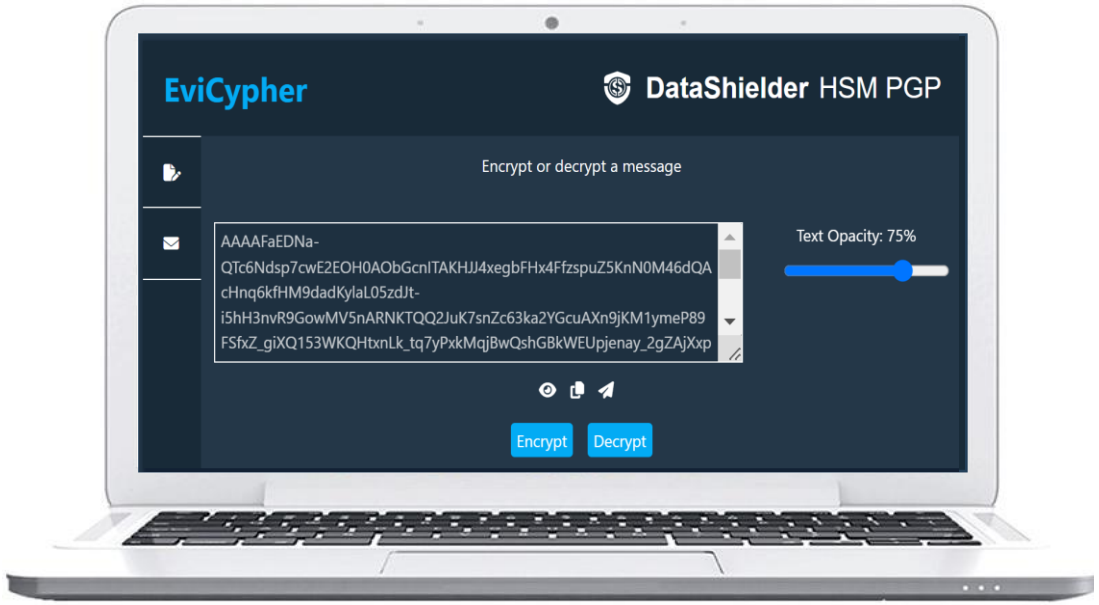
TUTORIAL DATASHIELDER HSM PGP EXTENSION

By Freemindtronic

CONTENTS

- Installation of the DataShielder HSM PGP extension
- Licence activation
- Operating principles
- Home page in detail
- Creation, sharing & importing of segmented encryption keys
- Automatic encryption and decryption of files
- Automatic encryption and decryption of texts via webmails
- Automatic encryption and decryption of texts
- Encrypted backup of Seed phrases (Bip 39)
- Digital signature of files
- Features and Settings

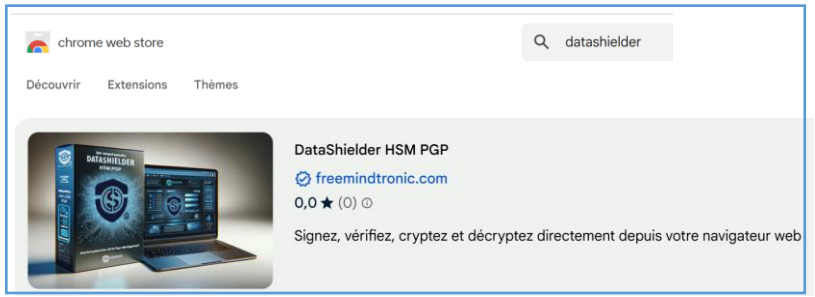


*For operation with an NFC device (contactless), see the "**DataShielder Extension Tutorial with NFC device**"*

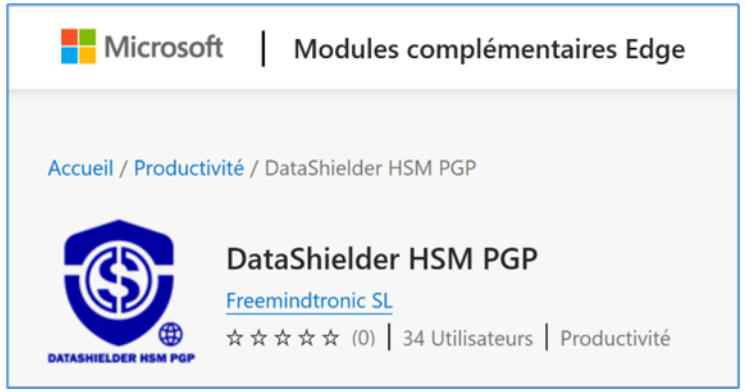
INSTALL THE EXTENSION

Download & install the DataShielder extension

CHROME : chrome web store



MICROSOFT EDGE : Edge Addons

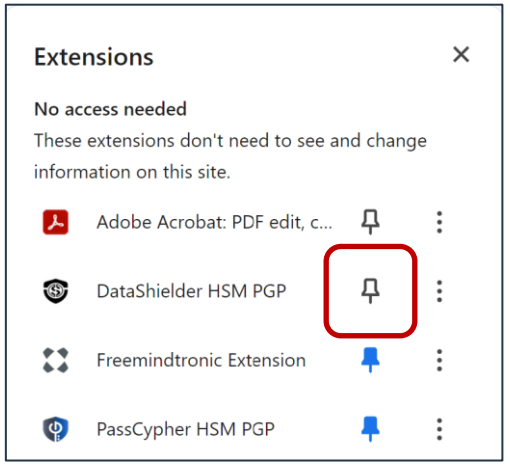


FIREFOX : in progress

OPERA : in progress

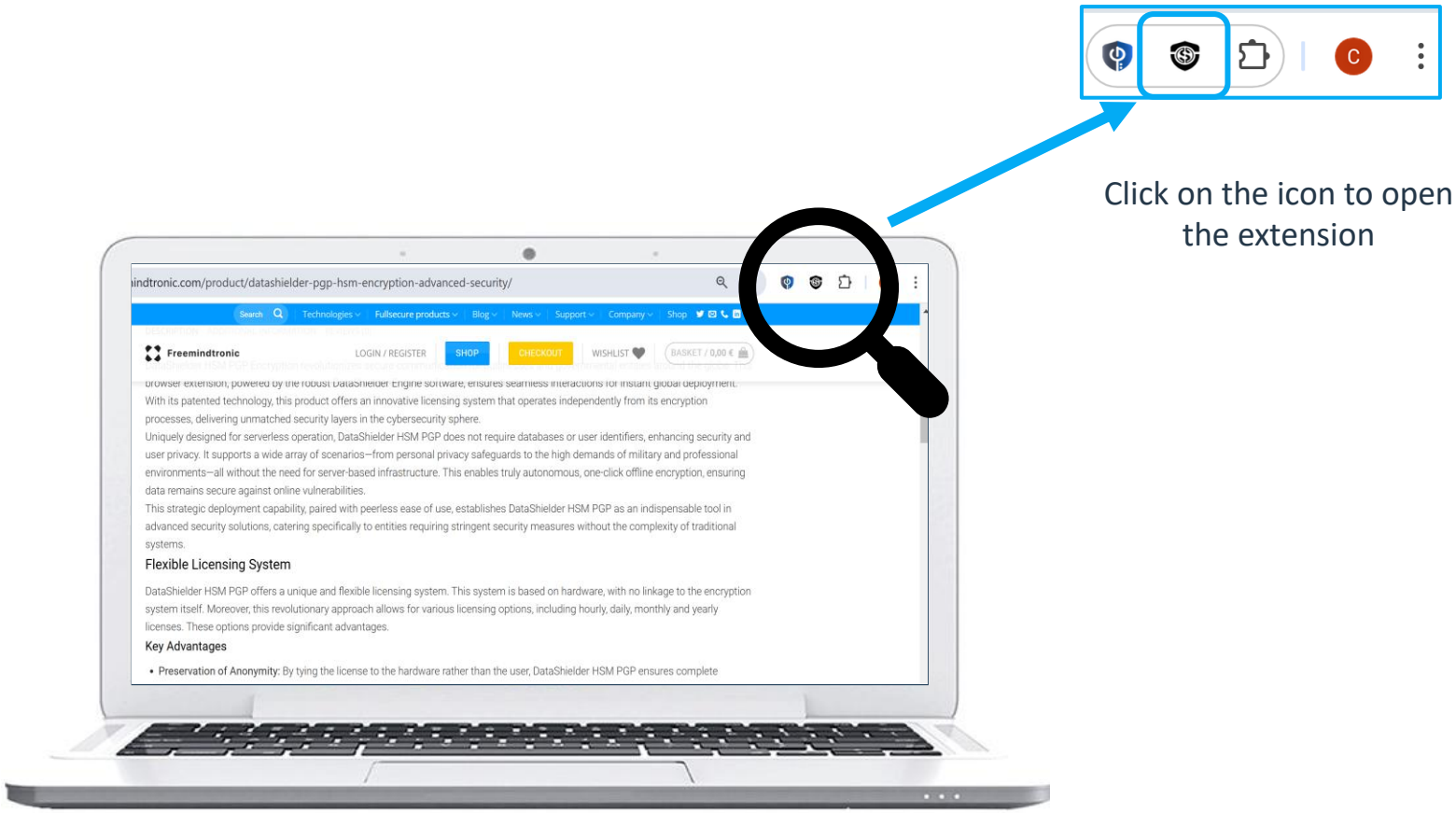
1 At the top right of your computer screen, click this icon to access extensions

2 Click the icon to pin DataShielder to your toolbar

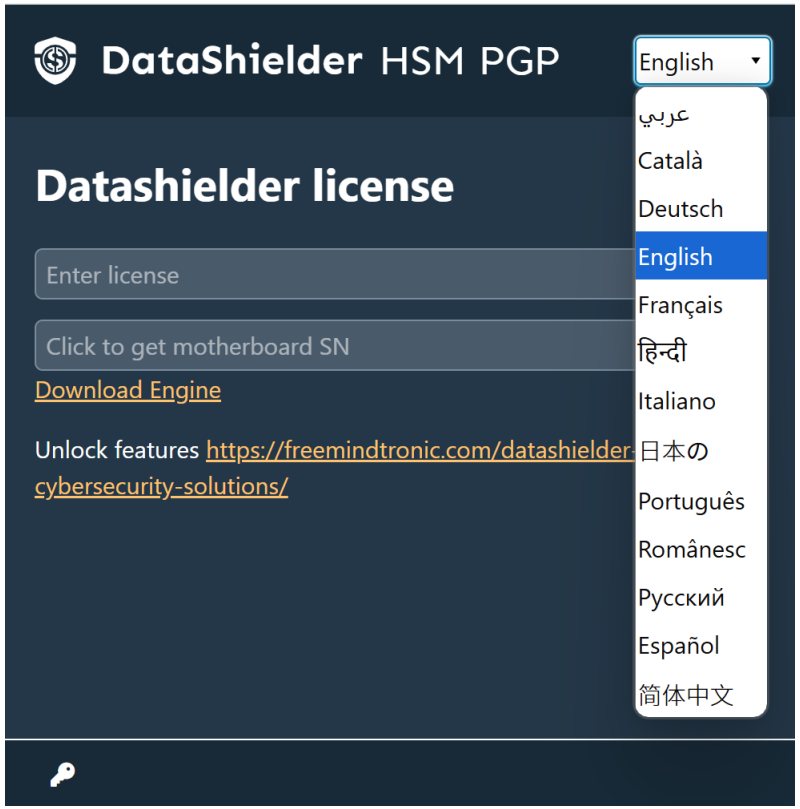


3 The DataShielder icon appears at the top right of your computer screen. Click to open the extension.

THE EXTENSION IS INSTALLED



Click on the icon to open the extension



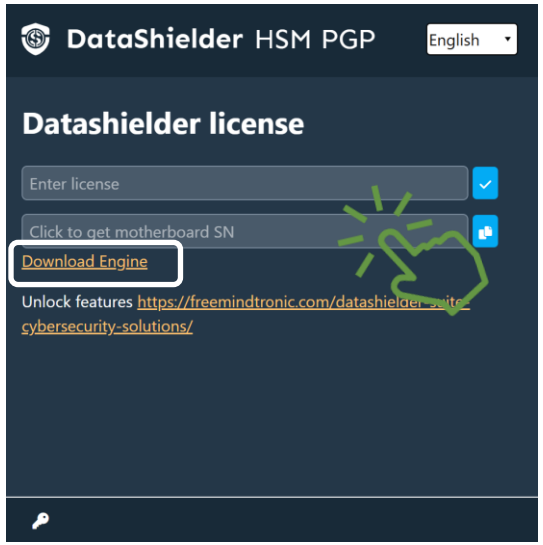
The DataShielder HSM PGP extension is translated in 13 languages : Arabic, German, English, Catalan, Chinese, Spanish, French, Hindi, Italian, Japanese, Portuguese, Romanian and Russian. You can choose in which language to display the extension.

ACTIVATE THE LICENSE

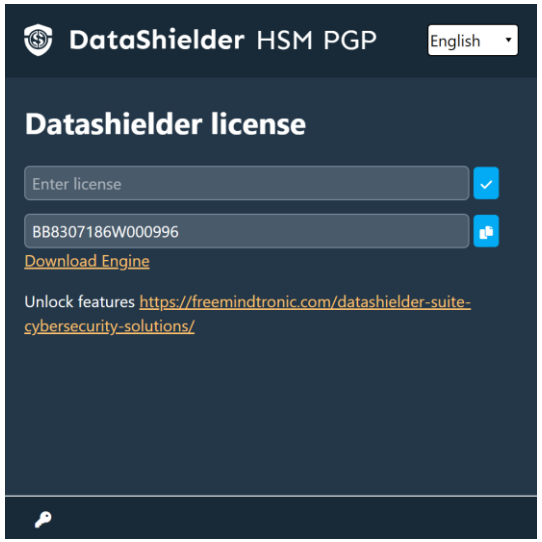
YouTube

Tutoriel : Activate the DataShielder License

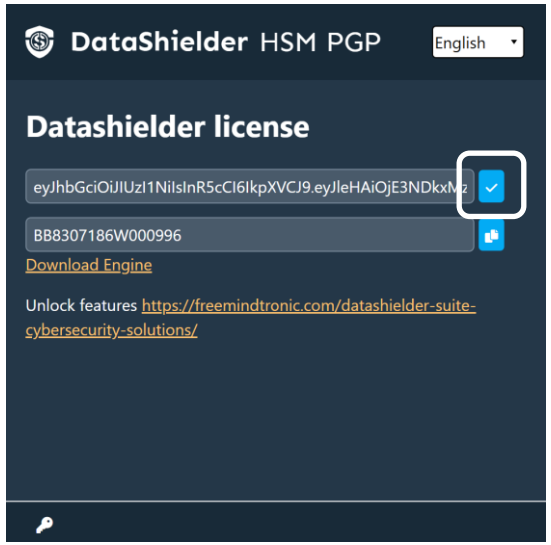
https://www.youtube.com/watch?v=3I_ZYnAFwik



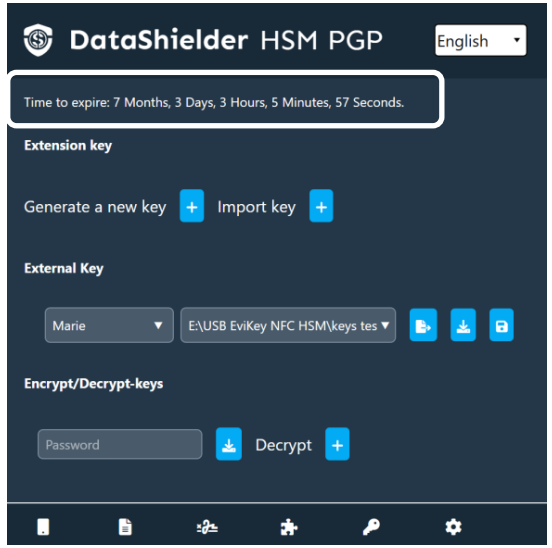
Click on "**Download Engine**" and install the software (Windows or MacOS). Then **click** to get **the serial number of your computer's motherboard**



Send this number by email to the address indicated on the Freemindtronic website.



Copy/paste the license number received in return. Then click on the indicated icon to activate the license.



The license is activated. The validity is indicated in real time at the top of the page.*

(*) Several subscriptions are available: hourly, daily, weekly, monthly or annually.

HOW DOES IT WORK?

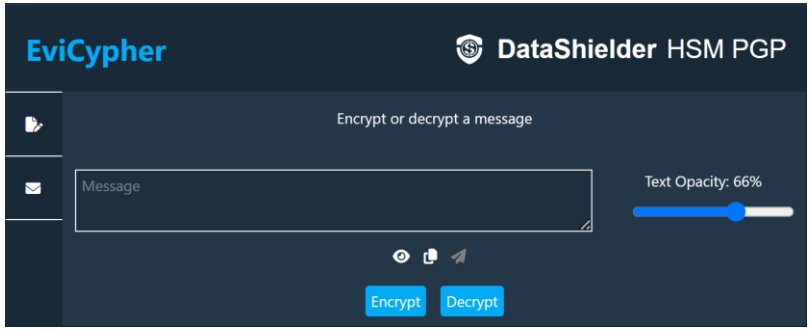
DataShielder HSM PGP is an extension that allows several methods of automatic encryption:

1. File encryption via the "Drag and Drop" functionality or double-click on the file.
2. Text encryption directly from the DataShielder HSM PGP extension.
3. Text encryption via webmail (Gmail, Gmail Pro, Outlook, Yandex, Yahoo, iCloud & Roundcube).

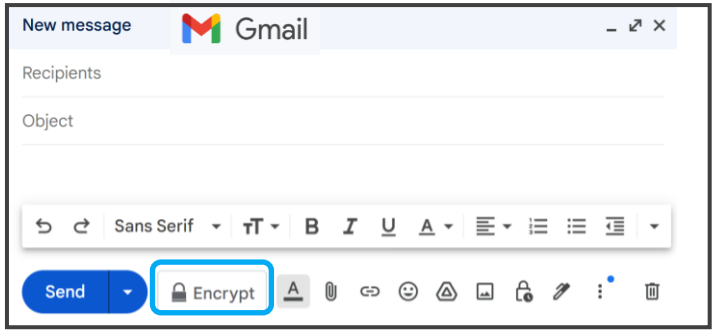
- Creation of your segmented encryption keys and sharing with your correspondent(s).
- A segmented key = an **extension key** stored in the local storage of your web browser and an **external key** stored in the location you choose (USB key, SSD, cloud, etc.).
- Write your message and click the "Encrypt" button. The encryption is automatic.

1

2



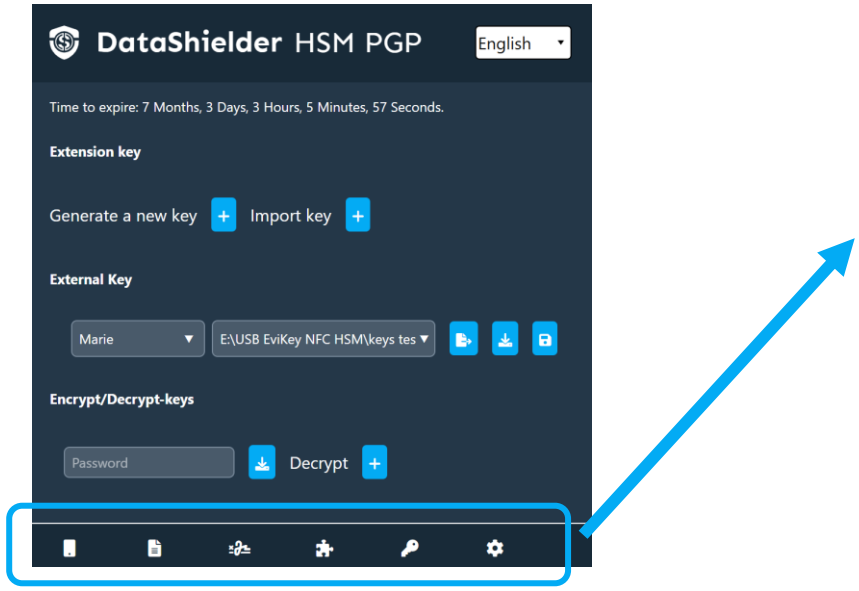
3

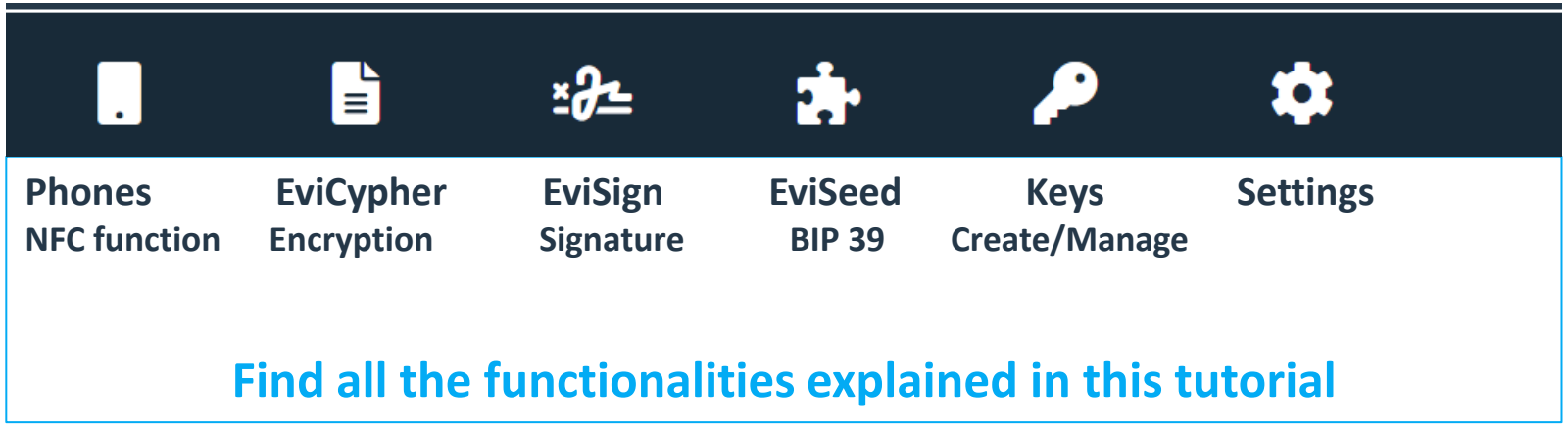


HOME PAGE IN DETAIL

When you open the DataShielder extension, the window below appears.

By default, the extension opens on the "keys" window.

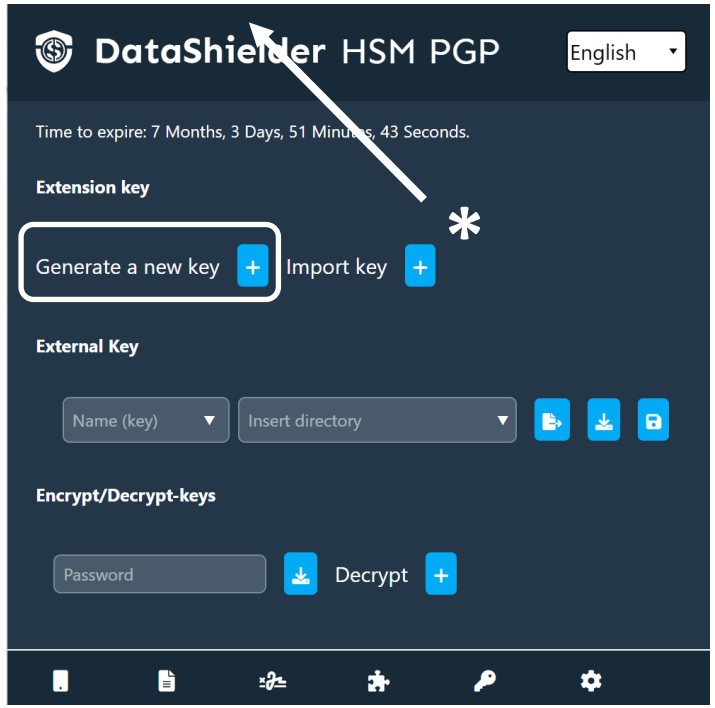




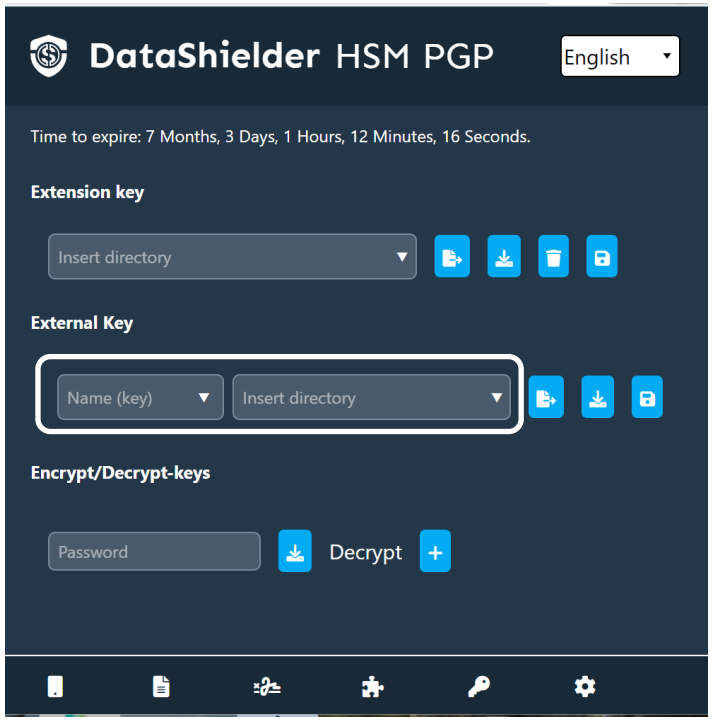
Find all the functionalities explained in this tutorial

CREATE* YOUR SEGMENTED ENCRYPTION KEY

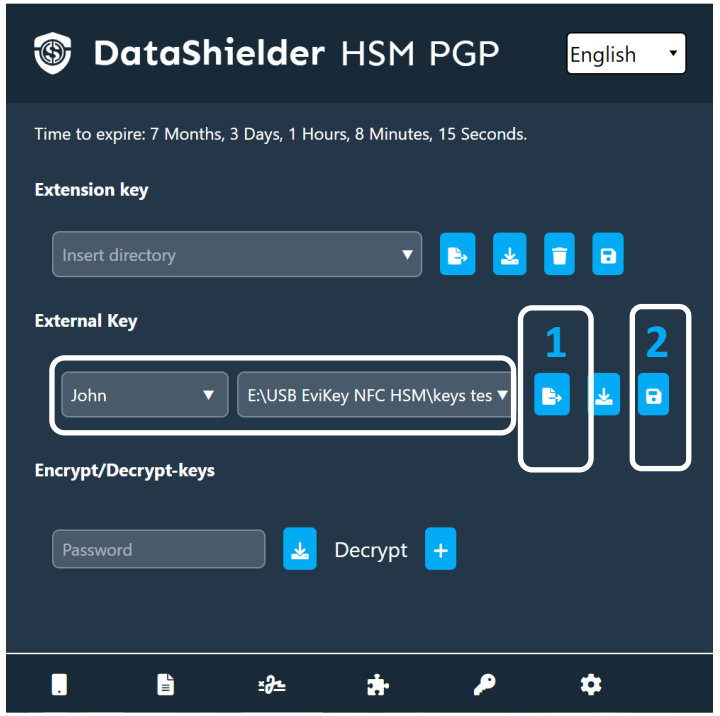
(*) If your correspondent sent you his segmented key (extension key & external key) see slides 11 to 13



Click on the "**+**" symbol to generate **extension key.** This key is recorded in the "**local storage**" of your web browser.



The **extension key** is created. You now need to create the **external key**. Name the key and insert the storage path. **It is recommended to use external storage (USB key, SSD, etc.).**



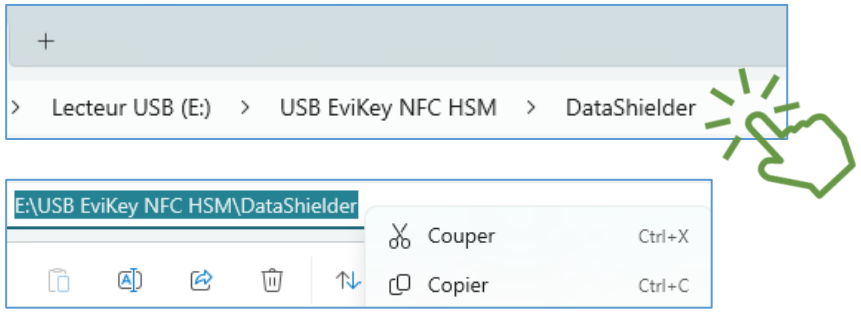
Now click on the "EXPORT" icon and then on the "SAVE" icon. The **external key** "**John**" is created and registered in the location you specified.

Inert the storage path*: detailled explanations in the next slide

INSERT THE ACCESS PATH

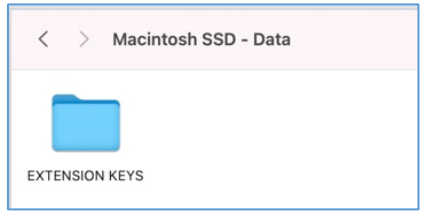
- **Choose** where you are going to **save your external key** (internal or external hard drive, USB key, etc.)
- Then provide the exact path of this location
- Below you will find out how to do this if you are using a **Windows or macOS** operating system.
- Strictly follow the instructions mentioned.

Windows

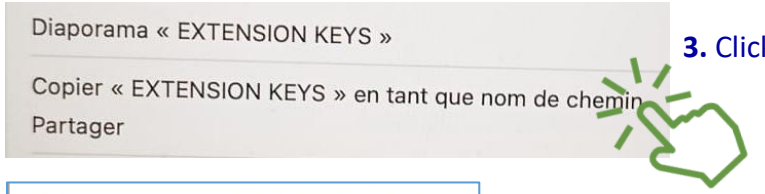


1. Location is displayed
2. Click in the window, the path is selected
3. Right click, “Copy” button appears
4. Click “Copy” and paste into the extension without adding any other characters

macOS



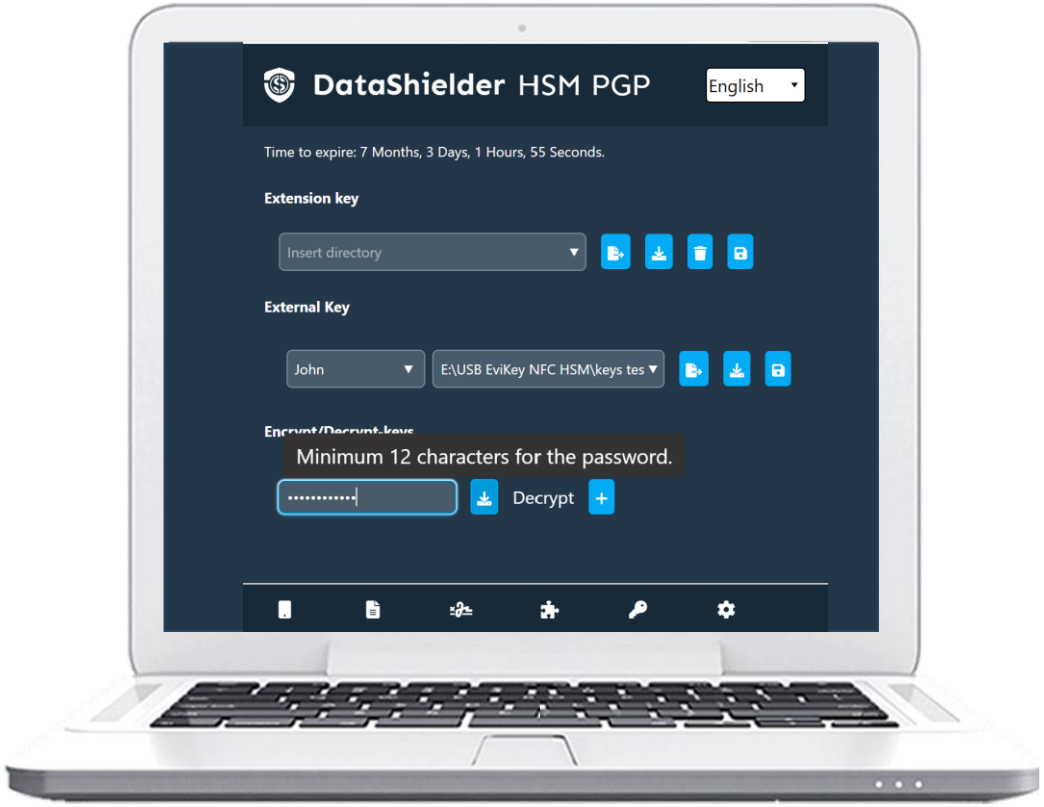
1. Location is displayed
2. Hold down the “alt” key and right-click the mouse



3. Click on « Copy »

4. and paste in the extension without adding any other characters

SHARE YOUR SEGMENTED ENCRYPTION KEY



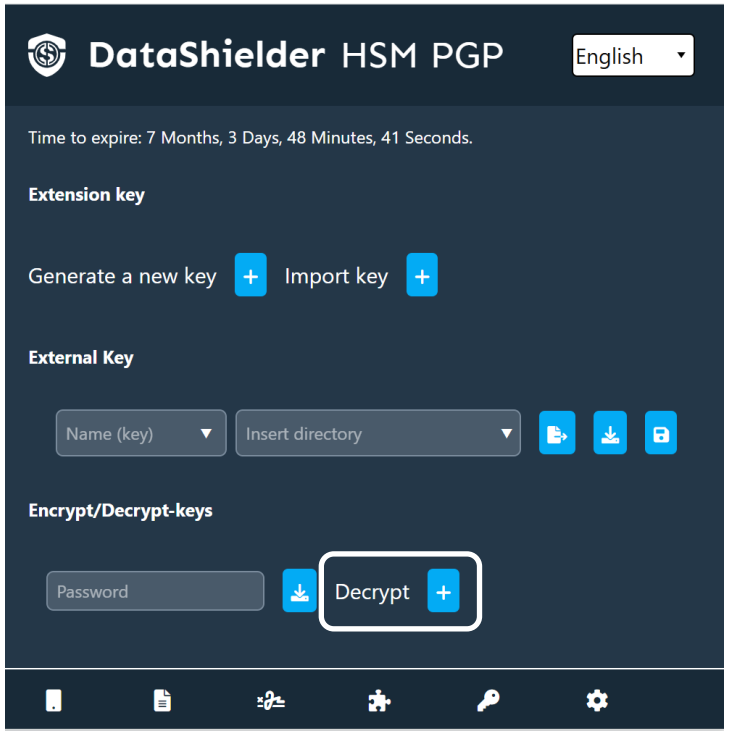
To share the keys with a correspondent, you will **encrypt** them: Enter a password of at least 12 characters and click on the "**IMPORT**" arrow.

The external key and the extension key are automatically **encrypted**. You can find them in the "**Downloads**" folder.

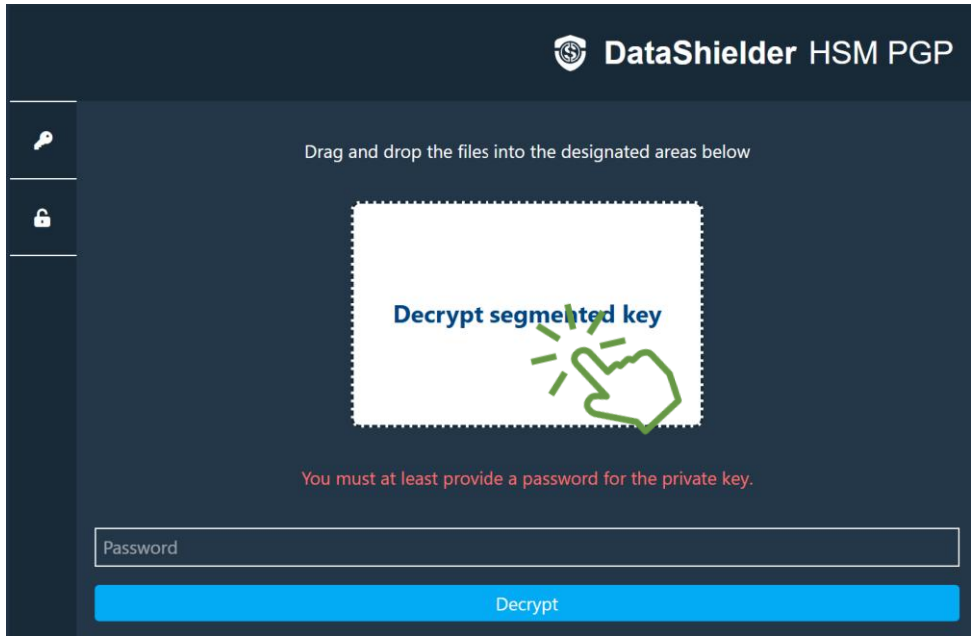
Send these 2 files by **email** (or other) to your correspondent and tell them the password through another channel (e.g., **SMS**).

IMPORT A SEGMENTED ENCRYPTION KEY 1/3

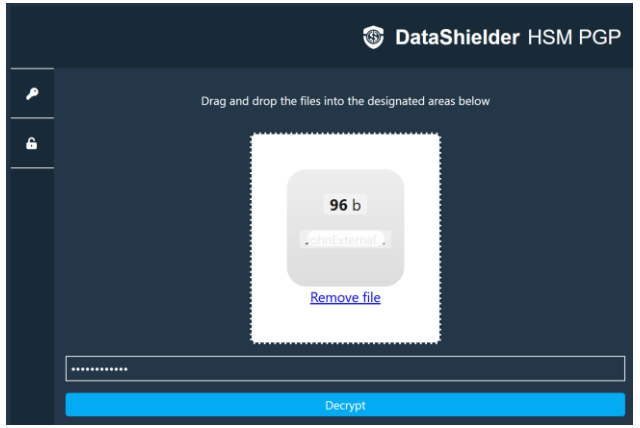
Start by decrypting the key segments

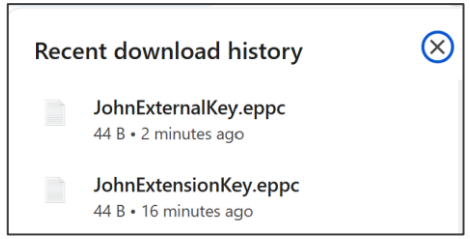


To decrypt the keys sent by a correspondent, **click on the indicated icon**.



Click in the white window and insert the encrypted extension key. Then enter the password in the indicated place and click "**Decrypt**".

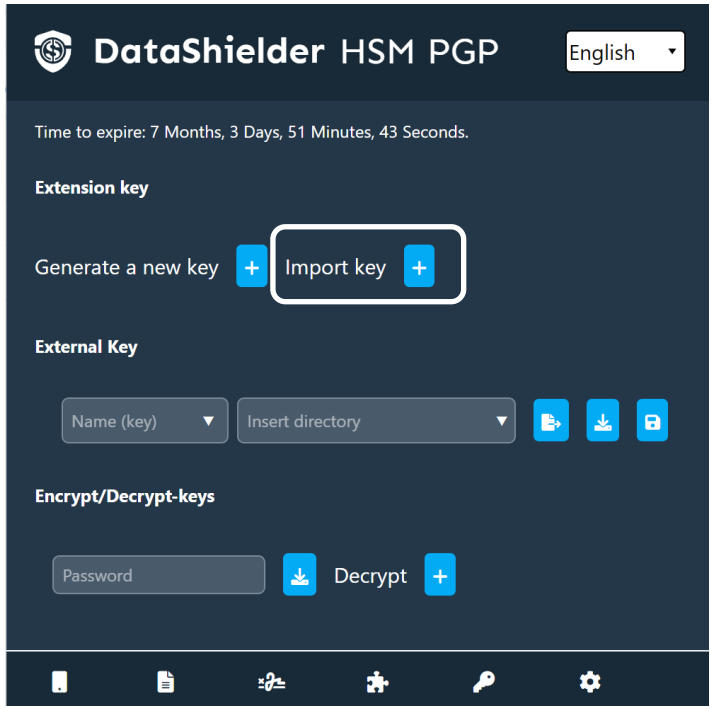




Do the same to decrypt the external key. The **2 decrypted files** are in the "**Downloads**" folder.

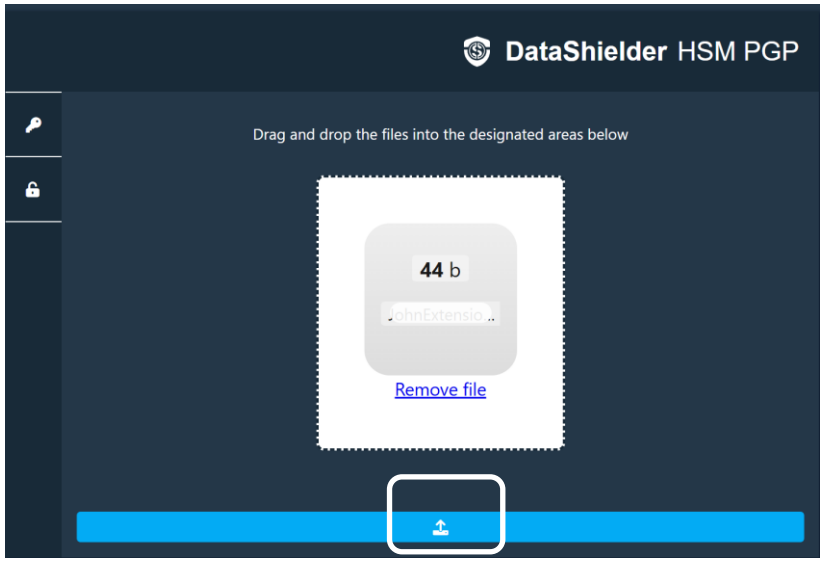
IMPORT A SEGMENTED ENCRYPTION KEY 2/3

Start by importing the extension key



The extension key sent by your correspondent is decrypted. Click on the "**Import key**" icon.

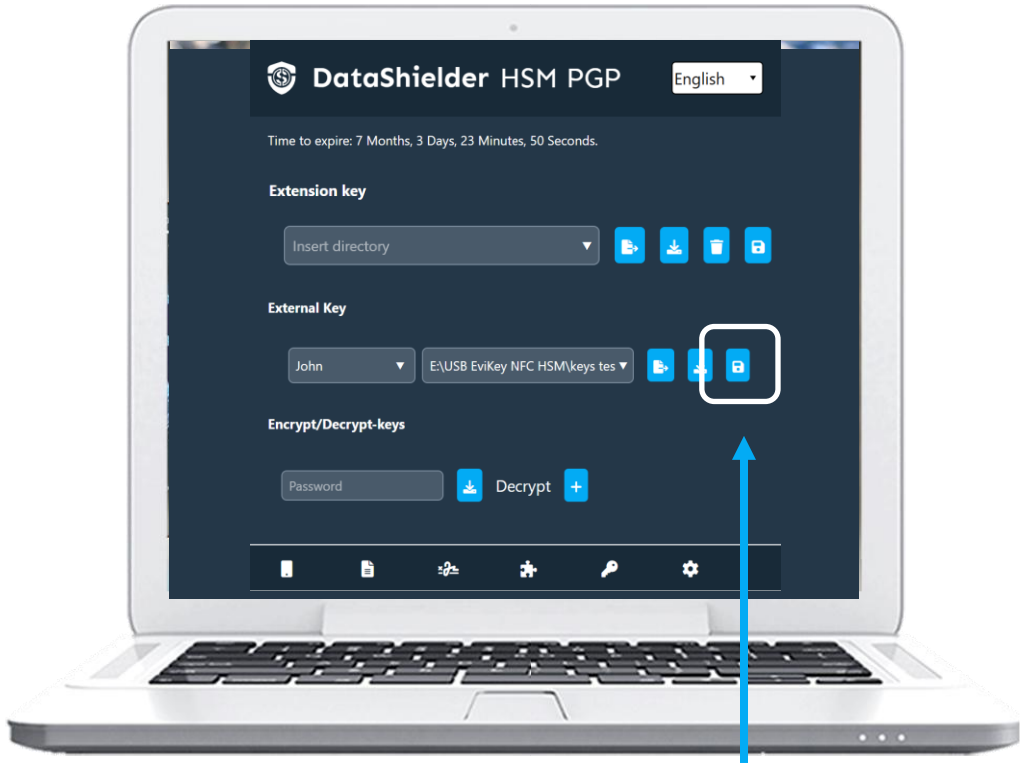
Retrieve the decrypted file and drop it in the indicated place.



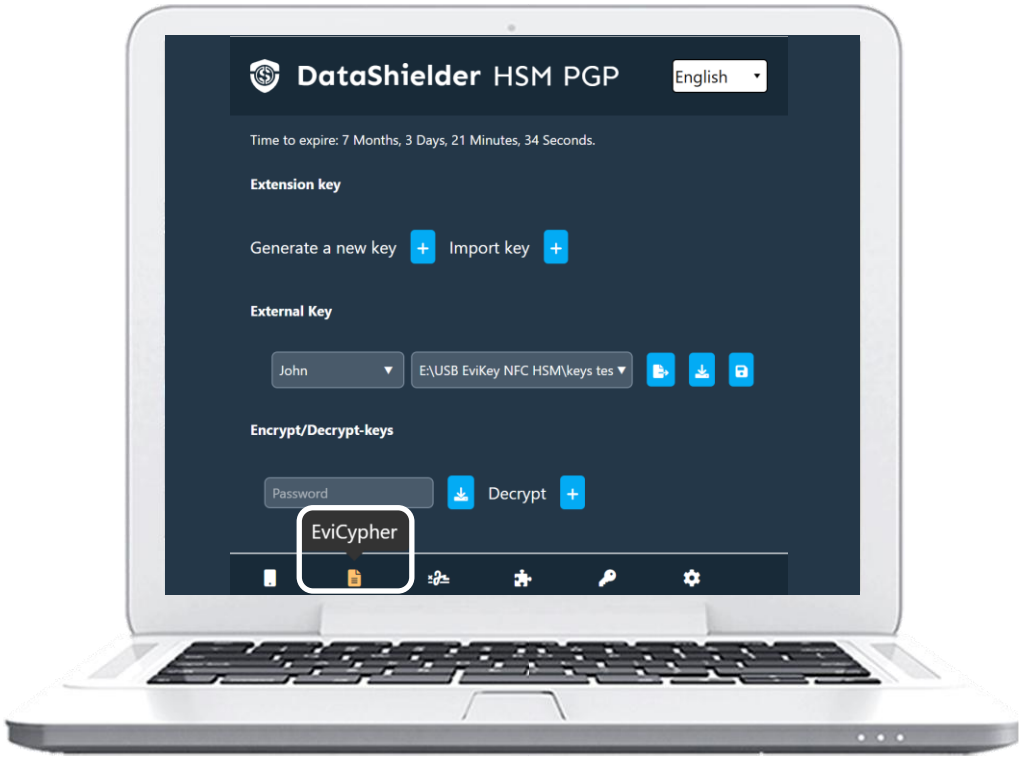
When the key is inserted, click on the arrow. A "**success**" message will appear. Close this window and reopen the extension.

IMPORT A SEGMENTED ENCRYPTION KEY 3/3

Specify the path where the external key is stored



Store the external key "**JohnExtensionKey.eppc**" in the location of your choice* (here an **external SSD**). For the extension to access the external key, write the key name (**John**) and enter the **path to access the key**. Then click on the indicated icon to save it.



The importation of the keys is complete. You can start encrypting messages or files. To do this, click on the **"EviCypher" icon**.

(*) We recommend storing the external key in removable media

YOU ARE NOW READY TO ENCRYPT TEXTS & FILES

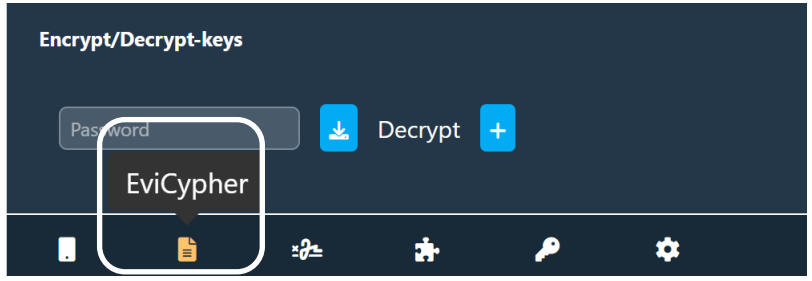
1. A first click on the icon framed in red below to **open the extension**

2. A second click to access **EviCypher**

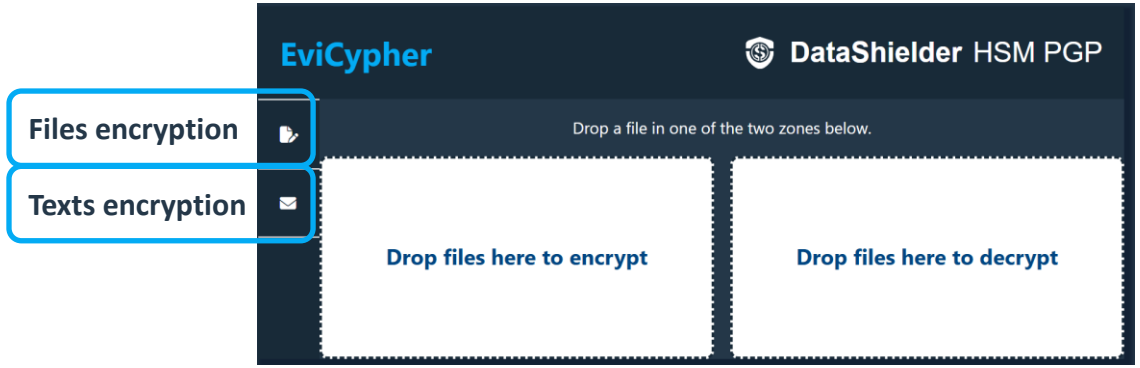
3. And finally, a click to choose “**file**” or “**text**” encryption

1

2



3 Texts or files encryption



FILES ENCRYPTION*

1. **Double clic or drop the file** to be encrypted in the provided place.
2. The **encryption is automatic**.
3. The encrypted file is available in the "**Downloads**" folder.

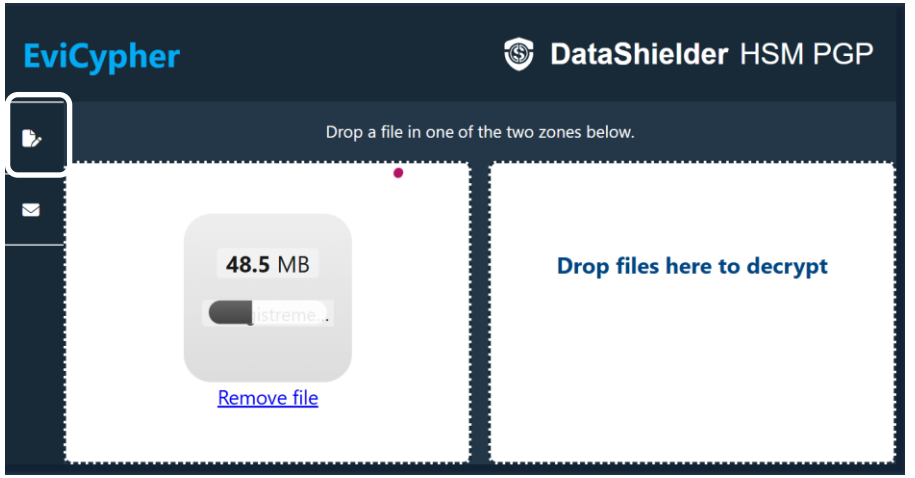
YouTube

Tutorial : How to encrypt files

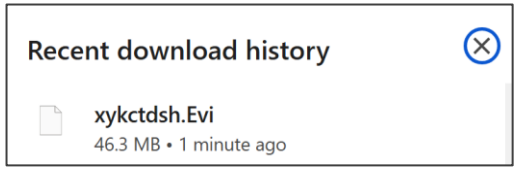
https://youtu.be/Uyk0XGmaU3w?si=HEzZ0ooN156OsT2U

1. Drop your file

2. Encryption in progress



3. Encrypted file is available



(*) All file types are compatible: jpeg, pdf, word, excel, PowerPoint, videos ….

FILES DECRYPTION

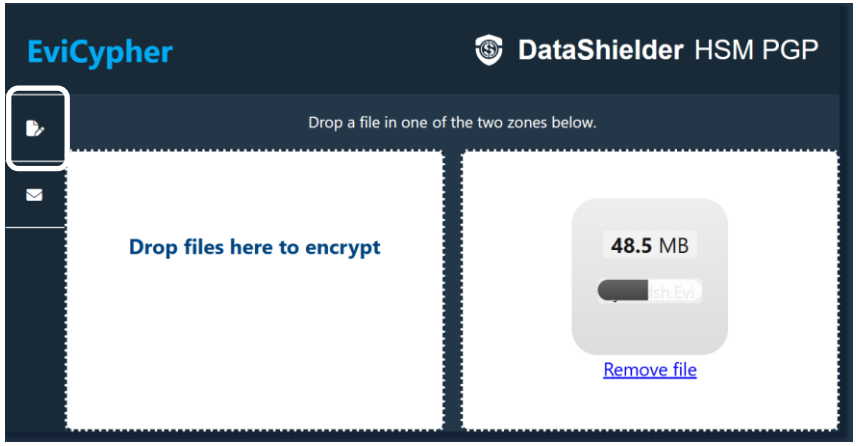
1. Drop the file to be decrypted in the provided place.

2. The **decryption is automatic**.

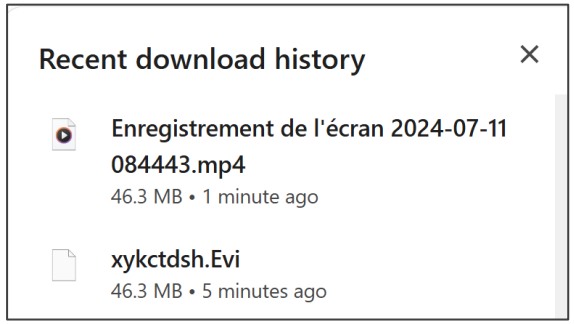
3. The decrypted file is available in the "**Downloads**" folder.

1. Drop your file

2. Decryption in progress

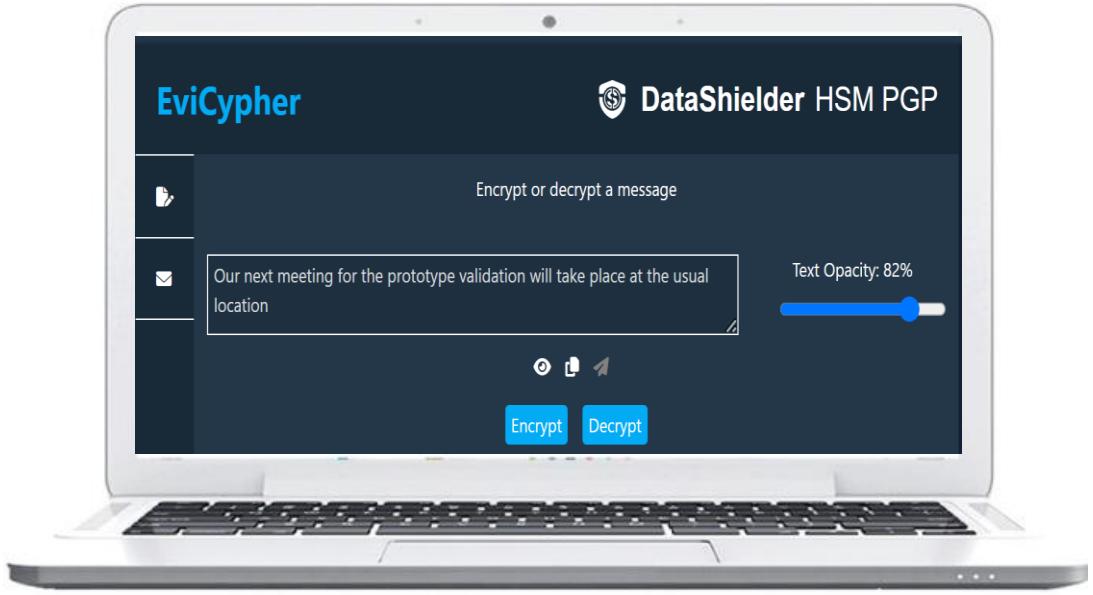


3. Decrypted file is available



TEXT ENCRYPTION: TWO POSSIBILITIES

UNIVERSAL USE



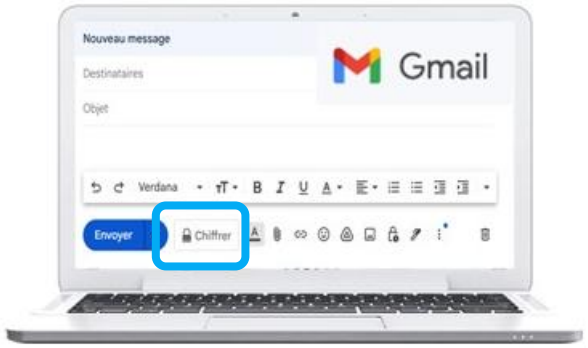
The extension is compatible with all messaging services, chats... In this case, encryption and decryption will be done **directly from the extension**.

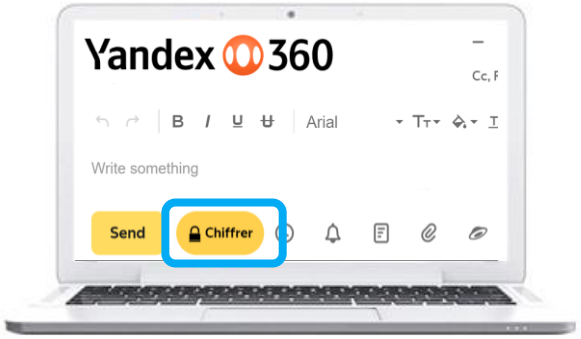
WEBMAILS USE

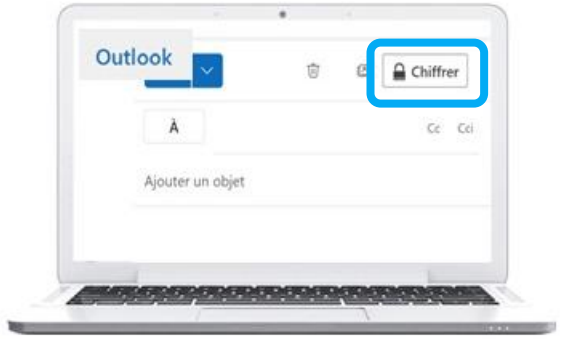
The extension is also compatible with certain email clients that use a web browser to access your emails (webmails). In this case, encryption and decryption will be done automatically **directly in the webmail**.

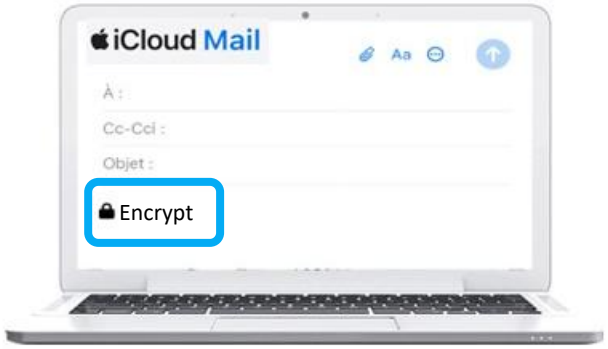
SOLUTION NUMBER 1 : WEBMAILS USE

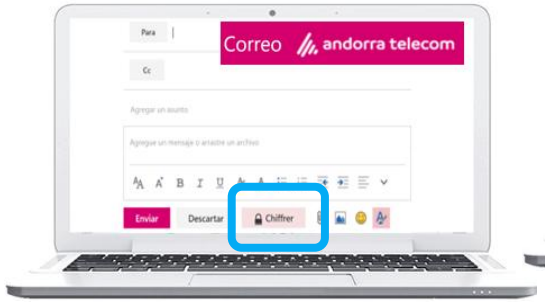
- If you use a webmail compatible with our extension, **you do not change your habits**
- Write your email and click on the “**ENCRYPT**” button before sending to your correspondent
- The latter, if he uses a compatible webmail, will simply have to click on the “**DECRYPT**” button to read your message

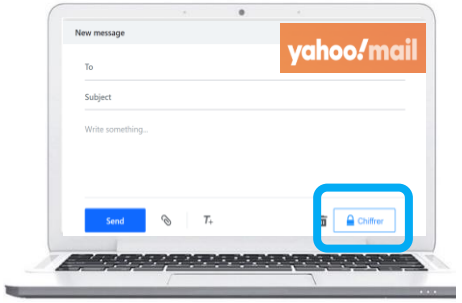


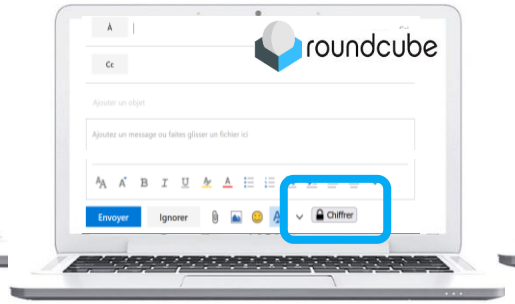


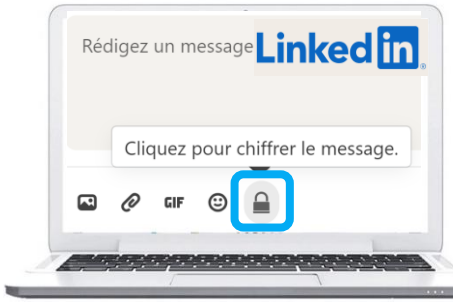


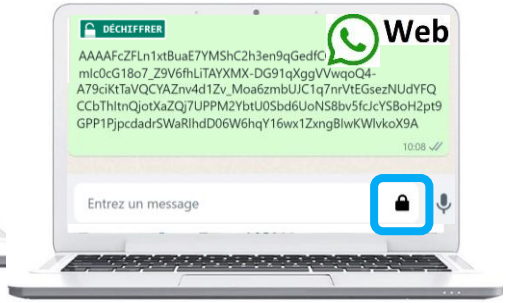




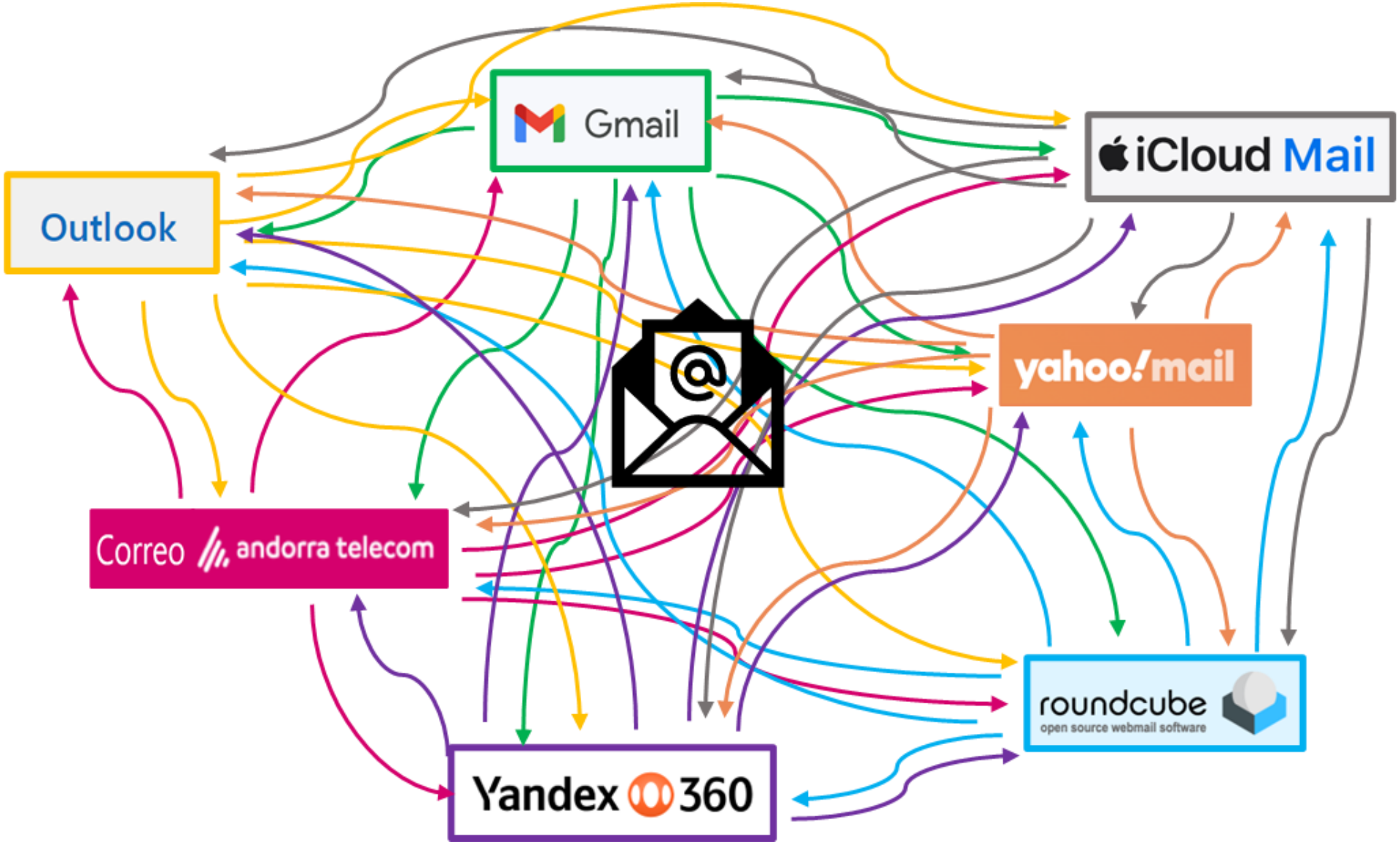








COMMUNICATE FREELY



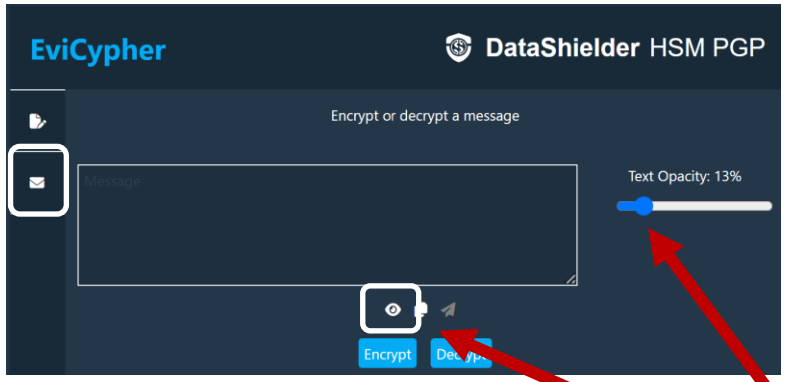
SOLUTION NUMBER 2 : UNIVERSAL USE

1. Write your message in the space provided.

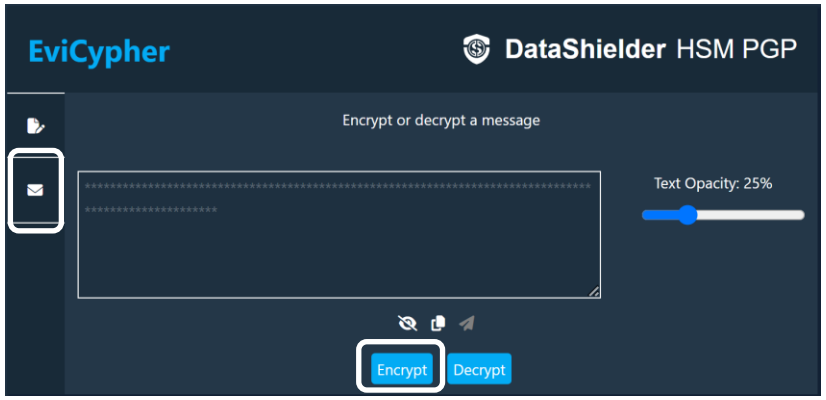
2. Click on “**ENCRYPT**”. The encryption is automatic.

3. The **encrypted message** is displayed on the screen, you can send it.

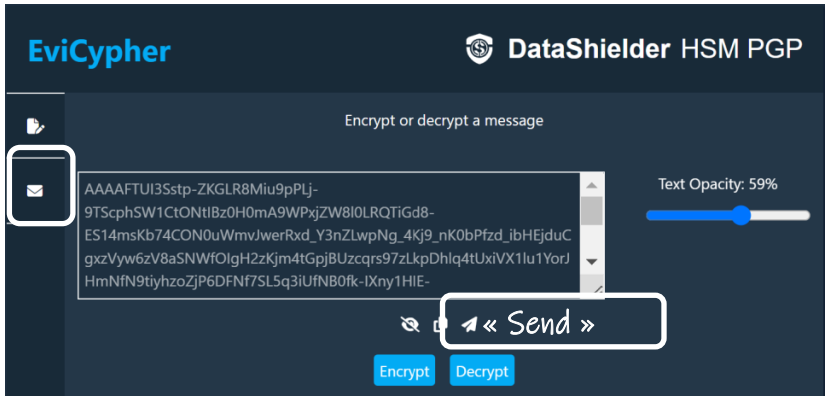
1. Write your message



2. Click on the « Encrypt » icon



3. The message is encrypted. You can copy it or click on the icon to send it directly



You can operate to obscure the text while typing for confidentiality reasons.
You can also make the text "disappear" by clicking on the indicated icon.

YouTube

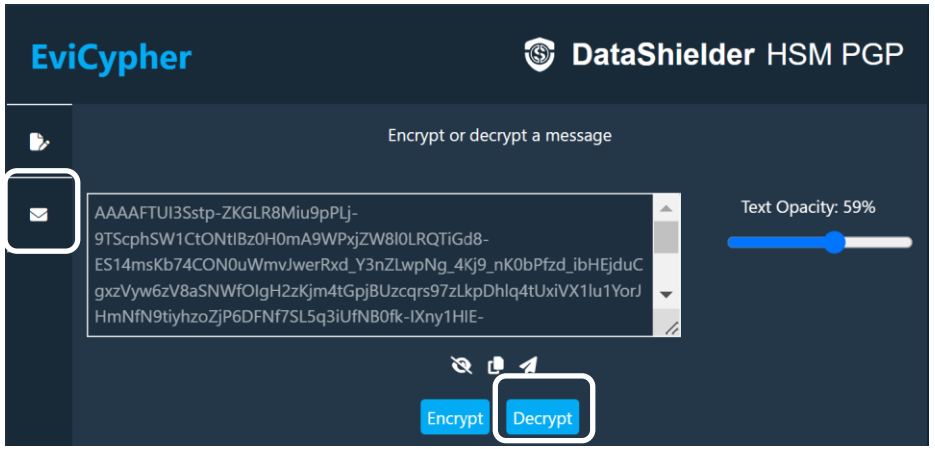
Tutorial : How to use opacity text

https://youtu.be/xdoJ9JGYtmo?si=OisOAElglAhcQZDV

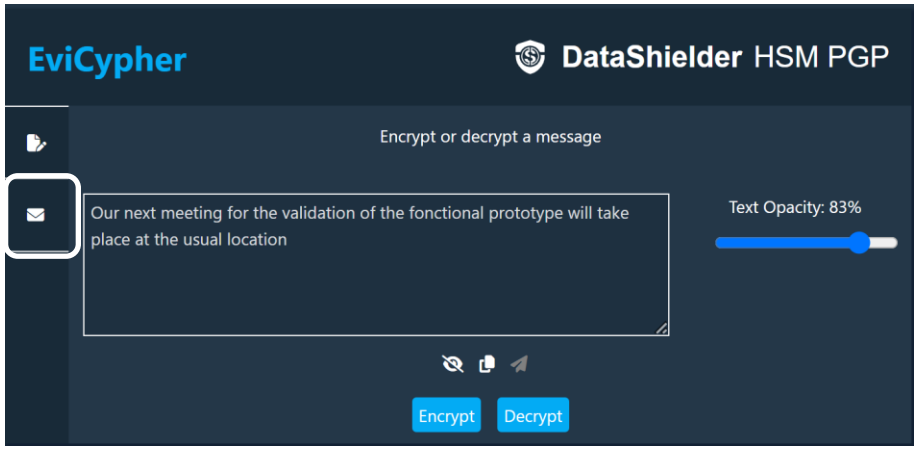
TEXT DECRYPTION

1. **Copy/paste** the encrypted message in the provided place.
2. Click on "**Decrypt**".
3. The decryption is **automatic**.

1. Copy/paste the encrypted message and click on « Decrypt »



2. The message is decrypted



THE EXTENSION KEY IN DETAIL

When the extension key is generated, the window below appears.

By default, this key is saved in the local storage of your web browser.
You can do nothing more, everything works. However, several options are available.

1. You can define and insert a path to save this key. You can define multiple paths.

2. By clicking on this icon, the key will be saved in the indicated path.

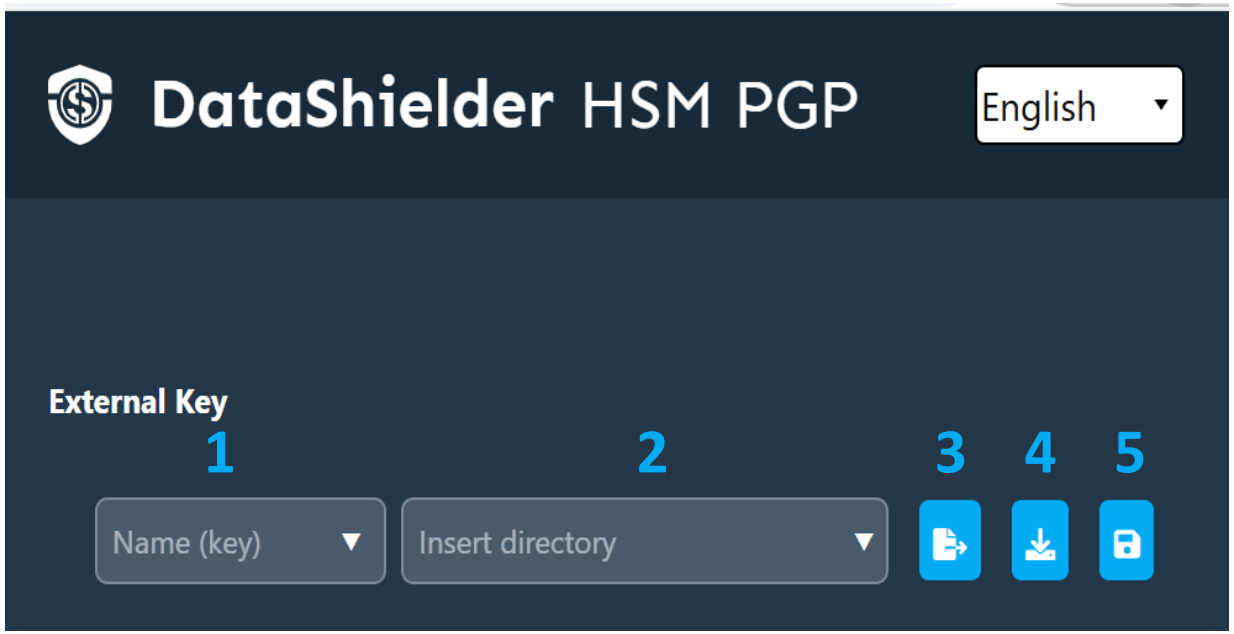
3. You can import the key (.eppc file) and save it wherever you want as a backup.

4. By clicking on this icon, you delete the key from the local storage.

5. Don't forget to click to save the defined path.

THE EXTERNAL KEY IN DETAIL

You can create multiple external keys linked to one extension key.



1. Define a name for the external key that will be created. You can define several different keys.

2. Insert the path where the external key will be stored. You can define multiple paths

3. Click to create and export the key.

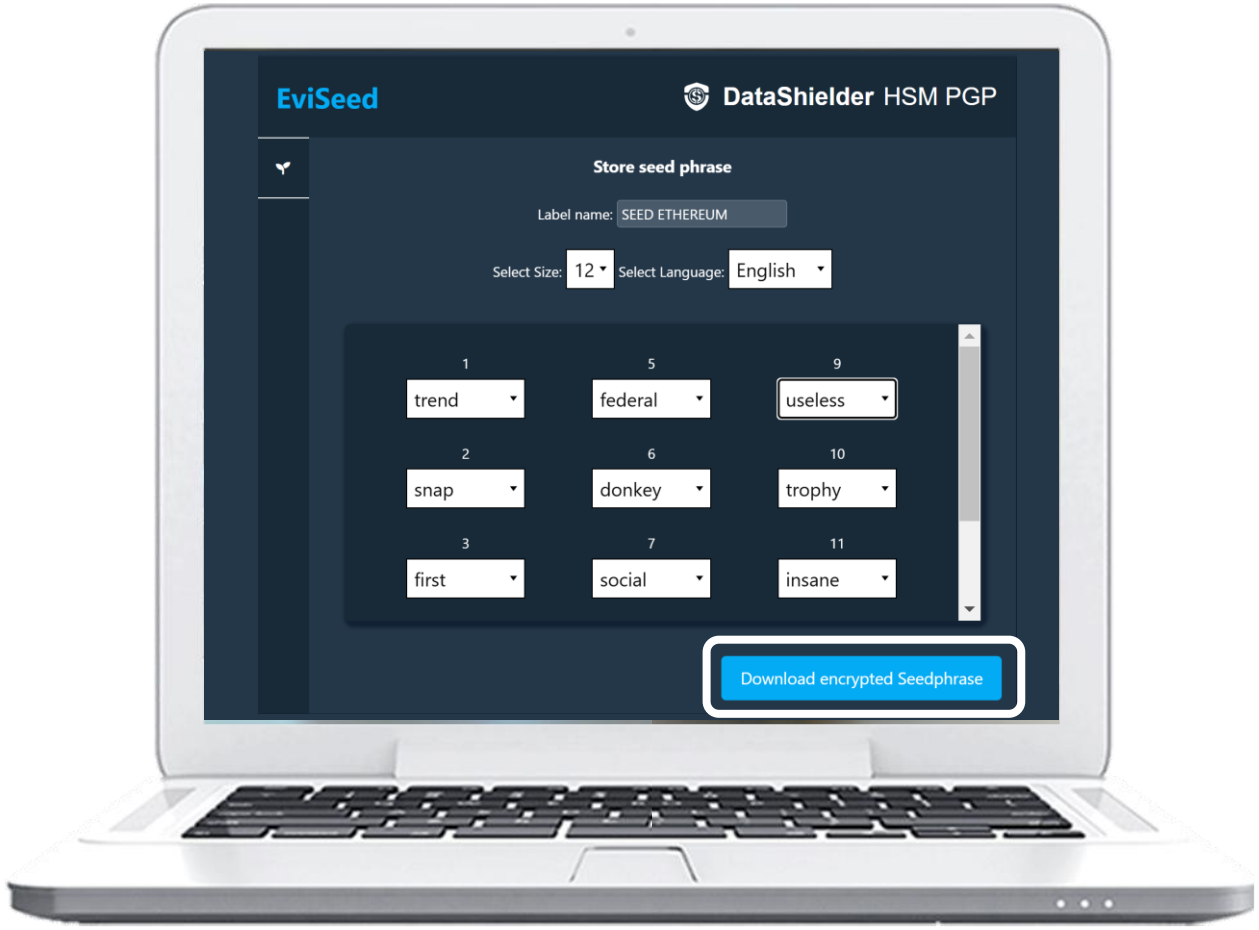
4. By clicking on this icon, you can download the key and save it wherever you want.

5. Don't forget to click to save the defined path.

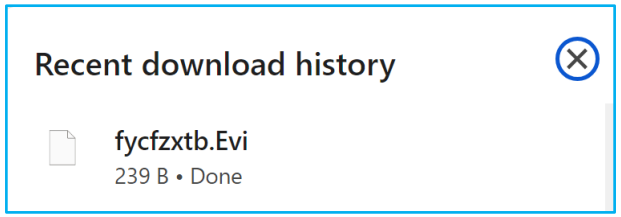
WHAT IS EVISEED?

- **EviSeed is a technology** that allows to secure SEED phrases
- **Seed phrases** should be saved offline
- They are composed of a variable number of words
- They can be written in different languages
- The backup is carried out encrypted

HOW TO SAVE A SEED PHRASE (BIP 39)



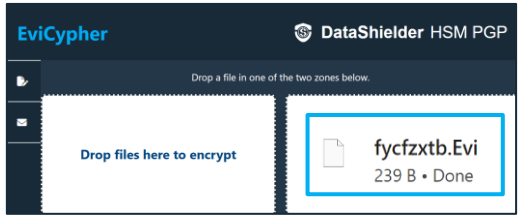
1. Give a name to your SEED phrase.
2. Select the number of words and choose the input language.
3. Enter the words in the correct order.
4. Click on "**Download encrypted Seedphrase**".



The **encrypted Seed phrase** is available in the "**Downloads**" folder.
You can safely store it in one or more locations of your choice.

To decrypt the file, go to **EviCypher**

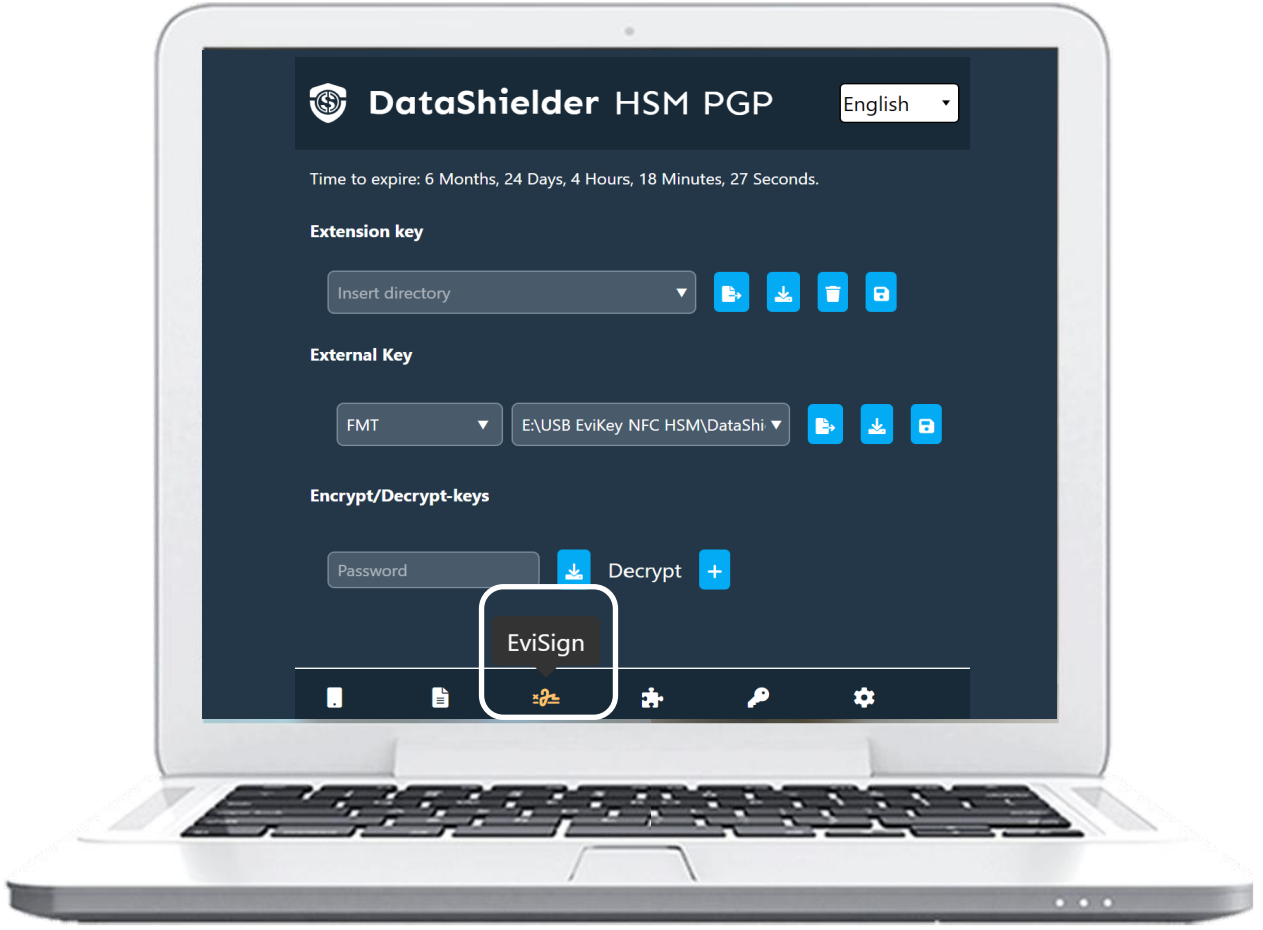
Follow the decryption procedure explained in the slide number 15



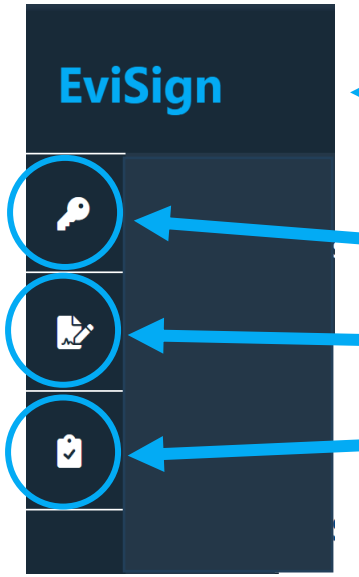
A check of the validity of the Seed phrase is carried out (CHECKSUM). If the words are incorrect or written out of order, an error message appears preventing the data from being saved.

DIGITAL SIGNATURE OF FILES

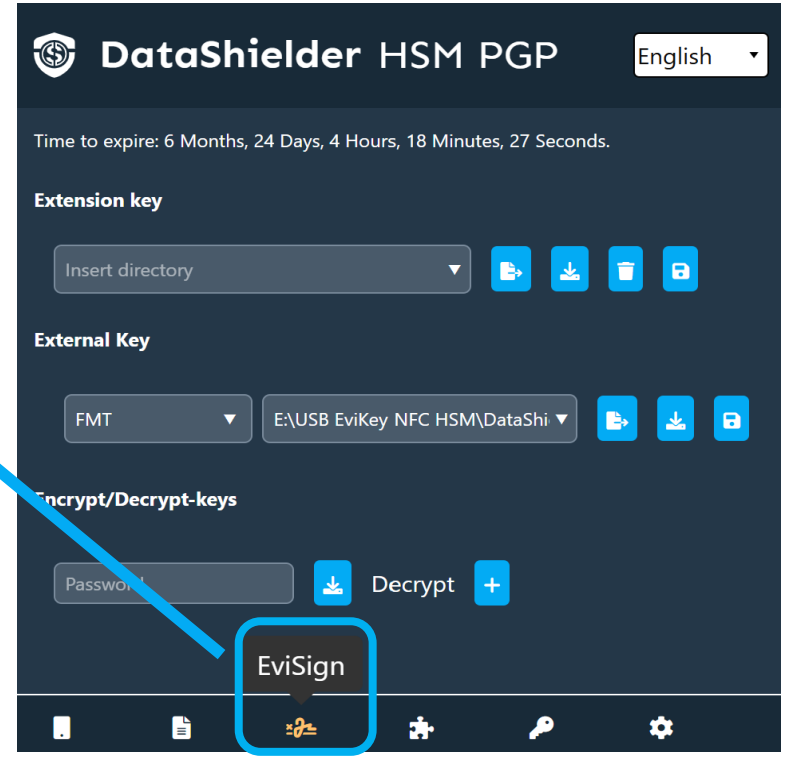
- **EviSign is an innovative technology** that allows you to sign electronic documents with complete confidence.
- Its **segmented key authentication system**, **timestamping**, and ability to give users full control over **their encryption keys** and sensitive data make it a reliable solution.
- It complies with current standards and regulations.



OPERATING PRINCIPLES

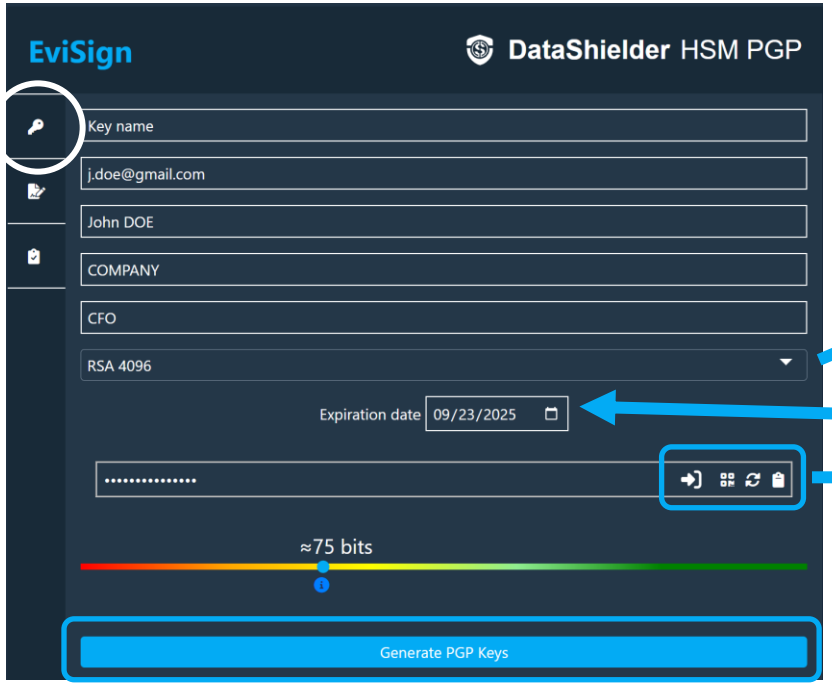


- **Create** a pair of PGP keys
- Drag and drop a file to **sign** it
- **Check** the authenticity of a file



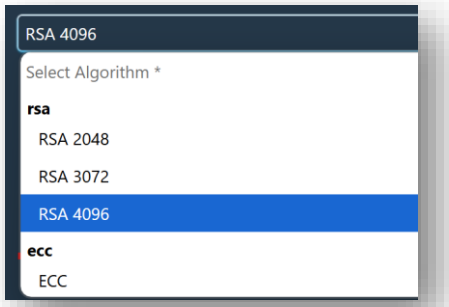
Click to access to EviSign

CREATE A PAIR OF PGP KEYS

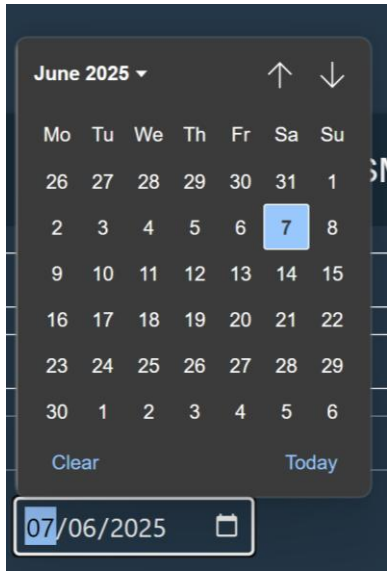


Complete the information: key name, email address, signer name, company name and choose the **algorithm**, and **expiration date**. Enter a **complex password** and click "**Generate PGP keys**".

Choose the algorithm



Choose the expiration date



Random Password

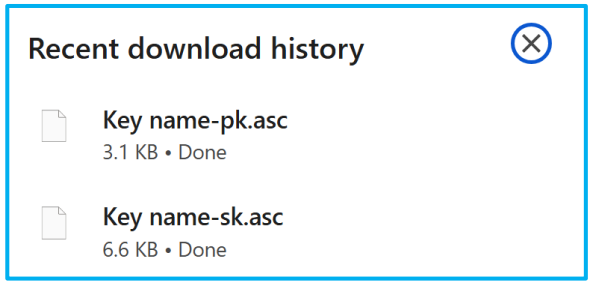
« Copy »

You need a Freemindtronic NFC device: Range PassCypher ou DataShielder

YouTube

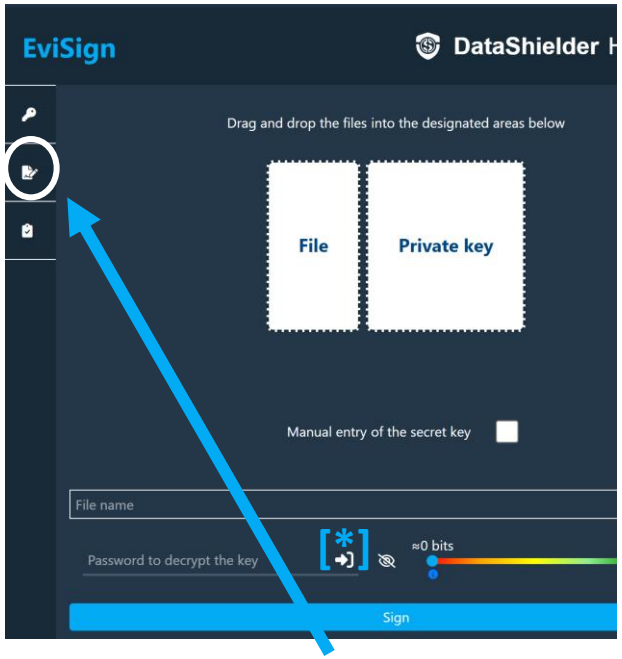
Tutorial : How to generate TSA/ECC Keys

https://youtu.be/Uyfktz1RcIg?si=B7_3bysQdUGAHpRj

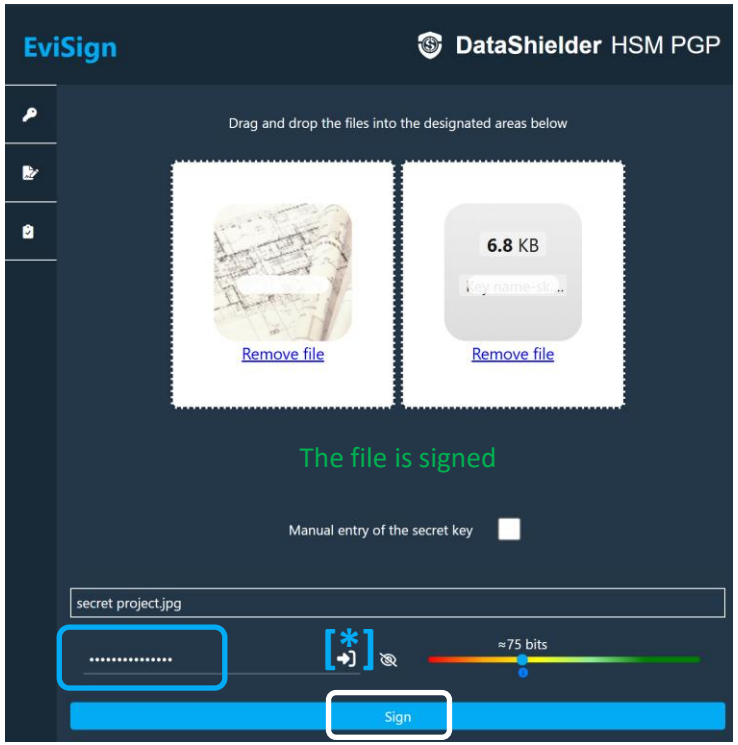


The keys are generated in **.asc format** and available in the "**Downloads**" folder. A public key -pk and a private (or secret) key -sk

SIGN A FILE

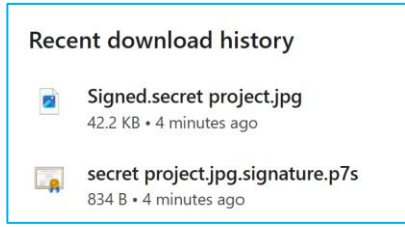


Click on the "**EviSign**" icon then on the indicated icon on the left side.



Drag the file to be signed as well as the private key. Name your file and enter a password. Finally, click on "**Sign**". The file is signed, a success message appears.

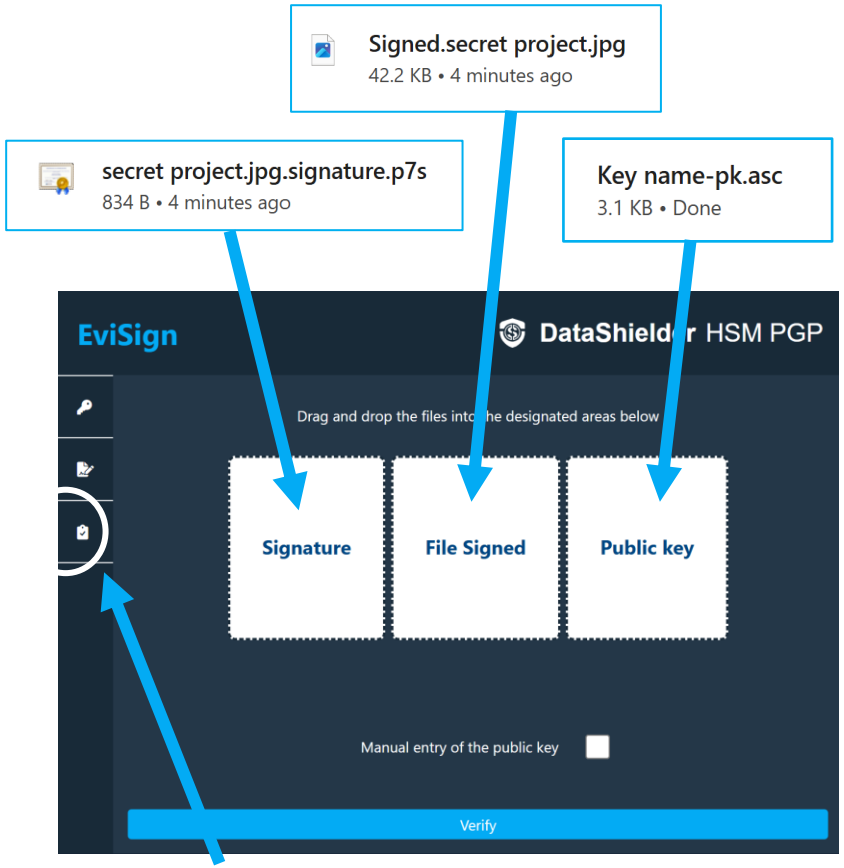
You can use the manual entry for the secret key. Just copy all the characters of this key. Then the process is the same.



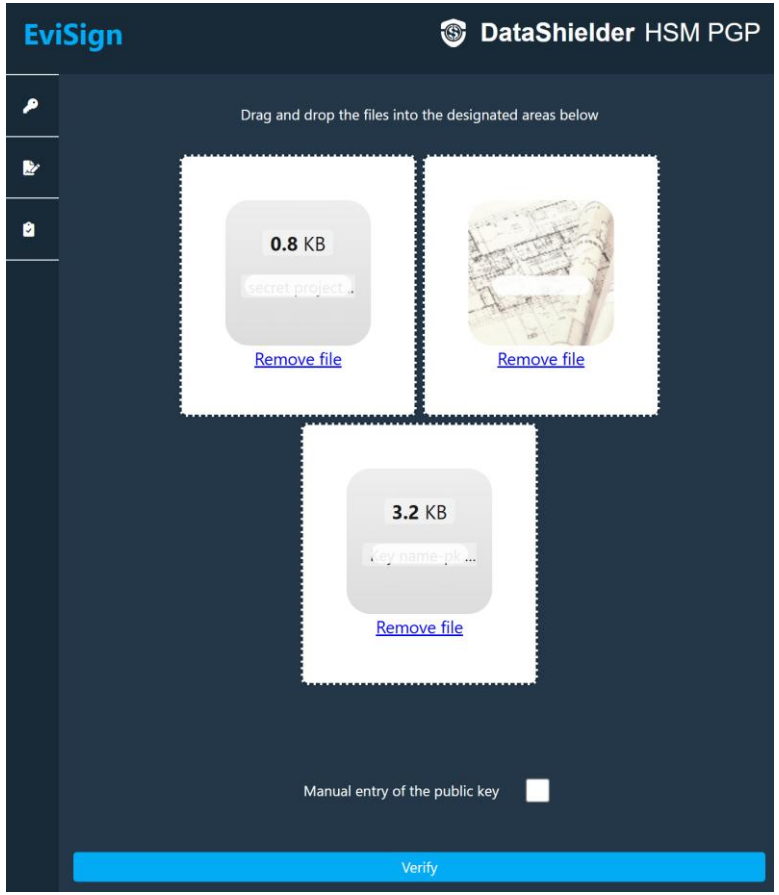
In the "**Downloads**" folder you can find the signed file and the digital signature key (.p7s)

[*] Functionnality available only with a Freemindtronic NFC device: Range PassCypher or DataShielder

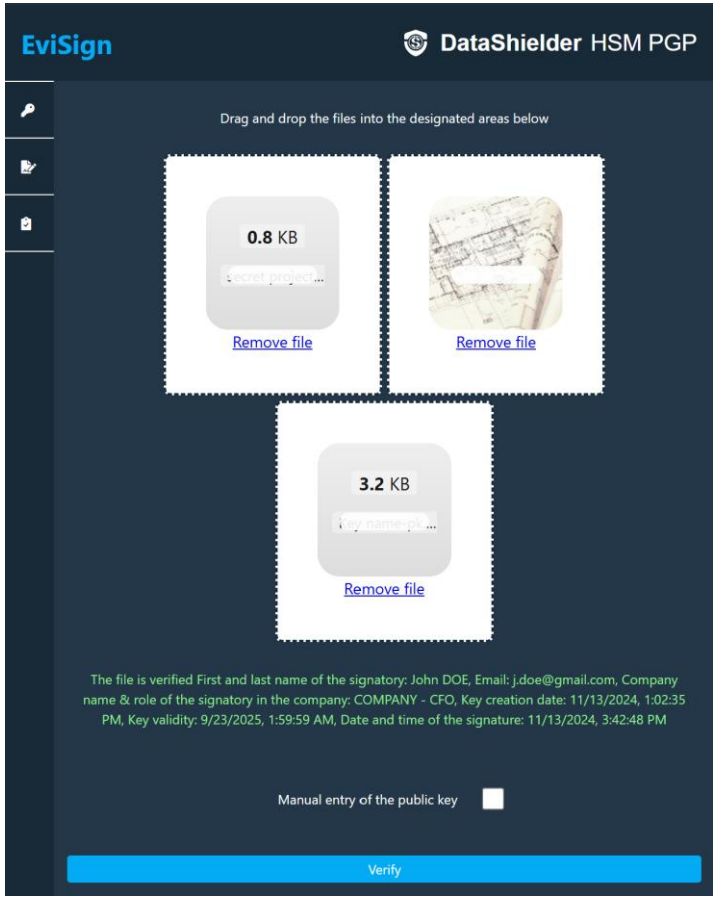
VERIFY THE AUTHENTICITY OF A FILE



Click on the "**EviSign**" icon then on the indicated icon on the left side



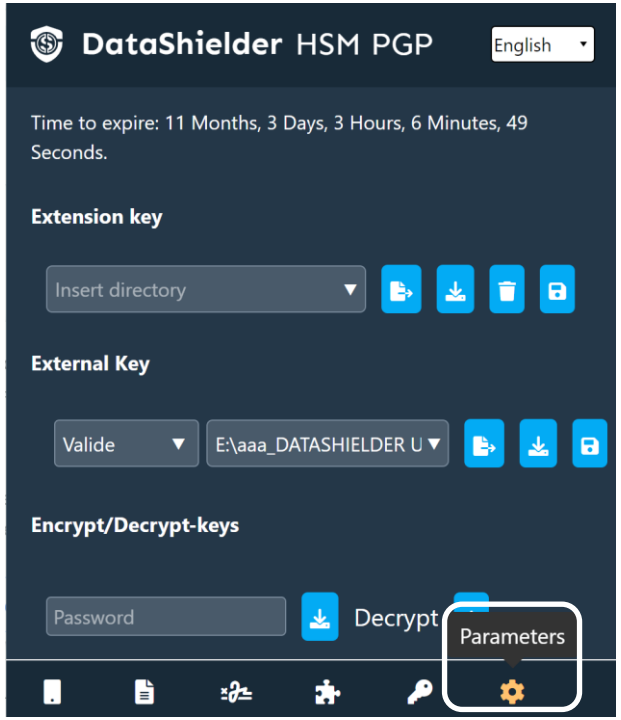
Drag the **signature**, the **signed file**, and the **public key**. Finally, click on '**Verify**".



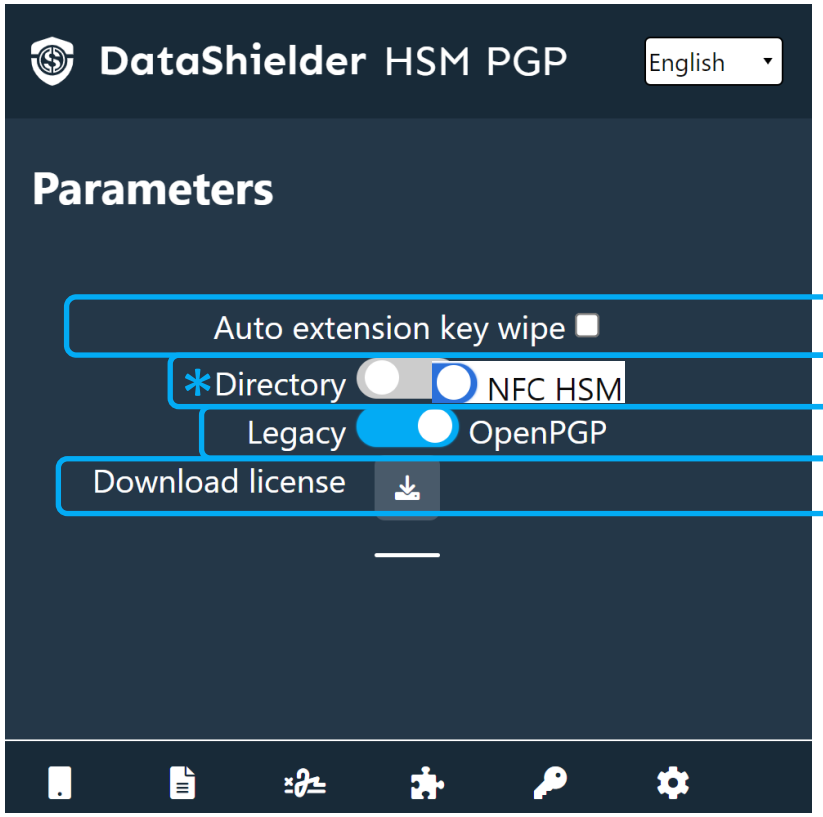
A success message appears with all the details about the signature.

In case of a problem, a message will appear: Verification failed

SETTINGS & FEATURES



Click on the « **Parameters** » icon



A window opens with different options that you can enable

The key will be deleted if the option is checked **

Enables the use of an NFC device ***

Choose the encryption algorithm for texts

Back up the license key on an external media!

(*) Operation explained in this tutorial: recording segmented keys in specific paths

(**) When the license expires, the key is automatically deleted for cybersecurity measures, especially if it is for temporary use on a computer that is not the user's.

(***) See the specific tutorial for the DataShielder Extension with Freemindtronic NFC device.

Take back control, Take back power

EviCypher Technology

By Freemindtronic Andorra

For more information: https://www.freemindtronic.com

Freemindtronic

Freemindtronic Channel