ACTIVATION OF A SECURITY KEY

A Security Key is a small external device which can be plugged in via USB (or can connect via Bluetooth or NFC) to your device, typically a , computer (PC, laptop). In order for it to work with EU Login, your device must be FIDO2 compliant, such as a Yubikey. Once your key has been activated as described below, you can plug it into any device (such as a hotel computer or your mobile phone) to allow you to authenticate safely even when travelling.

1. Access to your computer must be secured by some sort of access code, typically either biometrically (finger print/face), or via a PIN code. If you have not yet set up an access code, please follow the guidelines given in the guide on setting up a Trusted Platform (point 1).

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

3. Select *Manage my Security Keys and Trusted Platforms - Add a Security Key*.

Manage my Security Keys and Trusted Platforms

Add a Security Key

4. Give your device a name (e.g. "My Yubikey"..) 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).

5. You will be asked to accept certain precautions and indicate an access code which you must enter when you wish to use the key for logging in via EU Login. Follow instructions on the screen.

USE YOUR SECURITY KEY 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), tap your security key when prompted and you're in.

Security Key or Trusted Platform
Use a security key or trusted platform to authenticate with EU Login.

EU Login Mobile App PIN Code
Use your registered EU Login Mobile app to verify your identity.

EU Login Mobile App QR Code
Generate a one-time-password with the EU Login Mobile app.