COMPLETE TUTORIAL

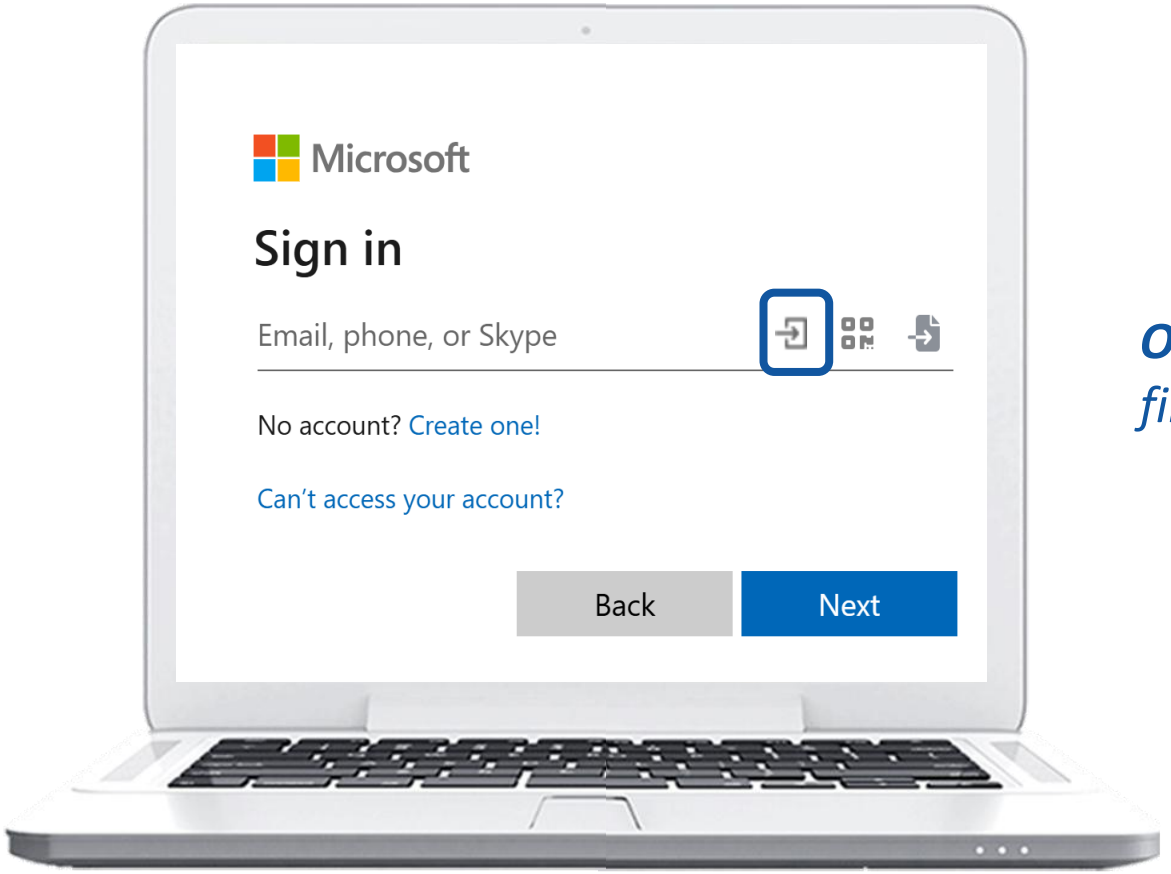
PASSCYPHER HSM PGP License

By Freemindtronic Andorra

Password manager with robust security

Serverless, Databaseless, without identication
« Zero Trust & Zero Knowledge »

INSTANT AUTOMATIC LOGIN

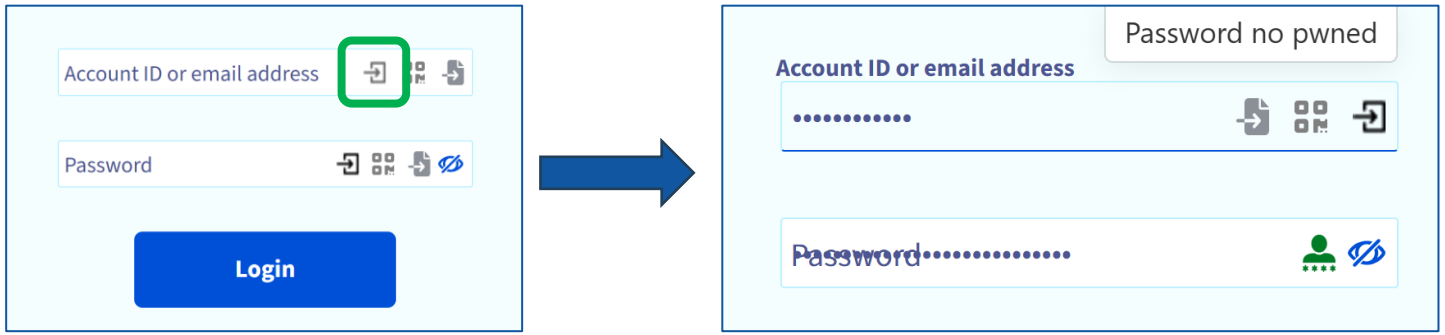


One click** on the indicated icon, the fields are filled**, and the connection is established.

CONTENTS

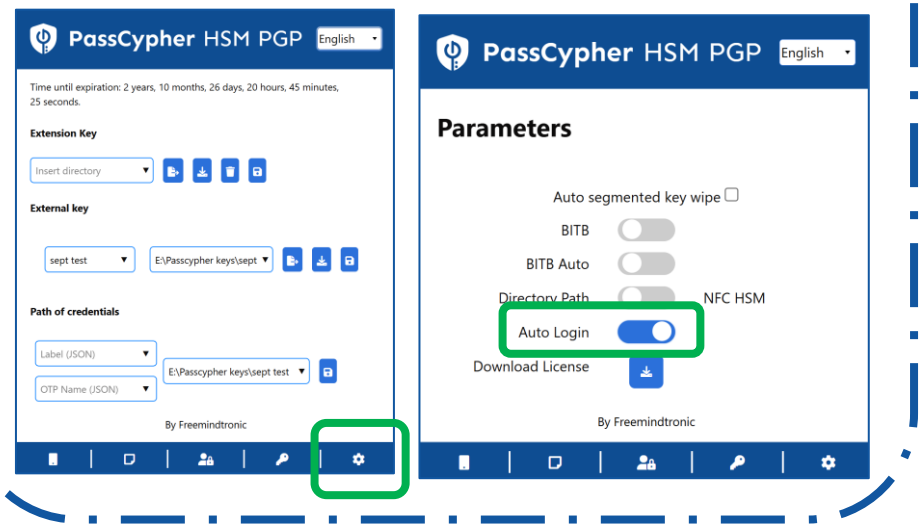
HOW DOES IT WORK?

- **PassCypher HSM PGP** is a browser extension that allows instant automatic login.
- **A patented system of segmented key authentication** is implemented.
- You benefit from **maximum security** and **unmatched execution speed.**
- **Click on the icon** shown below in the "Identifier" field.
- The fields are filled, and the login is completed
- Remember to enable Auto Login* in the extension settings.



(*) Enable Auto Login

Click the « **Settings** » icon, then slide the « **Auto Login** » button to the right.



INSTALL THE EXTENSION

Download and install the PassCypher HSM PGP extension:

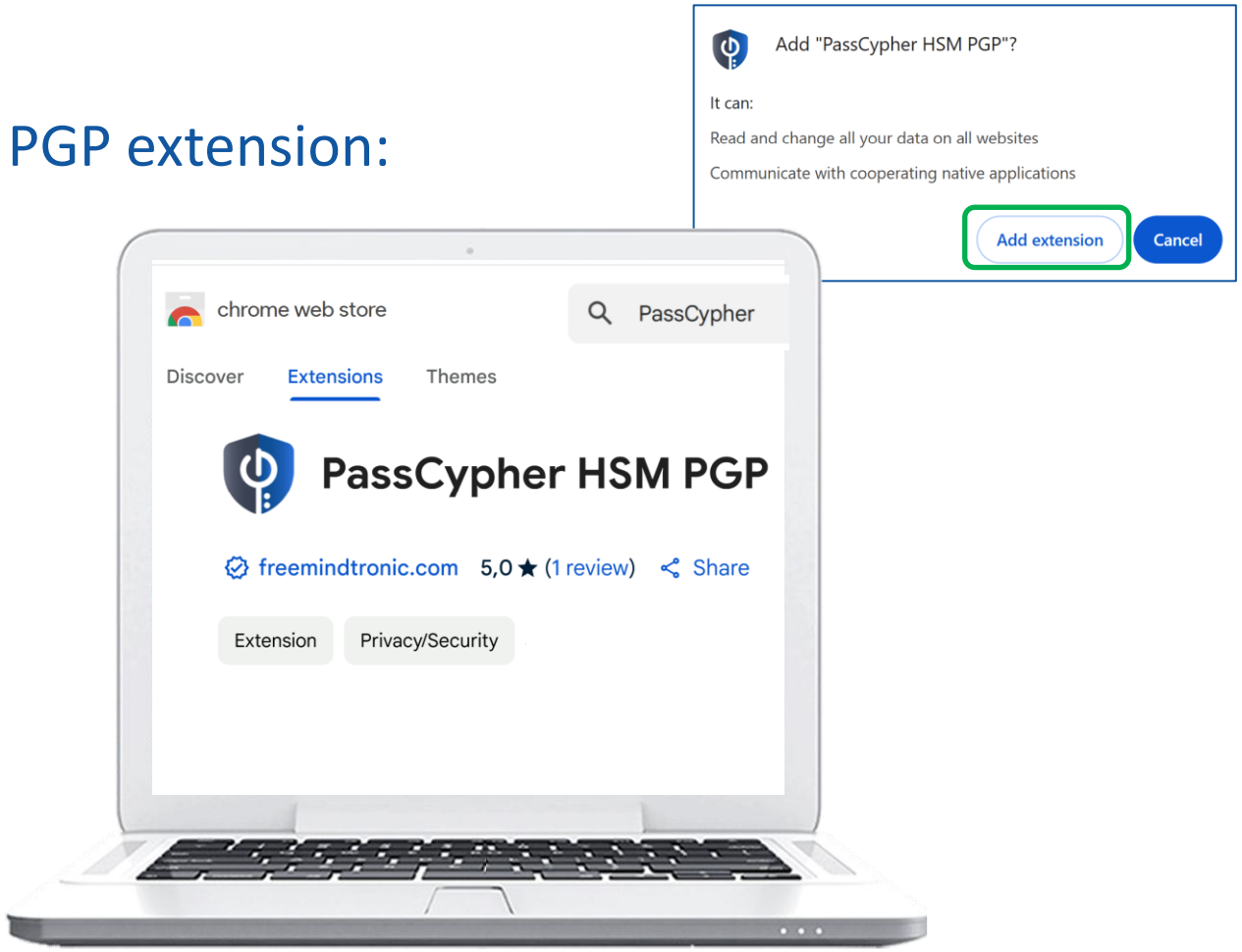
CHROME : chrome web store

BRAVE : chrome web store

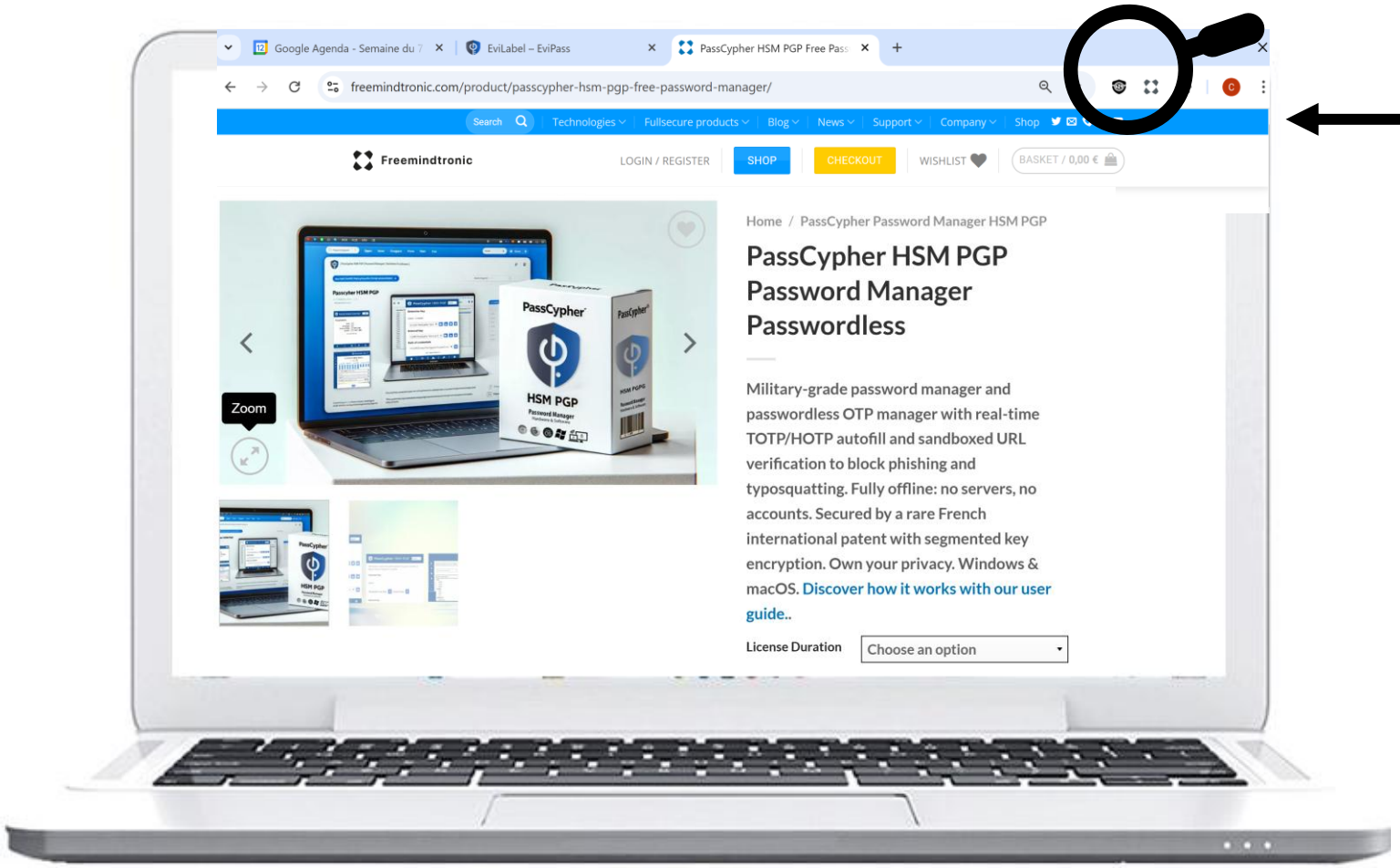
OPERA : chrome web store

MICROSOFT EDGE : PassCypher HSM PGP - Microsoft Edge Addons

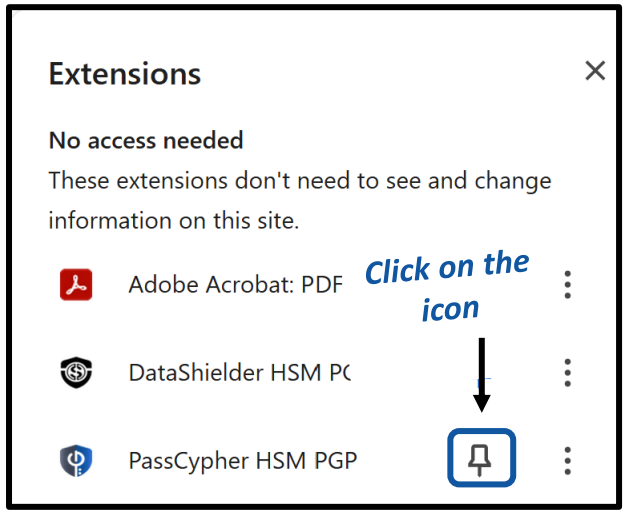
FIREFOX : in progress



COMPLETE THE INSTALLATION



Click on this icon to access the extensions.



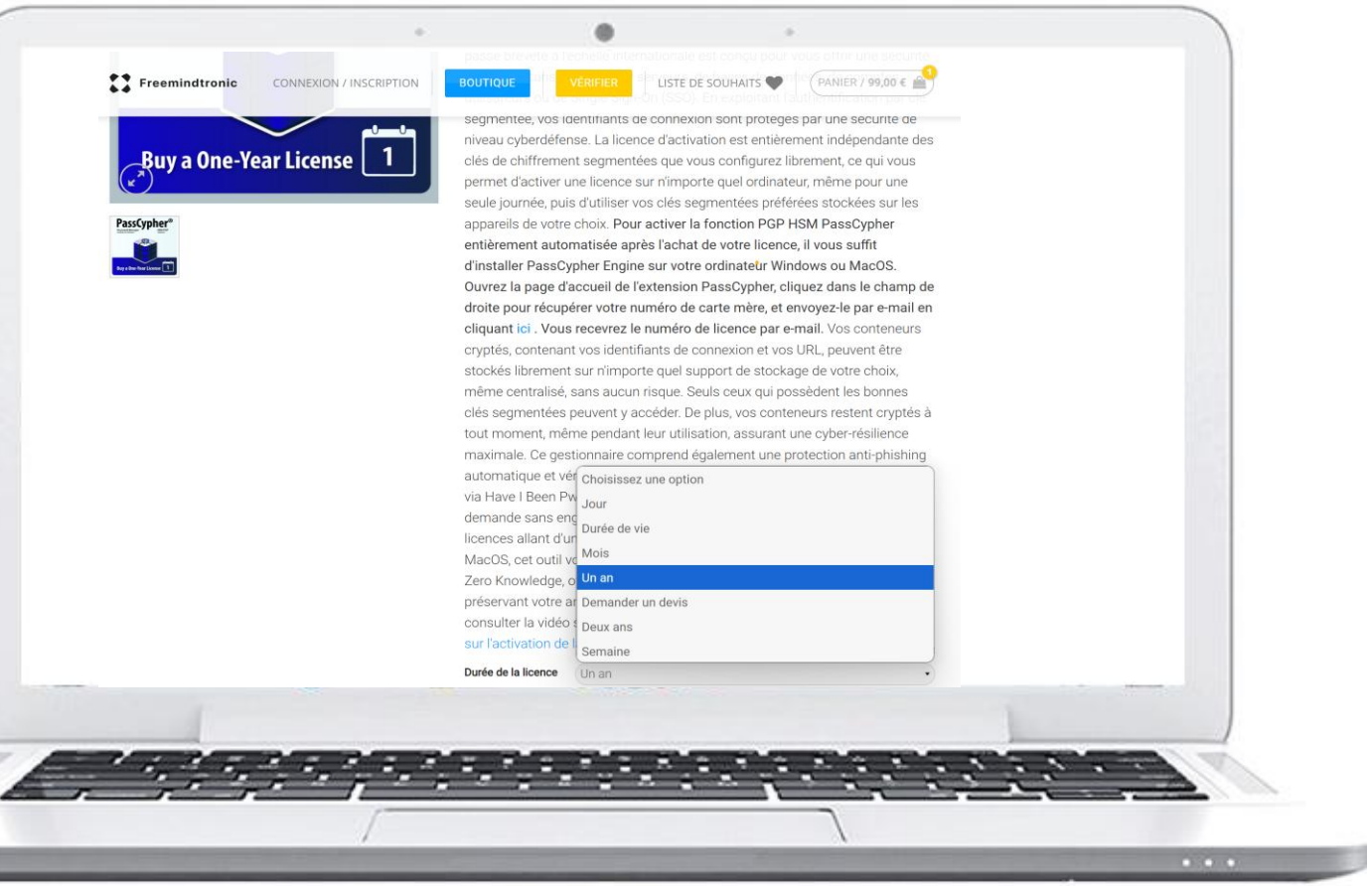
Click on the PassCypher icon at the top right of your computer screen to open the extension.

MULTILINGUAL EXTENSION

The PassCypher HSM PGP extension is translated into 13 languages: Arabic, German, English, Catalan, Chinese, Spanish, French, Hindi, Italian, Japanese, Portuguese, Romanian, and Russian.

You can choose the language in which the extension is displayed.

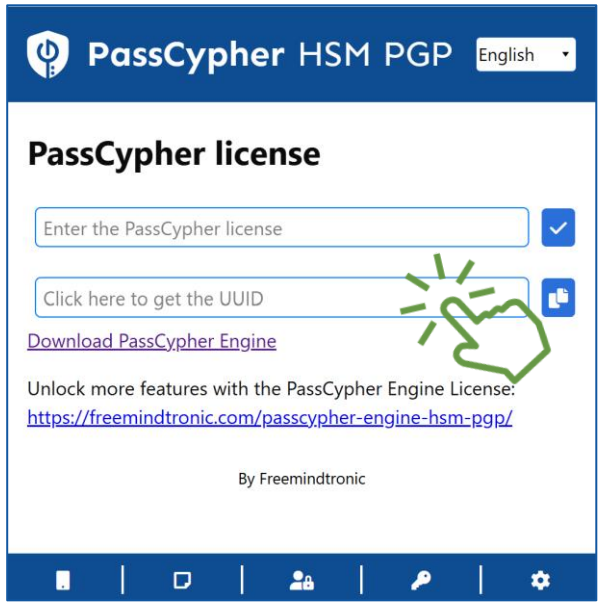
PURCHASE THE LICENSE



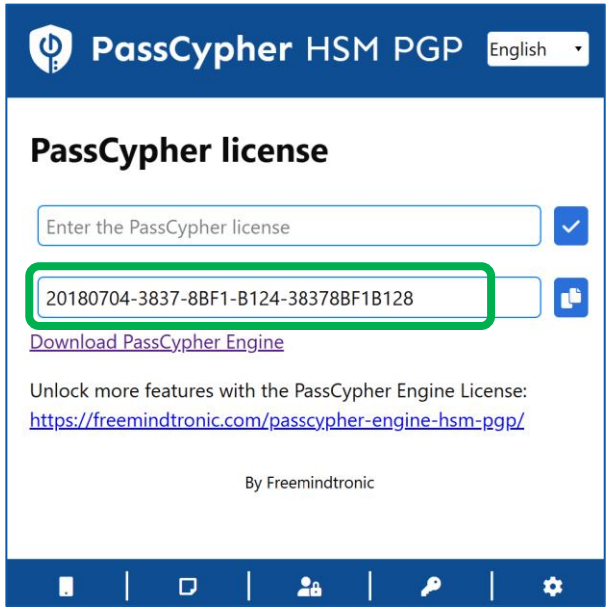
- Visit the FREEMINDTRONIC store
- Select **“PassCypher HSM PGP Password Manager”**
- Choose the option* that suits you best
- Proceed with the payment
- The next slide explains how to activate your license

(*) Note: There are several subscription options available: daily, weekly, monthly, or annually.

ACTIVATE THE LICENSE

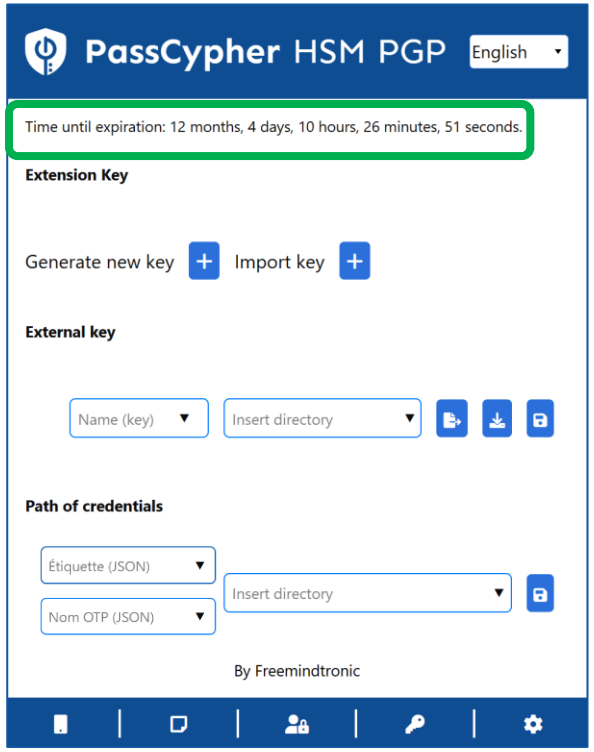


Click on "**Download PassCypher Engine**" and install the software (Windows or macOS)*. Then click to obtain the **UUID of your computer.**



Send this number to **fullsecure [at] freemindtronic.com**

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



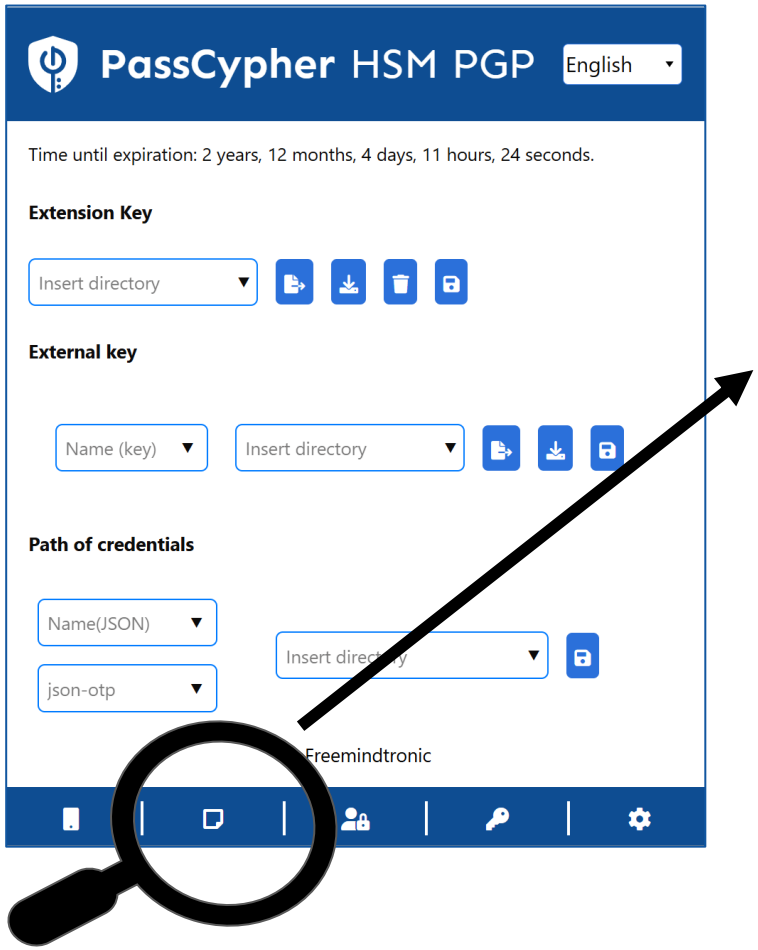
The license is activated. Its validity is displayed in real-time at the top of the page.

(*) Go to « **Download** Folder» and click on the file to install it

PassCypherEngine_1.3.0_x64 (3).exe

YouTube [Install PassCypher Engine]

HOME PAGE IN DETAIL



By default, the extension opens on the « keys » window

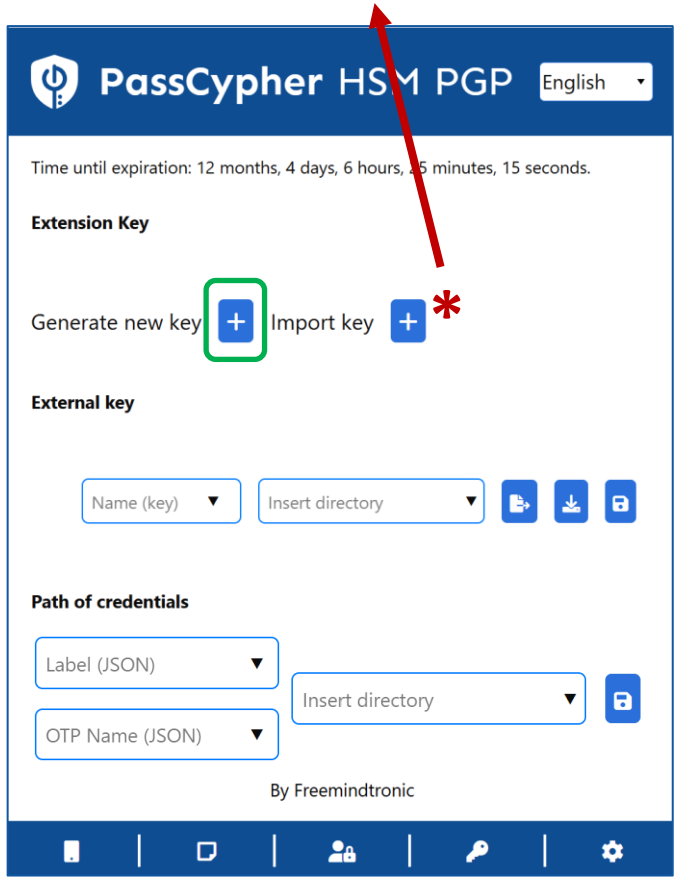
Phones *	Fetch a label	EviPass	Keys	Parameters
NFC function		Pwd management		

All these features are explained in this tutorial

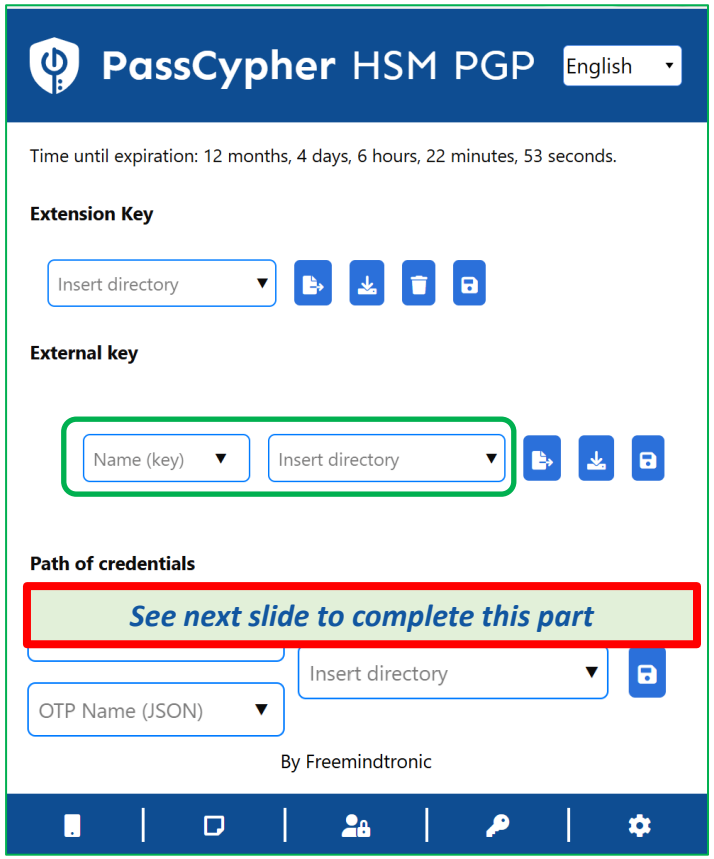
(*) Consult the tutorial for specifical NFC function: https://freemindtronic.com/how-it-works-products-in-depth-guide-to-fullsecure/

CREATE* YOUR SEGMENTED KEYS

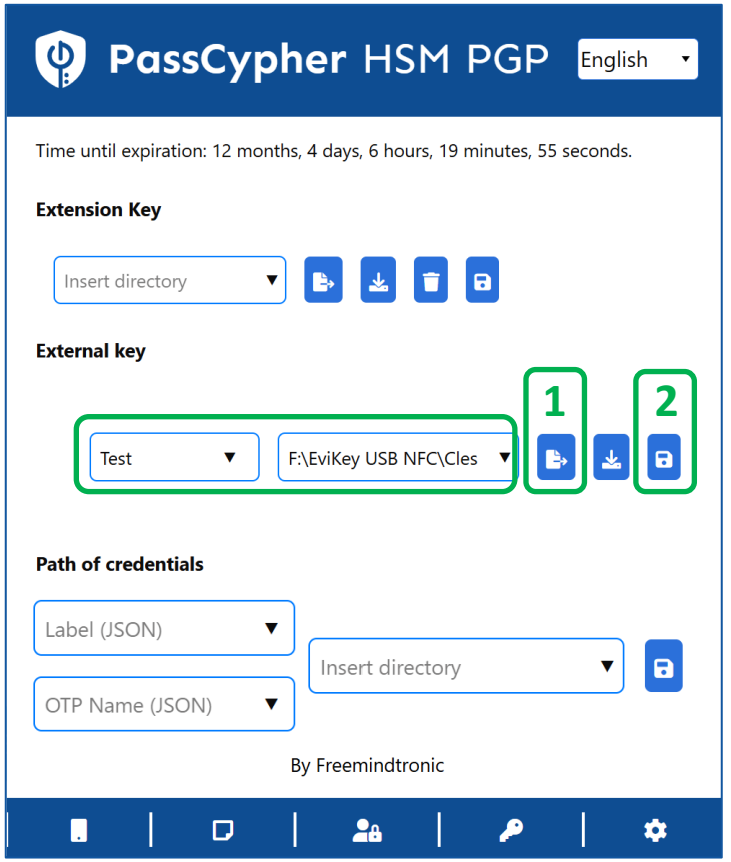
(*) If a segmented key already exists (extension key and external key), see next slides



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



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



Click on the « **EXPORT » icon [1]** follow by the « **SAVE » icon [2].** The external key « **Test** » is created and saved.

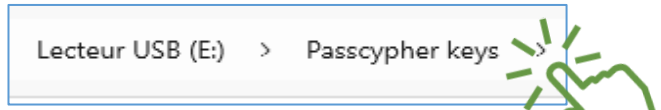
Insert the storage path*: detailled explanations in the next slide

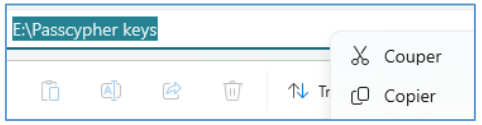
INSERT THE ACCESS PATH

- **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.**

To ensure optimal security, if the external media is not available or connected to the computer, it will not be possible to access the external key.

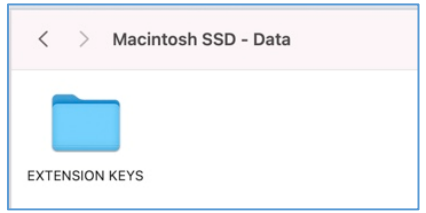
Windows



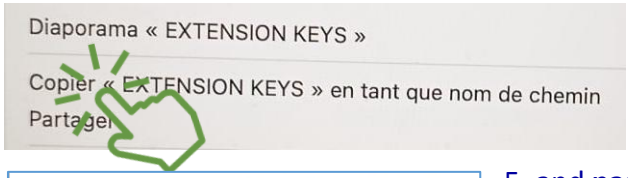


1. Create a folder [**here "PassCypher keys**] in your external media
2. Location is displayed
3. Click in the window, the path is selected
4. Right click, "Copy" button appears
5. Click "Copy" and paste into the extension without adding any other characters

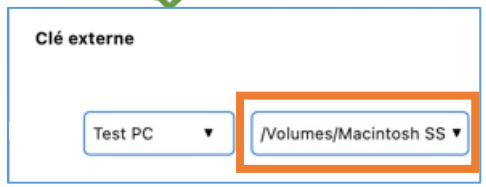
macOS



1. Create a folder **[here "EXTENSION KEYS]** in your external media
2. Location is displayed
3. Hold down the "**alt or option" key** and right-click the mouse



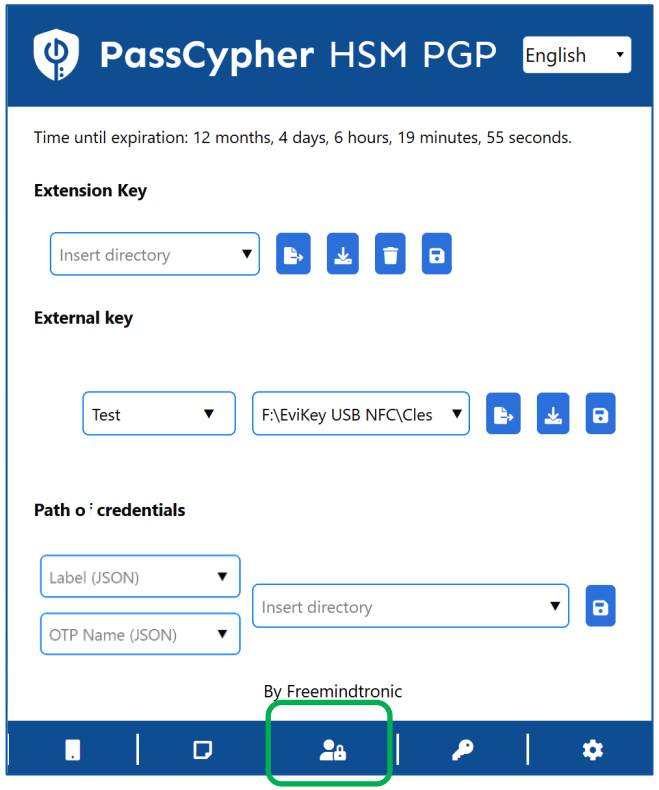
4. Click on « **Copy** »



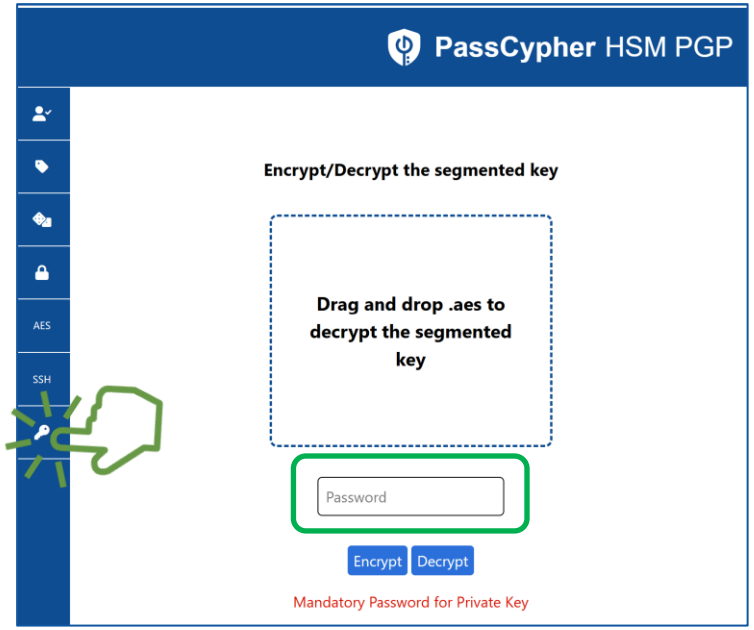
5. and **paste** in the extension without adding any other characters

When pasting, check that the character " is not added to the beginning of the pasted characters. If so, delete it.

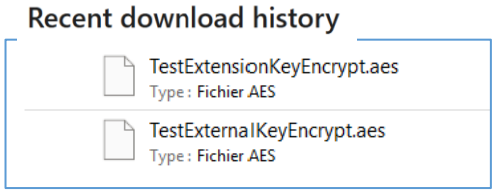
SHARE YOUR SEGMENTED ENCRYPTION KEYS



To share keys with a recipient, you must **encrypt** them. Click on the "**EviPass**" icon. A new window will open.



Click on the "**Keys**" icon and enter a **password** of at least 12 characters. Then click "**Encrypt**."

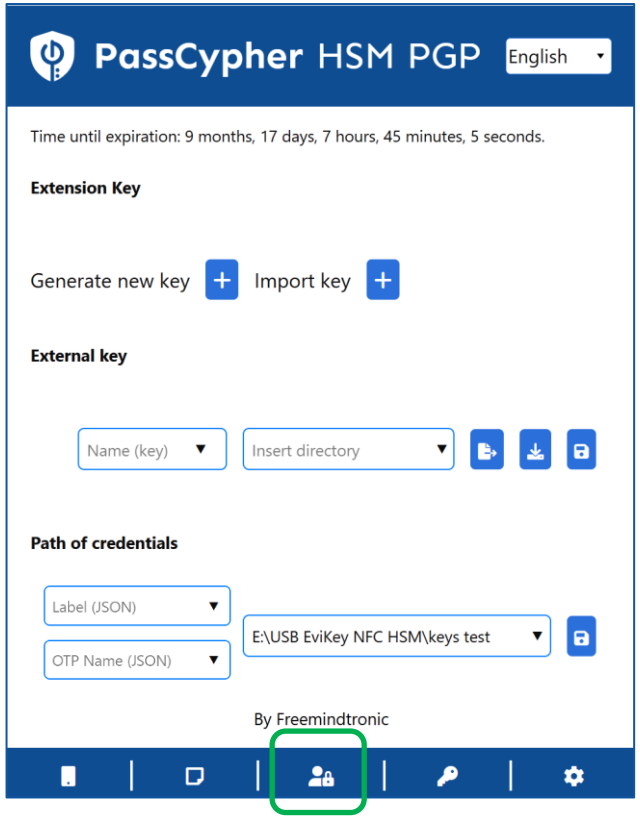


Automatically the external key and the extension key are encrypted. You can retrieve them from the “Downloads” folder.

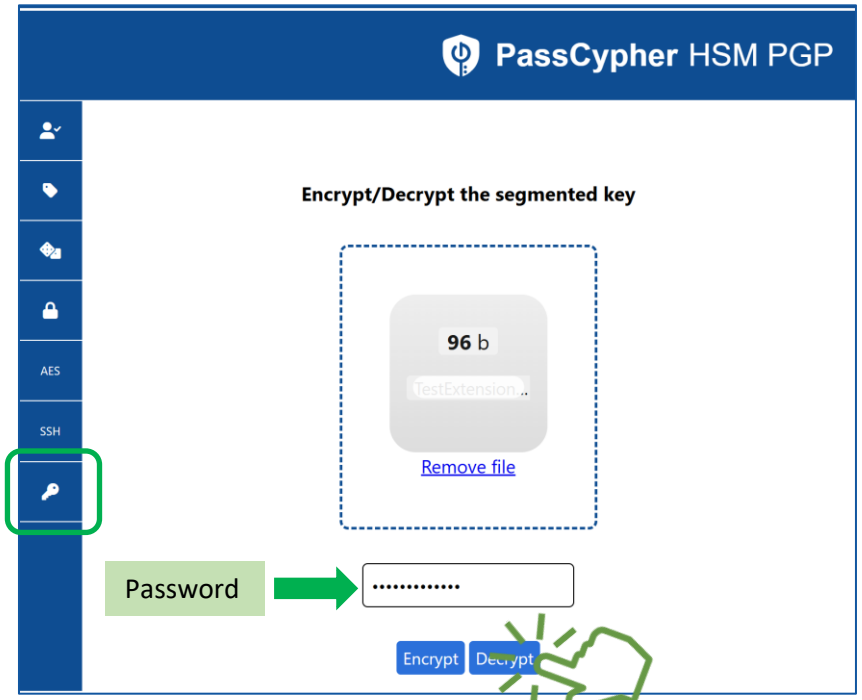
Send the 2 encrypted files by **email** (or other) to your recipient and provide the password via another channel (**e.g., SMS**).

IMPORT SEGMENTED ENCRYPTION KEY

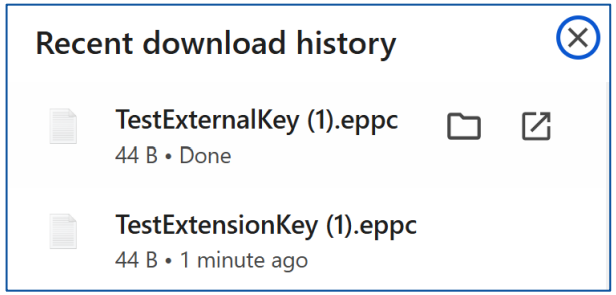
Start by decrypting the keys segments



To decrypt keys sent by a recipient, click the "**EviPass**" icon.



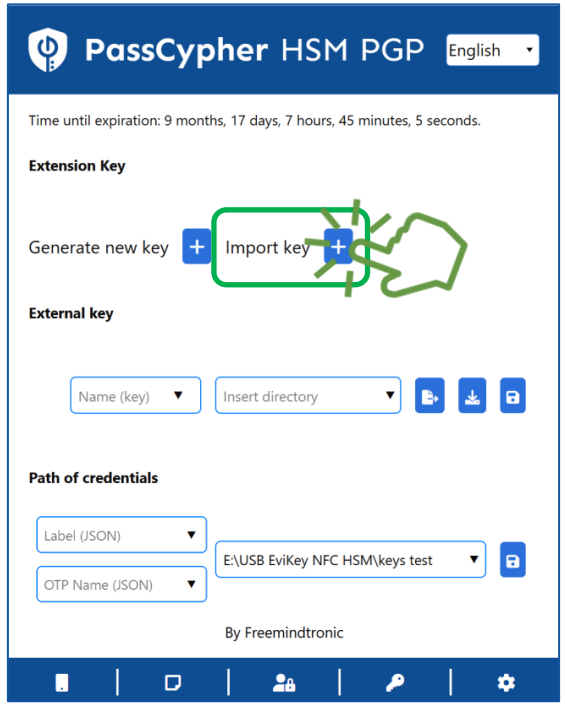
Click the Key icon, insert the **encrypted extension key** (Copy/Paste or Drag the file). Enter the password and click "**Decrypt**."



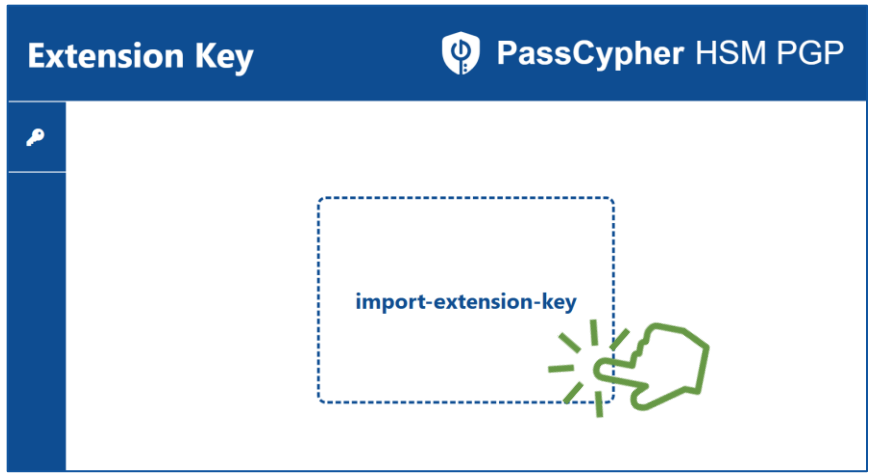
Repeat the process for the external key. The **2 decrypted files** will appear in the **"Downloads" folder.**

IMPORT SEGMENTED ENCRYPTION KEY

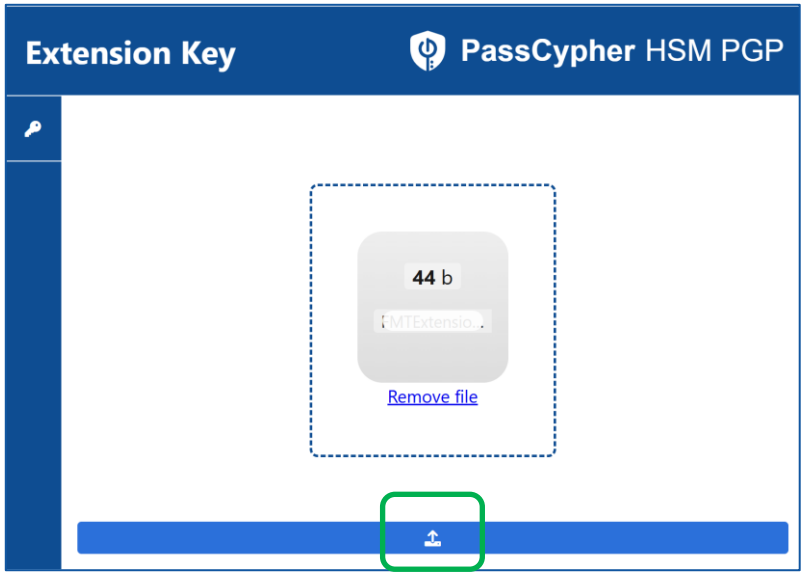
First, import the extension key



The segmented extension key sent by your correspondent is decrypted.
Click the “Import Key” icon



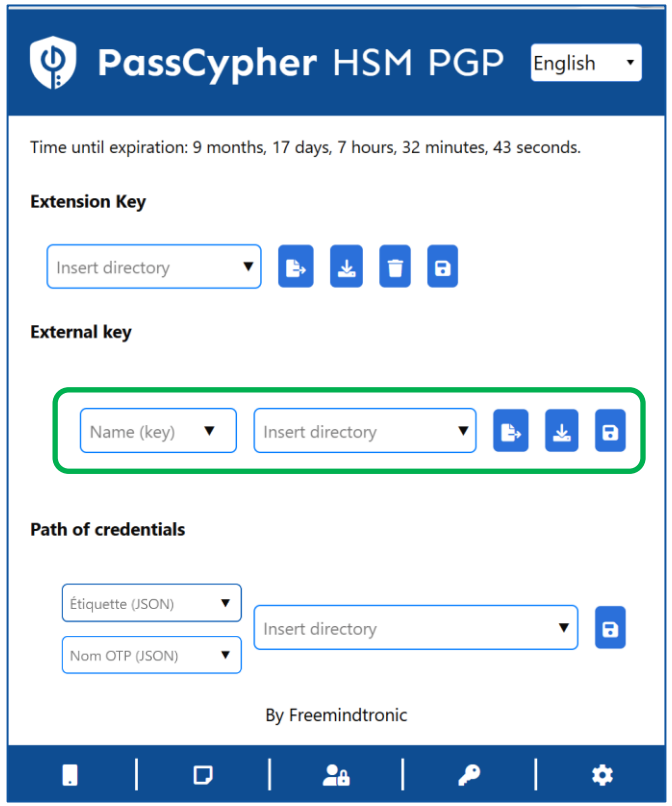
Click in the window and import the **decrypted extension key**



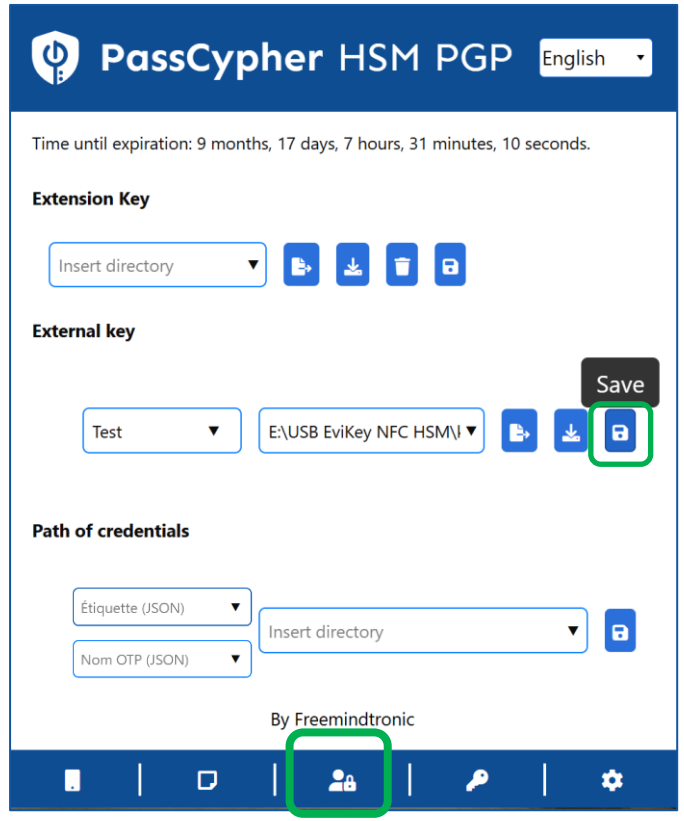
When the key is inserted, click the arrow. A "**Success**" message will appear. Close this window and reopen the extension.

IMPORT SEGMENTED ENCRYPTION KEY

Indicate the path where the external key is stored.



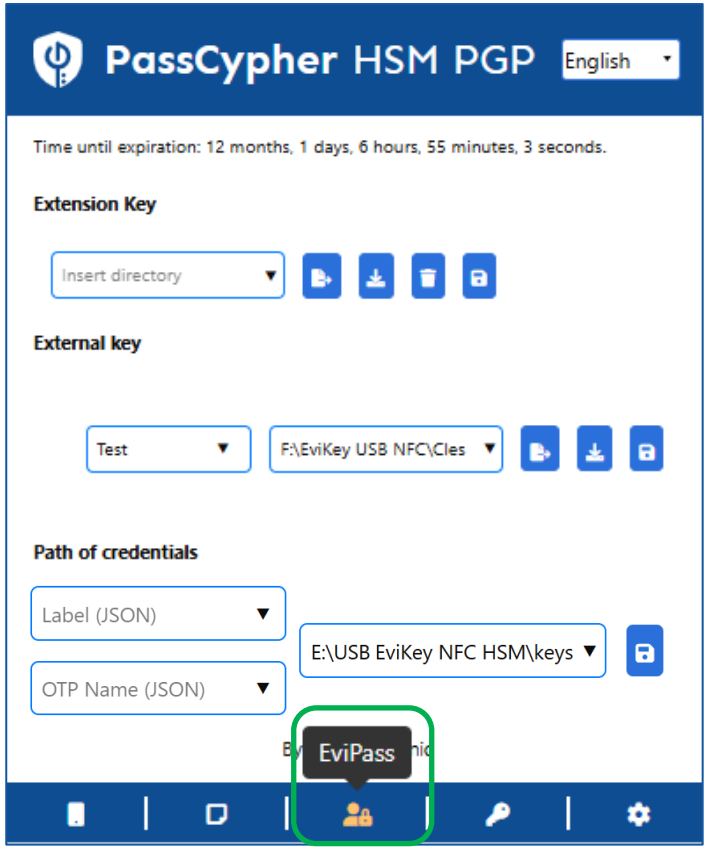
Store the external key "**TestExternalKey.eppc**" in the location of your choice* (here an **EviKey** USB key). For the extension to access the external key, write the key name (**Test**) and enter **the path to the key**. Then click on the "**Save**" icon.



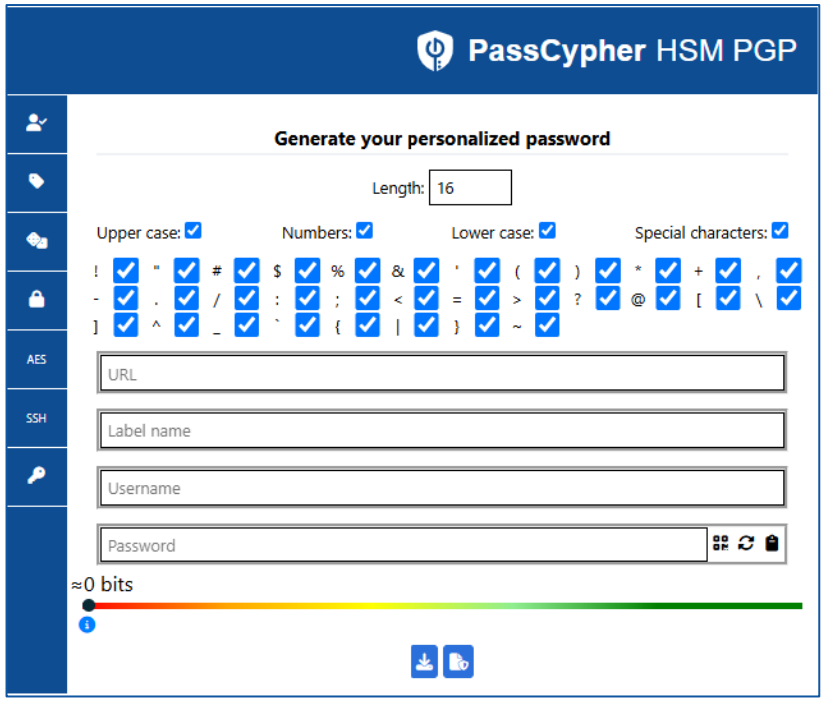
The key import is complete. You can now begin building your login credentials directory. To do that, click on the **« EviPass » icon**

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

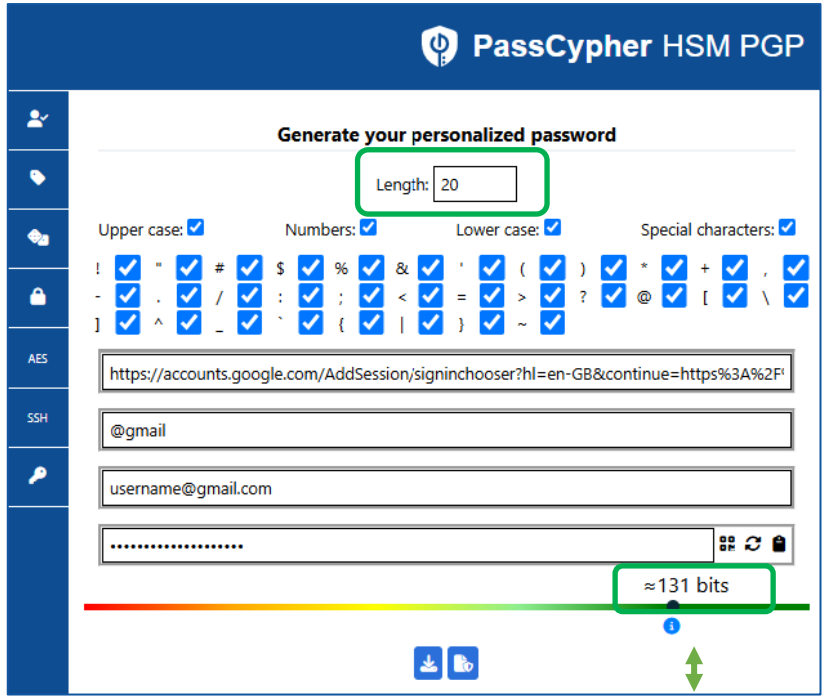
CREATE YOUR LOGIN CREDENTIALS



Open the extension and **click on the indicated icon "EviPass"** to create your login credentials.

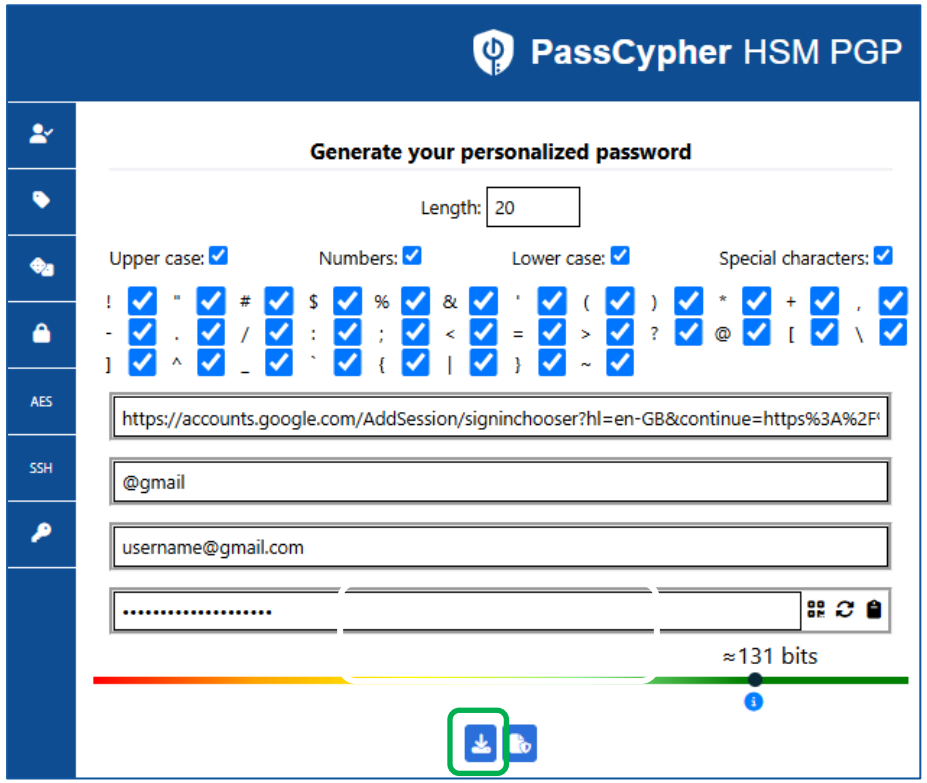


Fill in the required information. To complete the URL, copy the information displayed in the browser's address bar (**see the example below**).

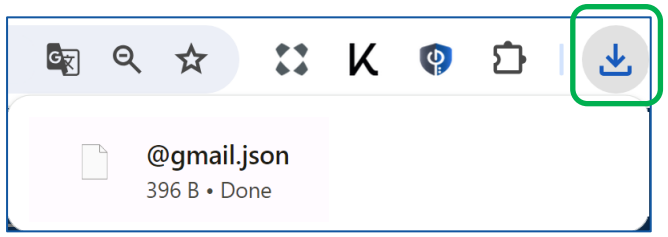


URL example = https://accounts.google.com/InteractiveLogin/signinchooser?continue=https%3A%2F%2Fmail.google.c...

SAVE YOUR LOGIN CREDENTIALS



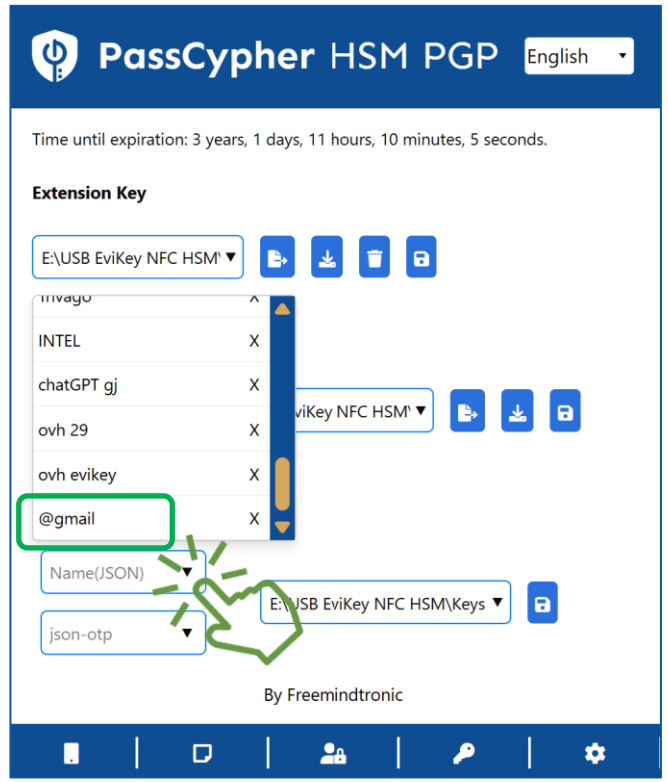
Click on the indicated icon to generate this credential.



The file **@gmail.json** will be available in the "Downloads" folder of your computer.

Choose a folder to save your encrypted containers (.json files). It is recommended to use an external storage device for security reasons.

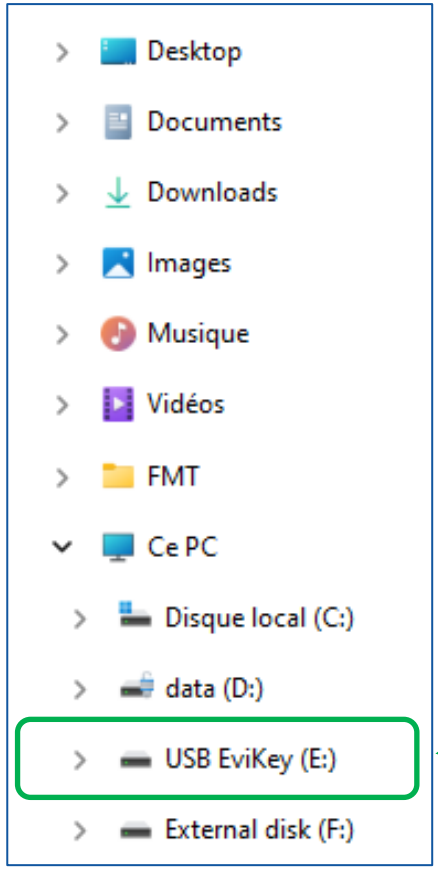
See the next page for details.



The created « **.json** » file is automatically added in the extension to the list of all the created credentials

Remember to make regular backups to different media, including the cloud since your containers are encrypted.

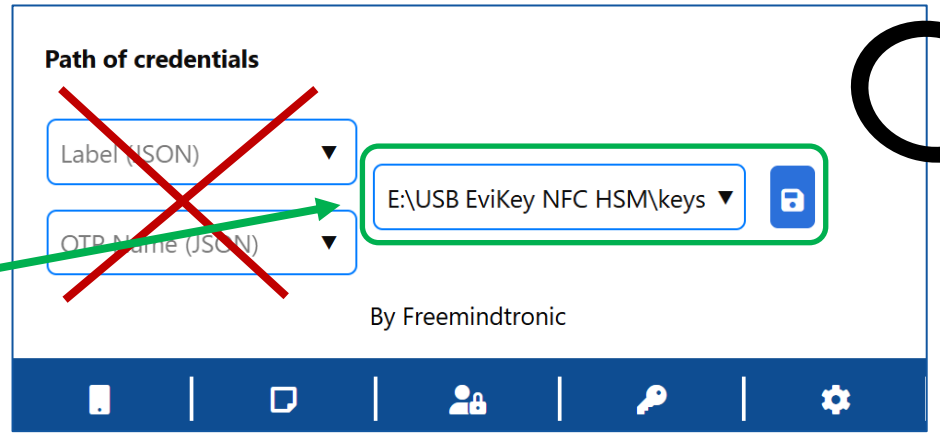
DETERMINE THE PATH TO SAVE YOUR LOGIN CREDENTIALS & OTP

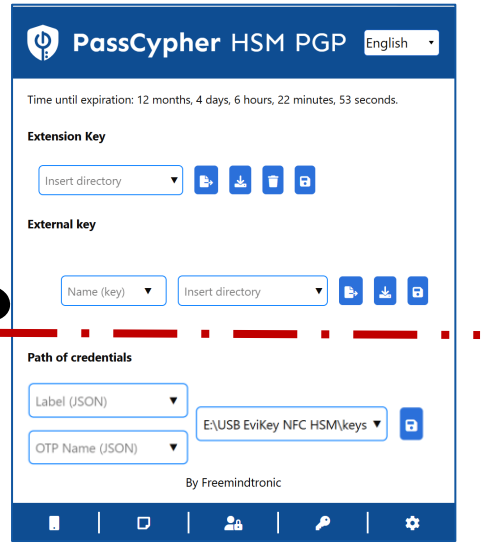


It is **essential to specify the access path to your encrypted containers** (.json files) very precisely to enable automatic login for websites and messaging platforms.

Then, click on the "**Save**" icon to confirm.

To ensure optimal security, if the external media is not available or connected to the computer, it will not be possible to use encrypted containers.

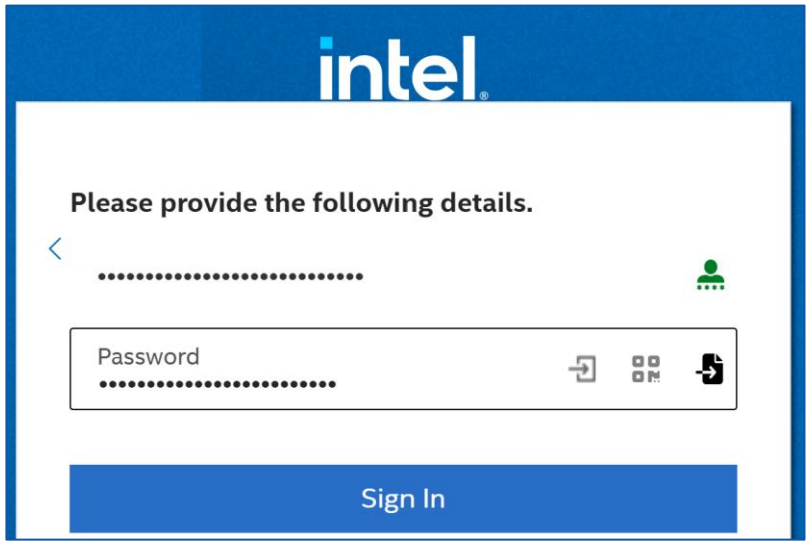




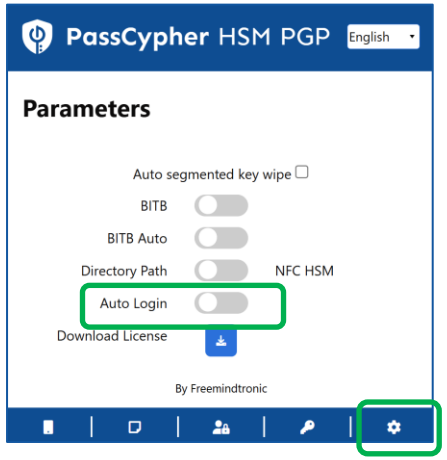
AUTOFILL

VS

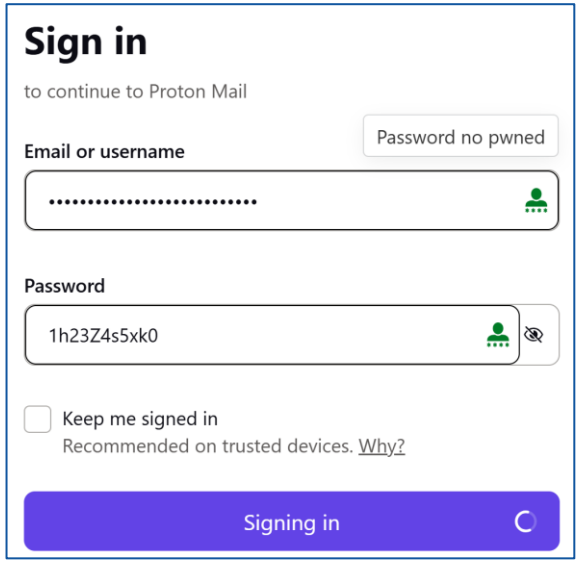
AUTOLOGIN



The "Username" and "Password" fields are automatically filled in. **All you have to do is click on “SIGN IN".**



To log in automatically, slide the "**Autologin**" button to the right. **You will no longer need to click "Login".**

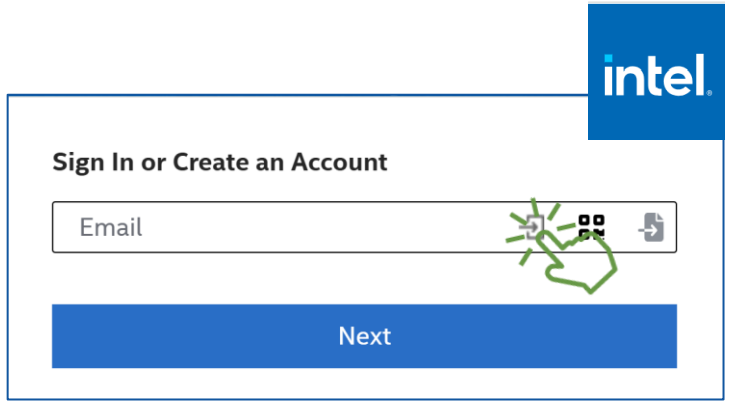


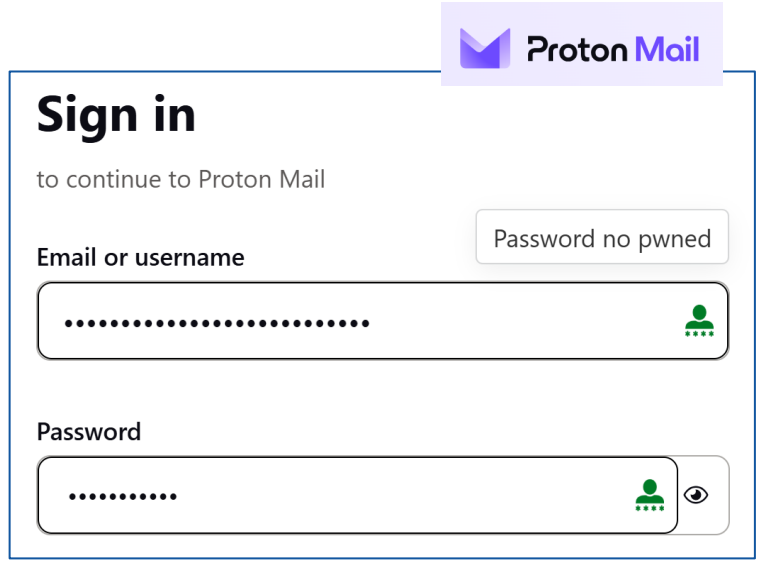
Autologin example here. The fields have been filled in and the **login is in progress** without any action on your part.

ENABLE THE AUTOLOGIN FEATURE IN THE EXTENSION SETTINGS (not all sites are compatible)

LOG IN NOW!

1. On your computer, open the website or email you want to connect to
2. Go to the login page [Username & Password]
3. Click on the icon visible in the connection field
4. The fields are filled automatically and the connection is made (**if you have activated Autologin in the Extension Settings**)





Your password is verified. The green symbol indicates that it has not been compromised

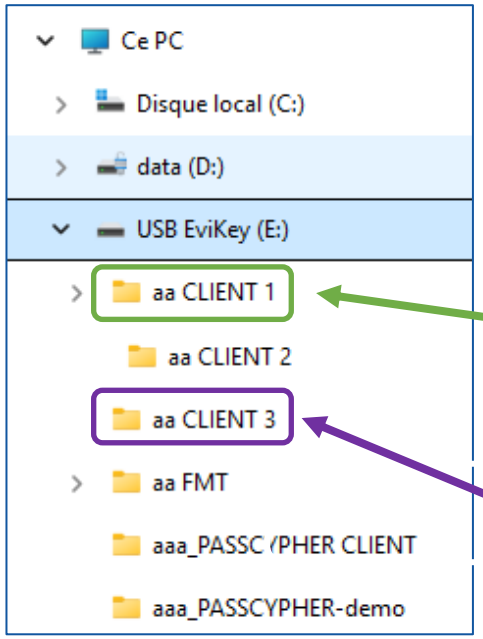
If this symbol appears, it indicates that your password is compromised. Change it!

AUTOLOGIN IN ONE CLICK!

Access your favorite messaging platforms or websites and enjoy a fast, secure, and automatic connection.

MANAGE MULTIPLE ACCOUNTS

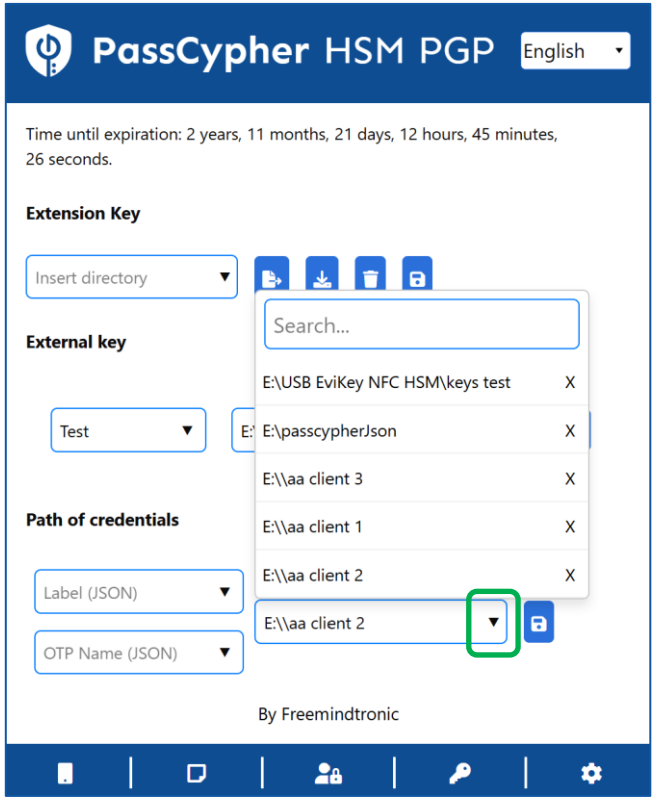
Example: Accounting or legal firm managing clients with accounts in the same bank



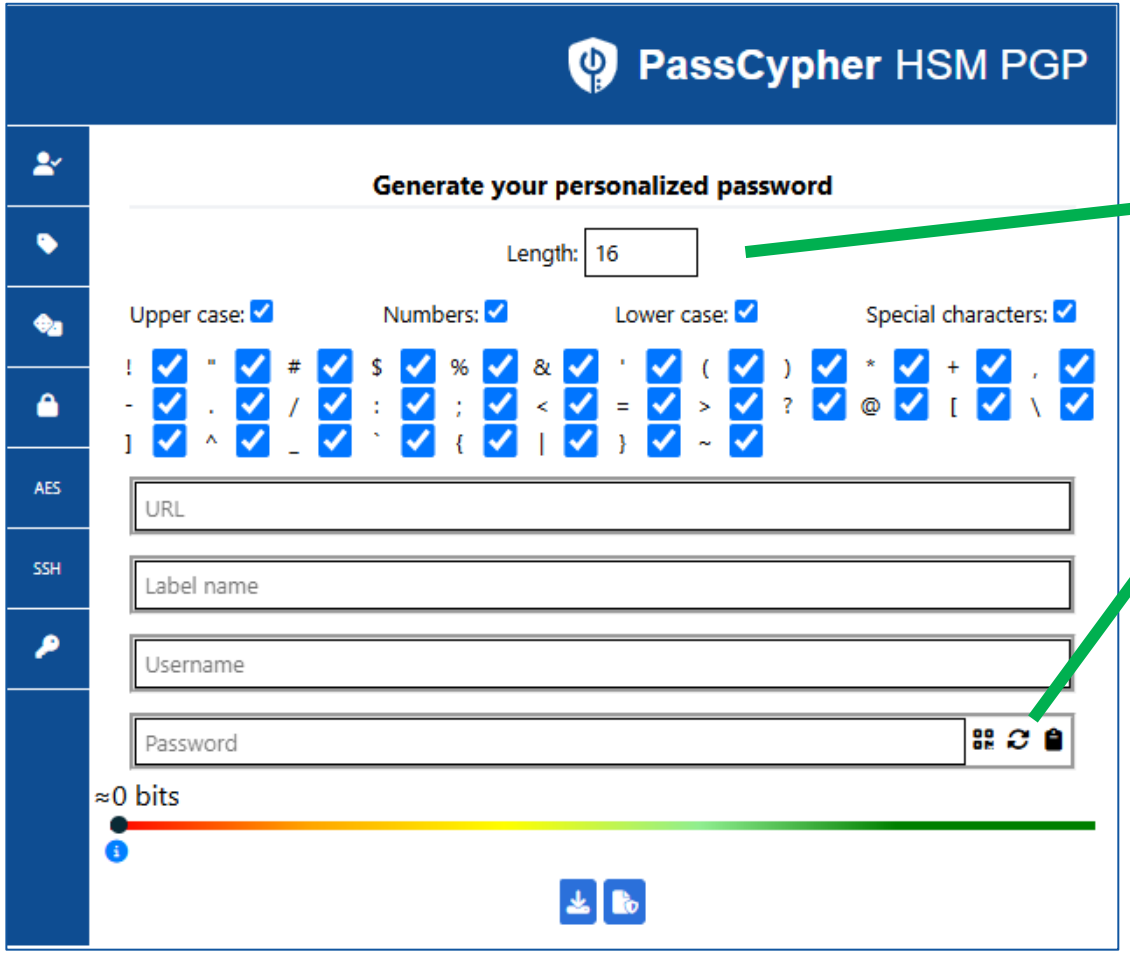
In each "**client folder**", save the different login credentials specific to that client.

During automatic login, **specify the path** where the client's credentials are located.

Click on the indicated symbol to access all CLIENT paths. You can use the "**Search**" window for quicker navigation. Click on the desired path.

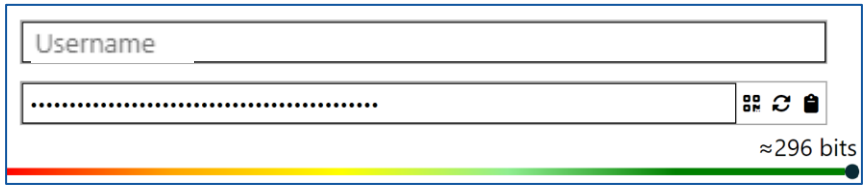


USE THE PASSWORD GENERATOR

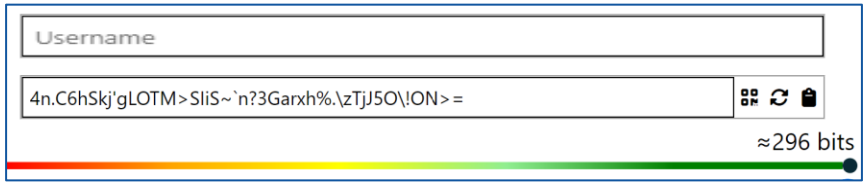


The default password length is 16 characters, but you can modify it in the window.

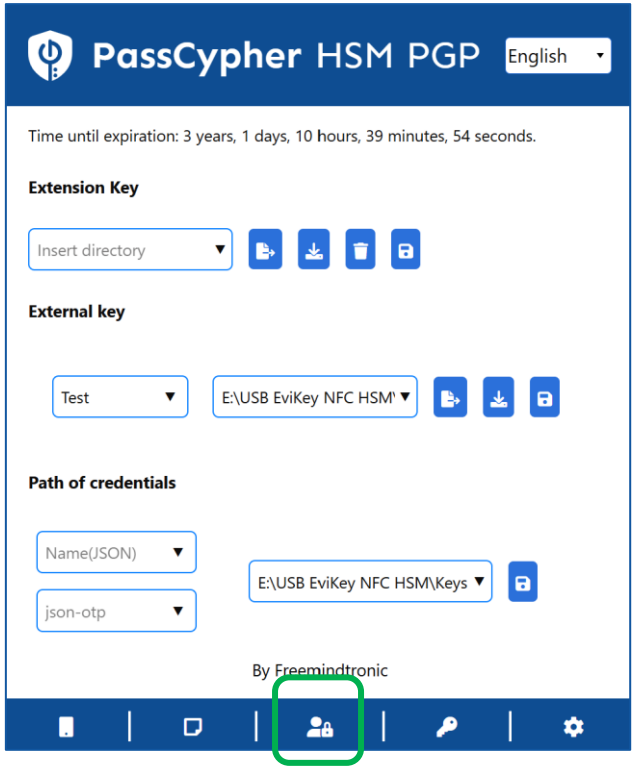
Click to generate the password (example shown: 45 characters).



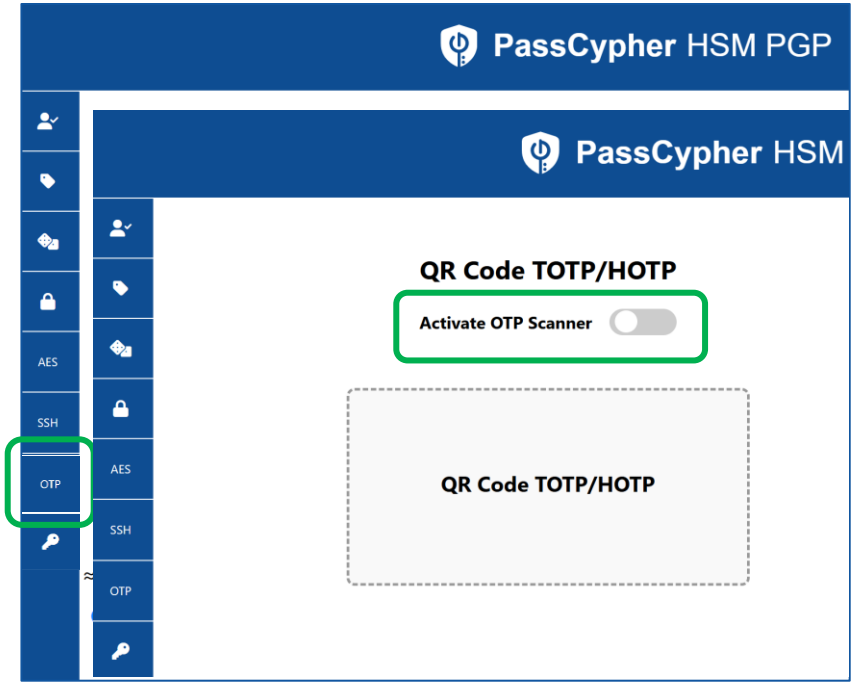
Hover your mouse over the field to view the password in plain text.



MANAGE YOUR TOTP/HOTP (2FA) 1/2



Open the extension then **click on the indicated icon** to manage your OTP



Click on « **OTP** ». A new window will open. **Drag and drop** the file or enable the **OTP scanner**

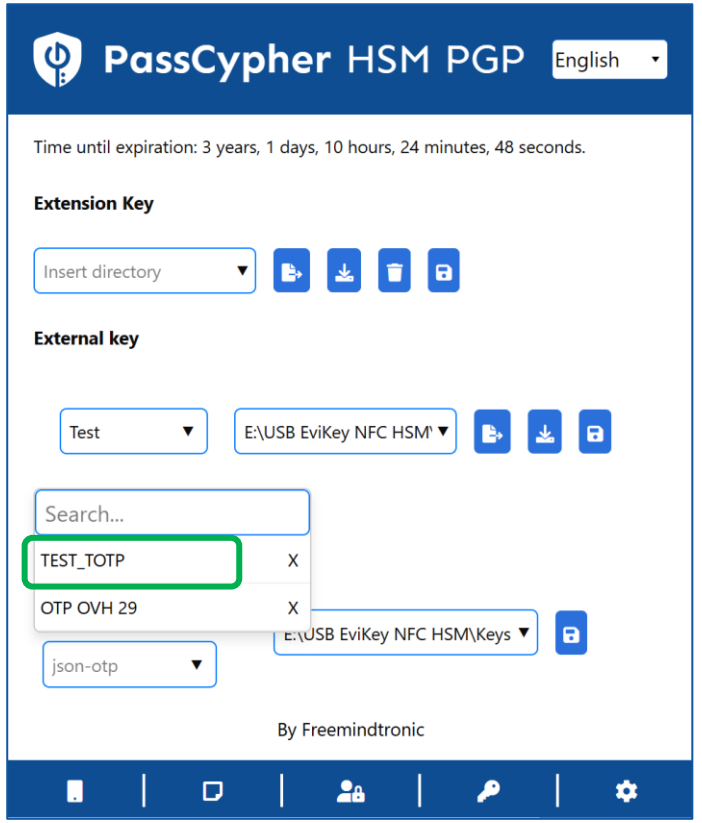
Position the QR code to be scanned in the camera field

MANAGE YOUR TOTP/HOTP (2FA) 2/2

The OTP type is detected. Give a name to this OTP code, enter the associated URL and click on the icon to generate a .json file

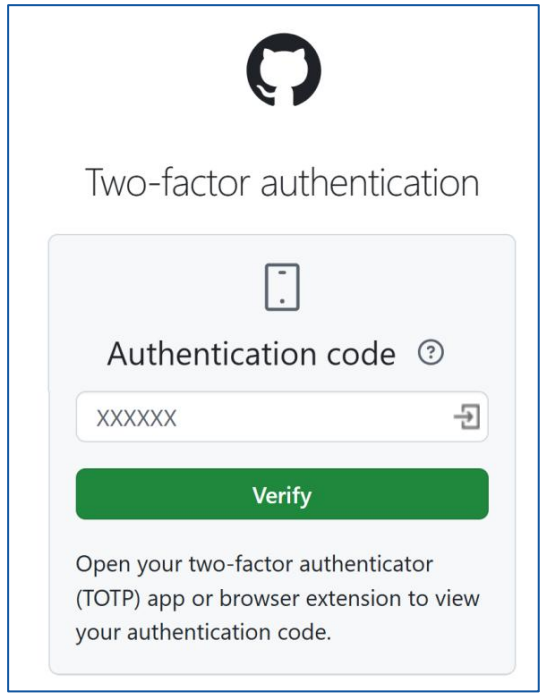
Retrieve the file from your **Downloads** and place it in the **appropriate folder (see slide 15).**

In this example, the file is saved in a USB stick

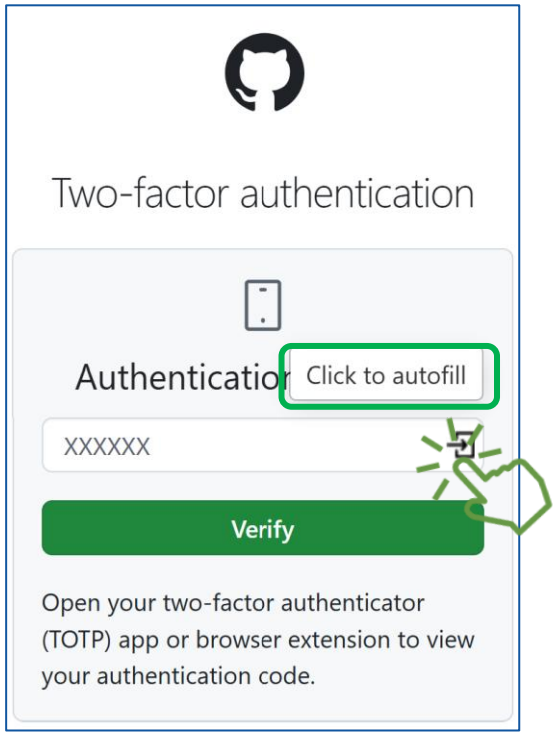


The created "**.json**" file is automatically added in the extension to the list of all created OTPs.

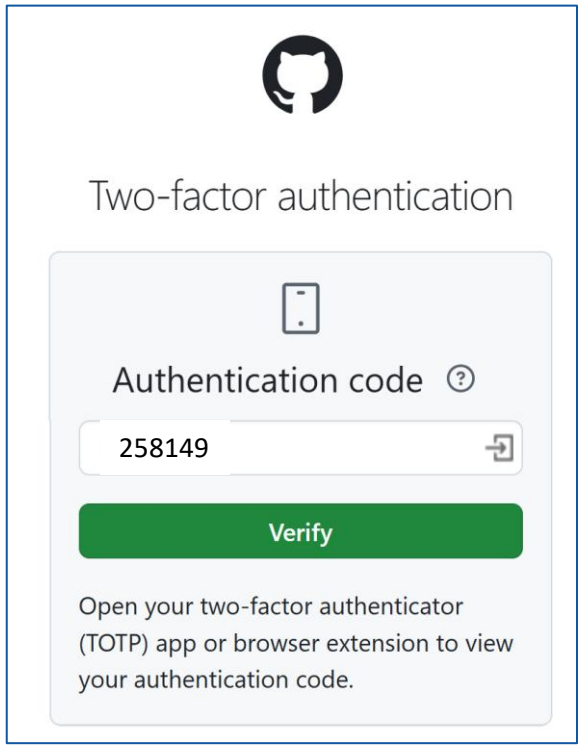
AUTHENTICATE WITH OTP



If you have enabled two-factor authentication on a website, this is the type of page that you will see

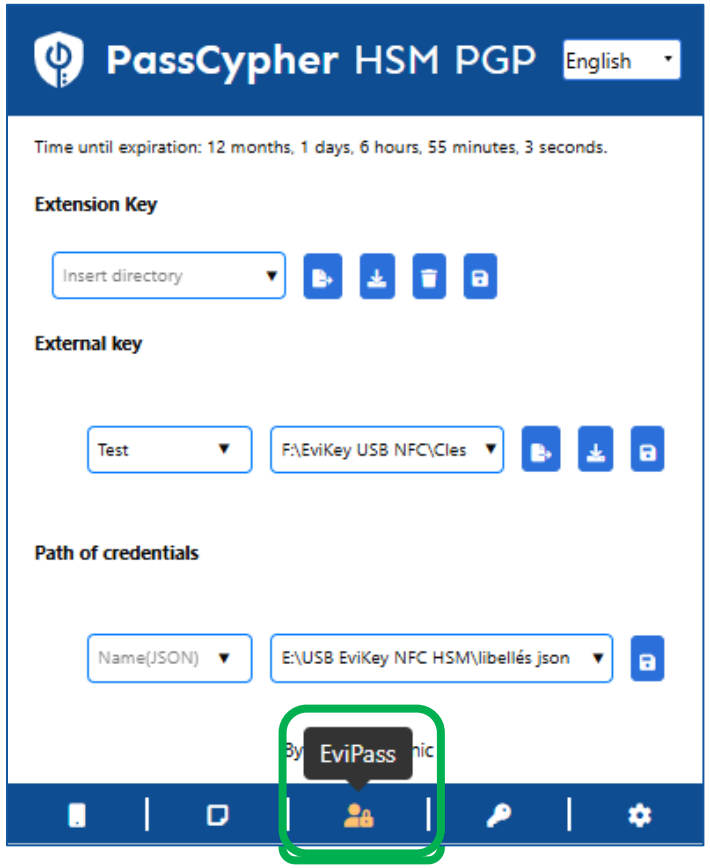


Click on the indicated icon, the code will automatically be inserted into the field…

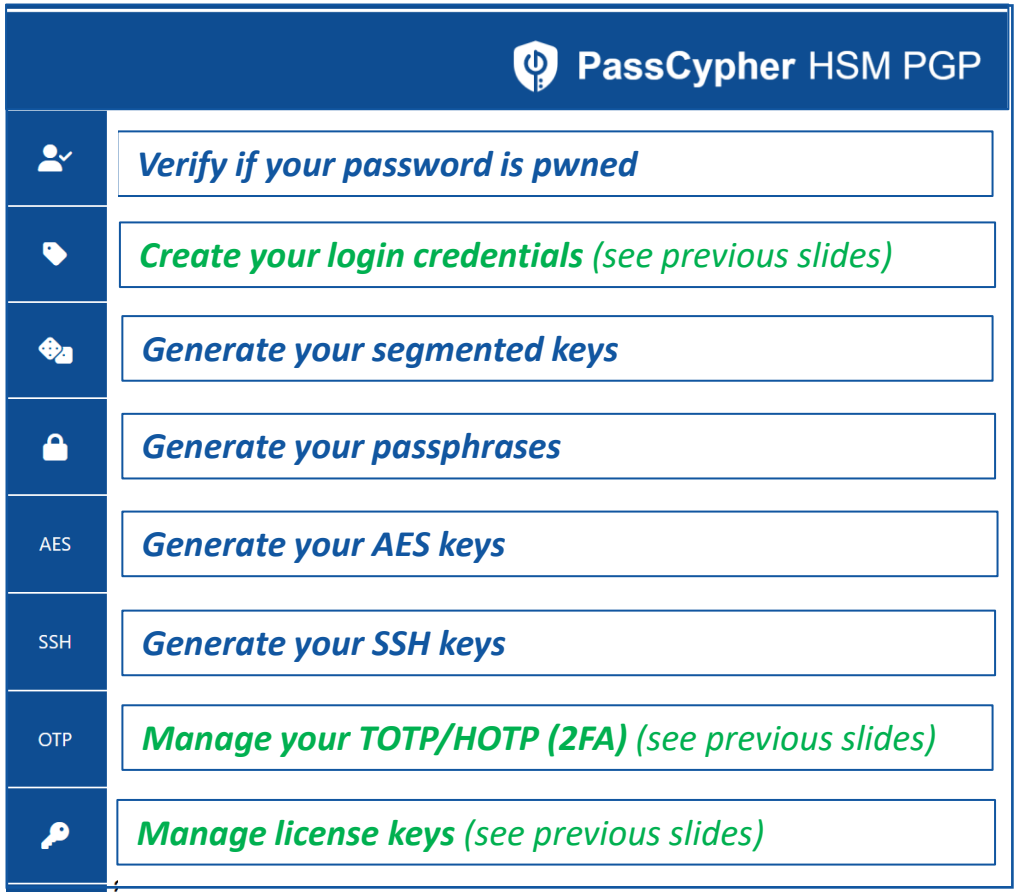


… and the connection is made

EVIPASS FUNCTIONNALITIES

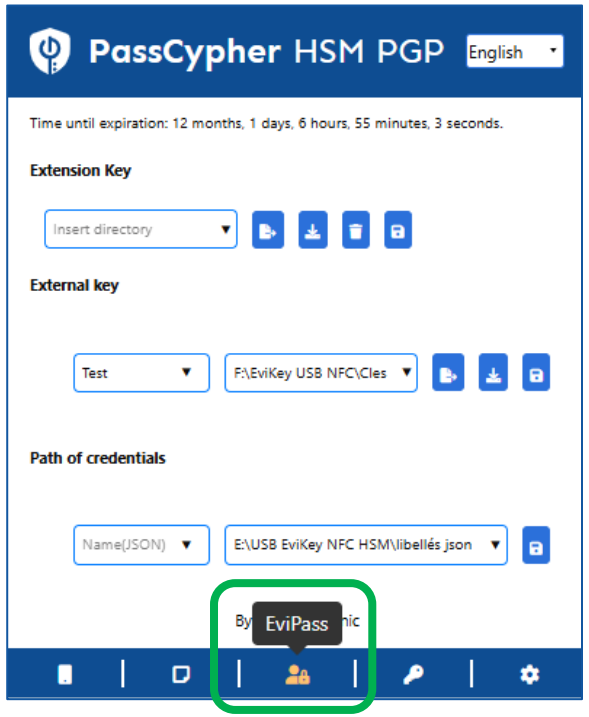


Click the indicated icon to access all the functionnalities available

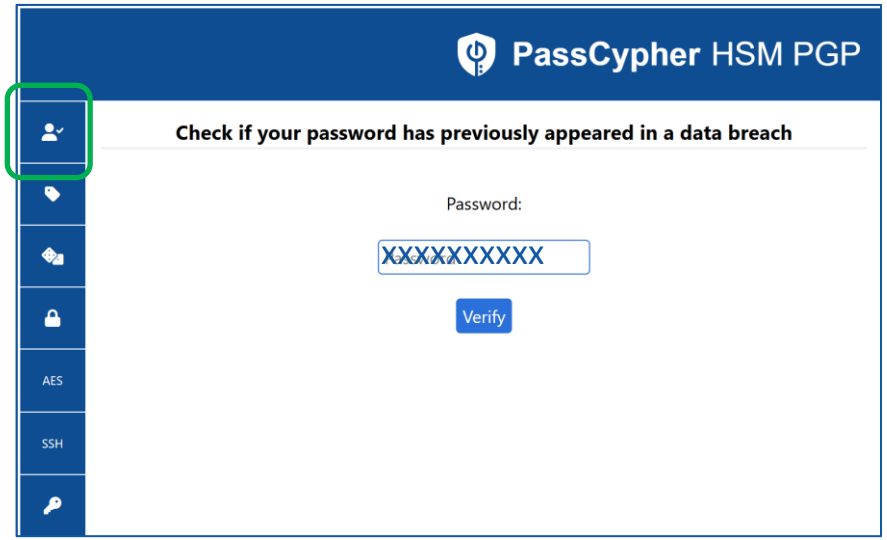


The functionalities written in blue are explained in the following slides

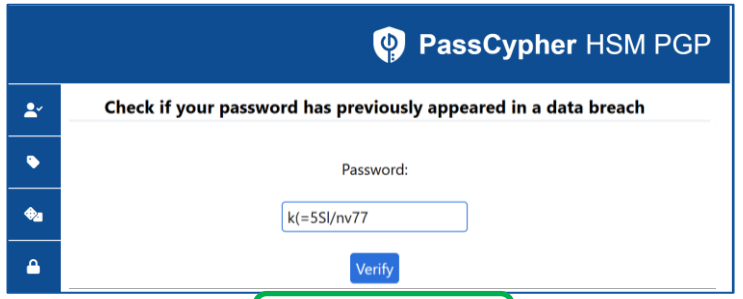
EVIPASS (PASSWORD CHECK)



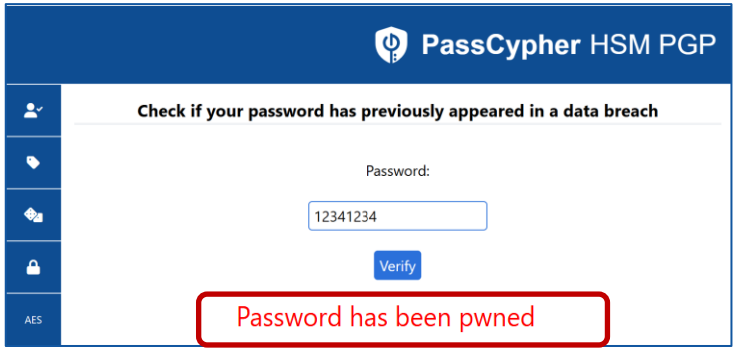
Click the indicated icon to access password verification.



Click the indicated icon to check if your **password is compromised.** Enter your password in the indicated field and click "**Check**." The result will display.



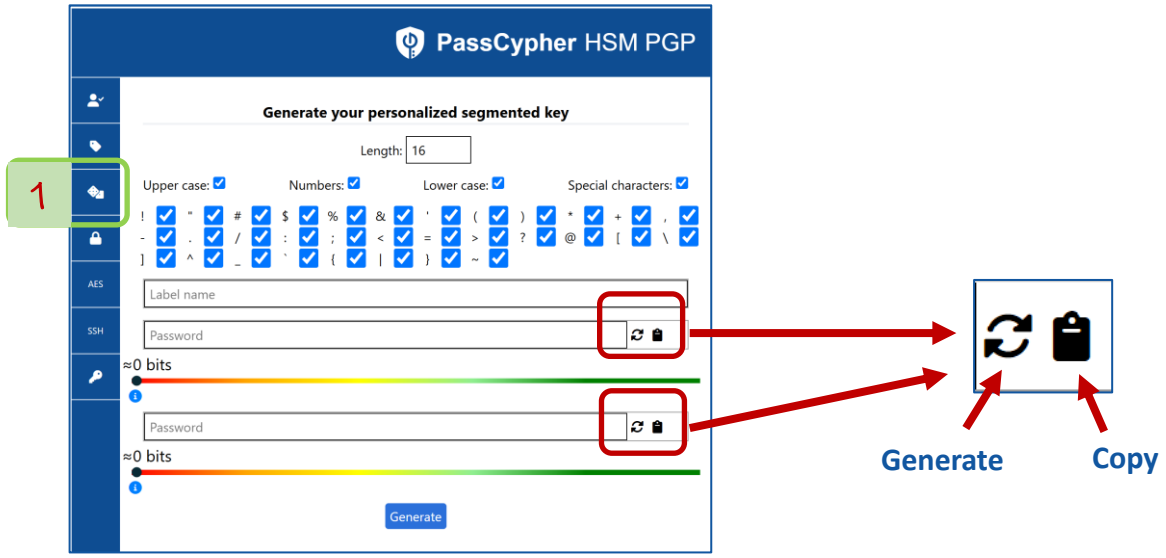
Password no pwned

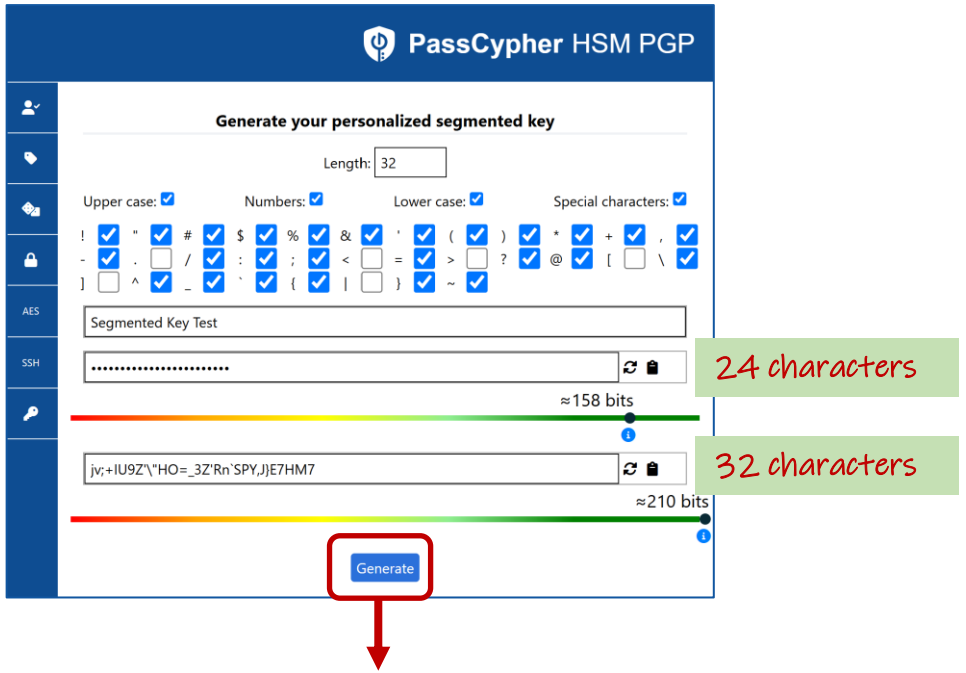


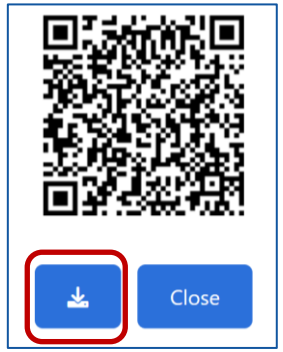
Password has been pwned

EVIPASS (SEGMENTED KEY)

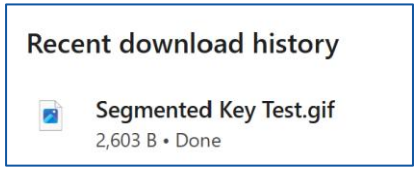
Functionality reserved for sovereign entities and IoT security







Click to download



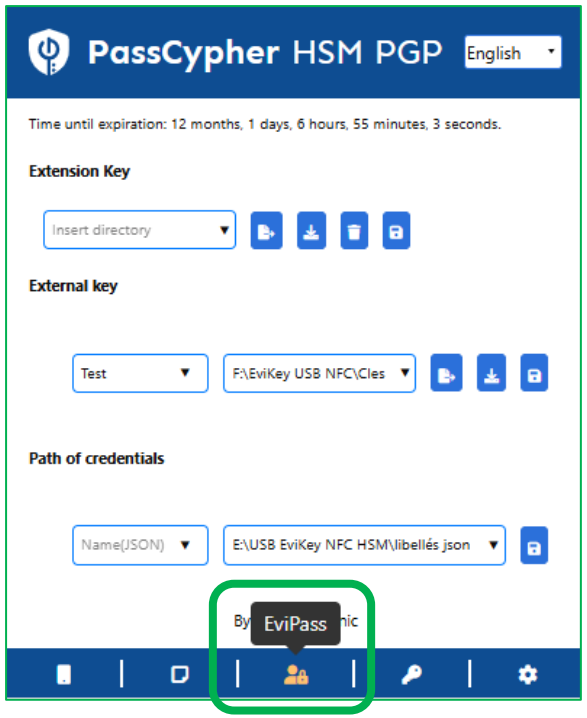
The .gif file is generated.

1. Click the indicated icon. A window will appear.
2. Name the segmented key and select the length of the segment (number of characters).
3. This length can be different for the two segments.
4. Choose the characters (uncheck some characters if necessary). Then click the icon to generate the segment.

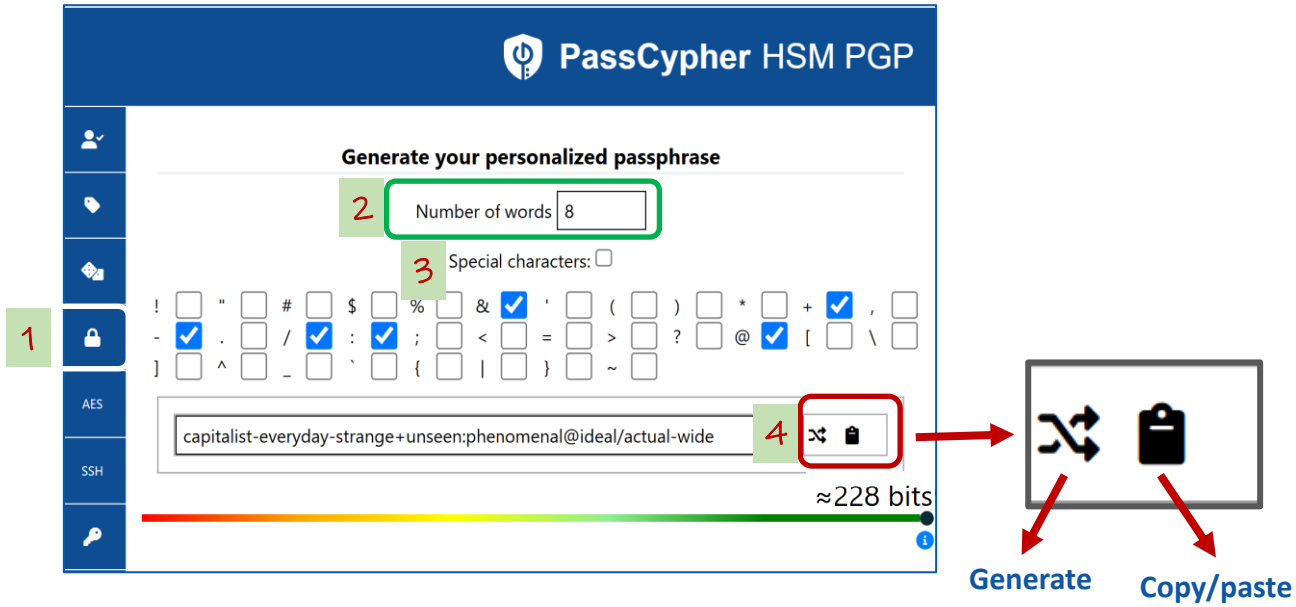
You can copy this segment to the clipboard.

Click the icon to generate the segmented key randomly.

EVIPASS (PASSPHRASE)

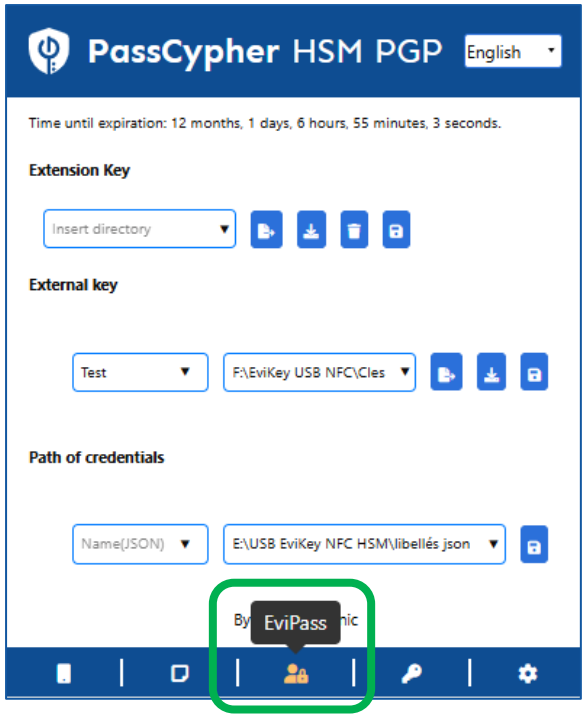


Click the indicated icon to access the passphrase creation features.

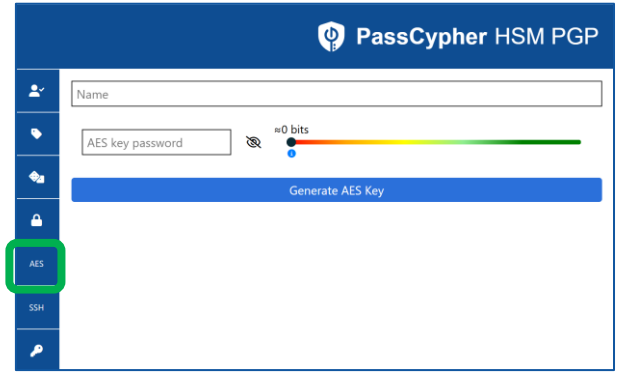


1. Click the indicated icon to generate a passphrase.
2. Choose the number of words for the passphrase.
3. Choose the characters that will separate the words.
4. Click the icon to generate the passphrase. You can copy/paste this passphrase.

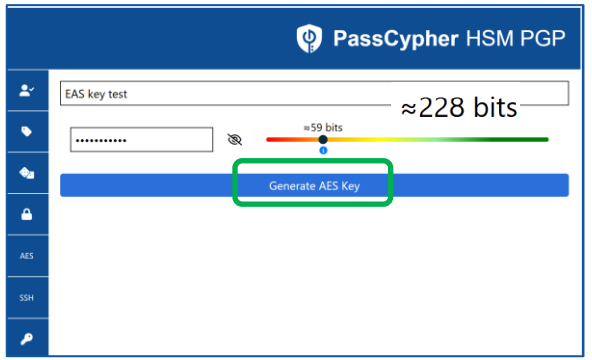
EVIPASS (AES KEY)



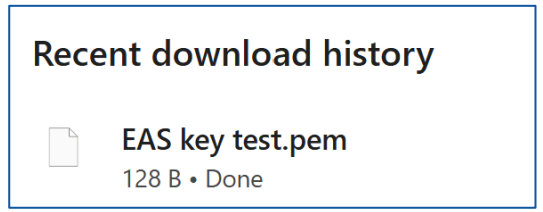
Click the indicated icon



Click the indicated icon to access the AES key generation.

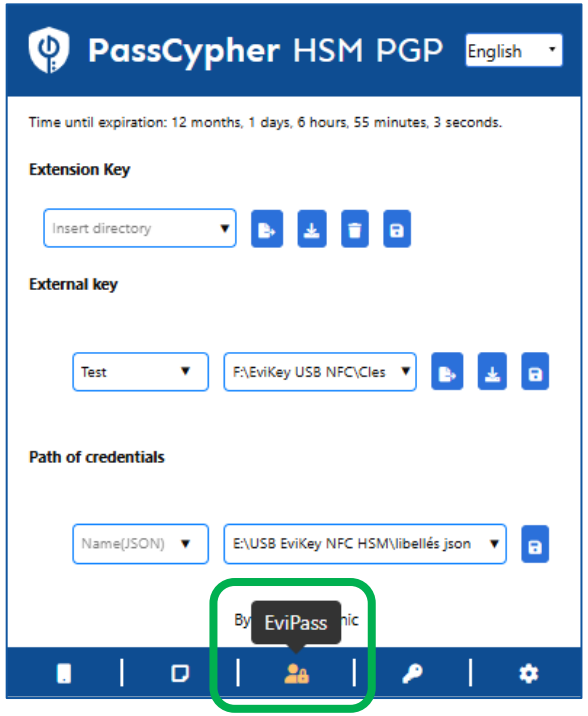


Enter a name for the key, enter a password, and then click the icon "**Generate AES key**".

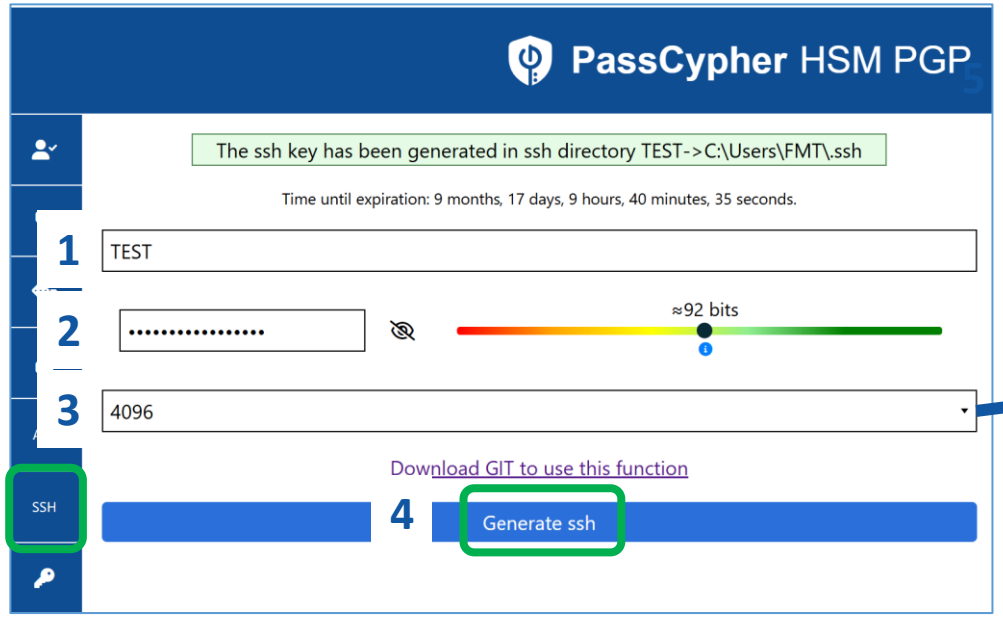


The .pem file is generated. You can store it where you want

EVIPASS (SSH KEY)



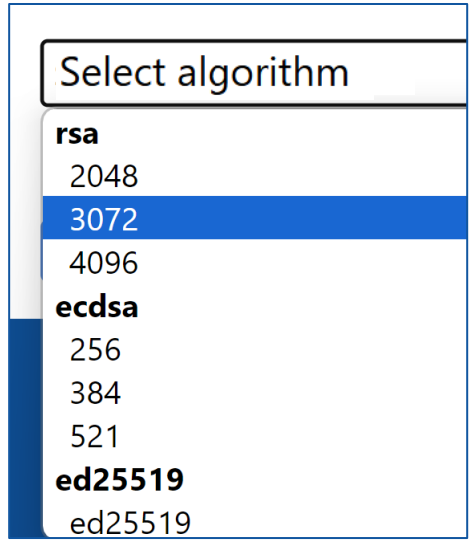
Click the indicated icon to access SSH key creation features.



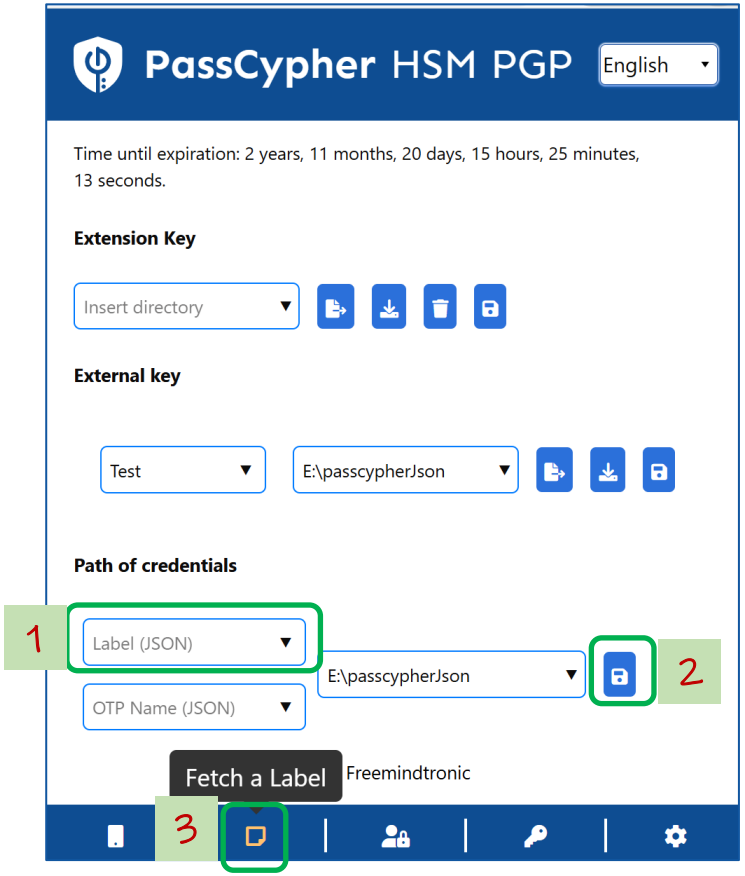
Click the « **SSH** » icon and complete the necessary fields:

1. Key **Name**
2. The **Password** associated with the key
3. Select the **algorithm**
4. Finally, click "**Generate SSH**".
5. The location where the key is **stored** appears at the top of the window

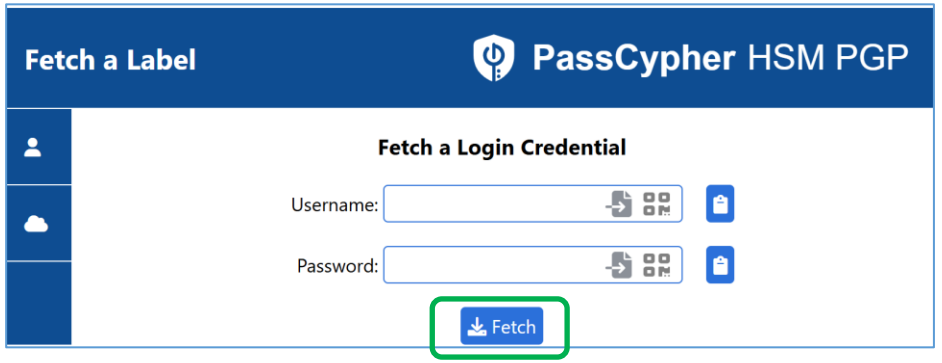
3. Algorithms available



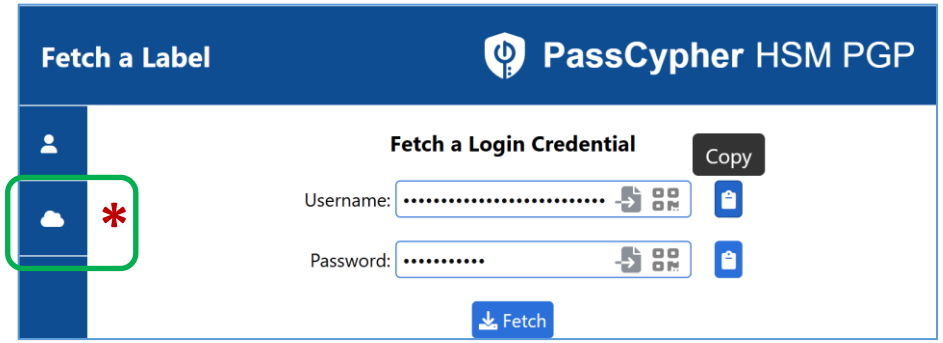
FETCH A LABEL



On the extension's homepage, enter the **name of the label** you want to retrieve and click "**Save**." Then, click the indicated icon to access the label retrieval.



A window opens, click "**Retrieve**."



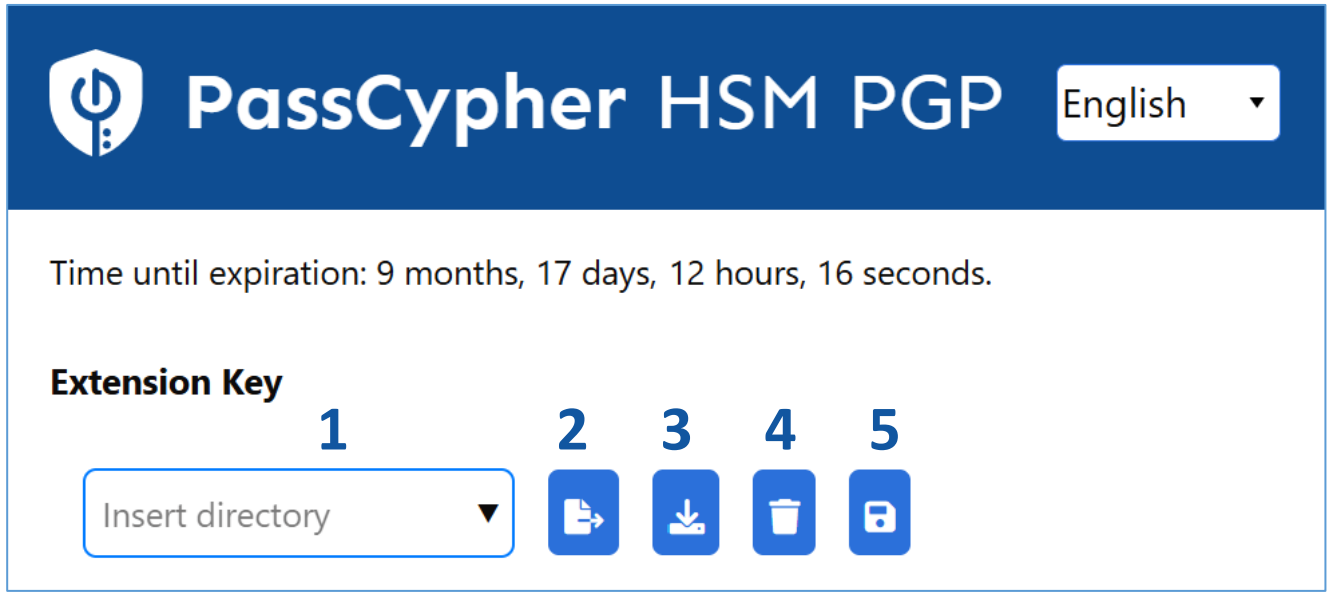
The information is displayed on the screen: **user name and password**. Click to copy useful information

(*) Recovering a Cloud key can only be done from an NFC device

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 specified path.

3. You can import the key (file.eppc) and save it to your desired location as a security backup.

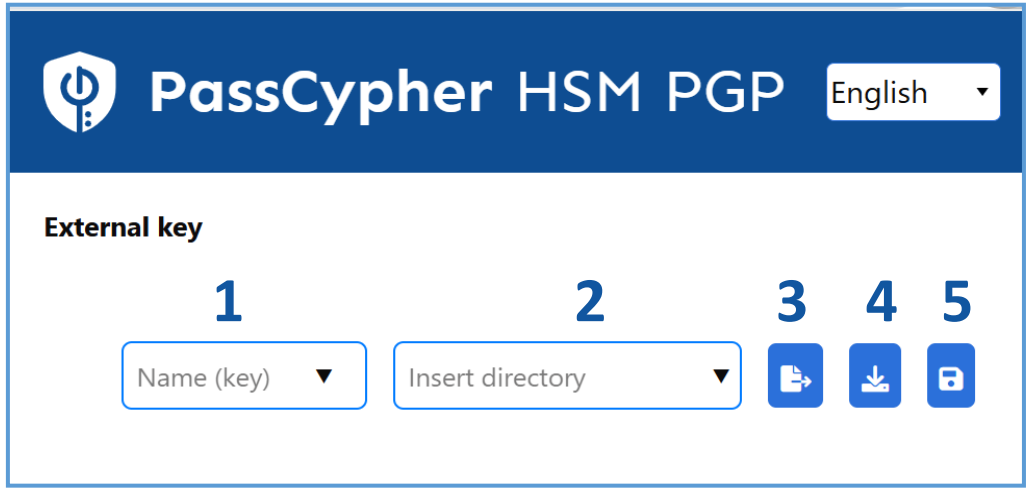
4. By clicking on this icon, you will delete the key from local storage.

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

THE EXTERNAL KEY IN DETAIL

You can create multiple external keys linked to the same extension key.

This allows multiple people to use PassCypher on the same computer, each using their own key.



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

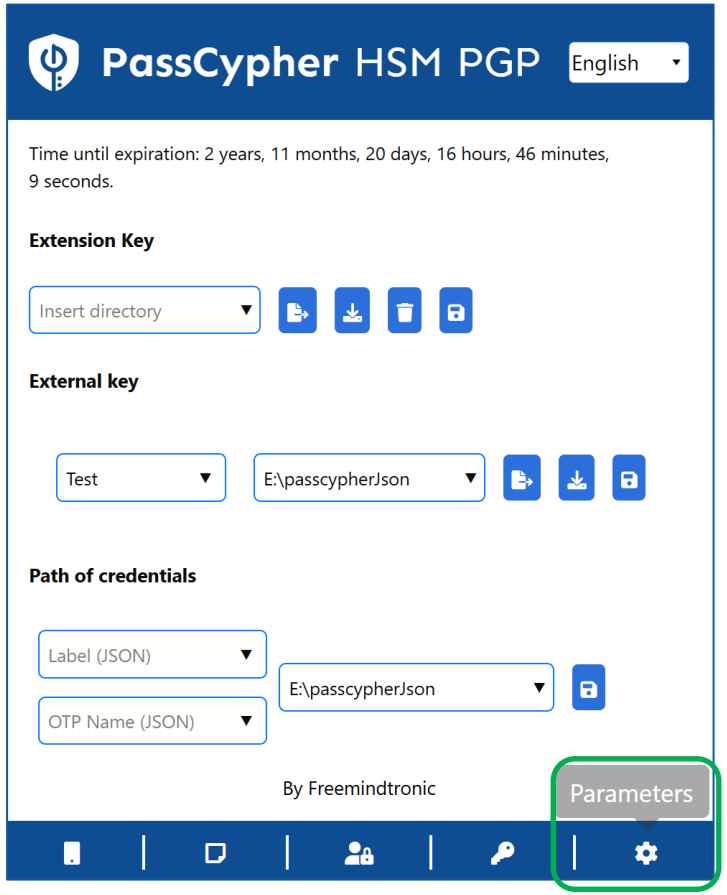
2. Insert the path where the external key will be stored. You can define multiple paths.

3. Click to create and export the key.

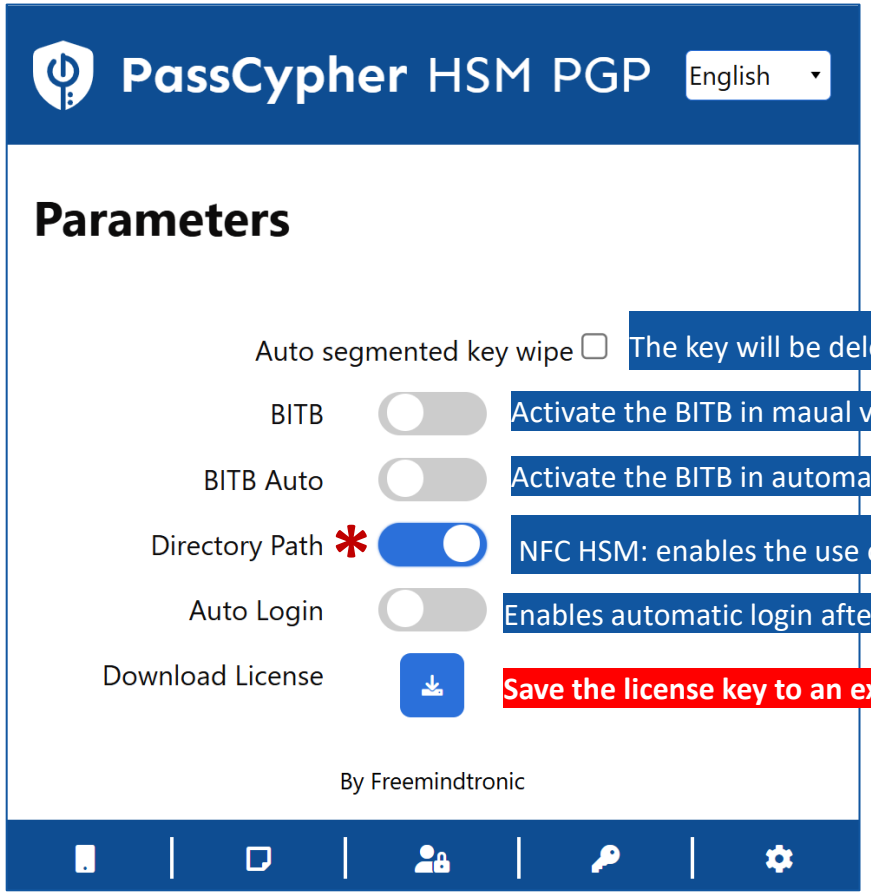
4. By clicking on this icon, you can download the key and save it to your desired location.

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

PARAMETERS & FEATURES



Click on « **Parameters** » icon



A window opens with different options that you can enable

BITB more information available ici

(*) 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 Freemindtronic NFC device https://freemindtronic.com/how-it-works-products-in-depth-guide-to-fullsecure/

Take back control, Take back power

EviPass Technology

By Freemindtronic Andorra

To known more: https://www.freemindtronic.com

Freemindtronic Channel Freemindtronic