



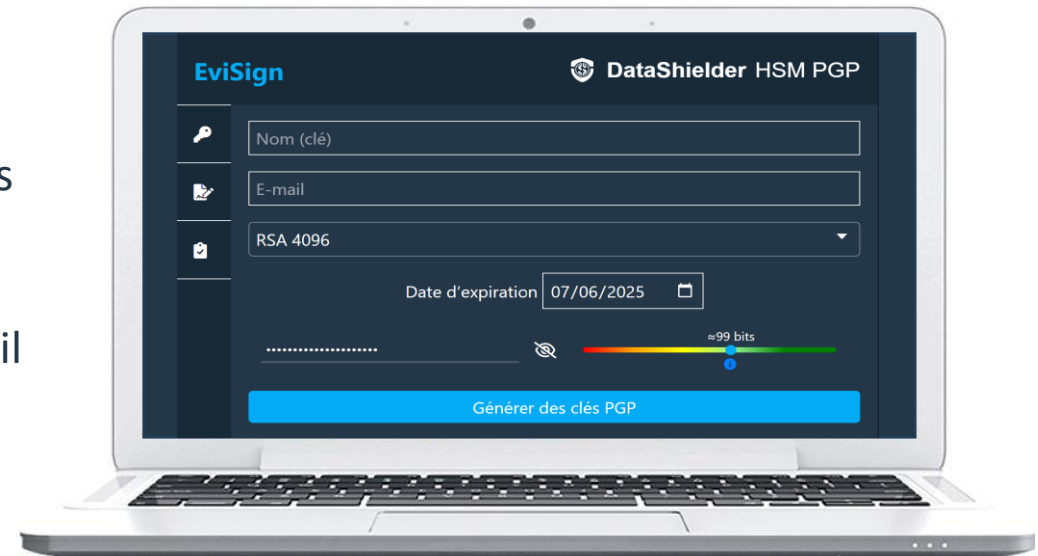
TUTORIEL EXTENSION DATASHIELDER HSM PGP

By Freemindtronic



SOMMAIRE

- Installation de l'extension DataShielder HSM PGP
- Activation de la licence
- Principes de fonctionnement
- Page d'accueil en détail
- Création, partage & importation de clés de chiffrement segmentées
- Chiffrement & déchiffrement automatique de fichiers
- Chiffrement & déchiffrement automatique de textes via un webmail
- Chiffrement & déchiffrement automatique de textes
- Sauvegarde chiffrée de Seed phrases (Bip 39)
- Signature numérique de fichiers
- Fonctionnalités et Paramètres

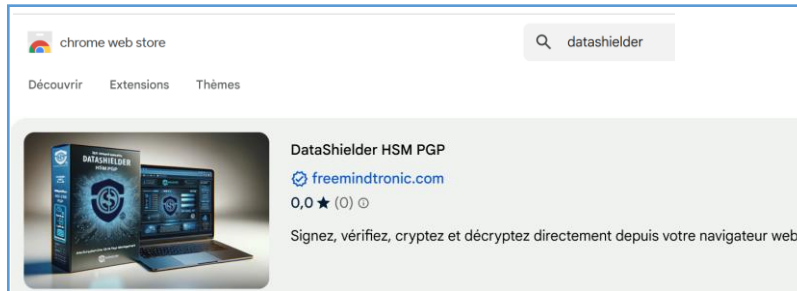


*Pour le fonctionnement avec un dispositif NFC (sans contact) voir le « **Tutoriel Extension DataShielder avec dispositif NFC** »*

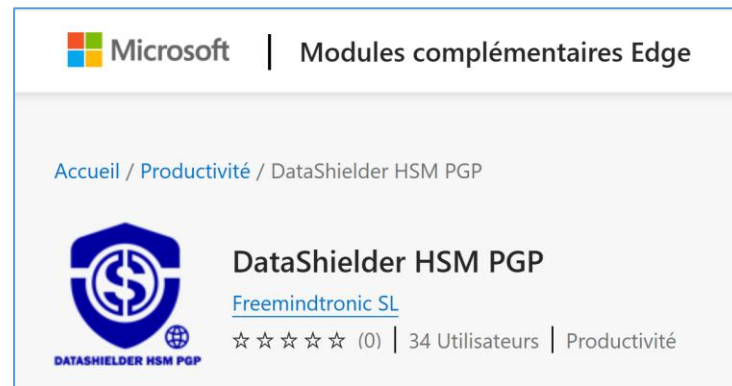
INSTALLATION DE L'EXTENSION

Téléchargez & installez l'extension DataShiolder HSM PGP

CHROME : [chrome web store](#)



MICROSOFT EDGE : [Edge Addons](#)



OPERA : en cours

FIREFOX : en cours

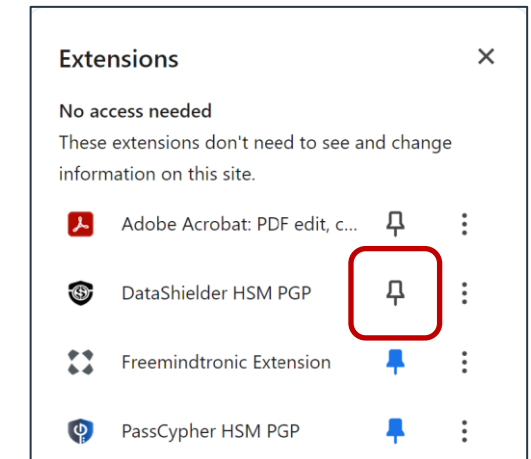
1

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



2

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

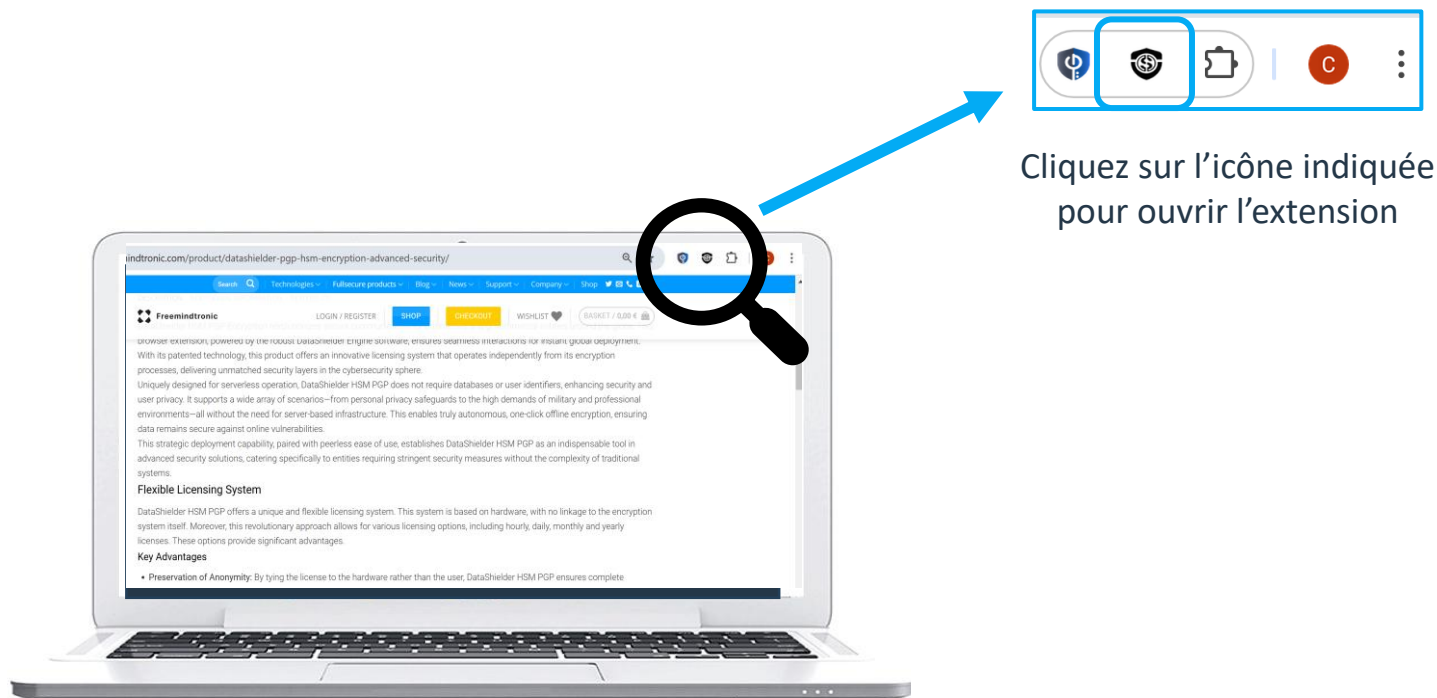


3

L'icône DataShiolder apparaît en haut à droite de l'écran de votre ordinateur. Cliquez pour ouvrir l'extension

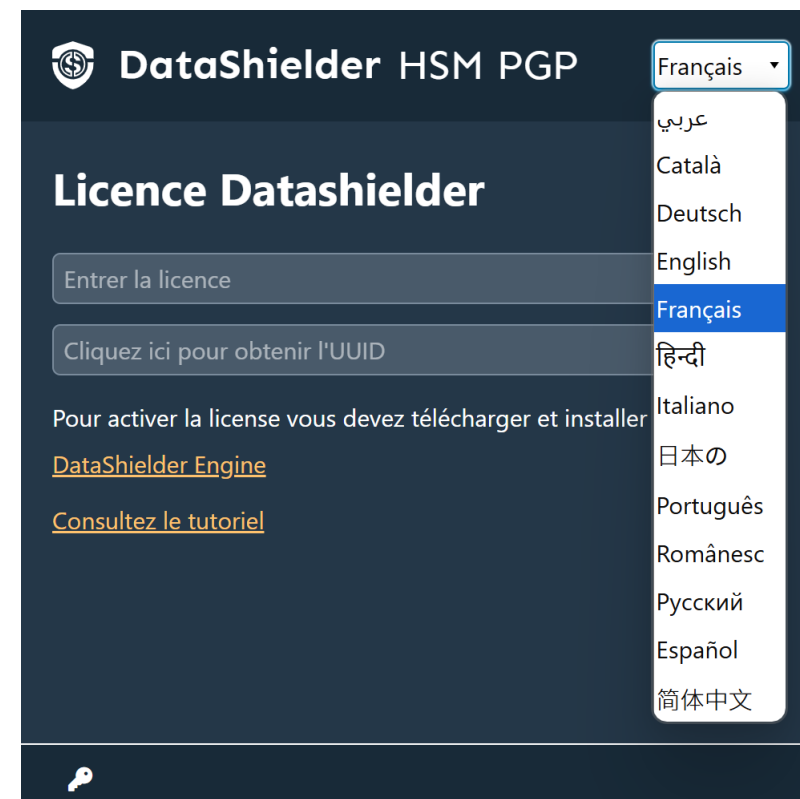


L'EXTENSION EST INSTALLÉE



Pour compléter le processus, cliquez [ici*](https://freemindtronic.com/support/download/#datashielder-engine-microsoft) pour **télécharger DataShielder Engine** et **installer the logiciel** (Windows ou MacOS). Puis allez sur la slide suivante.

(*) <https://freemindtronic.com/support/download/#datashielder-engine-microsoft>

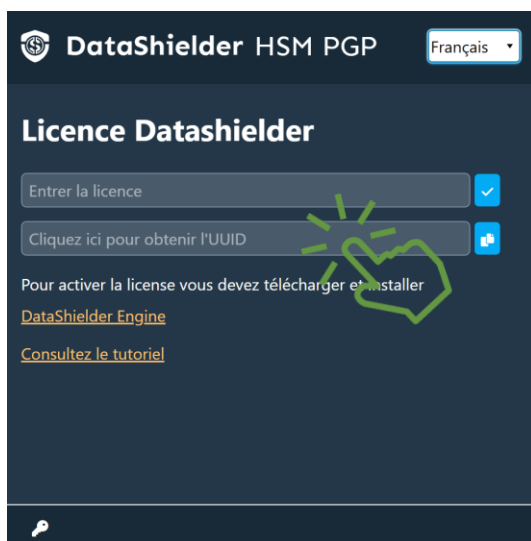


L'extension DataShielder HSM PGP est traduite en 13 langues : Arabe, Allemand, Anglais, Catalan, Chinois, Espagnol, Français, Hindi, Italien, Japonais, Portugais, Roumain et Russe. Vous pouvez choisir dans quelle langue afficher l'extension.

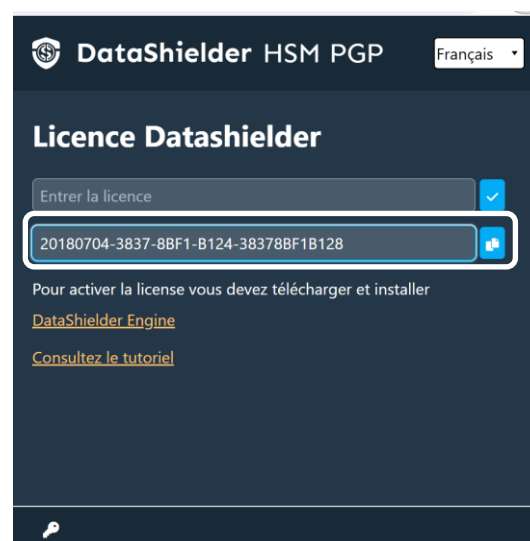
ACTIVEZ LA LICENCE



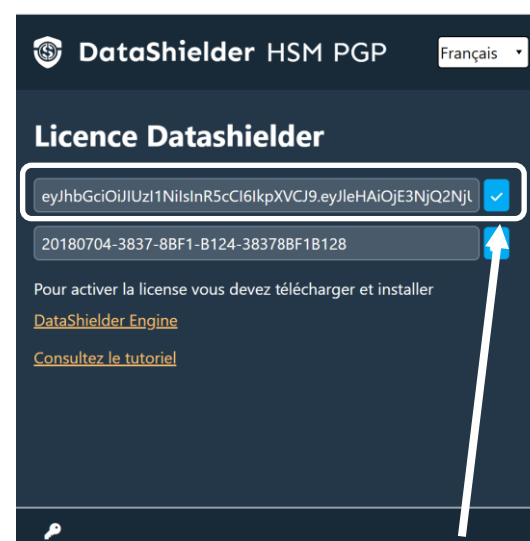
Tutoriel : Activer la licence DataShielder
https://www.youtube.com/watch?v=3I_ZYnAFwik



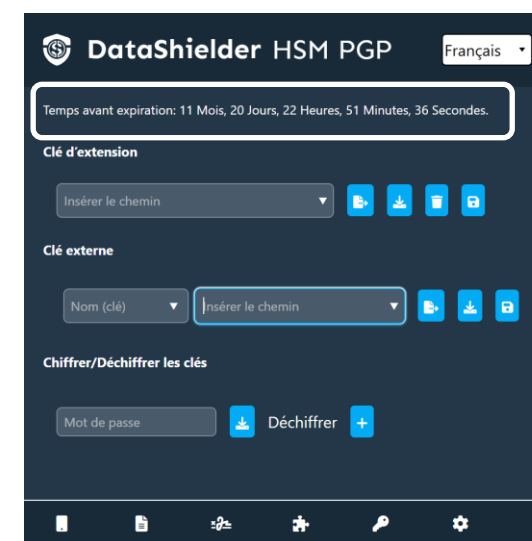
Quand DataShielder est installé, **cliquez** pour obtenir l'**UUID de la carte mère de votre ordinateur**



Copiez ce numéro et envoyez-le par mail à l'adresse indiquée sur le site web de Freemindtronic



Puis, copiez/collez le numéro de licence reçu en retour et 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*

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

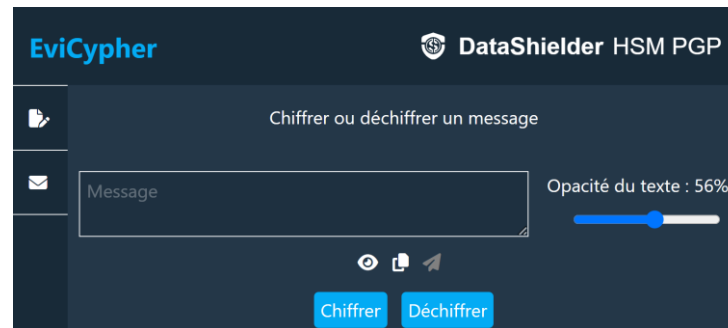
COMMENT CELA FONCTIONNE ?

- **DataShielder HSM PGP** est une extension qui permet plusieurs méthodes de chiffrement automatique
 1. Chiffrement de fichiers via la fonctionnalité « Glisser/déposer » ou double clic sur le fichier
 2. Chiffrement de textes directement depuis l'extension DataShielder HSM PGP
 3. Chiffrement de textes via un webmail (Gmail, Outlook, Yandex, Yahoo, iCloud, Roundcube ...)
- Création de vos clés de chiffrement segmentées et partage avec votre ou vos correspondant(s)
- Une clé segmentée = une **clé d'extension** stockée dans le local storage de votre navigateur web et une **clé externe** stockée à l'endroit que vous choisissez (clé USB, SSD, cloud ...)
- Rédaction de votre message et clic sur le bouton « Chiffrer ». Le chiffrement est automatique

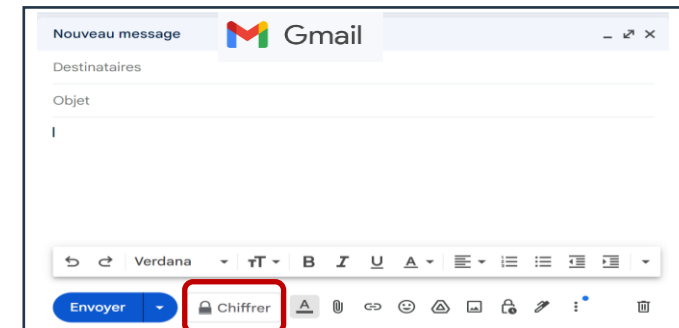
1



2



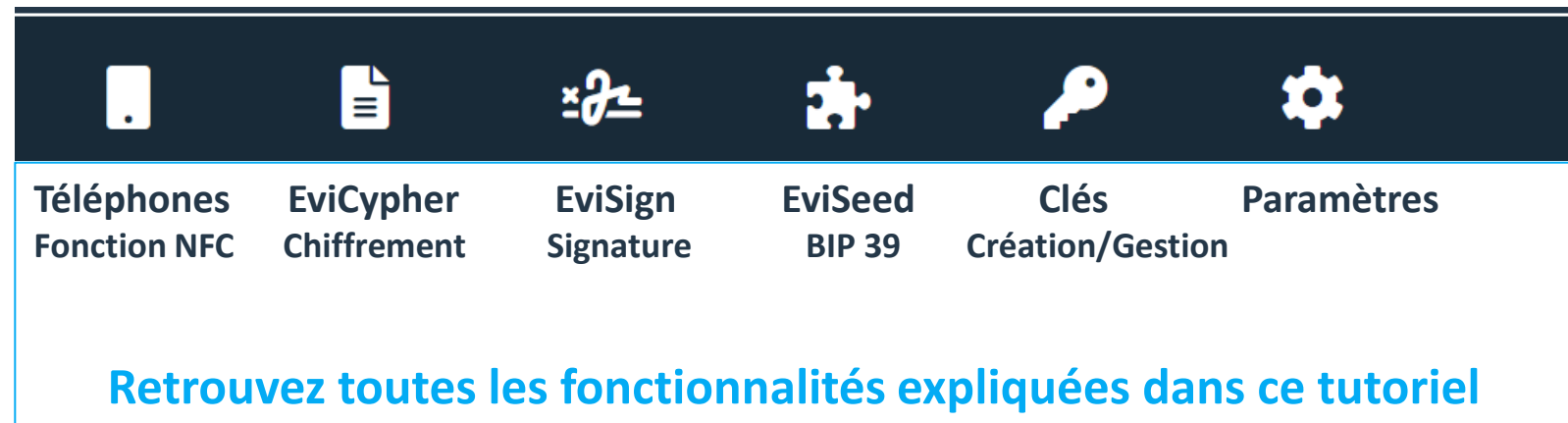
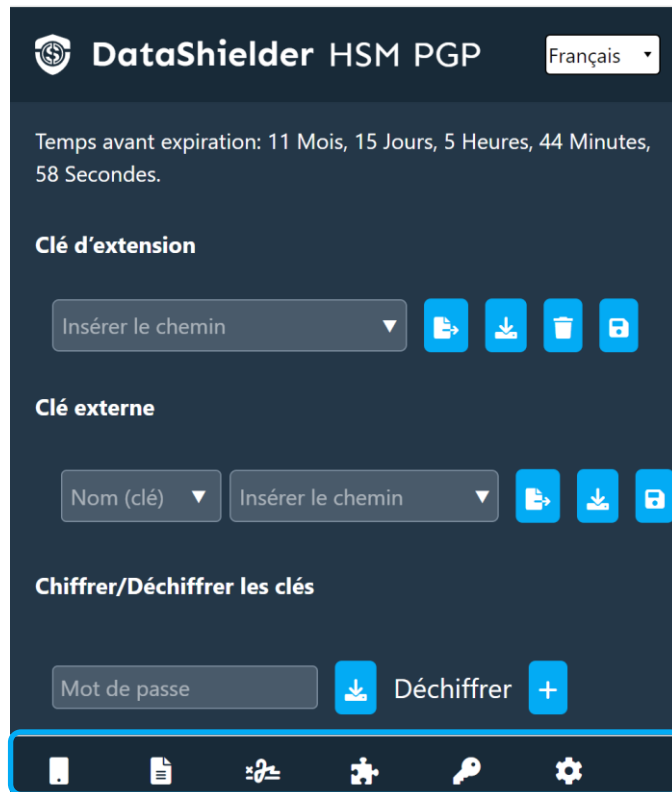
3



LA PAGE D'ACCUEIL EN DÉTAIL

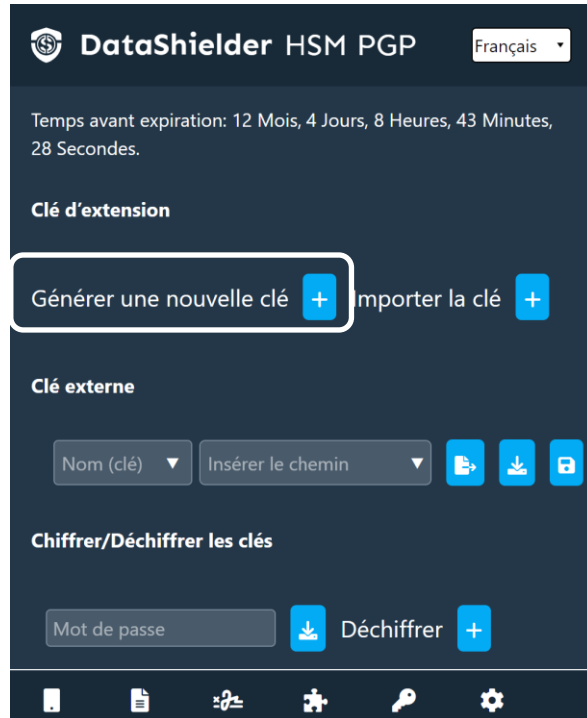
Lorsque vous ouvrez l'extension DataShielder, la fenêtre ci-dessous s'affiche.

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



CRÉEZ* VOS CLÉS DE CHIFFREMENT SEGMENTÉES

(*) Si votre correspondant vous envoie sa clé segmentée (clé d'extension & clé externe) allez aux slides 11 à 13



DataShielder HSM PGP Français

Temps avant expiration: 12 Mois, 4 Jours, 8 Heures, 43 Minutes, 28 Secondes.

Clé d'extension

Générer une nouvelle clé + Importer la clé +

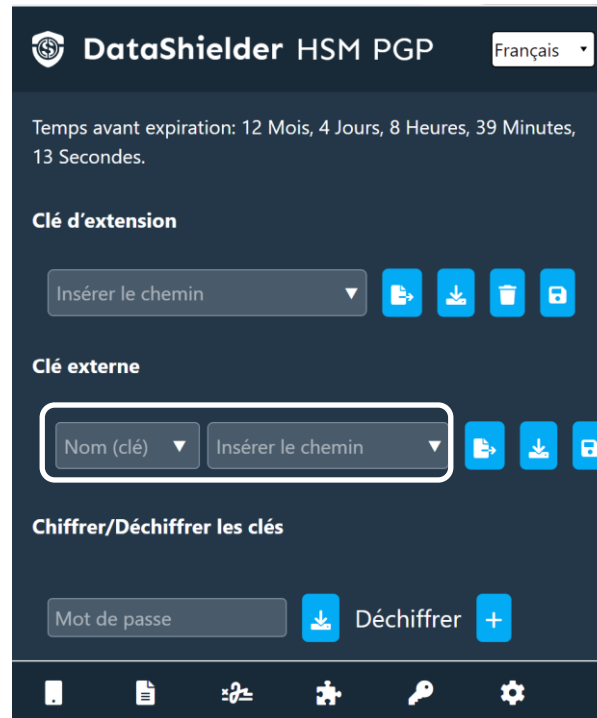
Clé externe

Nom (clé) Insérer le chemin

Chiffrer/Déchiffrer les clés

Mot de passe Déchiffrer +

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



DataShielder HSM PGP Français

Temps avant expiration: 12 Mois, 4 Jours, 8 Heures, 39 Minutes, 13 Secondes.

Clé d'extension

Insérer le chemin

Clé externe

Nom (clé) Insérer le chemin

Chiffrer/Déchiffrer les clés

Mot de passe Déchiffrer +

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...)



DataShielder HSM PGP Français

Temps avant expiration: 12 Mois, 4 Jours, 8 Heures, 34 Minutes, 2 Secondes.

Clé d'extension

Insérer le chemin

Clé externe

Marie E:\USB EviKey NFC HSM

Chiffrer/Déchiffrer les clés

Mot de passe Déchiffrer +

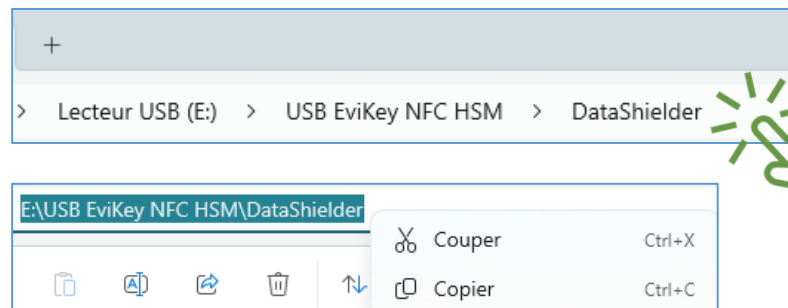
Cliquez ensuite sur l'icône « **EXPORTER** » puis sur l'icône « **SAUVEGARDER** ». La clé externe « **Marie** » est créée et enregistrée à l'endroit que vous avez indiqué.

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

INSÉREZ LE CHEMIN D'ACCÈS

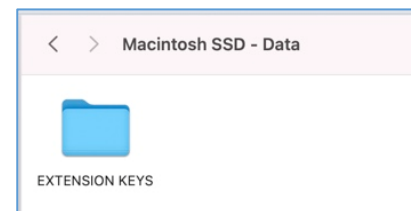
- Choisissez l'endroit où vous allez **sauvegarder votre clé externe** (disque dur interne ou externe, clé USB)
- Indiquez ensuite le chemin d'accès exact de cet emplacement
- Vous trouverez ci-dessous comment faire si vous utilisez un ordinateur sous système d'exploitation **Windows** ou **macOS**
-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

Windows

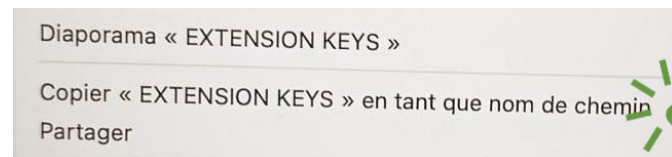


1. L'emplacement est affiché
2. Cliquez dans la fenêtre, le chemin d'accès est sélectionné
3. Faites un clic droit, le bouton « Copier » apparaît
4. Cliquez sur « Copier » et collez dans l'extension sans ajouter aucun autre caractère

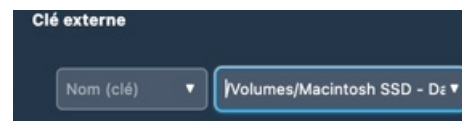
macOS



1. L'emplacement est affiché
2. Maintenez la touche « alt » enfoncée et faites un clic droit sur la souris

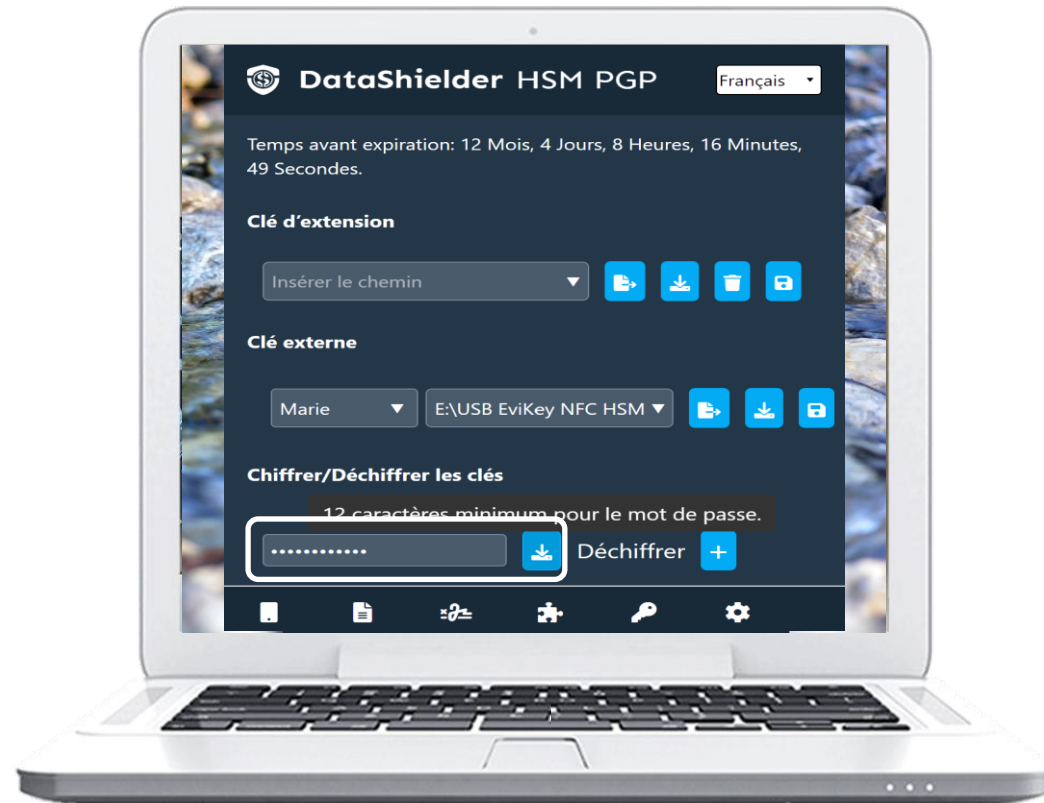


3. Cliquez sur « Copier »

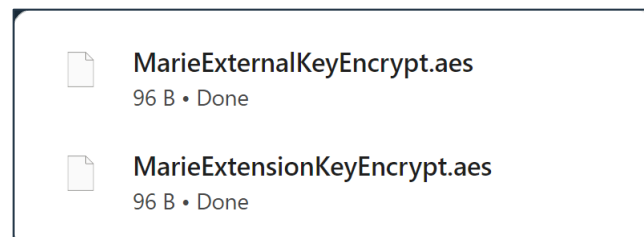


4. et collez dans l'extension sans ajouter aucun autre caractère

PARTAGEZ VOS CLÉS DE CHIFFREMENT SEGMENTÉES



Pour partager les clés avec un correspondant, vous allez les **chiffrer** : Saisissez un mot de passe de 12 caractères minimum et cliquez sur la flèche « **IMPORTER** »



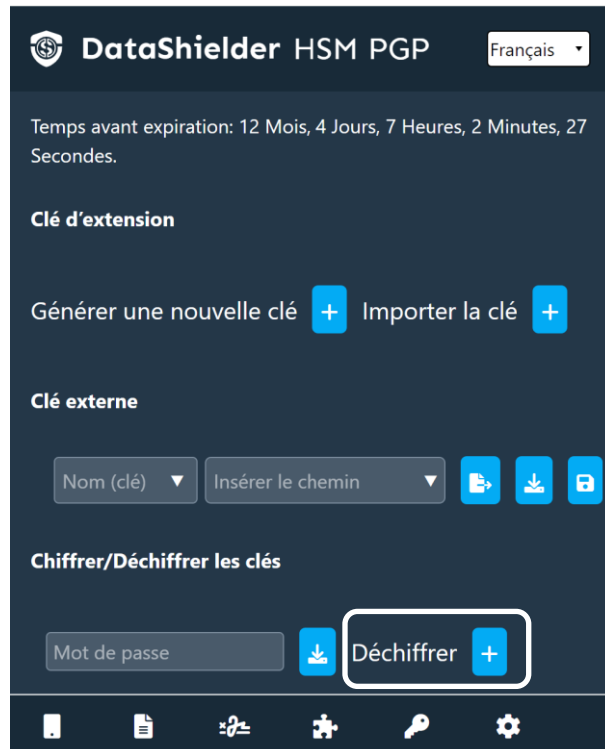
Automatiquement la clé externe et la clé d'extension sont **chiffrées**. Vous pouvez les récupérer dans le dossier « **Téléchargements** »



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

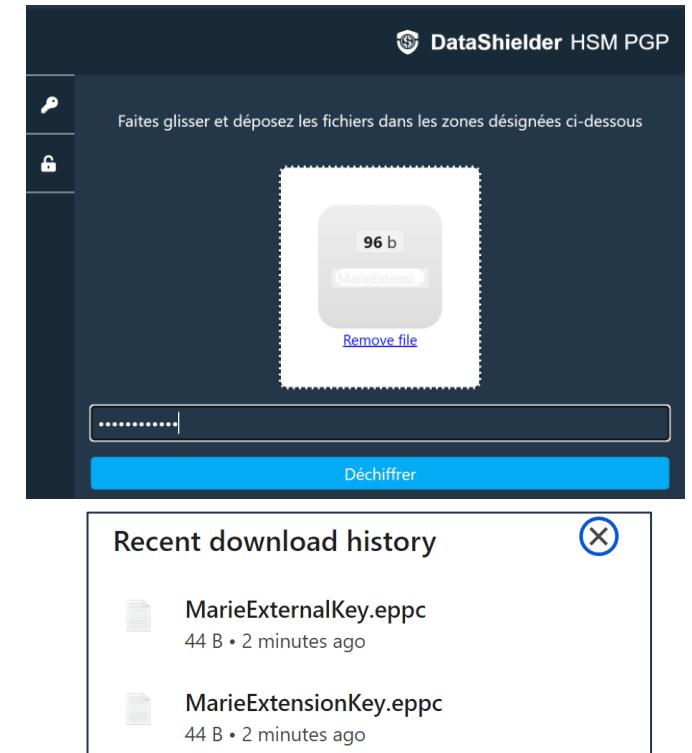
Commencez par déchiffrer les segments de clé



Pour déchiffrer les clés envoyées par un correspondant, cliquez sur l'icône indiquée



Cliquez dans la fenêtre blanche et insérez la **clé d'extension chiffrée**. 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

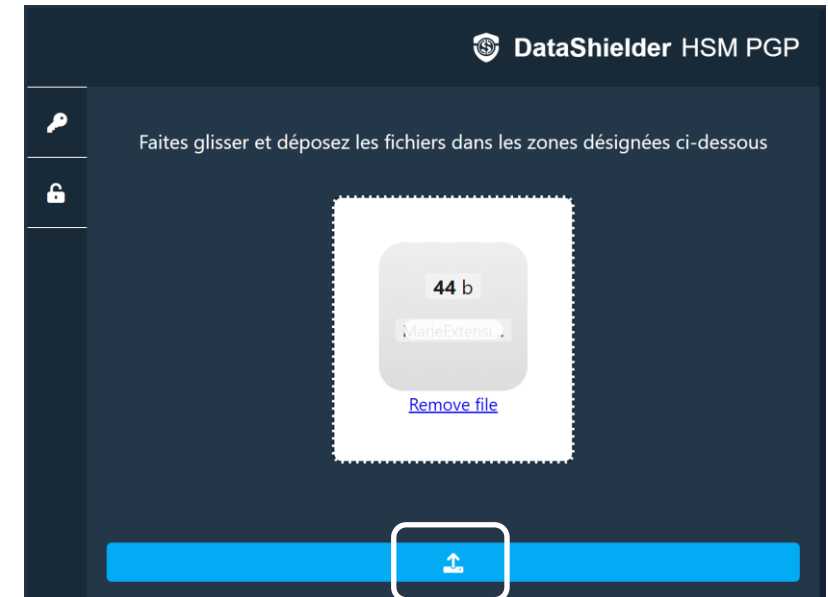
Importez d'abord la clé d'extension



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



Récupérez le fichier déchiffré et déposez-le à l'endroit que vous aurez choisi



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 3/3

Indiquez le chemin où est stockée la clé externe



Stockez la clé externe « **MarieExternalKey.eppc** » à l'endroit de votre choix* (ici un **SSD externe**). Pour que l'extension puisse accéder à la clé externe, écrivez le nom de la clé (**Marie**) et entrez le **chemin d'accès à la clé**. Cliquez ensuite sur l'icône indiquée pour la sauvegarder.



L'importation des clés est terminée. Vous pouvez commencer à chiffrer des messages ou des fichiers. Pour cela, cliquez sur l'icône « **EviCypher** »

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

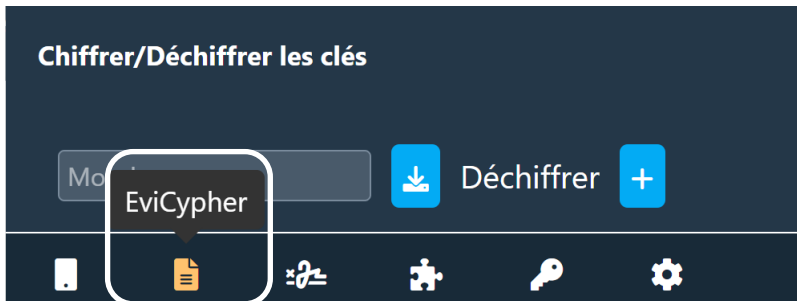
TOUT EST PRÊT MAINTENANT POUR CHIFFRER DES TEXTES ET DES FICHIERS

1. Un premier clic sur l'icône encadrée en rouge ci-dessous pour ouvrir l'extension
2. Un second clic pour accéder à EviCypher
3. Et enfin un clic pour choisir le chiffrement de fichiers ou de textes

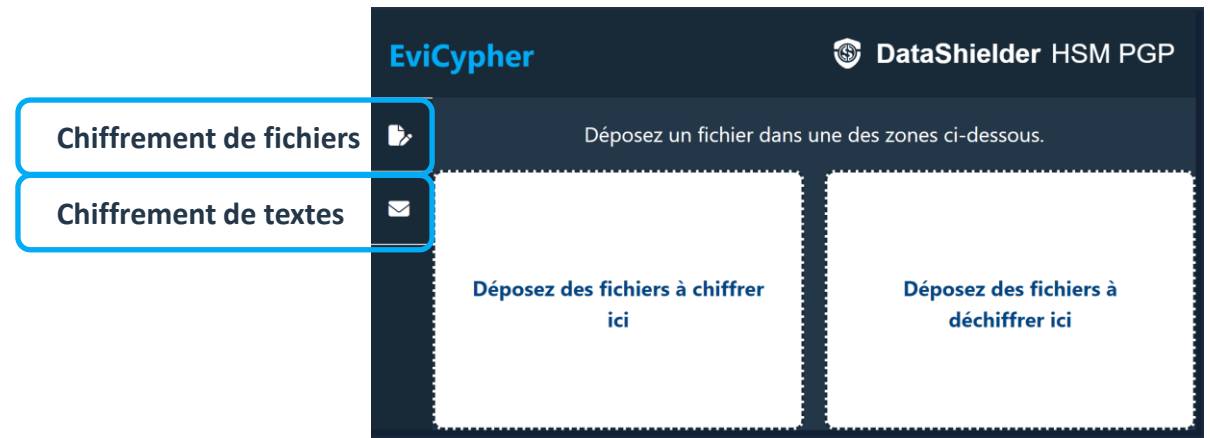
1



2



3 Chiffrement de textes ou de fichiers



CHIFFREMENT DE FICHIERS*



Tutoriel : Comment chiffrer des fichiers

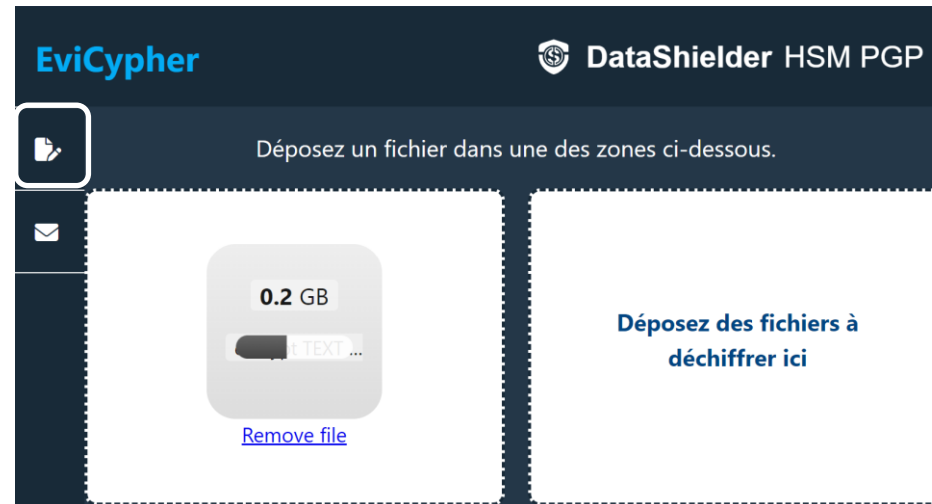
<https://youtu.be/Uyk0XGmaU3w?si=HEzZ0ooN156OsT2U>

1. **Double/clic ou dépôt du fichier** à chiffrer à l'emplacement prévu
2. Le chiffrement est **automatique**
3. Le **fichier chiffré** est disponible dans le dossier « Téléchargements »

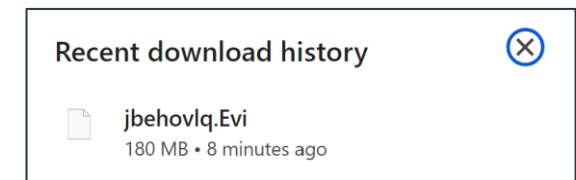
1. Déposez votre fichier



2. Chiffrement en cours



3. Fichier chiffré disponible



(*) Tous les types de fichiers sont compatibles : jpeg, pdf, word, excel, PowerPoint, vidéos

DÉCHIFFREMENT DE FICHIERS

1. **Déposez le fichier** à chiffrer à l'emplacement prévu
2. Le déchiffrement est **automatique**
3. Le **fichier déchiffré** est disponible dans le dossier « Téléchargements »

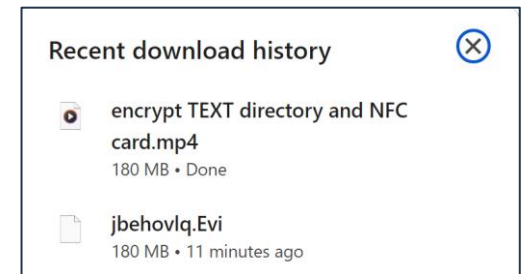
1. Déposez votre fichier



2. Déchiffrement en cours



3. Fichier déchiffré disponible



CHIFFREMENT DES TEXTES : DEUX POSSIBILITÉS

UTILISATION UNIVERSELLE



L'extension est compatible avec tous les services de messageries, chats... Dans ce cas-là, le chiffrement et le déchiffrement se feront **directement depuis l'extension**.

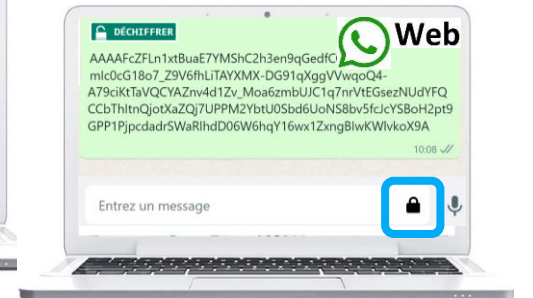
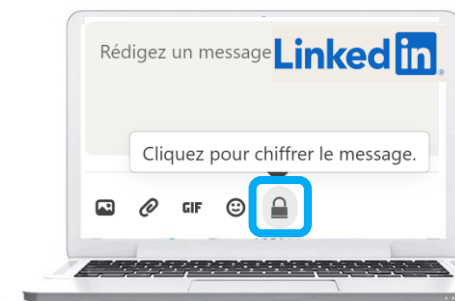
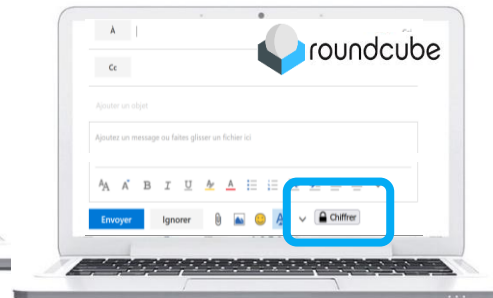
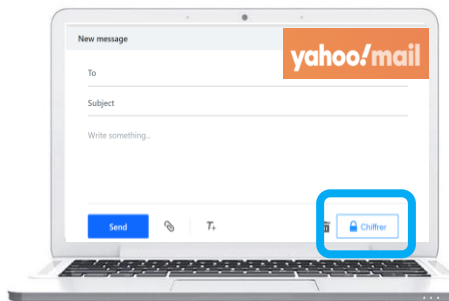
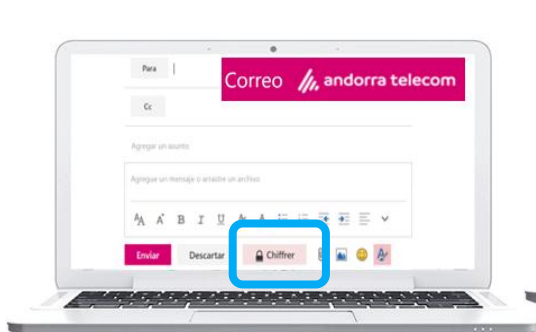
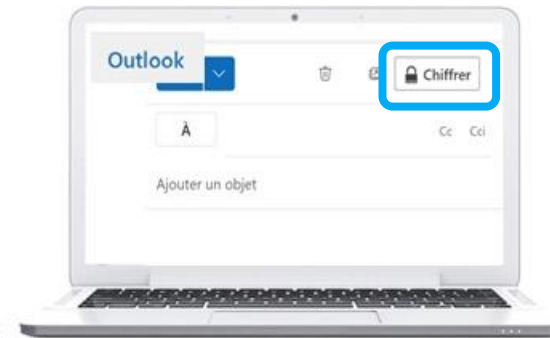
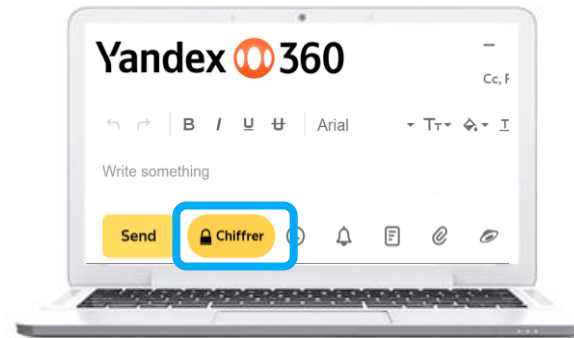
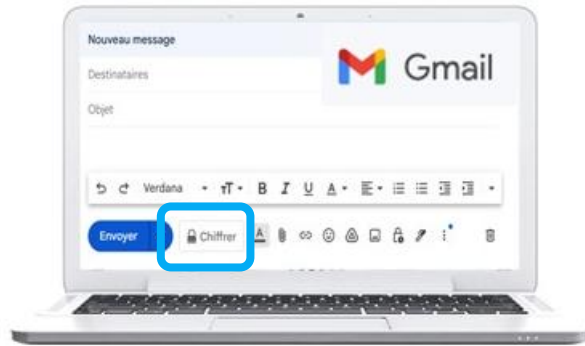
UTILISATION WEBMAILS



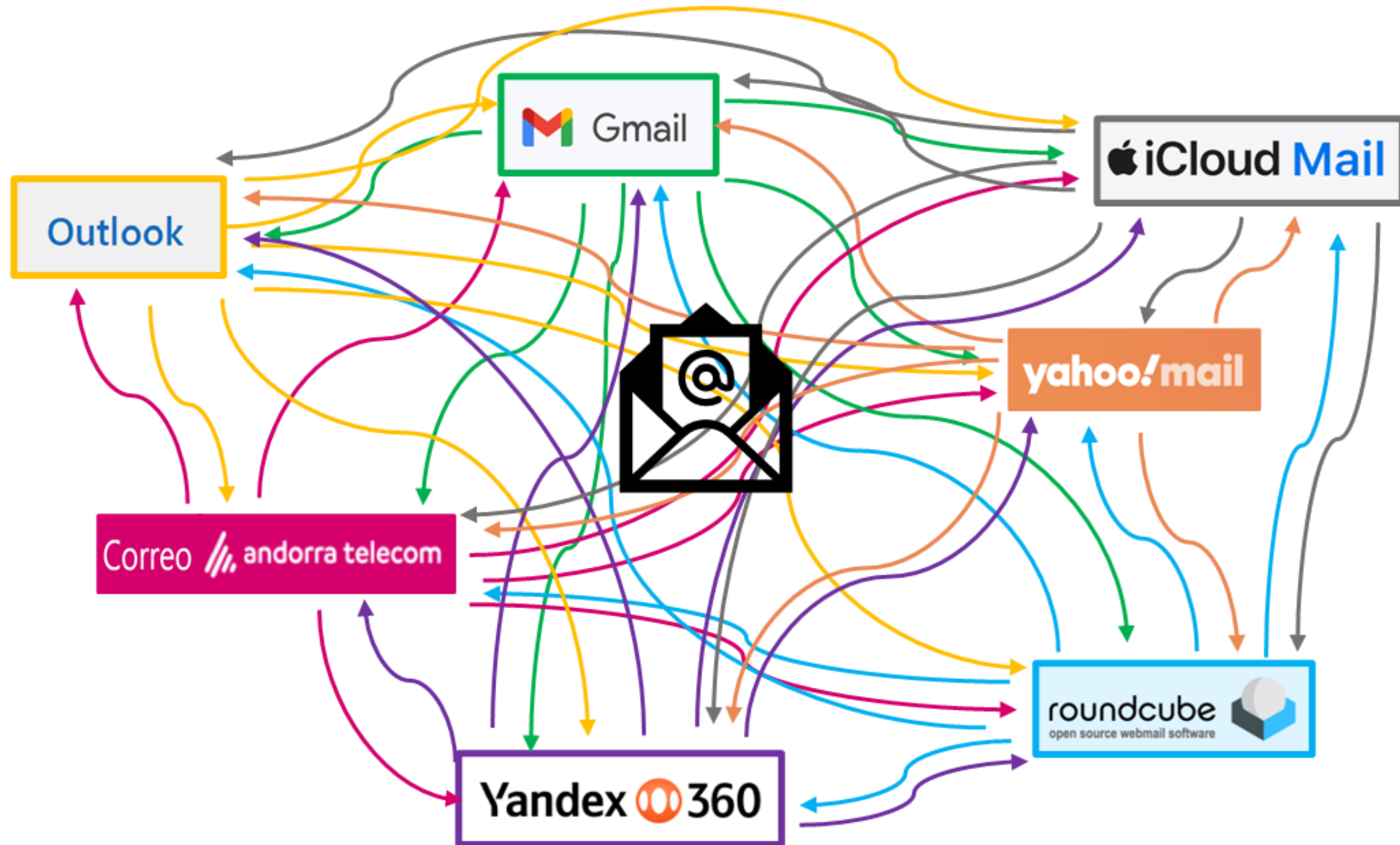
L'extension est compatible avec certains clients de messagerie qui utilisent un navigateur web pour accéder à vos emails (webmails). Dans ce cas là, le chiffrement et le déchiffrement se feront automatiquement **directement dans le webmail**.

SOLUTION N° 1 : UTILISATION WEBMAILS

- Si vous utilisez un webmail compatible avec notre extension, **vous ne changez pas vos habitudes**
- Rédigez votre mail et cliquez sur le bouton « **CHIFFRER** » avant d'envoyer à votre correspondant
- Ce dernier, s'il utilise un webmail compatible, devra simplement cliquer sur le bouton « **DÉCHIFFRER** » pour lire votre message



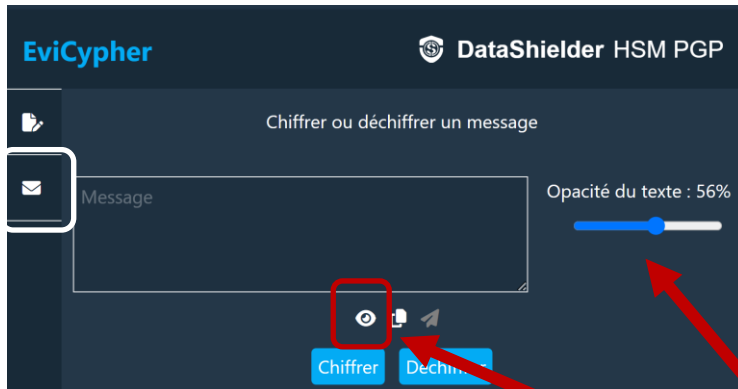
COMMUNIQUEZ SANS CONTRAINTE



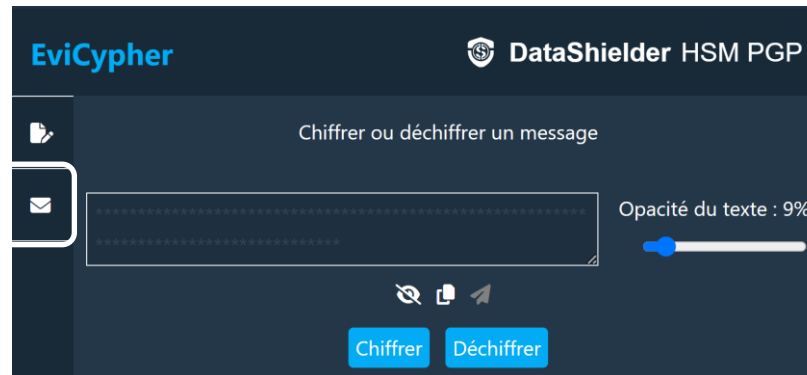
SOLUTION N° 2 : UTILISATION UNIVERSELLE

1. **Rédigez** votre message dans l'emplacement prévu
2. Cliquez sur « **CHIFFRER** ». Le chiffrement est automatique
3. Le **message chiffré** s'affiche à l'écran, vous pouvez l'envoyer

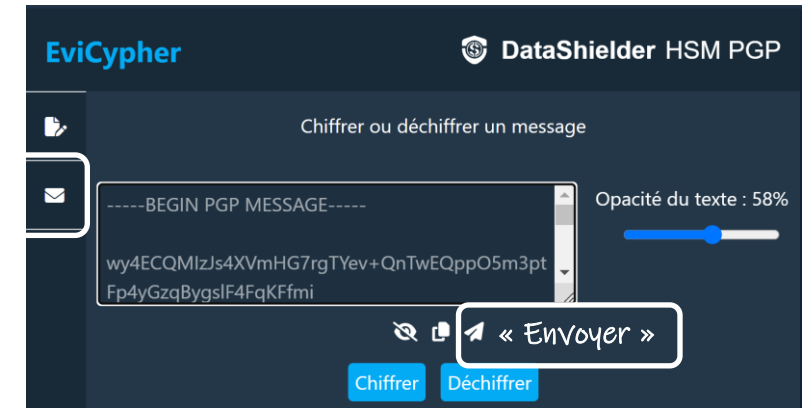
1. Rédigez votre message



2. Cliquez sur l'icône « Chiffrer »



3. Le message est chiffré. Vous pouvez le copier ou cliquez sur l'icône pour l'envoyer



Vous pouvez intervenir pour opacifier le texte lors de sa saisie pour des raisons de confidentialité. Vous pouvez également faire « disparaître » le texte en cliquant sur l'icône indiquée.



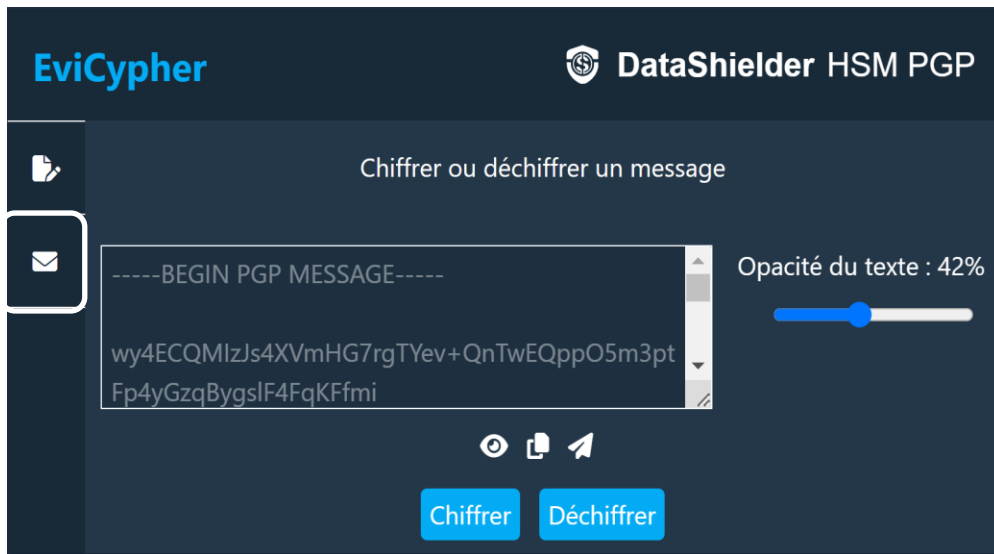
Tutoriel : Comment utiliser l'opacité du texte

<https://youtu.be/xdoJ9JGYtmo?si=OisOAEIglAhcQZDV>

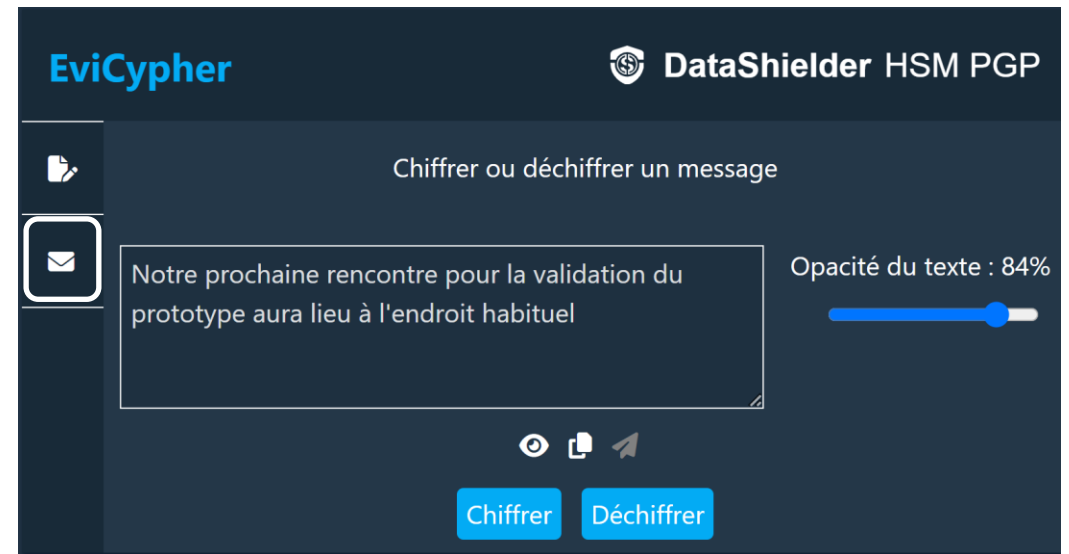
DÉCHIFFREMENT DE TEXTES

1. **Copiez** le message reçu et **collez-le** dans l'emplacement prévu
2. Cliquez sur « **Déchiffrer** »
3. Le déchiffrement est **automatique**

1. Copiez/collez le message chiffré & cliquez sur « Déchiffrer »



2. Le message est déchiffré.



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.

 **DataShielder HSM PGP** Français ▼

Temps avant expiration: 12 Mois, 4 Jours, 8 Heures, 39 Minutes, 13 Secondes.

Clé d'extension

1

Insérer le chemin ▼

2



3



4



5



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 clé d'extension

The screenshot shows the 'DataShieler HSM PGP' interface. At the top right, there is a language dropdown set to 'Français'. Below the header, the 'Clé externe' section is visible. It contains five numbered steps: 1. A dropdown menu labeled 'Nom (clé)'. 2. A dropdown menu labeled 'Insérer le chemin'. 3. A blue button with a document icon. 4. A blue button with a download icon. 5. A blue button with a save icon.

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

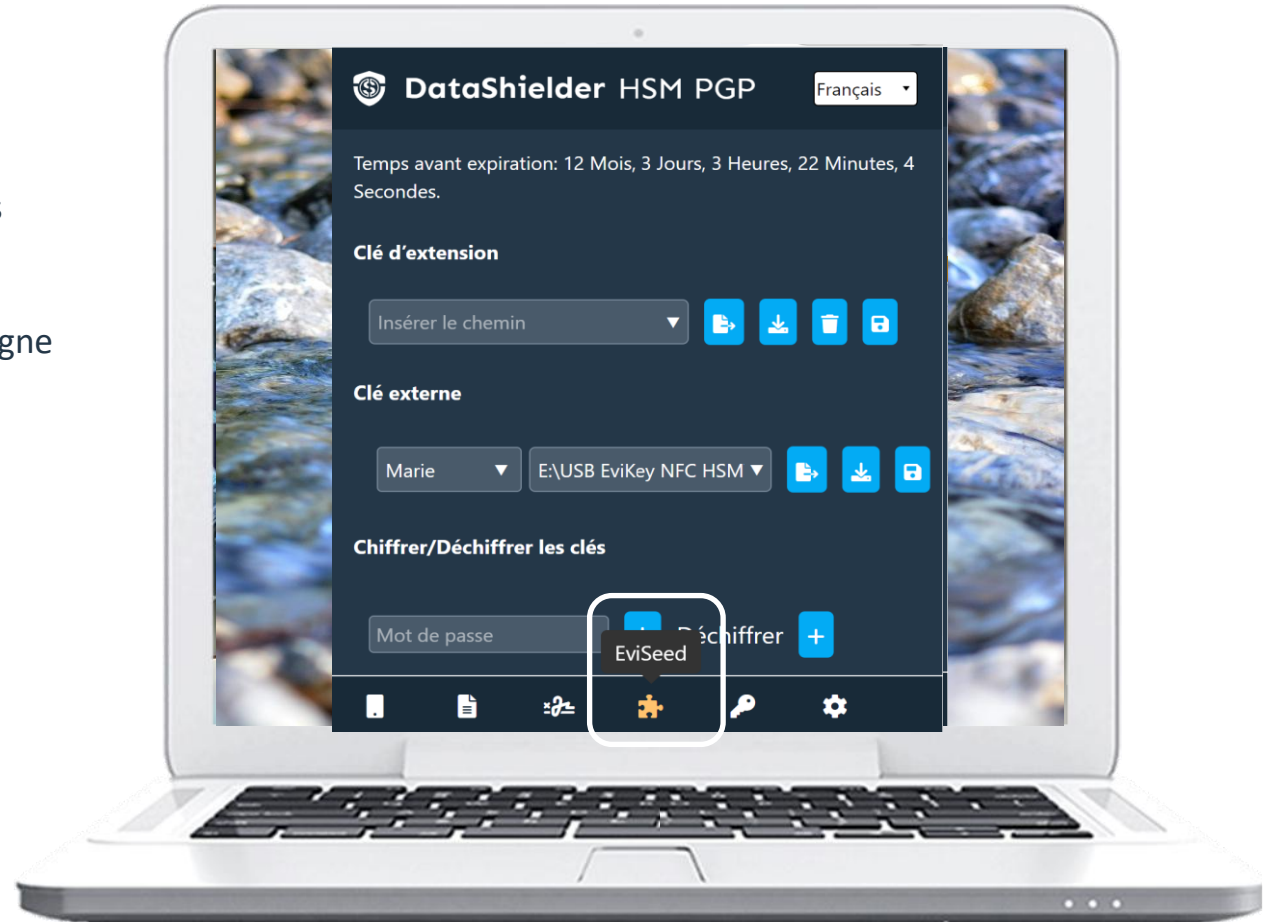
4. En cliquant sur cette icône vous pouvez télécharger la clé et la sauvegarder à l'endroit de votre choix

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

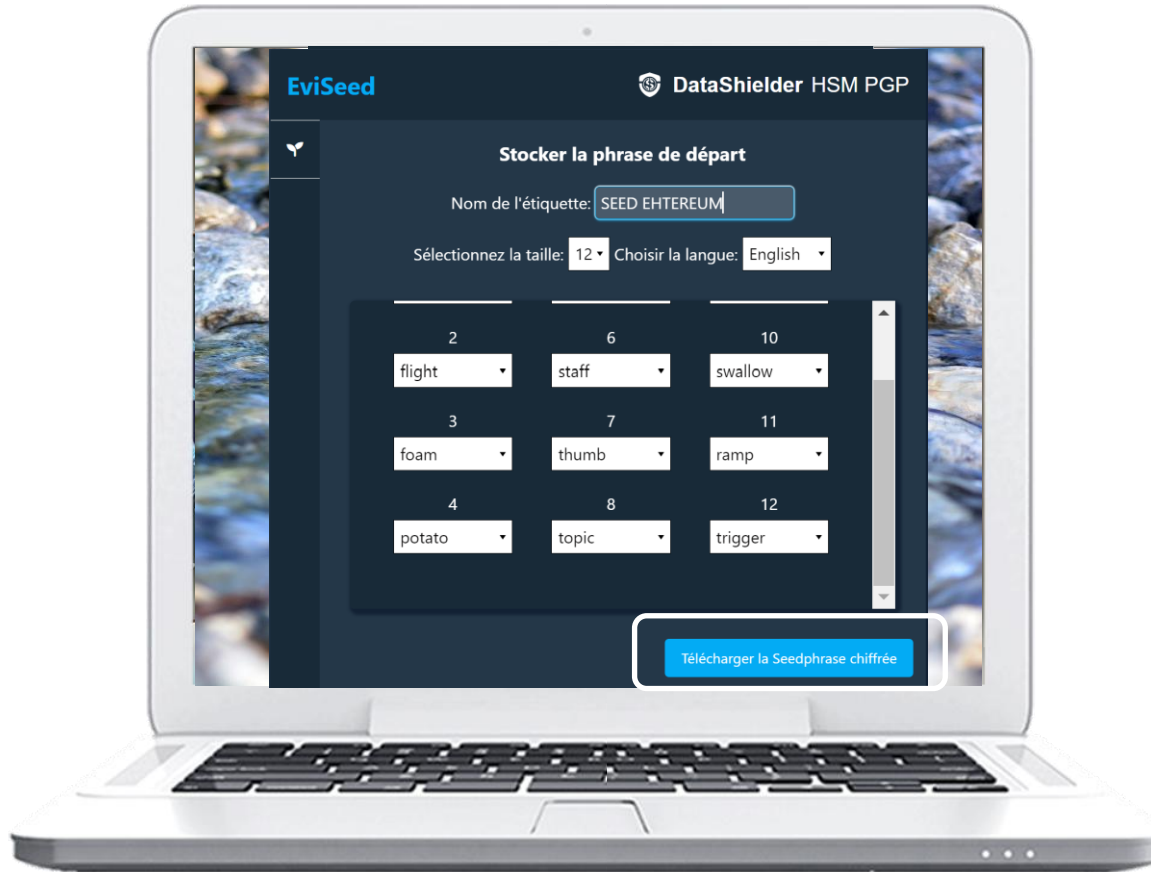
This screenshot shows the 'Clé externe' section with a dropdown menu open for step 2. The dropdown menu lists three paths: 'F:\Clés DataShieler', 'E:\USB EviKey NFC HSM', and 'D:\DataShieler Keys'. Each path has an 'X' icon to its right. The 'Nom (clé)' dropdown is set to 'Krys'. Below the dropdowns, there is a 'Chiffrer/Déchi' section with a 'Mot de passe' field and a blue button with a plus sign.

DÉCOUVERTE D'EVISEED

- **EviSeed est une technologie** qui permet de sécuriser les SEED phrases (BIP 39)
- **Les phrases de départ** doivent être sauvegardées hors ligne
- Elles sont composées d'un nombre de mots variables
- Elles peuvent être écrites dans plusieurs langues
- La sauvegarde est effectuée de manière chiffrée



SAUVEGARDEZ UNE PHRASE DE DÉPART (BIP 39)



1. Donnez un nom à votre SEED phrase
2. Sélectionner le nombre de mots et choisissez la langue de saisie
3. Entrer les mots dans le bon ordre
4. Cliquez sur « **Télécharger la Seed phrase chiffrée** »

Recent download history

 fycfzxtb.Evi
239 B • Done

La **Seedphrase chiffrée** est disponible dans le dossier « **Téléchargements** ».

Vous pouvez la stocker en toute sécurité dans un ou plusieurs emplacements de votre choix.

Pour déchiffrer le fichier, allez dans EviCypher

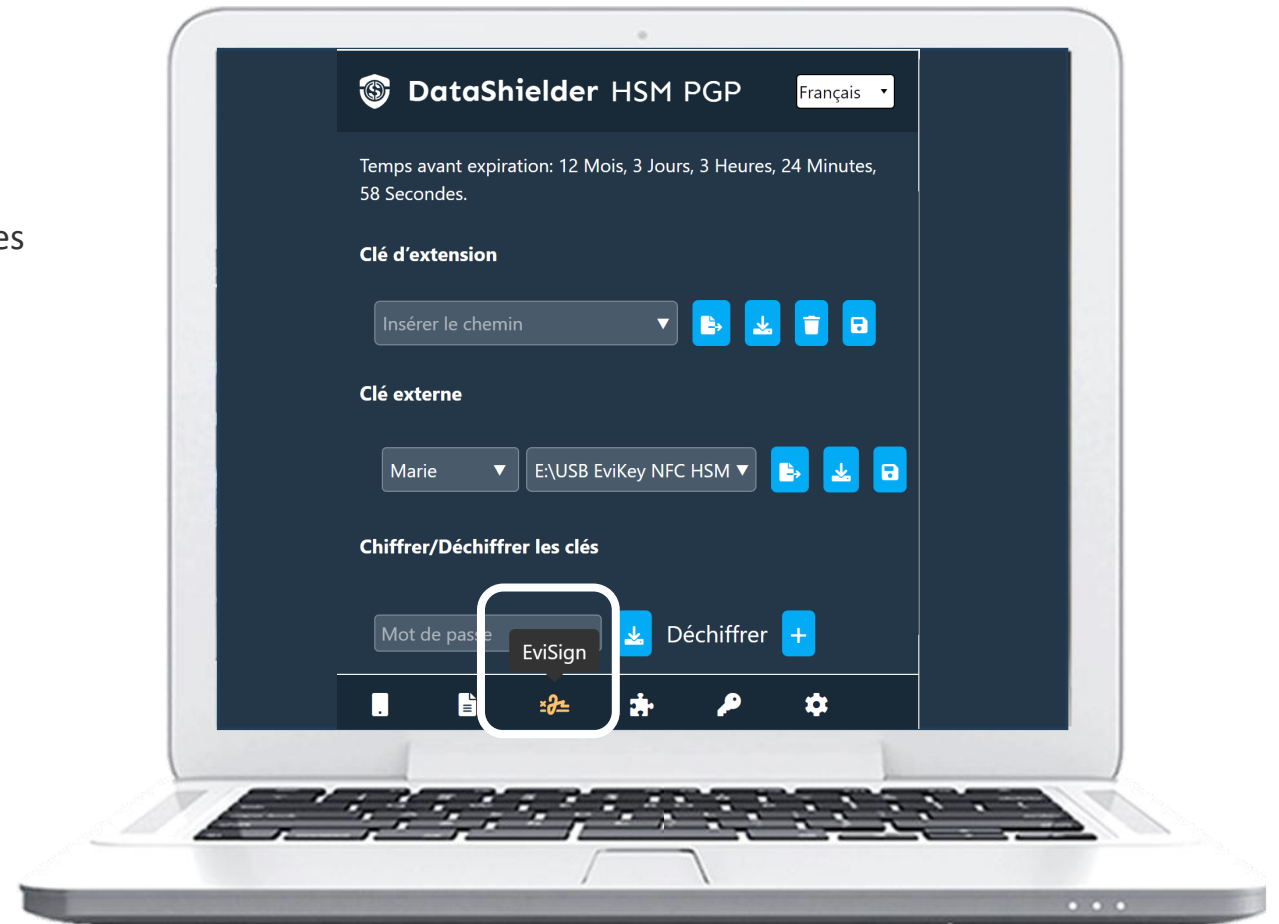
Suivez la procédure de déchiffrement expliquée dans les slides précédentes



Une vérification de la validité de la phrase de départ est effectuée (CHECKSUM). Si les mots sont incorrects ou écrits dans le désordre, un message d'erreur apparaît empêchant la sauvegarde des données.

SIGNATURE NUMÉRIQUE DE FICHIERS

- **EviSign est une technologie innovante** qui permet de signer des documents électroniques en toute confiance.
- Son système **d'authentification par clé segmentée**, son **horodatage** et sa capacité à permettre aux utilisateurs de contrôler entièrement leurs **clés de chiffrement** et leurs données sensibles en font une solution fiable.
- Elle est conforme aux normes et réglementations en vigueur.



PRINCIPE DE FONCTIONNEMENT



Cliquez pour accéder à EviSign

CRÉÉZ UNE PAIRE DE CLÉS PGP



Tutoriel : Générer une paire de clés RSA/ECC

https://youtu.be/Uyfktz1Rclg?si=B7_3bysQdUGAHpRi

Choisissez l'algorithme

Choisissez la date d'expiration

Compléter toutes les informations : nom de la clé, adresse mail...
choix de l'**algorithme** et **date d'expiration**. Saisissez un **mot de passe** complexe et cliquez sur « **Générer des clés PGP** ».

Fonctions NFC*



Mot de passe
aléatoire

« Copier »

**Il vous faut un dispositif NFC de Freemindtronic :
Gamme PassCypher ou DataShielder**

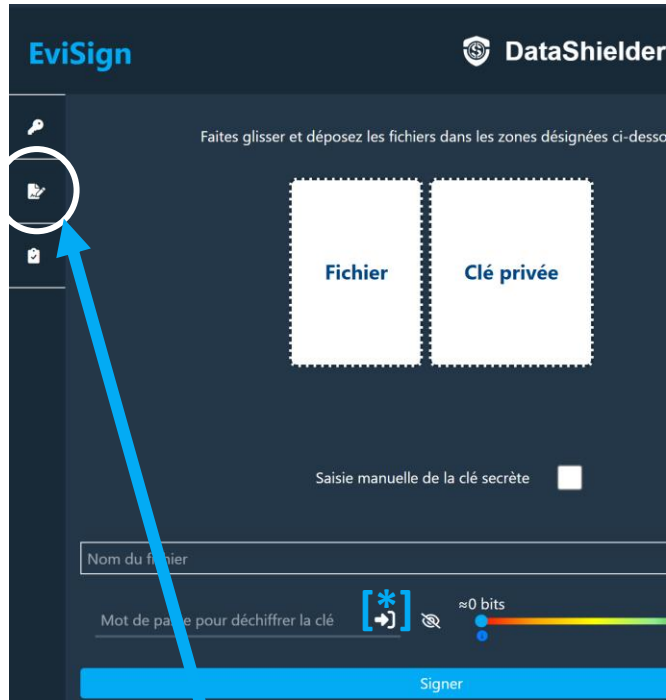
Recent download history

Finances-pk.asc
3.1 KB • Done

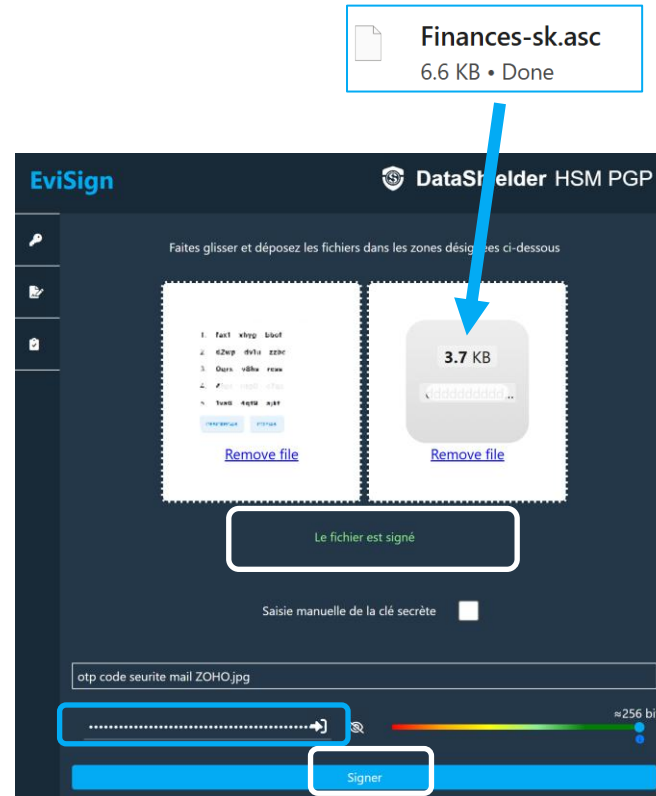
Finances-sk.asc
6.6 KB • Done

Les clés sont générées au format .asc et disponibles
dans le dossier « **Téléchargements** ». Une **clé**
publique -pk et une **clé privée** (ou secrète) -sk

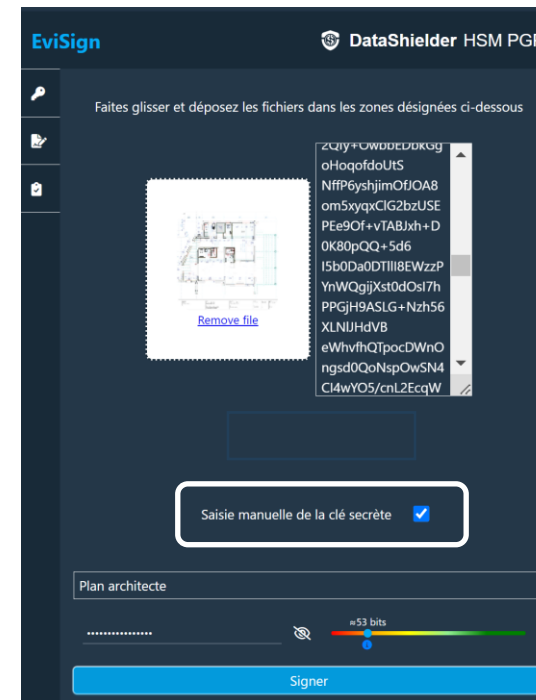
SIGNEZ UN FICHIER



Cliquez sur l'icône « **EviSign** » puis sur l'icône indiquée coté gauche.



Glissez le fichier à signer ainsi que la clé privée. Donnez un nom à votre fichier et saisissez le mot de passe. Cliquez enfin sur « **Signer** ». Un message de succès apparaît.

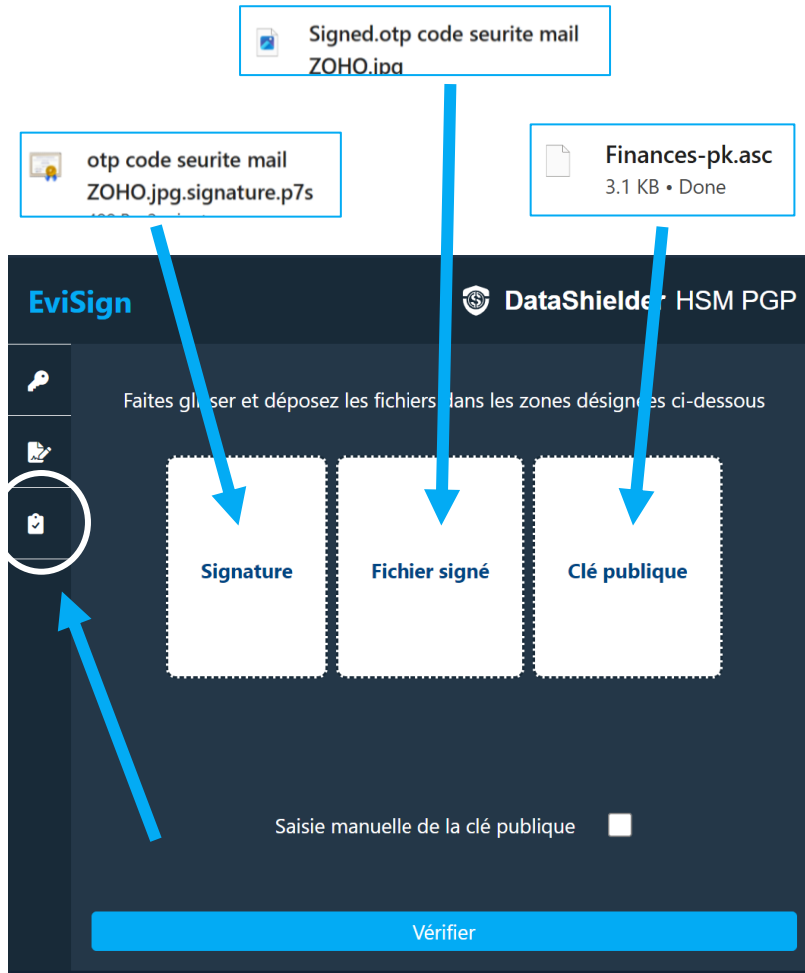


Vous pouvez utiliser la saisie manuelle pour la clé secrète. Pour cela copiez tous les caractères qui composent cette clé. La suite de la procédure est identique.

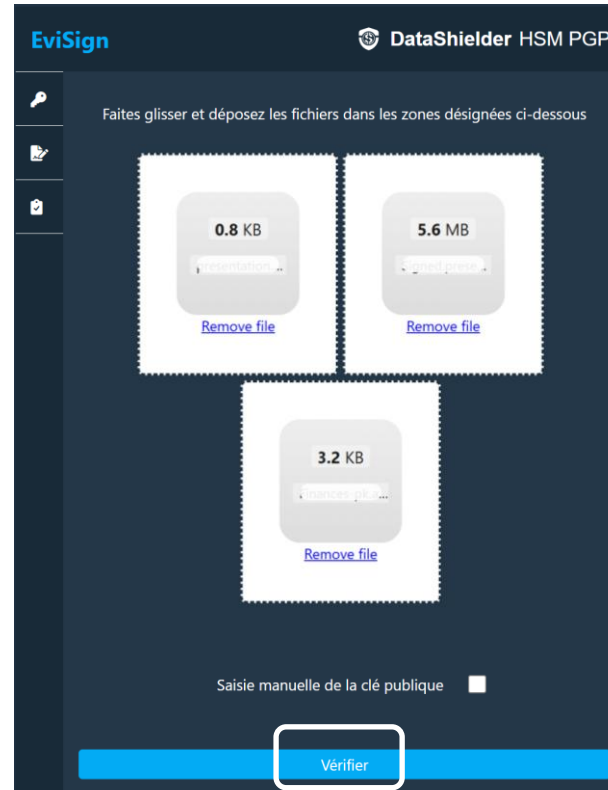


Retrouvez dans le dossier « **Téléchargements** » le fichier signé et la clé de signature numérique au format .p7s.

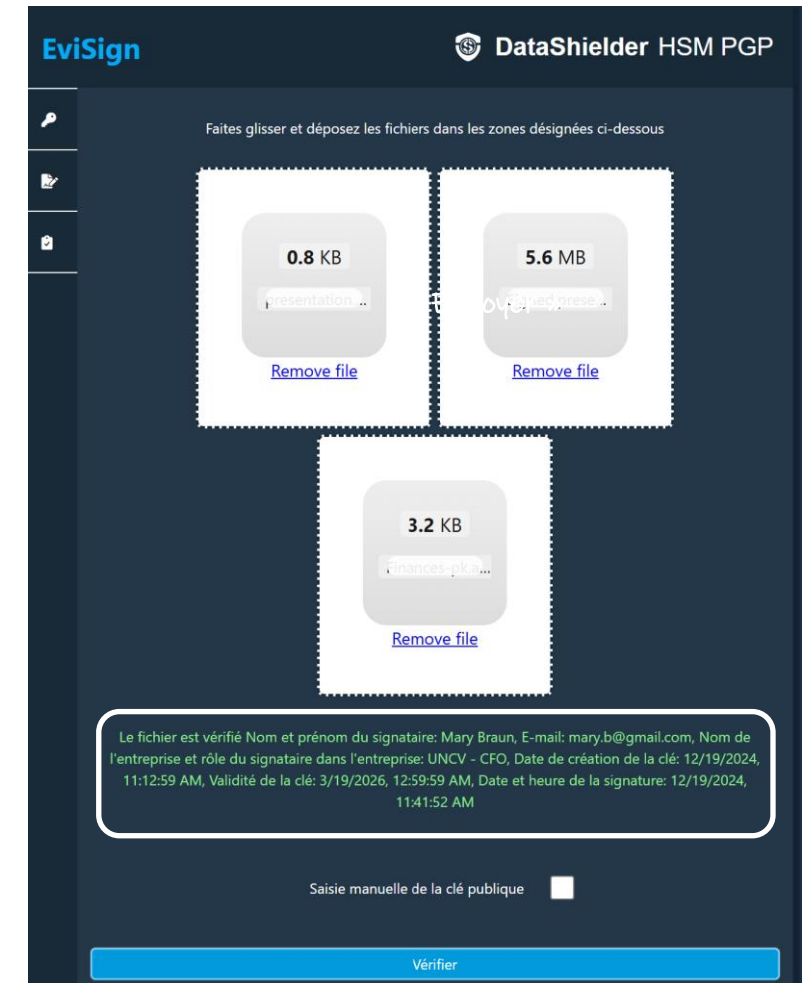
VÉRIFIEZ UNE SIGNATURE



Cliquez sur l'icône « **EviSign** » puis sur l'icône indiquée coté gauche.

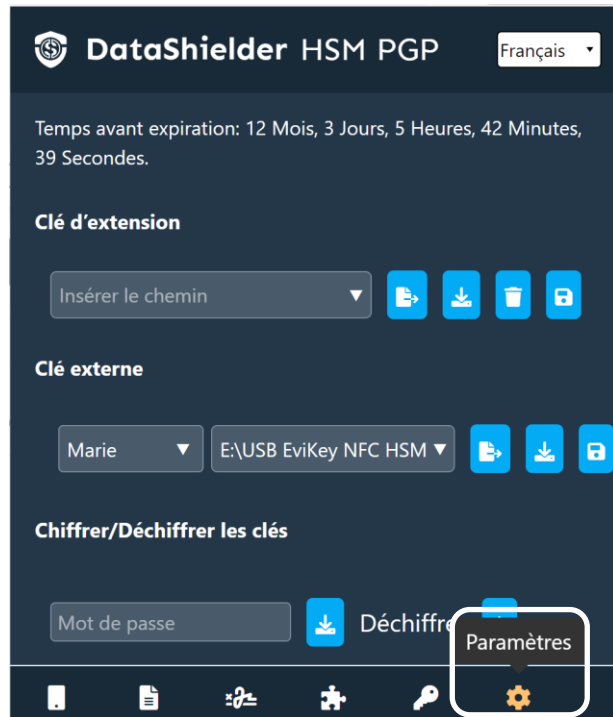


Glissez la **signature**, le **fichier signé** ainsi que la **clé publique**. Cliquez ensuite sur « **Vérifier** ».

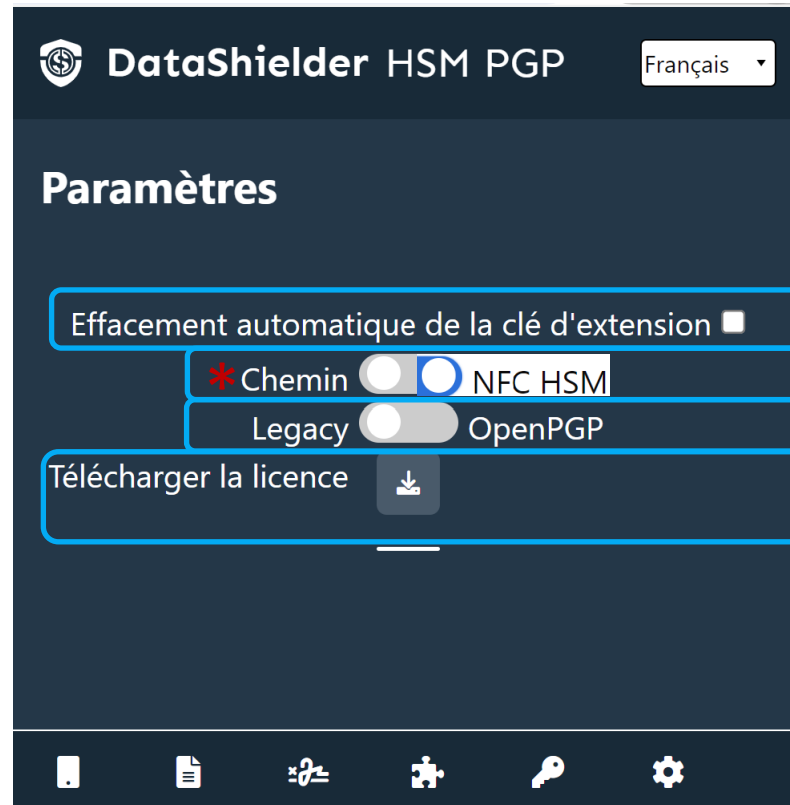


Un message de succès apparaît avec tous les détails concernant la signature.

PARAMÈTRES & FONCTIONNALITÉS



Cliquez sur l'icône « Paramètres »



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

La clé sera effacée si l'option est cochée**

Active l'utilisation d'un dispositif NFC ***

Choisir l'algorithme de chiffrement pour les textes

Sauvegardez la clé de licence sur un support externe de préférence

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

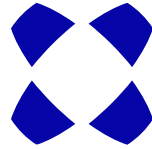
(**) lorsque la licence expire, il y a effacement automatique de la clé pour des mesures de cybersécurité surtout s'il s'agit d'un usage temporaire sur un ordinateur qui n'est pas celui de l'utilisateur.

(***) Consultez le Tutoriel spécifique Extension DataShielder avec dispositif NFC

Take back control, Take back power

EviCypher Technology

By Freemindtronic Andorra



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



Freemindtronic



Chaine Freemindtronic