

TUTORIEL EXTENSION PASSCYPHER HSM PGP Free

By Freemindtronic Andorra

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



SOMMAIRE

- **Installation de l'extension PassCypher HSM PGP Free**
- **Principes de fonctionnement**
- **Schéma détaillé**
- **Connexion via un QR code « codé »**
- **Connexion via un identifiant chiffré en AES 256**
- **Fonctionnalités EviPass : création de Passphrases, clés AES et clés segmentées**
- **Récupérer un libellé**
- **Fonctionnalités et Paramètres**
- **Connexion avec un dispositif NFC de Freemindtronic (installation du logiciel EviDNS)**

INSTALLATION

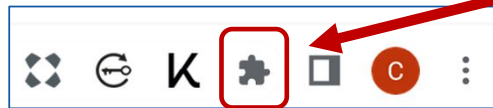
Télécharger et installer l'extension PassCypher HSM PGP

CHROME : [chrome web store](#)

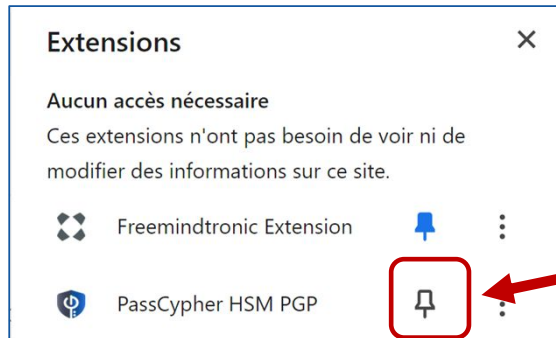
FIREFOX : en cours

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

OPERA : en cours



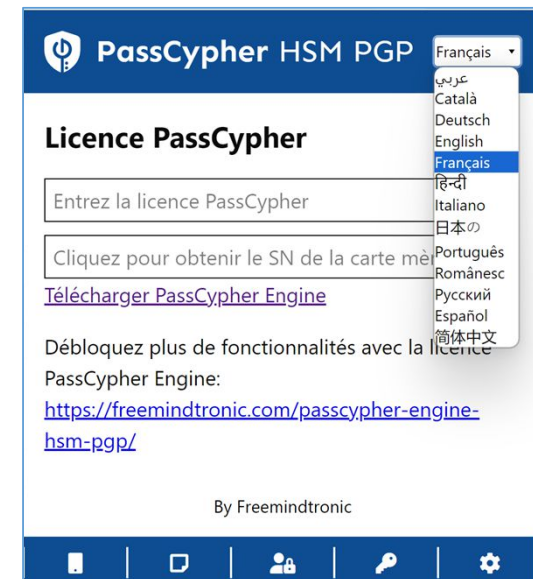
En haut à droite de l'écran de votre ordinateur, cliquez sur cette icône pour accéder aux extensions



Cliquez sur cette icône pour l'épingler sur votre barre d'outils

L'icône PassCypher apparaît en haut à droite de l'écran de votre ordinateur.

Cliquez sur l'icône, la page d'accueil s'affiche





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.

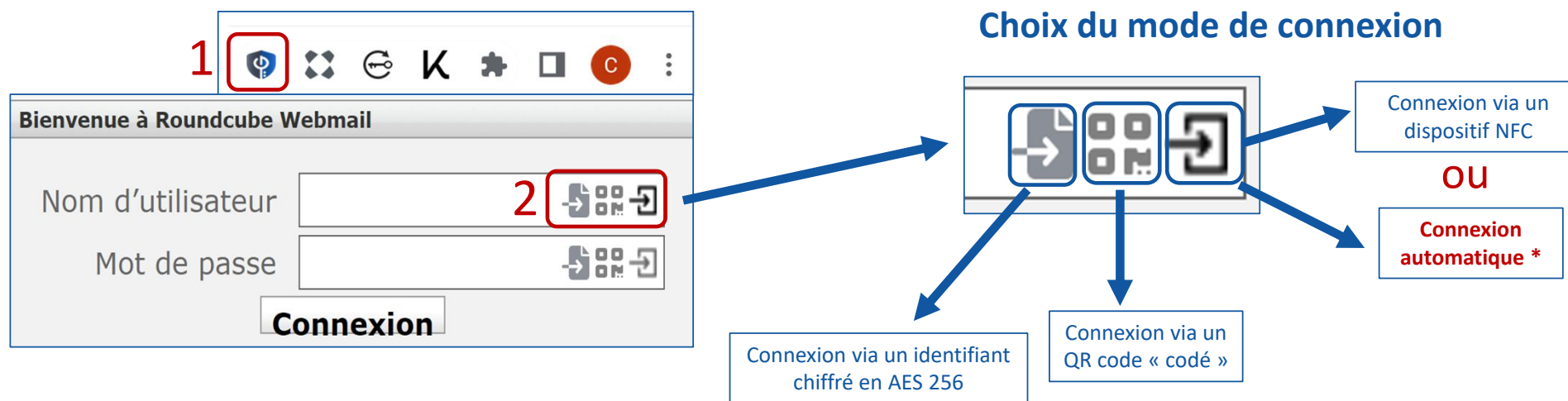
Comment cela fonctionne ?

- **PassCypher HSM PGP** est une extension gratuite qui permet plusieurs modes de connexion automatique
 1. avec des identifiants de connexion au format **QR code « codé »** (fichiers gif)
 2. avec des identifiants de connexion **chiffrés en AES 256** (fichiers PGP)
 3. avec des identifiants de connexion sauvegardés dans un **dispositif NFC**
- La sécurité liée à ces différents modes de connexion n'est pas la même
- La facilité et la rapidité d'utilisation ne sont pas les mêmes non plus
- Il existe une **version payante de l'extension** (activation d'une licence) qui permet une **sécurité maximale** ainsi qu'une **rapidité d'exécution inégalable**
- Dans les champs « **Nom d'utilisateur** » et « **Mot de passe** » vous verrez apparaître **3 icônes** qui vous permettent d'accéder aux **3 modes de connexion**

Nom d'utilisateur	<input type="text"/>	
Mot de passe	<input type="password"/>	

Connexion automatique avec l'extension PassCypher HSM PGP Free

1. Un premier clic sur l'icône encadrée en rouge ci-dessous pour ouvrir l'extension
2. Un second clic pour choisir le mode de connexion
3. Le remplissage des champs et la connexion se font automatiquement





() Disponible dans la version payante de l'extension*

Connexion via un QR code “codé”

- Créez, sauvegardez et gérez vos identifiants de connexion
- Principe de connexion
- Connexion à une messagerie
- Connexion à un site web

Bienvenue à Roundcube Webmail

Nom d'utilisateur 

Mot de passe 

Connexion

Connectez-vous 

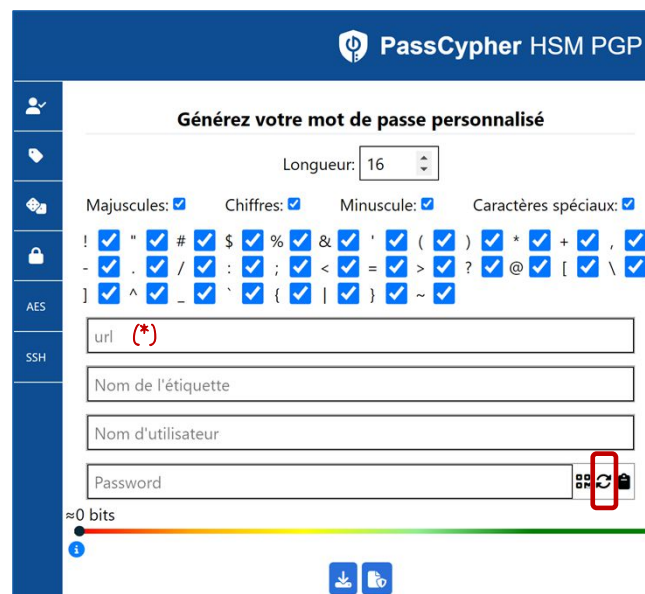
E-mail ou nom d'utilisateur 


Mot de passe 

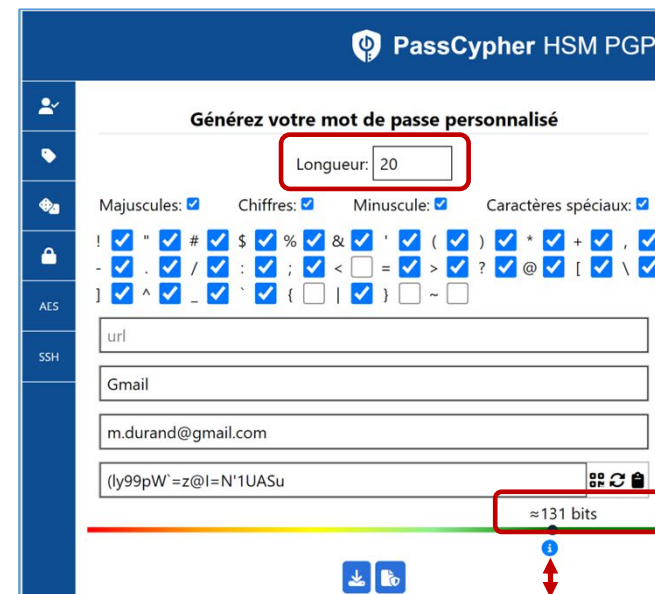
Créez vos identifiants de connexion



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



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.

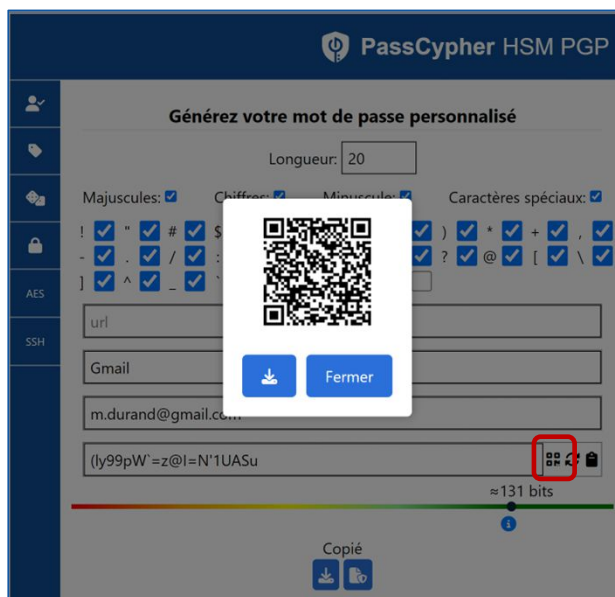



L'entropie du mot de passe est calculée et s'affiche sous forme de code couleur

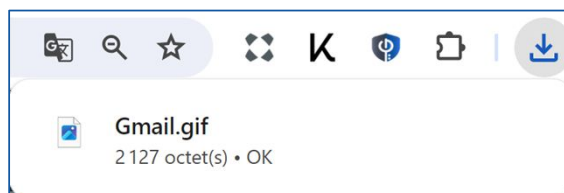
La force de votre mot de passe est calculée en fonction de la taille de l'alphabet qu'il utilise et de sa longueur. Plus la taille de l'alphabet et la longueur du mot de passe sont grandes, plus il sera sécurisé.

() Inutile de compléter l'URL pour cette version « QR code codé »*

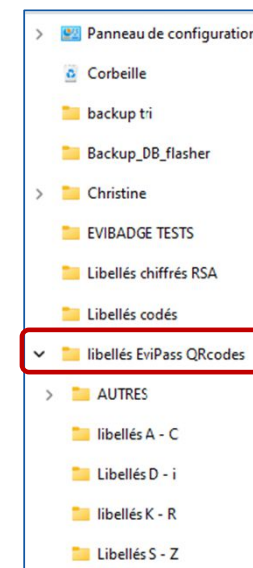
Sauvegardez vos identifiants de connexion



Cliquez ensuite sur l'icône « QR code » puis sur l'icône  afin de sauvegarder cet identifiant

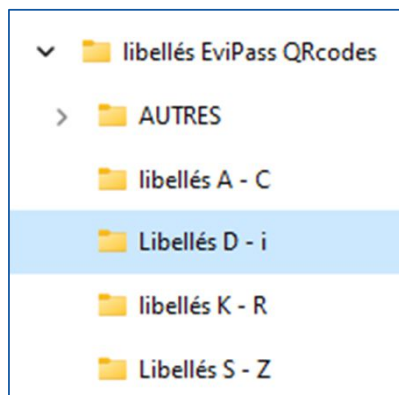


Le fichier Gmail.gif est enregistré dans le dossier « Téléchargements » de votre ordinateur

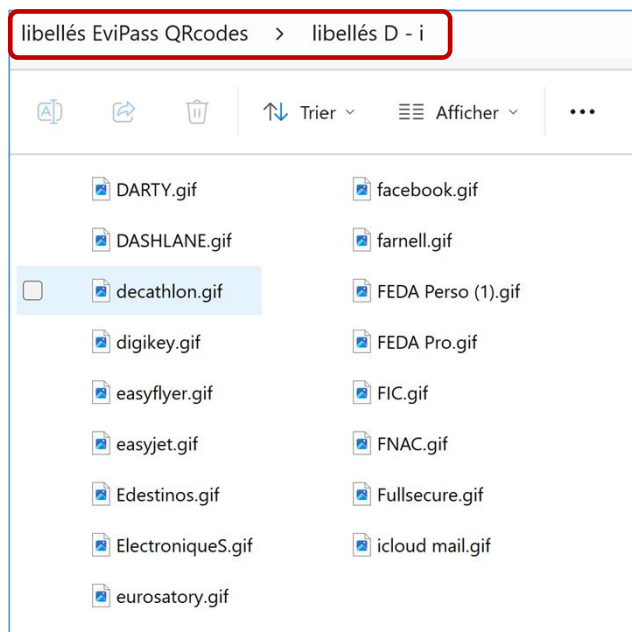


Choisissez un dossier pour le sauvegarder, il servira pour la connexion automatique à la messagerie Gmail. Vous pouvez utiliser une clé USB, un disque externe, une sauvegarde Cloud ou autre. Pensez également à **sécuriser ce dossier** (Bitlocker, mot de passe d'ouverture ...).

Gérez vos identifiants de connexion



Organisez à votre manière les différentes sauvegardes : ici c'est le tri alphabétique qui a été retenu



Tous les identifiants de connexion apparaissent au format de fichiers .gif



N'oubliez pas de sécuriser l'accès à ce dossier et de faire une sauvegarde régulièrement





Principe de connexion

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 du « **QR code** » indiquée ci-dessous
4. Une fenêtre s'ouvre, cliquez pour accéder au dossier dans lequel sont sauvegardés vos identifiants
5. Cliquez sur celui qui convient
6. Les champs sont remplis automatiquement et la connexion est réalisée (si vous avez activé l'Autologin dans les Paramètres de l'extension)

Je suis déjà client OVHcloud

Cliquez pour remplir automatiquement

Identifiant ou adresse e-mail  

Mot de passe    

Se connecter

Faites glisser ou sélectionnez le code QR GIF/PNG

Annuler

Identifiant ou adresse e-mail  



Exemples de connexion à une messagerie

Apple iCloud
Sign in with Apple ID

Email or Phone Number

Sign in with Apple ID

Email or Phone Number

Remplissage automatique réussi.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Email or Phone Number
password

Un seul clic remplit les 2 champs

Proton
Sign in
to continue to Proton Mail

Email or username

Password

Sign in

Remplissage automatique réussi.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Password

Keep me signed in
Recommended on trusted devices. [Why?](#)

Sign in

Un seul clic remplit les 2 champs

Microsoft Outlook
Sign in
to continue to Outlook

Email, phone or Skype

No account? Create one!

1er clic

Sign in
to continue to Outlook

.....

No account? Create one!

Sign in with a security key ?

Next

Microsoft
← test_evicypher@outlook.com

Enter password

.....

Forgotten your password?

Other ways to sign in

2nd clic

Sign in

Sites appelés « authentification en deux étapes » : 2 clics sont nécessaires

Se connecter à Yahoo Mail
à l'aide de votre compte Yahoo

Nom d'utilisateur, mail ou téléphone

1er clic

Suivant

Se connecter à Yahoo Mail
à l'aide de votre compte Yahoo

Nom d'utilisateur, mail ou téléphone

.....

Suivant

Mot de passe

.....

2nd clic

Suivant

Exemples de connexion à un site web

Connectez-vous 

E-mail ou nom d'utilisateur

Mot de passe

Remplissage automatique réussi.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

.....

Mot de passe

.....

Se souvenir de moi

Connectez-vous

Un seul clic remplit les 2 champs

fnac Connexion / Inscription

Saisissez votre e-mail pour vous connecter ou créer un compte

E-mail

Connexion / Inscription

E-mail

.....

Connexion / Inscription

Mot de passe

Mot de passe

.....

Restez connecté(e)

Se connecter

Site appelé « authentification en deux étapes » : 2 clics sont nécessaires

Accès usuaris registrats

CERTIFICAT

Remplissage automatique réussi.
Ce mot de passe est déjà apparu lors d'une violation de données

.....

.....

Has oblidat la contrasenya?

ENTRAR

Vérification du mot de passe et alerte en cas de mot de passe corrompu

Connexion via un identifiant chiffré en AES 256

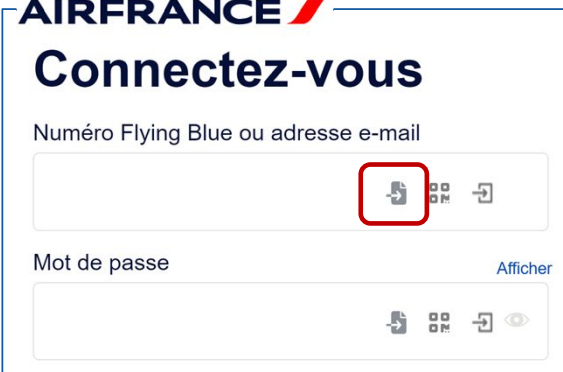
- Créez, sauvegardez et gérez vos identifiants de connexion
- Principe de connexion
- Connexion à une messagerie
- Connexion à un site web



Google
Connexion
Accéder à Gmail

Adresse e-mail ou numéro de téléphone

Adresse e-mail oubliée ?



AIRFRANCE
Connectez-vous

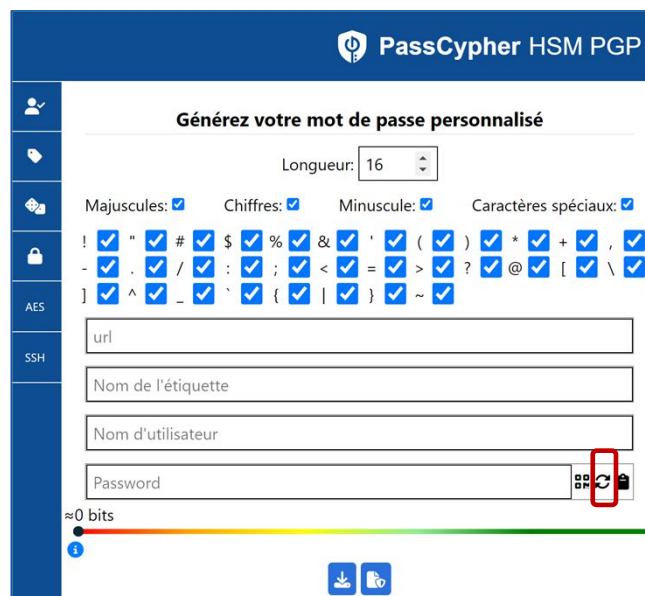
Numéro Flying Blue ou adresse e-mail


Mot de passe [Afficher](#)

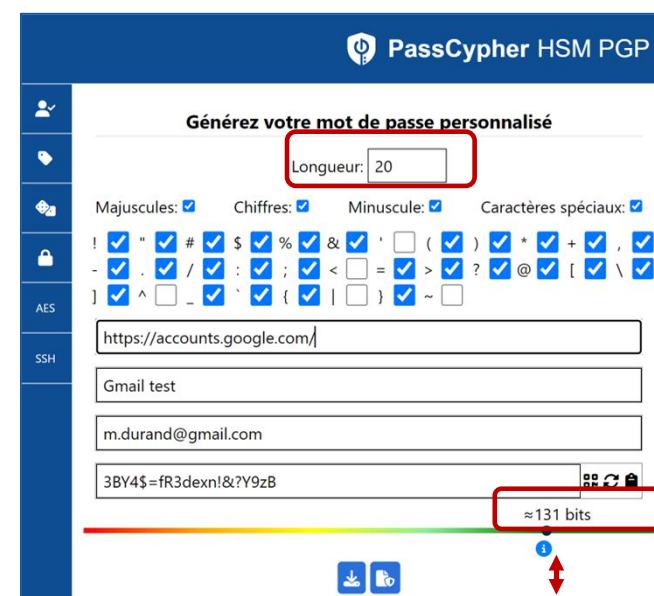
Créez vos identifiants de connexion



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



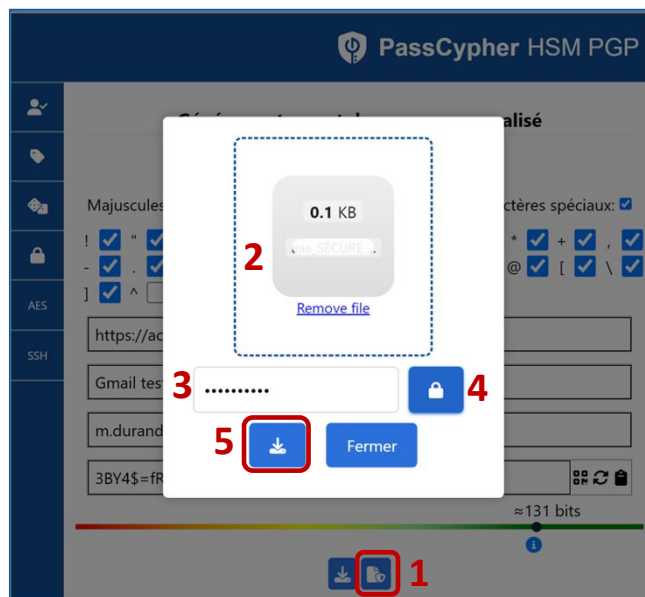
Complétez les informations. Cliquez sur l'icône  pour générer un mot de passe aléatoire. Par défaut la longueur du mot de passe est de 16 caractères, vous pouvez la modifier. Vous pouvez également saisir votre mot de passe manuellement.



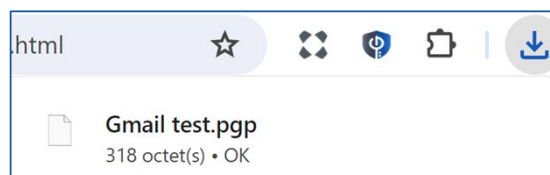
L'entropie du mot de passe est calculée et s'affiche en code couleur

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.

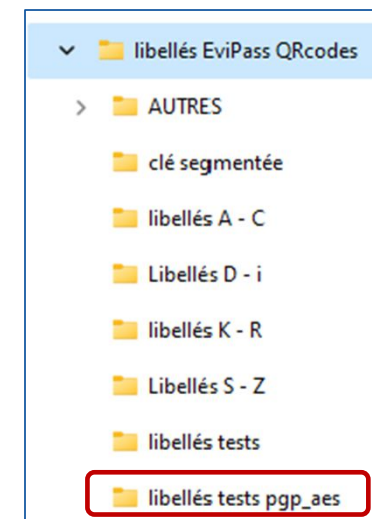
Sauvegardez vos identifiants de connexion



Cliquez sur l'icône indiquée (1), glissez la clé AES* (2), inscrivez le mot de passe associé (3), cliquez sur l'icône du cadenas (4) et cliquez sur l'icône de sauvegarde (5) afin de sauvegarder ce libellé



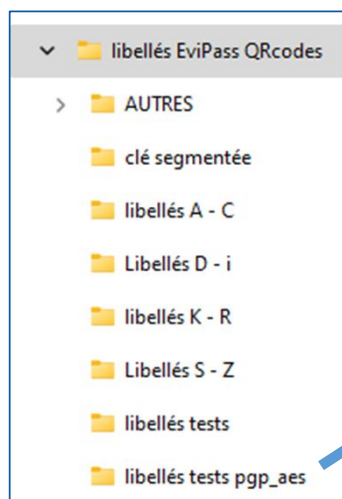
Le fichier « Gmail test.pgp » est enregistré dans le dossier « Téléchargements » de votre ordinateur



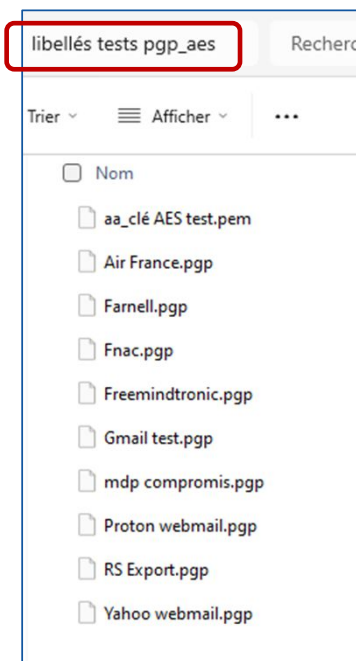
Choisissez un dossier pour le sauvegarder, il servira pour la connexion automatique à la messagerie Gmail. Vous pouvez utiliser une clé USB, un disque externe, une sauvegarde Cloud ou autre. Pensez également à **sécuriser ce dossier** (Bitlocker, mot de passe d'ouverture ...).

(*) Pour créer une clé AES avec l'extension, voir les slides suivantes

Gérez vos identifiants de connexion



Organisez à votre manière les différentes sauvegardes : ici c'est le tri alphabétique qui a été retenu



Tous les identifiants de connexion apparaissent sous la forme de fichiers .pgp

La clé AES apparaît sous la forme d'un fichier.pem. Vous pouvez utiliser des clés AES différentes pour identifier vos libellés Pro et Perso par exemple.




Vous pouvez les stocker, les dupliquer sur tout support de stockage de votre choix, ils sont sécurisés par défaut.

Principe de connexion





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 indiquée ci-dessous
4. Une fenêtre s'ouvre, cliquez pour accéder au dossier dans lequel sont sauvegardés vos identifiants
5. Glissez dans la fenêtre l'identifiant (1) ainsi que la clé AES (2) et saisissez le mot de passe associé (3)
6. Cliquez sur l'icône → pour valider (4)
7. Les champs sont remplis automatiquement et la connexion est réalisée (**si vous avez activé l'Autologin dans les Paramètres de l'extension**)

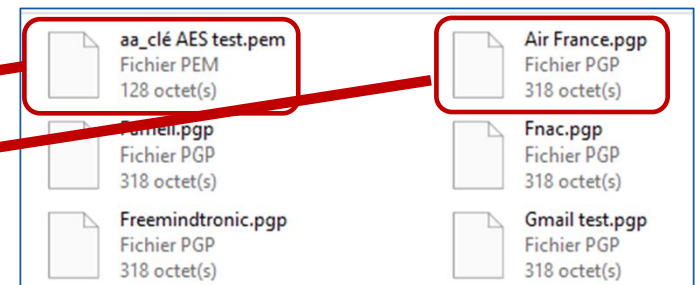
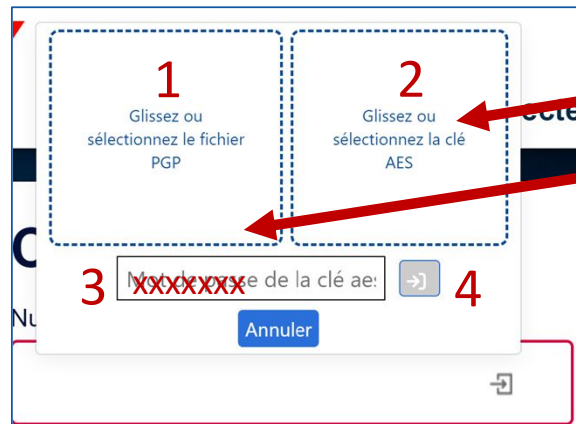
Connectez-vous

Numéro Flying Blue ou adresse e-mail



Mot de passe Afficher





Exemples de connexion à une messagerie

Site appelé « authentification en deux étapes » : 2 clics sont nécessaires

Google
Connexion
Accéder à Gmail

Adresse e-mail ou numéro de téléphone

Adresse e-mail oubliée ?

Créer un compte

Suivant

Cliquez

Glissez ou sélectionnez le fichier PGP

Glissez ou sélectionnez la clé AES

Mot de passe de la clé ae:

Annuler

Adresse e-mail ou numéro de téléphone

Créer un compte

Suivant

0,3 KB

Remove file

0,1 KB

Remove file

xxxxxxxxxxxxx

Annuler

1^{er} clic adresse mail

Répétez la même opération *2nd clic Mot de Passe*

Google

Jacques Gascuel

evicypher.demo@gmail.com

Saisissez votre mot de passe

Remplissage automatique réussi.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Mot de passe oublié ?

Suivant

Correu @andorra.ad

Usuari

Mot clau

ENTRAR

Glissez ou sélectionnez le fichier PGP

Glissez ou sélectionnez la clé AES

Mot de passe de la clé ae:

Annuler

0,3 Ko

Effacer le fichier

0,1 Ko

Effacer le fichier

xxxxxxxxxxxxxxxxxxxx

Annuler

1 seul clic

Remplissage automatique réussi.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Usuari

Mot clau

ENTRAR

Un seul clic remplit les 2 champs

Exemples de connexion à un site web

AIRFRANCE

Connectez-vous

1 Numéro Flying Blue ou adresse e-mail

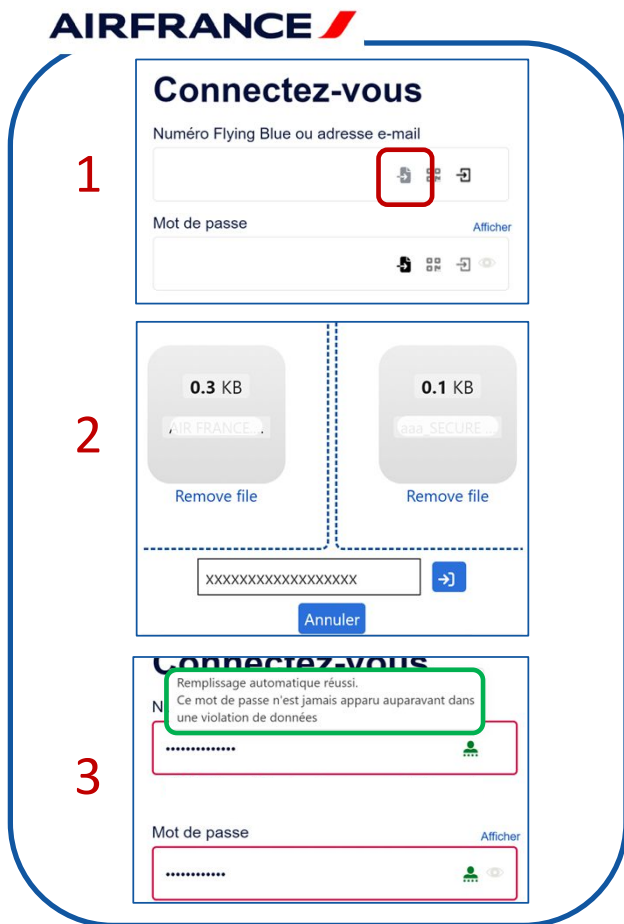
Mot de passe

2 0.3 KB AIR FRANCE... Remove file

0.1 KB aaa_SECURE... Remove file

3 REMPLISSAGE AUTOMATIQUE RÉUSSI.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Mot de passe



Un seul clic remplit les 2 champs

MY MEX Global Markets
PART OF **MultiBank Group**
EST. 2005

1 Nom d'utilisateur *

Entrez votre adresse e-mail

Mot de passe *

Entrez votre mot de passe

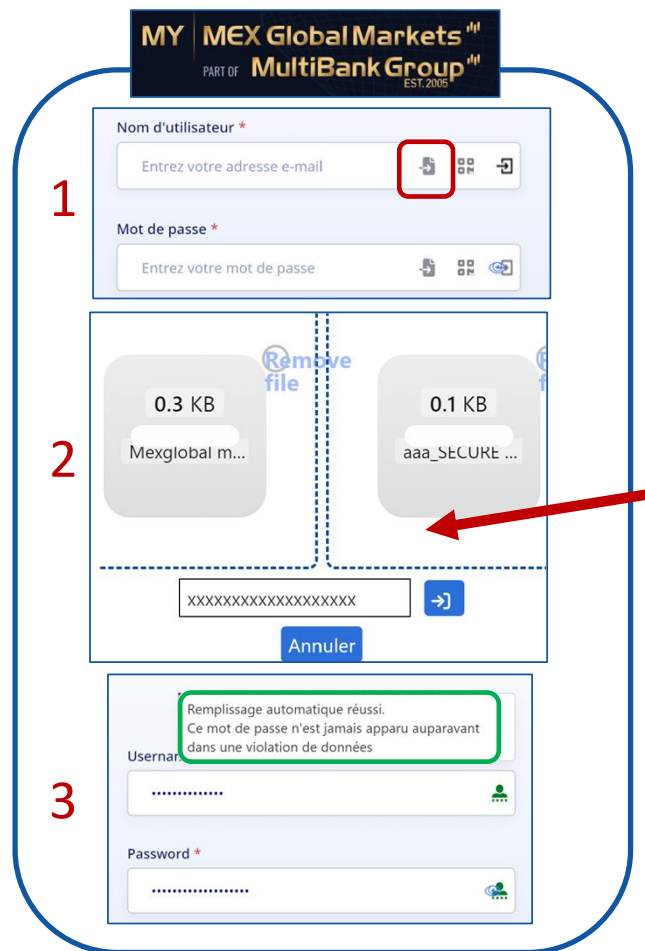
2 0.3 KB Mexglobal m... Remove file

0.1 KB aaa_SECURE... Remove file

3 REMPLISSAGE AUTOMATIQUE RÉUSSI.
Ce mot de passe n'est jamais apparu auparavant dans une violation de données

Username

Password *



Un seul clic remplit les 2 champs

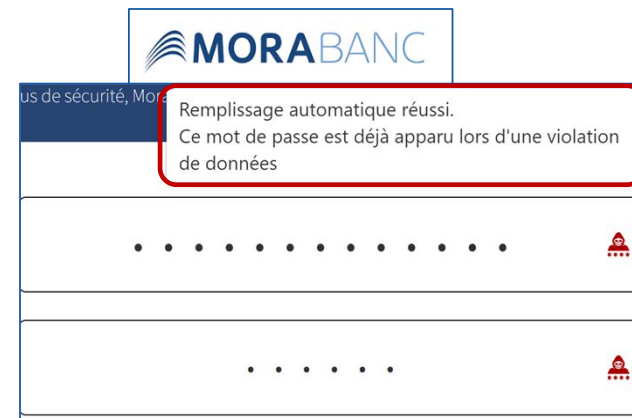
MORABANC

us de sécurité, Mor

Remplissage automatique réussi.
Ce mot de passe est déjà apparu lors d'une violation de données

.....

.....

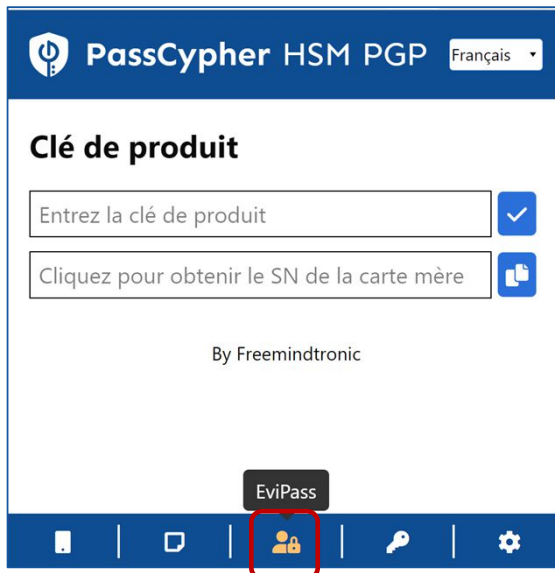


Vérification du mot de passe et **alerte** en cas de mot de passe corrompu

INFORMATION

Pour les sites appelés « authentification en deux étapes » : 2 clics sont nécessaires

EviPass (vérification mot de passe) 1/4



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 (Passphrase)

2/4



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

1

2

3

Générer Copier/coller

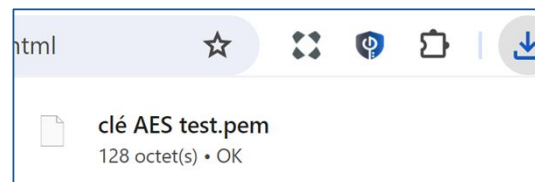
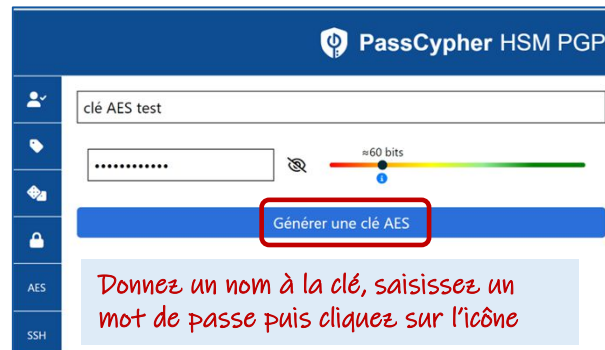
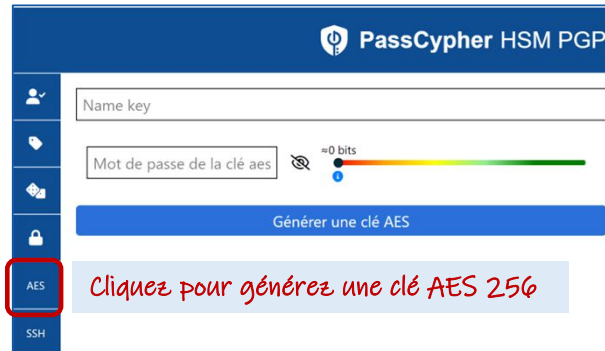
1. Cliquez sur l'icône indiquée pour générer une passphrase
2. Choisissez le nombre de mots de la passphrase
3. Choisissez les caractères qui vont séparer les mots

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

EviPass (clé AES/clé SSH, identifiant) 3/4



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



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



Cette fonctionnalité de **création d'identifiants de connexion** est expliquée dans les slides précédentes

(*) disponible dans la version payante

EviPass (clé segmentée)

4/4

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.

24 caractères

32 caractères

Cliquez pour télécharger

clé segmentée test.gif
3 066 octet(s) • OK

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

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.

24 caractères

32 caractères

Cliquez pour télécharger

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

Récupérer un libellé



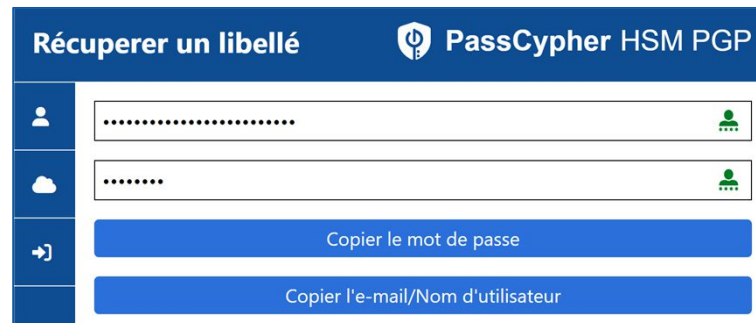
Cliquez sur l'icône indiquée pour accéder à la récupération de vos libellés



Utilisez le mode adapté à votre situation :

PGP chiffré en AES cliquez sur l'icône indiquée

QR code cliquez sur l'icône indiquée

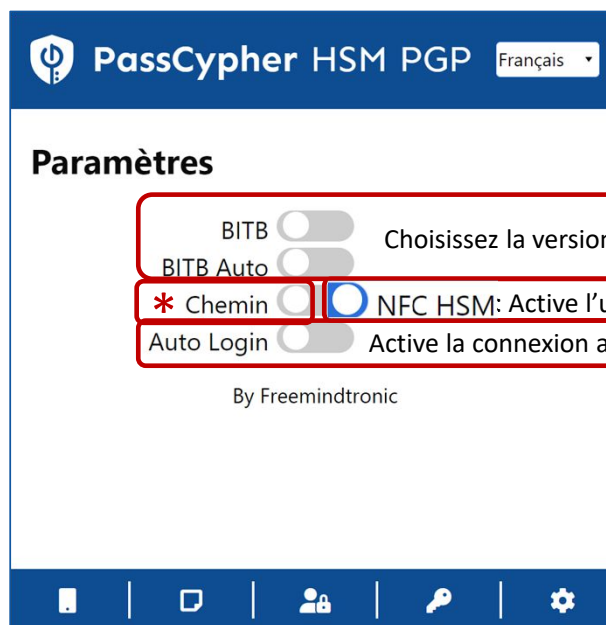


Les informations s'affichent à l'écran : nom d'utilisateur et mot de passe. Cliquez pour copier les informations utiles

Paramètres & Fonctionnalités



Cliquez sur l'icône « Paramètres »



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

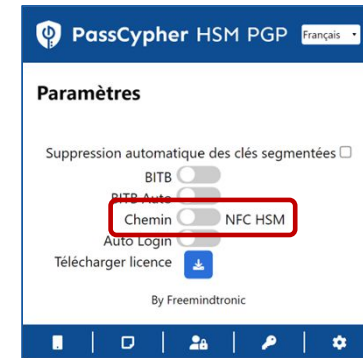
(*) disponible dans la version payante

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

Connexion via un dispositif NFC

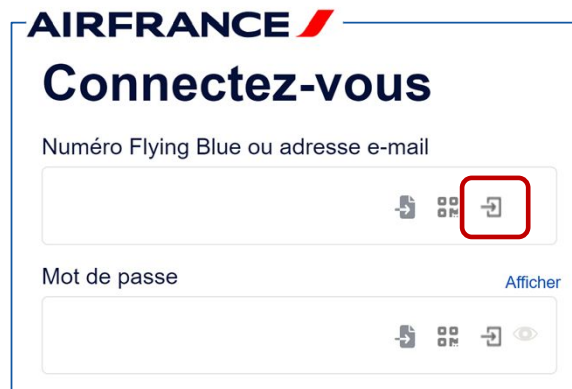
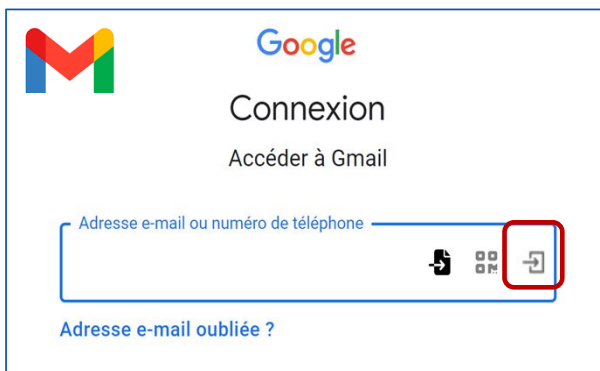
avec un téléphone Android et l'Application Freemindtronic

ACTIVEZ la fonctionnalité NFC dans les paramètres de l'extension



1. Télécharger et installer le logiciel EviDNS disponible [ici](#) pour Windows, Linux ou Apple

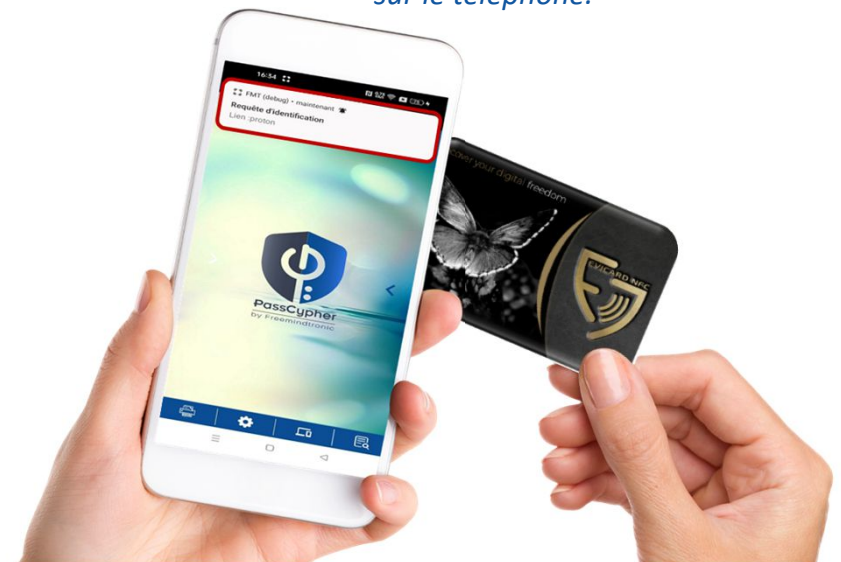
- Un simple clic sur l'icône encadrée en rouge ci-dessous
- Une requête est envoyée au téléphone Android
- Le remplissage des champs et la connexion se font automatiquement



La connexion en détail

Lorsque vous cliquez sur "**Connexion**" depuis votre ordinateur, une requête est envoyée au téléphone (via le réseau WIFI).

Cliquez sur la requête et suivez les instructions affichées sur le téléphone.

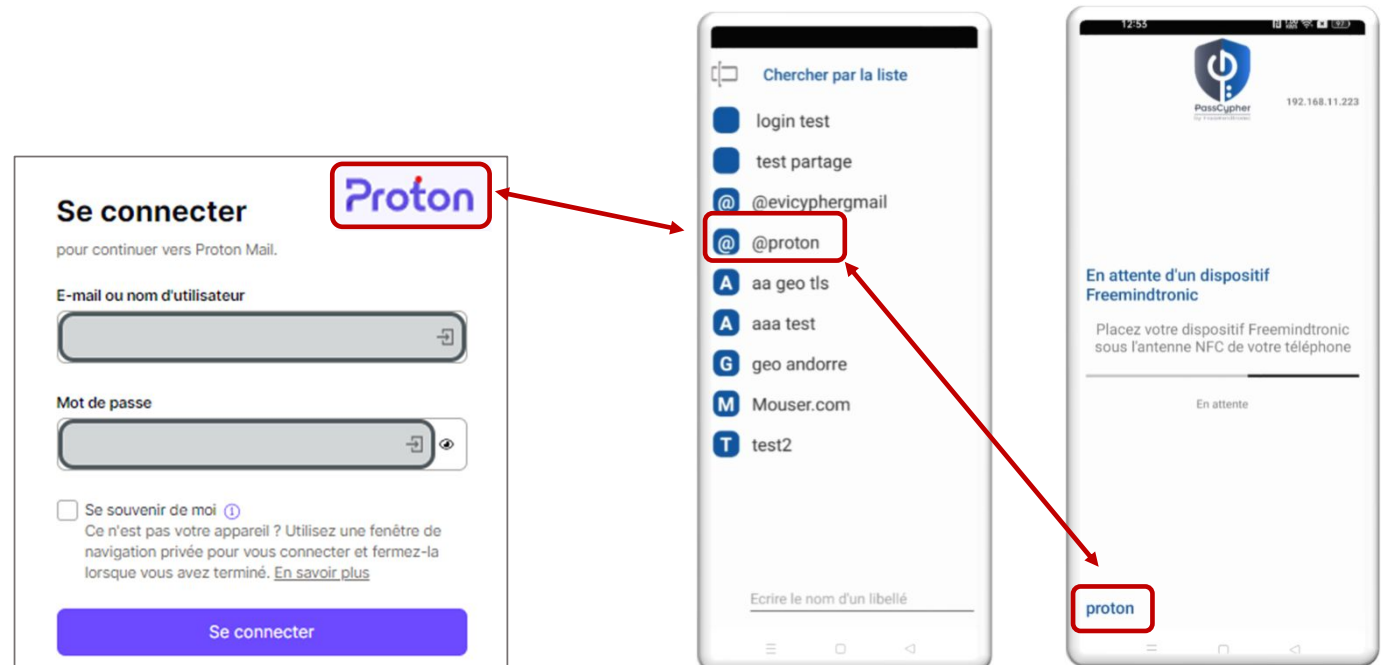


Principe de la connexion

Lors de la première connexion à un site Internet (ou une messagerie), vous devez associer le libellé sauvegardé dans la carte NFC correspondant au site ou à la messagerie.

Lors des visites ultérieures sur ce même site, la connexion sera automatique, le libellé ayant déjà été associé au site.

Il est possible d'utiliser plusieurs libellés sur un même site (exemple : compte professionnel **et** compte personnel). Les explications figurent sur les slides suivantes.



Appairer votre téléphone avec l'Extension 1/2



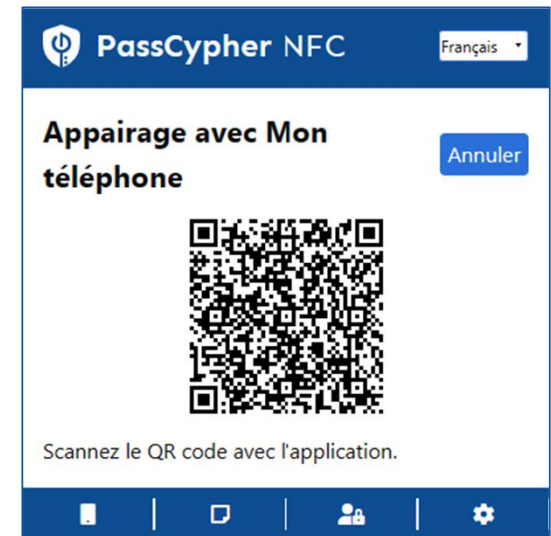
Ouvrez l'extension PassCypher, écrivez le nom du téléphone et cliquez sur « Ajouter »



Ouvrez l'App. et cliquez sur l'icône indiquée ci-dessus



Cliquez sur l'icône « + » et ...



... un QR code s'affiche à l'écran

Plus d'informations sur le fonctionnement de l'Application Freemindtronic dans le tutoriel spécifique

Appairer votre téléphone avec l'Extension 2/2



... scannez le QR code affiché sur l'ordinateur

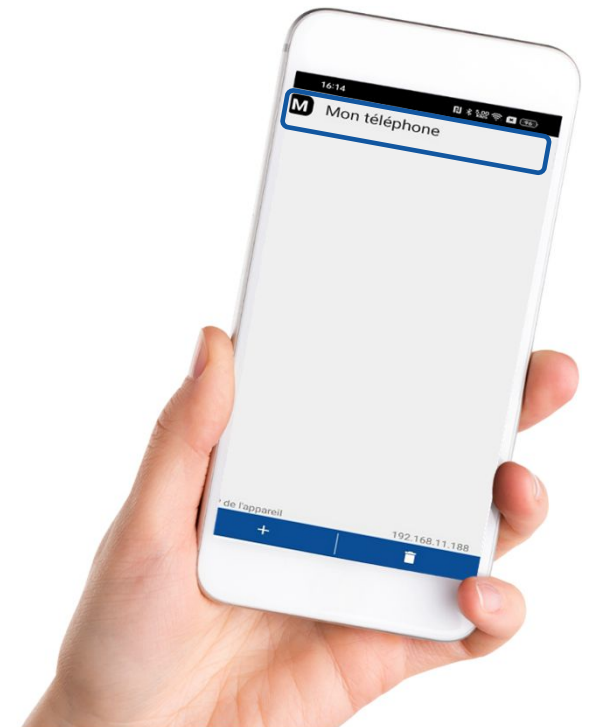


Un **code de sécurité** s'affiche sur votre téléphone



Vérifiez que le code de sécurité affiché est le même que celui sur votre ordinateur. S'ils sont identiques, cliquez sur "**OUI**"

Votre téléphone est maintenant appairé avec l'extension PASSCYPHER. Le nom choisi apparaît dans la liste des téléphones. Vous pouvez appairer un grand nombre de téléphones.



Gestion des téléphones appairés avec l'extension sur votre ordinateur



Ouvrez l'extension PassCypher, cliquez sur l'icône indiquée pour accéder à la liste des téléphones avec indication de leur état (en ligne ou hors ligne)



Cliquez sur l'étoile pour définir un **téléphone favori** auquel les requêtes seront envoyées.

- ✓ Vous pouvez appairer un grand nombre de téléphones différents avec l'extension PassCypher.
- ✓ Pour cela, répétez la procédure d'appairage et donnez un nom différent à chaque téléphone.

Première connexion à la messagerie Proton

Se connecter
pour continuer vers Proton Mail.

E-mail ou nom d'utilisateur

Mot de passe

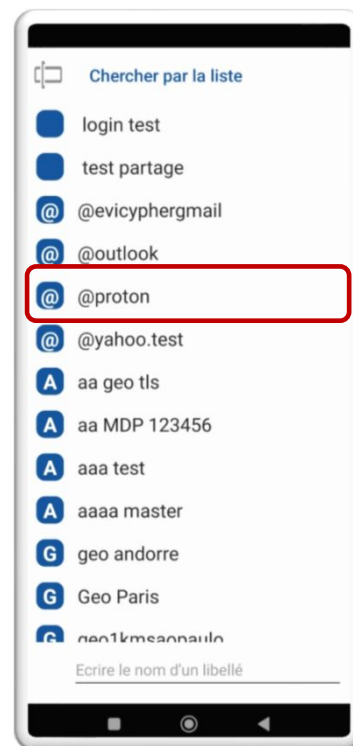
Se souvenir de moi
Recommandé sur les appareils de confiance.
[Pourquoi ?](#)

Se connecter

Allez sur la page de connexion de la messagerie Proton et cliquez sur l'icône indiquée en rouge.



Cliquez sur la requête reçue sur le téléphone et placez la carte sous l'antenne NFC



La liste des libellés s'affiche, cliquez sur « @proton » et placez la carte sous l'antenne NFC

Se connecter
pour continuer vers Proton Mail.

E-mail ou nom d'utilisateur

Mot de passe

Se souvenir de moi
Ce n'est pas votre appareil ? Utilisez une fenêtre de navigation privée pour vous connecter et fermez-la lorsque vous avez terminé. [En savoir plus](#)

Connexion en cours

L'adresse mail et le mot de passe sont remplis automatiquement. La connexion est en cours

Lors des connexions ultérieures, l'étape du choix du libellé est supprimée. Il vous suffit d'ouvrir la requête et de placer le dispositif NFC sous l'antenne NFC du téléphone. Le remplissage des champs et la connexion sont automatiques.

Première connexion à un site internet [Mouser]

CONNEXION

Si vous avez déjà un compte My Mouser, merci de vous connecter.
* Signale un champ obligatoire.
Identifiant utilisateur *

Mot de passe *

Les mots de passe respectent la casse.

Retenir mon identifiant utilisateur sur cet ordinateur

Connexion

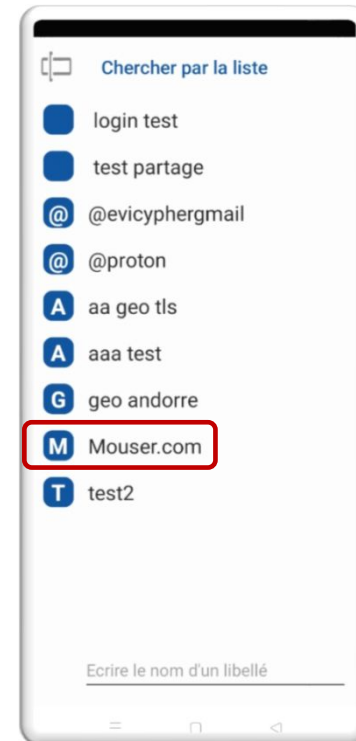
Allez sur la page de connexion du site web « Mouser » et cliquez sur l'icône indiquée en rouge.



Cliquez sur la requête reçue sur le téléphone et placez la carte sous l'antenne NFC



La liste des libellés sauvegardés dans la carte va s'afficher



Cliquez sur le libellé « Mouser.com » et placez la carte sous le téléphone

Si vous avez déjà un compte My Mouser, merci de vous connecter.
* Signale un champ obligatoire.
Identifiant utilisateur *

Mot de passe *

Les mots de passe respectent la casse.

Retenir mon identifiant utilisateur sur cet ordinateur

Connexion

Les informations sont remplies automatiquement. Cliquez sur « Connexion ».

Pour activer la connexion automatique aller dans les Paramètres de l'extension

PassCypher HSM PGP Français

Licence PassCypher

Entrez la licence PassCypher

Cliquez pour obtenir le SN de la carte mère

Télécharger PassCypher Engine

Débloquez plus de fonctionnalités avec la licence PassCypher Engine:
<https://freemindtronic.com/passcypher-engine-hsm-ppg/>

By Freemindtronic

Lors des connexions ultérieures, l'étape du choix du libellé est supprimée. Il vous suffit d'ouvrir la requête et de placer le dispositif NFC sous l'antenne NFC du téléphone. Le remplissage des champs et la connexion sont automatiques.

Récupérer un libellé via le NFC



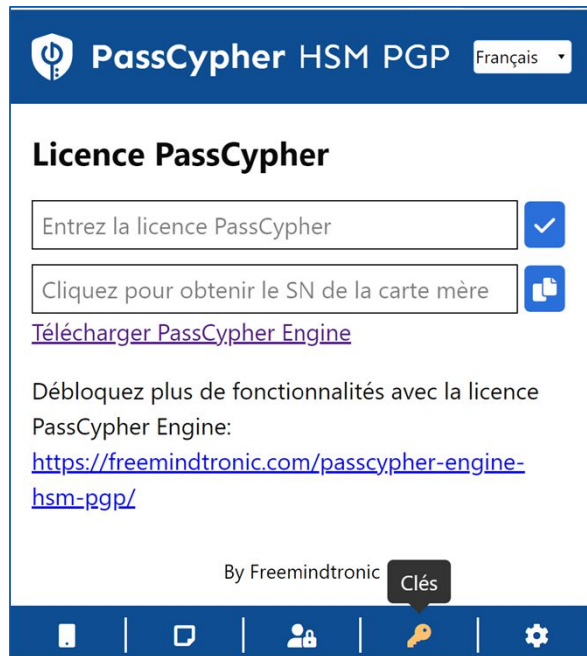
Cliquez sur l'icône indiquée pour accéder à la récupération de vos libellés



Cliquez sur l'icône « Récupérer »

Une **requête** est envoyée à votre téléphone. Placez la carte sous le téléphone et **choisissez le libellé ou la clé Cloud** adéquate. Vous pouvez ensuite **Copier/coller** les informations affichées

Activer la licence (version payante)



Page d'accueil de l'extension

Concerne la version payante de l'extension PassCypher

Plus d'informations cliquez ici [Extension PassCypher HSM PGP](#)

Take back control, Take back power

EviPass Technology

By Freemindtronic Andorra



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



Copyright© 2024 *Tous droits réservés - Produits brevetés - Freemindtronic Andorra*