

GUIDE DE DEMARRAGE RAPIDE 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 via l'extension
- La clé d'extension en détail
- La clé externe en détail
- Fonctionnalités et Paramètres



INSTALLATION DE L'EXTENSION

Téléchargez & installez l'extension DataShielder HSM PGP

CHROME : chrome web store



MICROSOFT EDGE : Edge Addons



OPERA : en cours

FIREFOX : en cours



Cliquez pour ouvrir l'extension

C

L'EXTENSION EST INSTALLÉE



Pour compléter le processus, cliquez <u>ici</u>* 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



Cliquez sur l'icône indiquée pour ouvrir l'extension

🚳 DataShielder HSM PGP	Français 🔻
	عربي
Liconco Dotochioldor	Català
Licence Datasmeluer	Deutsch
Entrer la licence	English
	Français
Cliquez ici pour obtenir l'UUID	हिन्दी
Pour activer la license vous devez télécharger et installer	Italiano
DataShielder Engine	日本の
Consultez le tutoriel	Português
	Românesc
	Русский
	Español
	简体中文

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

VouTube <u>Tutoriel</u> : Activer la licence DataShielder <u>https://www.youtube.com/watch?v=31_ZYnAFwik</u>



Quand DataShielder Engine 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

Temps avant expira Clé d'extension	tion: 11 Mois, 20	Jours, 22 Heures, 3	51 Minutes, 36 S	econdes.
Insérer le chemi			b 🛃 🚺	
Clé externe				
	▼ Insérer I	e chemin	_	
Chiffrer/Déchiffre	er les clés			
		Déchiffrer	•	

La licence est activée. Sa 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, Gmail Pro, 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



Slide 6

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.

TataShielder 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
E)
E)</

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.

+						
> Lecteur	USB (E:)	> US	B EviK	ey NFC HSM >	DataShielder	5
E:\USB EviKey NFC HSM\DataShielder						
lo @) ¢	Ŵ	∿	(D Copier	Ctrl+C	
 L'emplacement est affiché Cliquez dans la fenêtre, le chemin d'accès est sélectionné 						

aucun autre caractère

1 l'emplacement est affiché
2. Maintenez la touche « alt » enfoncée
et faites un clic droit sur la souris
3. Cliquez sur « Copier
ant que nom de chemin
and que nom de chemin
\sim
4. et collez dans l'extension sans

PARTAGEZ VOTRE CLÉ DE CHIFFREMENT SEGMENTÉE



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 »



MarieExtensionKeyEncrypt.aes 96 B • Done

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

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**



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

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 »

correspondant, cliquez sur l'icône indiquée

IMPORTEZ UNE CLÉ DE CHIFFREMENT SEGMENTÉE Commencez par importer la clé d'extension 2/3



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 indiqué.

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

Importez des clés de chiffrement segmentées 3/3 Indiquez le chemin où est stockée la clé externe



Stockez la clé externe « MarieExtensionKey.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

VOUS ÊTES PRÊT MAINTENANT À CHIFFRER VOS TEXTES ET VOS FICHIERS

1. Un premier clic sur l'icône encadrée en rouge ci-dessous pour ouvrir l'extension DataShielder

2. Un second clic pour accéder à EviCypher

£٦

 (\mathfrak{D})

Ø

3. Et enfin un clic pour choisir le chiffrement de **fichiers** ou de **textes**

.



 \mathbf{T}

C

3 Chiffrement de textes ou de fichiers



CHIFFREMENT DE FICHIERS*

- 1. Double/clic ou dépôt du fichier à chiffrer à l'emplacement prévu
- 2. Le chiffrement est automatique

DataShielder HSM PGP

Déposez des fichiers à

déchiffrer ici

1. Déposez votre fichier

Déposez un fichier dans une des zones ci-dessous.

EviCypher

Déposez des fichiers à chiffrer

ici

3. Le fichier chiffré est disponible dans le dossier « Téléchargements »



2. Chiffrement en cours





(*) 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



EviCypher DataShielder HSM PGP Déposez un fichier dans une des zones ci-dessous. \bigtriangledown 0.2 GB Déposez des fichiers à chiffrer ici

Remove file

3. Fichier déchiffré disponible

Rece	ent download history	\otimes
0	encrypt TEXT directory and NFC card.mp4 180 MB • Done	
	jbehovlq.Evi 180 MB • 11 minutes ago	

2. Déchiffrement en cours

CHIFFREMENT DES TEXTES : DEUX POSSIBILITÉS



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 également 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 cliquer sur l'icône pour l'envoyer



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

Slide 20

Déchiffrement de textes

- 1. Copiez/collez le message chiffré reçu 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.



La clé externe en détail

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

🕲 DataShi	ielder HSM PGP	Fr	ançais	•
Clé externe <mark>1</mark>	2	3	4	5
Nom (clé) 🔻	Insérer le chemin V		*	8



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

Slide 23

Paramètres & Fonctionnalités



Cliquez sur l'icône « Paramètres »

DataShielder HSM PGP Français			
Paramètres			
Effacement automatique de la clé d'extension 🗖	La clé sera effacée si l'option est cochée**		
*Chemin NFC HSM	Active l'utilisation d'un dispositif NFC ***		
Legacy OpenPGP	Choisir l'algorithme de chiffrement pour les textes		
Télécharger la licence 🛃	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 tempora		

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

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

sur un ordinateur qui n'est pas celui de l'utilisateur.

Slide 24

Take back control, Take back power

EviCypher Technology

By Freemindtronic Andorra



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





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