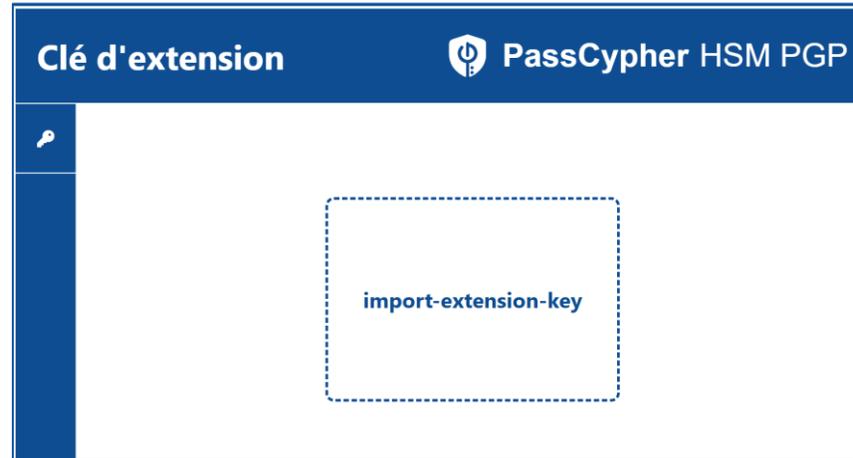
Importez une clé de chiffrement segmentée

Importez d'abord la clé d'extension

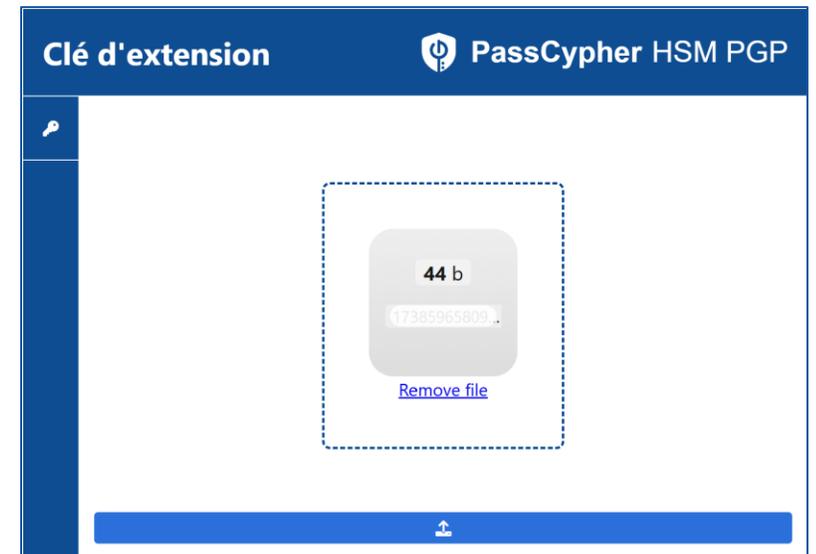
2/3



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



Cliquez dans la fenêtre et importez 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 des clés de chiffrement segmentées

Indiquez le chemin où est stockée la clé externe

3/3

PassCypher HSM PGP Français

Temps avant l'expiration: 9 mois, 27 jours, 7 heures, 39 minutes, 24 secondes.

Clé d'extension

Insérer le chemin

Clé externe

Nom (clé) Insérer le chemin

Chemin d'accès aux informations d'identification

Nom(JSON) Insérer le chemin

By Freemindtronic



PassCypher HSM PGP Français

Temps avant l'expiration: 9 mois, 27 jours, 7 heures, 10 minutes, 41 secondes.

Clé d'extension

Insérer le chemin

Clé externe

Test E:\USB EviKey NFC HSM\...

Chemin d'accès aux informations d'identification

Nom(JSON) Insérer le chemin

By Freemindtronic

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

PassCypher HSM PGP Français

Temps avant l'expiration: 14 jours, 17 heures, 16 minutes, 56 secondes.

Clé d'extension

Statut: Créé

Insérer un répertoire

Clé externe

Test F:\EviKey USB NFC\Cles

Chemin d'accès aux informations d'identification

json-name E:\USB EviKey NFC HSM\libellés j

By F EviPass onic

Cliquez pour ouvrir l'extension puis cliquez sur l'icône **EviPass** pour créer vos identifiants de connexion

PassCypher HSM PGP

Générez votre mot de passe personnalisé

Longueur: 16

Majuscules: Chiffres: Minuscule: Caractères spéciaux:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

url

Nom de l'étiquette

Nom d'utilisateur

Password

≈0 bits

Complétez les informations. Cliquez sur l'icône  pour générer un mot de passe aléatoire. Par défaut la longueur du mot de passe est de 16 caractères, vous pouvez la modifier. Vous pouvez également saisir votre mot de passe manuellement.

PassCypher HSM PGP

Générez votre mot de passe personnalisé

Longueur: 16

Majuscules: Chiffres: Minuscule: Caractères spéciaux:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

https://accounts.google.com/v3/signin/

@gmail

evicypher.demo@gmail.com

.....

≈131 bits

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

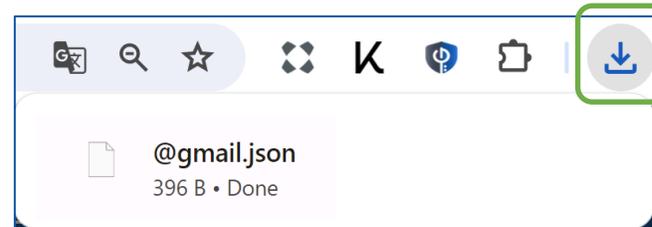
La force de votre mot de passe est calculée en fonction de la taille de l'alphabet qu'il utilise et de sa longueur. Plus la taille de l'alphabet et la longueur du mot de passe sont grandes, plus il sera sécurisé.

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

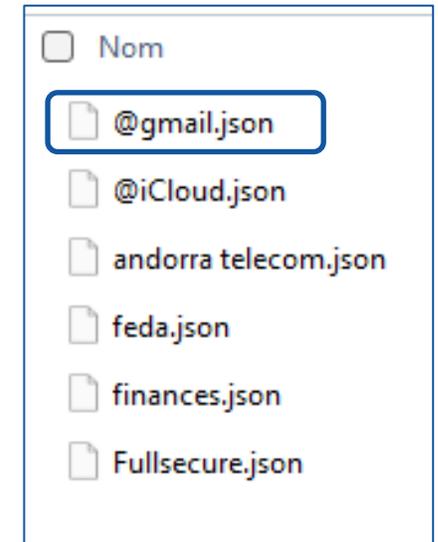
Sauvegardez vos identifiants de connexion

The screenshot shows the 'PassCypher HSM PGP' application interface. At the top, it says 'Générez votre mot de passe personnalisé'. Below this, there is a 'Longueur:' field set to '20'. There are four checked options: 'Majuscules:', 'Chiffres:', 'Minuscule:', and 'Caractères spéciaux:'. A grid of characters is shown with checkboxes, all of which are checked. Below the grid, there are three input fields: the first contains a long URL, the second contains '@gmail', and the third contains 'prenom.nom@gmail.com'. At the bottom, there is a password field with a strength indicator bar and the text '≈131 bits'. A download icon is highlighted with a green box at the bottom center.

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

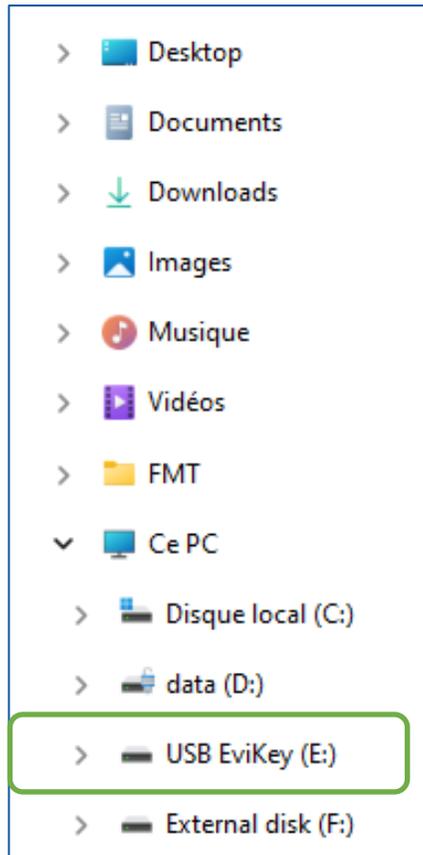


Le fichier **@gmail.json** est disponible dans le dossier « Téléchargements » de votre ordinateur



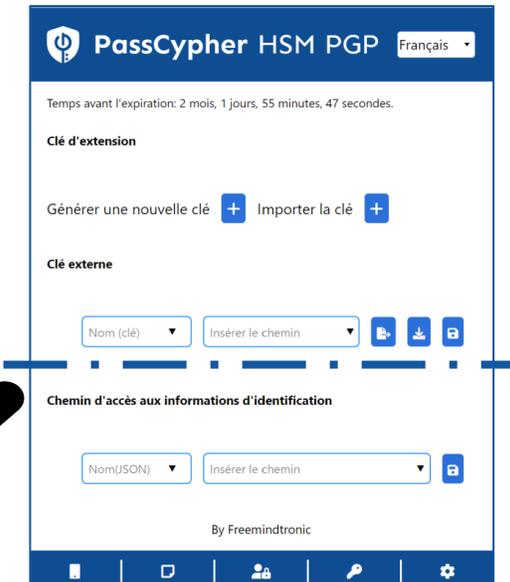
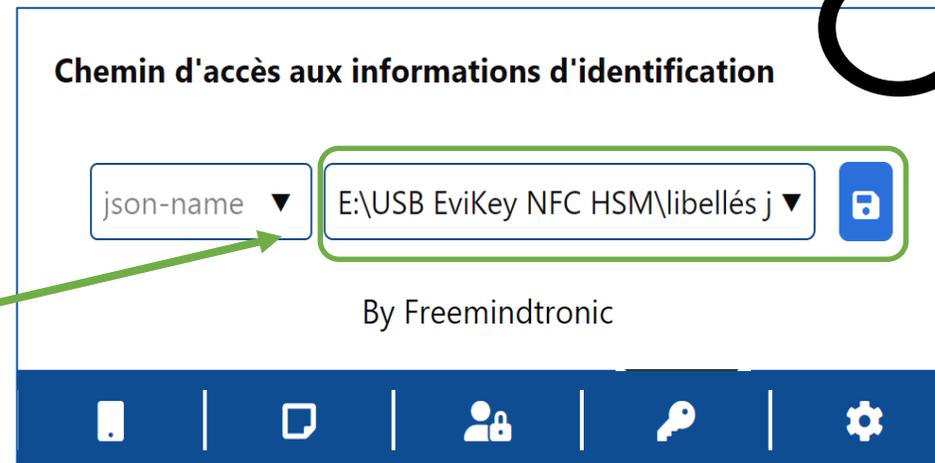
Choisissez un dossier pour sauvegarder tous vos fichiers json. Vous pouvez utiliser une clé USB, un disque externe, une sauvegarde Cloud ou autre.

Déterminez le chemin d'accès à vos identifiants de connexion



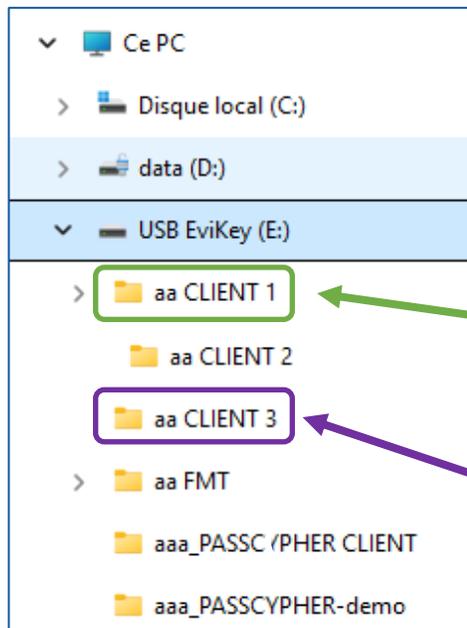
Il est **indispensable** d'indiquer **très précisément le chemin d'accès** à vos fichiers .json pour la connexion automatique aux sites internet et messageries.

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



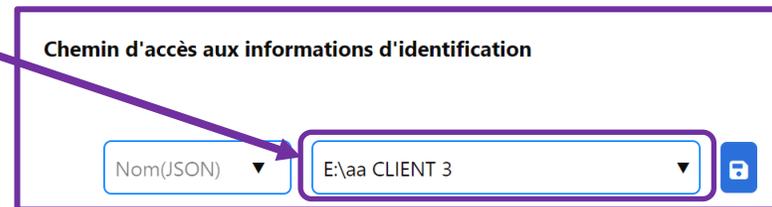
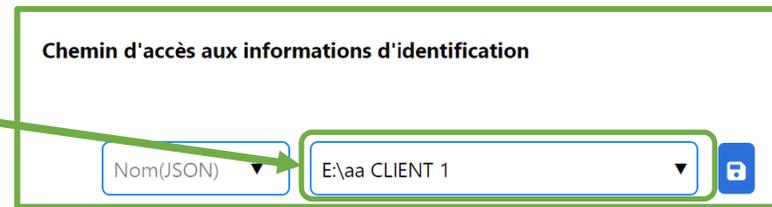
Gérez plusieurs comptes sur le même site web

Exemple : plusieurs clients possédant tous un compte dans la même Banque

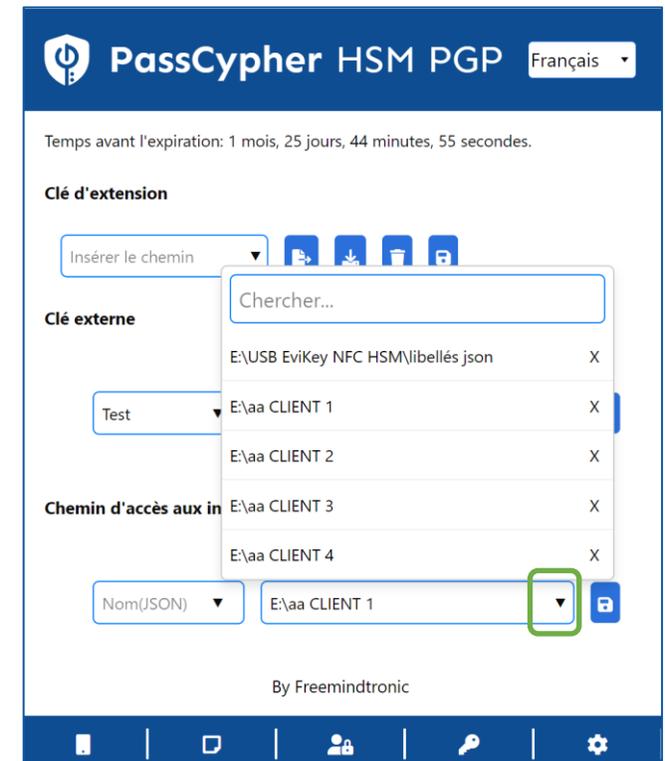


Dans chaque « dossier client » enregistrez les différents identifiants de connexion spécifiques à ce client.

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



Générez votre mot de passe personnalisé

Longueur:

Majuscules: Chiffres: Minuscule: Caractères spéciaux:

! " # \$ % & ' () * + ,
- . / : ; < = > ? @ [\
] ^ _ ` { | } ~

AES

SSH

≈ 0 bits 

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)

≈ 296 bits 

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

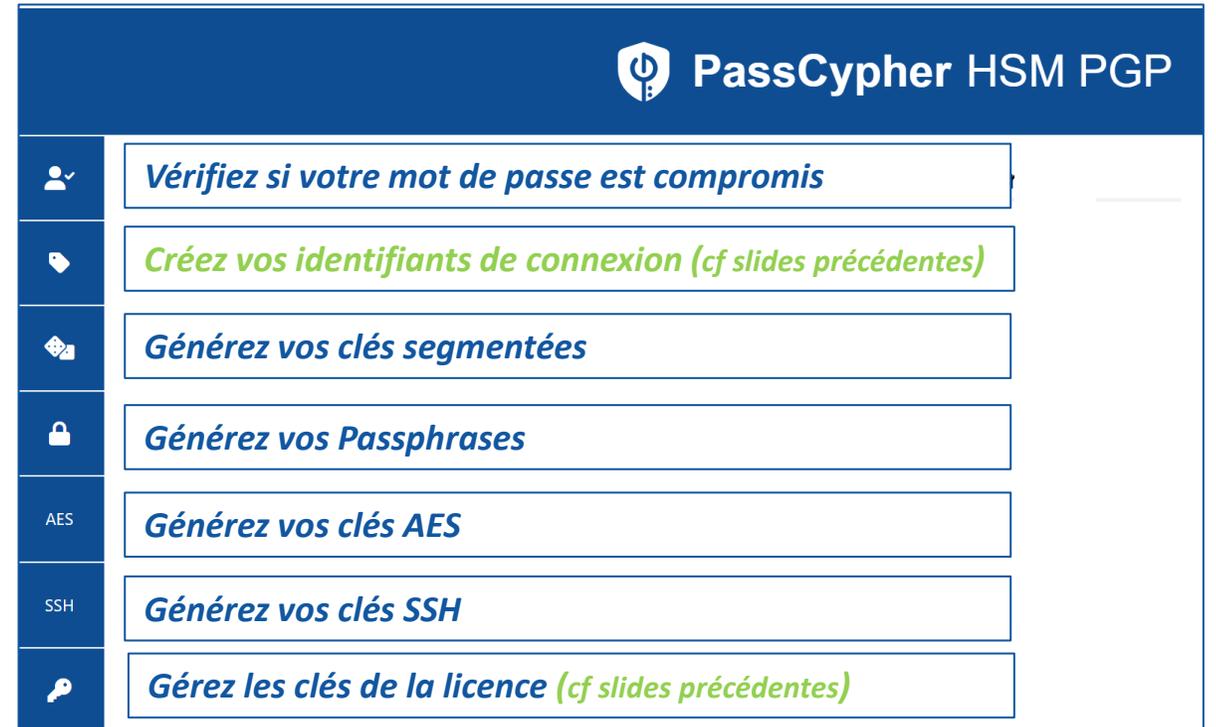
  

≈ 296 bits 

EviPass : fonctionnalités



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



Les différentes fonctionnalités sont expliquées dans les slides suivantes.

EviPass (vérification mot de passe) 1/5



PassCypher HSM PGP Français

Clé de produit

Entrez la clé de produit ✓

Cliquez pour obtenir le SN de la carte mère

By Freemindtronic

EviPass

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



PassCypher HSM PGP

Vérifiez si votre mot de passe est déjà apparu dans une violation de données

Mot de passe:

XXXXXXXXXXXX

Vérifier

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.



PassCypher HSM PGP

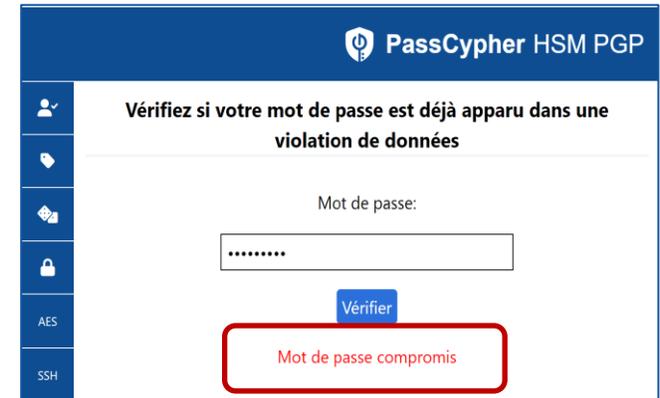
Vérifiez si votre mot de passe est déjà apparu dans une violation de données

Mot de passe:

.....

Vérifier

Mot de passe non compromis



PassCypher HSM PGP

Vérifiez si votre mot de passe est déjà apparu dans une violation de données

Mot de passe:

.....

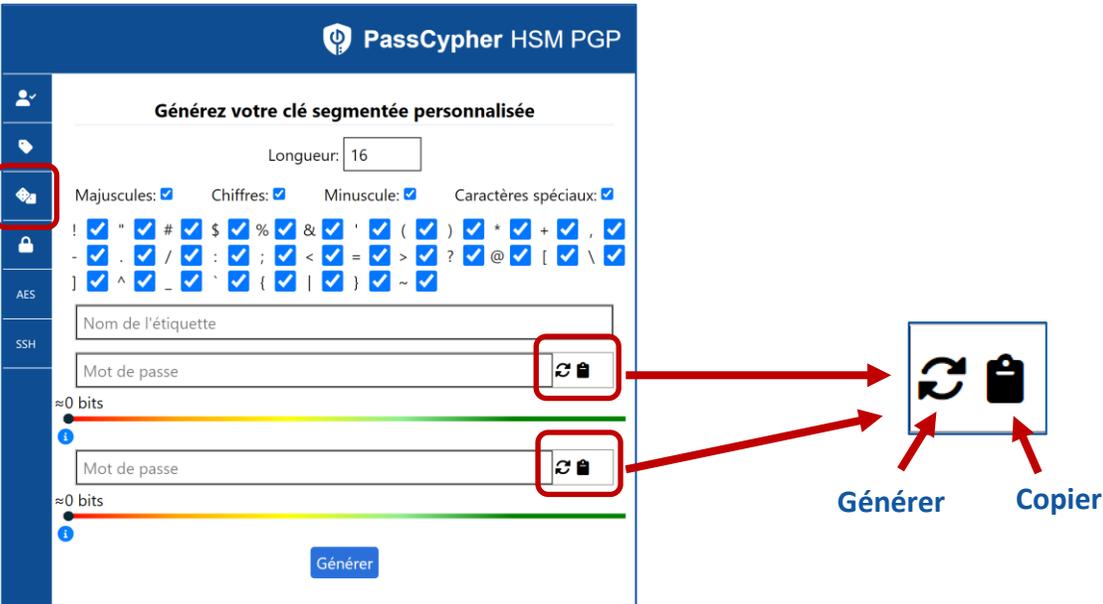
Vérifier

Mot de passe compromis

EviPass (clé segmentée)

2/5

1



PassCypher HSM PGP

Générez votre clé segmentée personnalisée

Longueur: 16

Majuscules: Chiffres: Minuscule: Caractères spéciaux:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

Nom de l'étiquette

Mot de passe

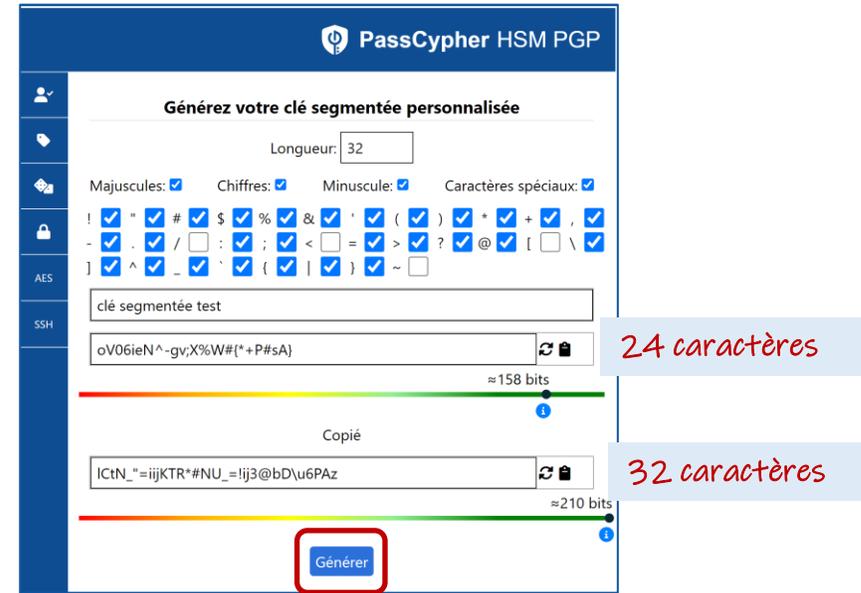
≈0 bits

Mot de passe

≈0 bits

Générer

Générer Copier



PassCypher HSM PGP

Générez votre clé segmentée personnalisée

Longueur: 32

Majuscules: Chiffres: Minuscule: Caractères spéciaux:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

clé segmentée test

oV06ieN^-gv;X%W#(*+P#sA)

≈158 bits

Copié

IcTn_"=ijjKTR*#NU_=ljj3@bD\u6PAz

≈210 bits

Générer

24 caractères

32 caractères

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.



Cliquez pour télécharger



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

EviPass (Passphrase)

3/5



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

Cliquez sur l'icône pour générer la passphrase. Vous pouvez copier/coller cette passphrase.

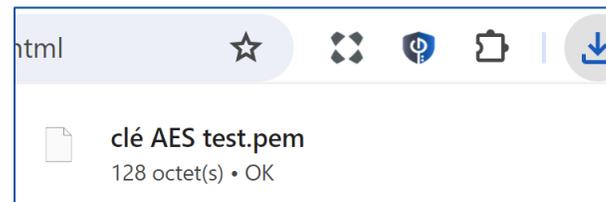
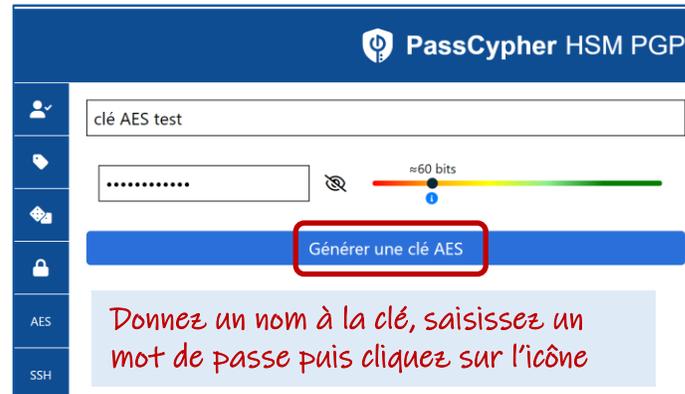
Générer Copier/coller

EviPass (clé AES)

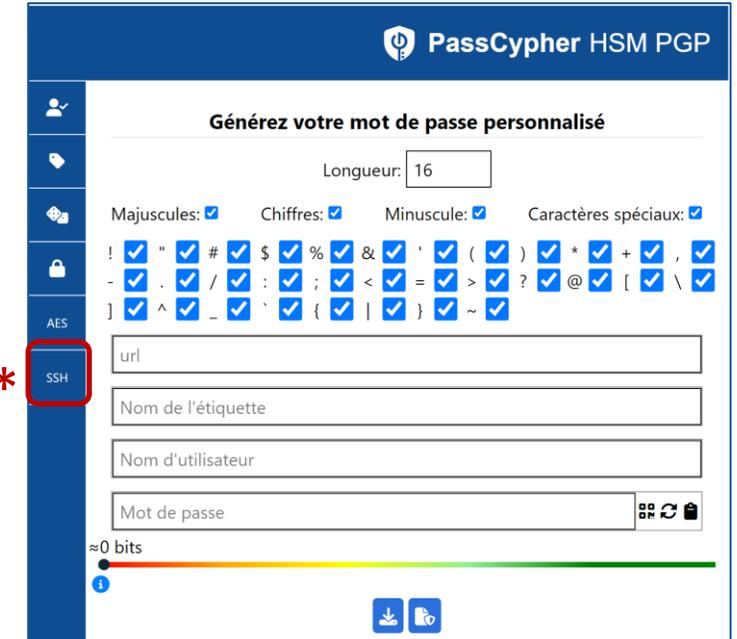
4/5



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



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



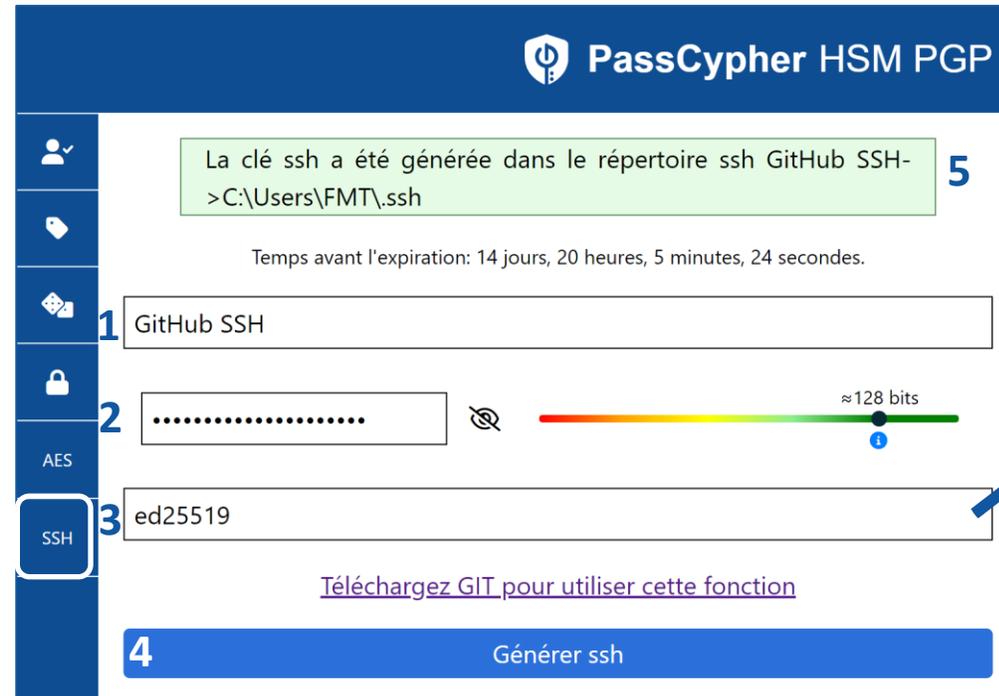
(*) Cette fonctionnalité de génération de clé SSH est disponible dans la version payante

EviPass (clé SSH)

5/5

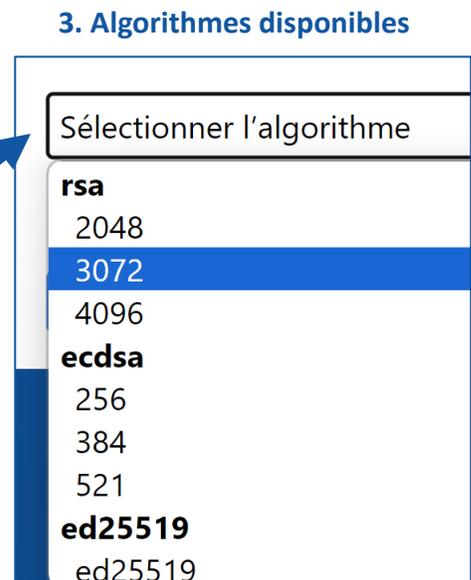


Cliquez sur l'icône indiquée pour accéder aux fonctionnalités de création de clé SSH

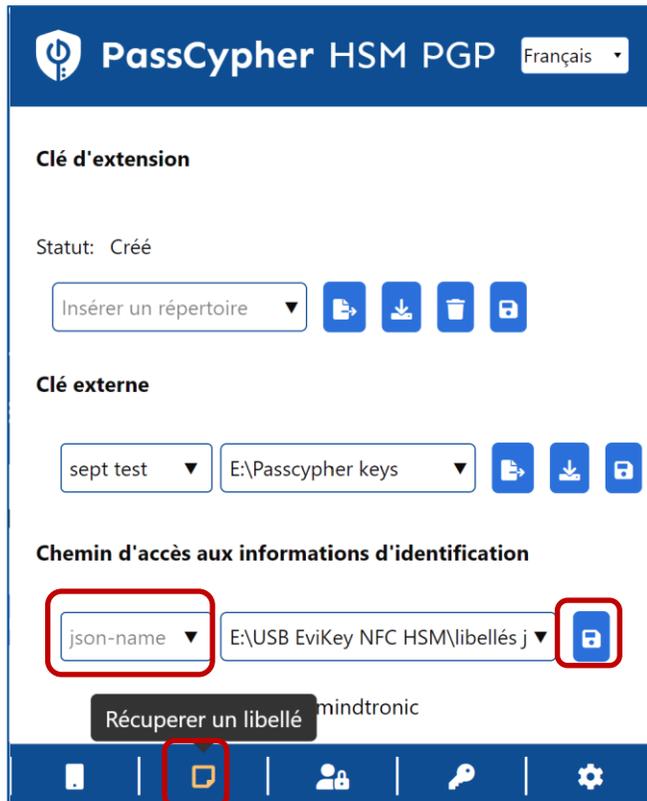


Cliquez sur l'icône « SSH » et compléter les différents champs :

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



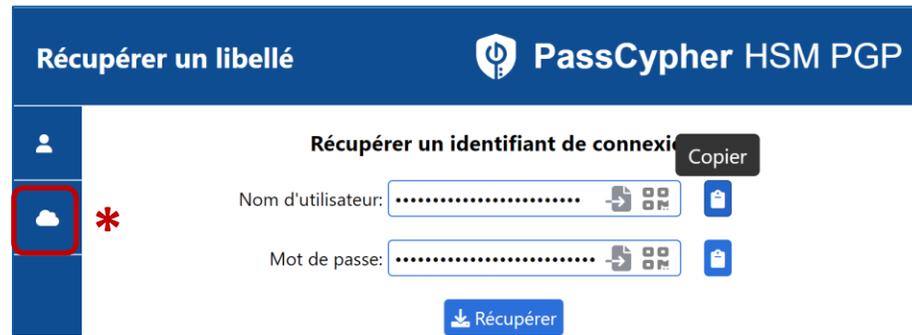
Récupérer un libellé



Sur la page d'accueil de l'extension, écrivez le **nom du libellé** concerné puis cliquez 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.

 **PassCypher HSM PGP** Français ▾

Temps avant l'expiration: 14 jours, 23 heures, 58 minutes, 50 secondes.

Clé d'extension

Statut: Créé **1** **2** **3** **4** **5**

Insérer un répertoire ▾    

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.

 **PassCypher HSM PGP** Français ▾

Clé externe

1

2

3 

4 

5 

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

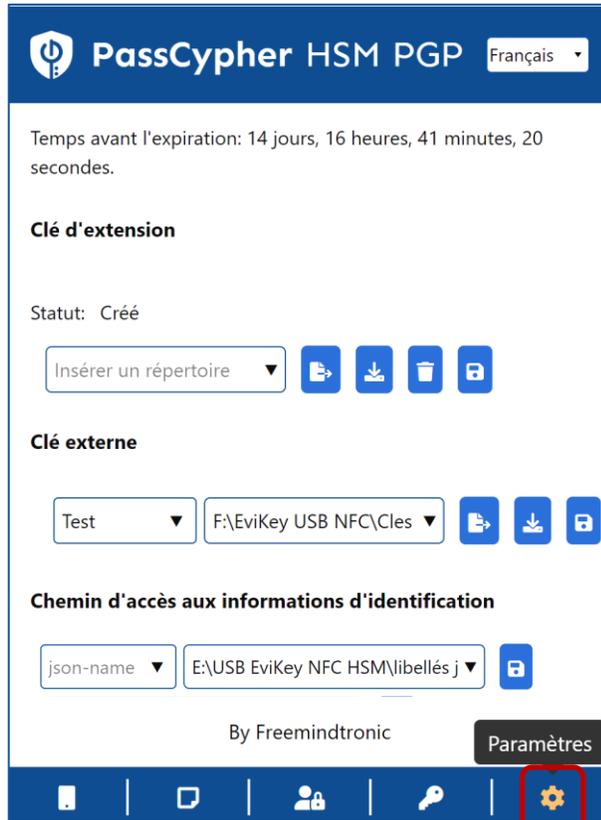
2. Insérez le chemin où sera stockée la clé externe. Vous pouvez définir plusieurs chemins

3. Cliquez pour créer et exporter la clé

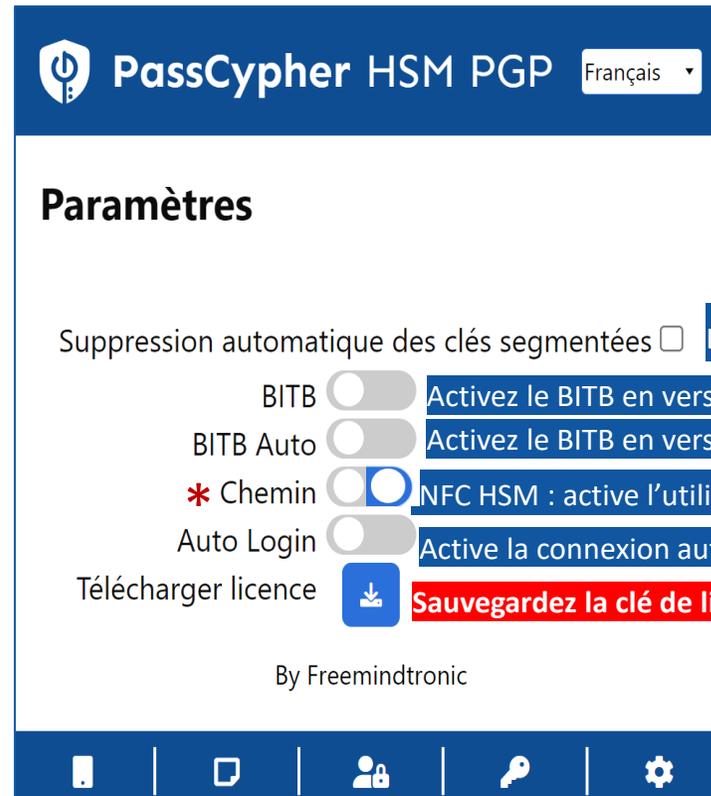
4. En cliquant sur cette icône vous pouvez télécharger la clé et la sauvegarder à l'endroit de votre choix

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 spécifique Extension PassCypher avec dispositif NFC

BITB plus d'informations disponibles [ici](#)

Connectez-vous en UN CLIC !

Accédez à vos messageries ou sites internet favoris et profitez d'une connexion rapide, sécurisée et automatique.



Take back control, Take back power

EviPass Technology

By Freemindtronic Andorra



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

