TRUSTED PLATFORM

Most modern PCs are equipped with a TPM module (chip) which allows you to safely store biometric information (fingerprint or facial recognition) or a secret code, offering you safe and easy access to various locked functions, such as JSIS. See below on how to enable and use a TPM on a computer or iPad.

1 – SETTINGS - WINDOWS

Click on the Windows symbol at the bottom of your screen, open the **Windows Settings** and select **Accounts.**

Under **Sign in options**, among the three Windows Hello options, select the one which corresponds to the method you normally use to access your device: Windows Hello Face or Fingerprint or Windows Hello PIN. If you select PIN, you will be asked to configure your Windows Hello code which must be the same as the access code you use for your device. You may need to select "Change your PIN" and enter the same code again. Finally, you may be asked to enter your Microsoft password.

The Trusted Platform will only work on the Windows device on which it was enabled. If, however, you have a Google account and choose to enable synchronisation, your TPM will work on all the devices on which you are logged in with Google.

1 – APPLE (the exact terminology may vary according to the specific model)

If you accept synchronisation of your Apple devices, you only need to enable Trusted Platform on one of them, and it will work on all your Apple devices – **select the most recent device**.

iPad: Go to **System Settings** **> Passwords**. If "Passwords" are locked, just enter your code and click "Return". To the right, under **Password Options**, make sure that **AutoFill Passwords and Passkeys** and **iCloud Keychain** (and any preferred browser you may have) are all enabled.

MAC: Open **System Settings**. Under **General**, click on **Autofill & Passwords**, make sure that "**AutoFill Passwords and Passkeys"** and **"Passwords"** (or **iCloud Keychain** or **Access codes**) are all turned **on**. Similarly, under "**Touch ID & Passwords**", make sure to turn on **unlocking your Mac** and **autofilling passwords** (by biometry or by entering a code).

2 – ENABLING FOR EU LOGIN (WINDOWS AND APPLE)

Launch **MyRemote** via https://myremote.ec.europa.eu/ , log in and click on **EU Login**.

Select **Manage my Security Keys and Trusted Platforms** → **Add a Trusted Platform.** Give your device a name (my laptop, iPad ..) and click on **Submit**.

Authenticate using the method you normally use to unlock your device (by biometry face/fingerprint or by entering your access code).

If you handle several EU Login accounts, you must activate each account separately on the Trusted Platform.

3 – USE WITH EU LOGIN

Launch for example https://mypmo.europa.eu/. Enter your email and password if prompted and select **Security key or Trusted Platform** as your verification method. Authenticate (biometrically or with your access code) and you're in.

4 – EU LOGIN PASSWORD

By enabling a Trusted Platform passkey, you authorise Windows/Apple to administer your access codes and passwords. Whenever your EU Login password needs updating (every 6 months), you will need to make sure that it is updated at the same time in your passwords folder/keychain under **Settings** in your device.