EUROPEAN COMMISSION
DIRECTORATE-GENERAL EMPLOYMENT, SOCIAL AFFAIRS AND INCLUSION
DIRECTORATE-GENERAL REGIONAL AND URBAN POLICY

Directorate DAC. Joint Audit Directorate for Cohesion
DAC1 Audit 1

ARACHNE
EU login and two-factor authentication (2FA)

Table of Contents

1 Introduction 2

2 How to sign in to "EU Login" using 2FA 2
- 2.1 EU Login Mobile App – PIN code 3
- 2.2 EU Login Mobile App – QR code 4
- 2.3 EU Login Mobile phone + SMS 5
- 2.4 Trusted Platform 6

3 Annexes 7
- 3.1 ANNEX A : Install and initialize the EU Login mobile app 7
- 3.2 ANNEX B : Install and initialize the EU Login mobile app 9
- 3.3 ANNEX C : Activate Windows Hello 11

1 Introduction

All web-applications of the European Commission dealing with (1) Sensitive Non-Classified data according to System Security Plan or (2) Sensitive Non-Classified personal data according to the GDPR definition MUST implement two-factor Authentication.

Enabling two-factor authentication (2FA) is one of the most effective measures to combat credential theft. It requires a second piece of information beyond username and password. This can be a knowledge factor (something the user knows e.g. a PIN), a possession factor (something the user has e.g. a security token, a mobile device or smartphone app) or a biometric factor (e.g. fingerprints, facial and voice recognition).

By providing a second layer of authentication, 2FA increases the security of data to a much greater extent. If, for instance, a password is compromised, it offers another layer of protection to block unauthorized access.

ARACHNE users will have to use their EU Login plus a second means of identifying themselves when accessing the application.

2 How to sign in to "EU Login" using 2FA

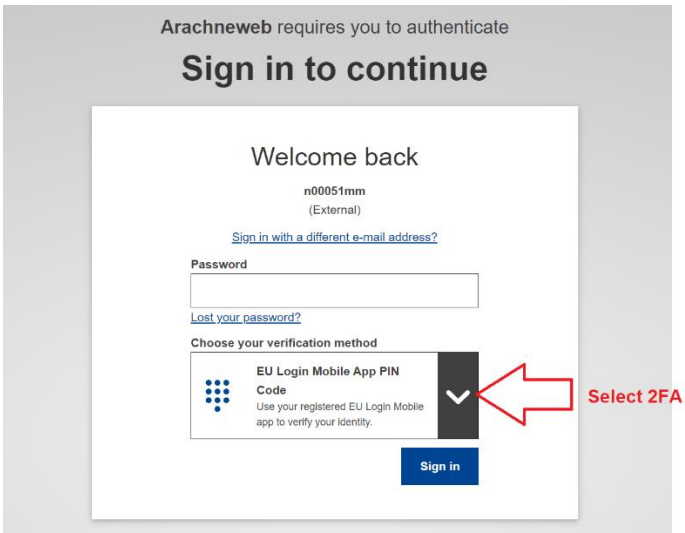
In this section we will list briefly the different types of 2FA methods used by EU login when connecting to ARACHNE.

A more detailed explanation can be found in the EU Login User Guide via the following link: https://webgate.ec.europa.eu/cas/manuals/EU_Login_Tutorial.pdf.

ARACHNE supports four verification methods of 2FA available to non-Commission staff to sign in to "EU Login":

1. EU Login Mobile App PIN Code
2. EU Login Mobile App QR Code
3. Mobile Phone + SMS
4. Trusted Platform

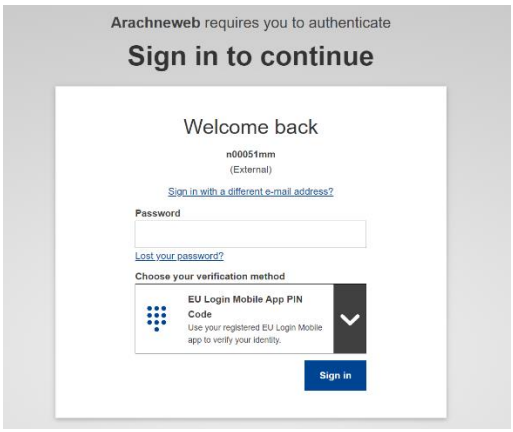
- Introduce your email address and your password,
- Select your 2FA verification method and click sign in.



The following sections explain which preliminary actions need to be taken by the user before 2FA can be used with EU login.

2.1 EU Login Mobile App – PIN code

User installs an App on his/her smartphone and the authentication will be done through the App via a pin code:



Prerequisite: User has already added his/her mobile under "My Account". If not yet done, the steps are described in detail in 3.1 ANNEX A : Install and initialize the EU Login mobile app.

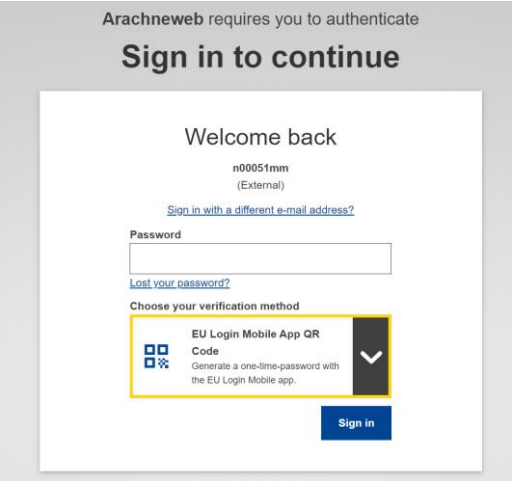
Steps to perform:

1. Enter your password in the "Password" field, select "EU Login Mobile App PIN Code" as the verification method and click on "Sign in".
2. If you have registered more than one device with an initialized EU Login Mobile App, you will be asked to select the one you would like to use (Click on the device using the name you provided).
3. EU Login sends a notification to your mobile device.
4. Tapping on the notification triggers the launch of the EU Login Mobile App.
5. The EU Login App prompts you to enter your PIN code. Enter your PIN code or use biometric recognition and tap on "Authenticate".

   This automatically completes the process on your PC that proceeds to the service you requested to use.

2.2 EU Login Mobile App – QR code

User installs an App on his/her smartphone and the authentication will be done through the App via a QR code:



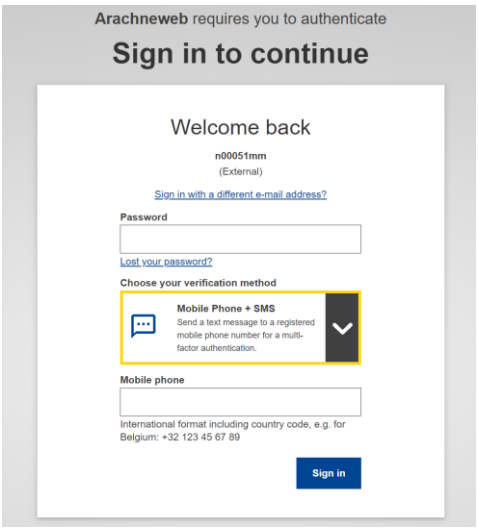
Prerequisite: User has already added his/her mobile under "My Account". If not yet done, the steps are described in detail in 3.1 ANNEX A : Install and initialize the EU Login mobile app.

Steps to perform:

1. Enter your password in the "Password" field, select "EU Login Mobile App QR Code" as the verification method and click on "Sign in".
2. A QR code is displayed on the screen.
3. Start the EU Login Mobile App on a mobile device where it has been previously initialised. Tap on "Scan QR Code".
4. The QR code scanner starts on your mobile device. Point the camera of your mobile phone to your PC screen until the QR code is recognised.
5. The EU Login Mobile App displays a one-time password composed of digits and characters.
6. Type the one-time password in the "code generated by your app" field and click "Sign in" to proceed to the service you requested to use.

2.3 EU Login Mobile phone + SMS

Authentication is done via an SMS that will be sent to your mobile phone.



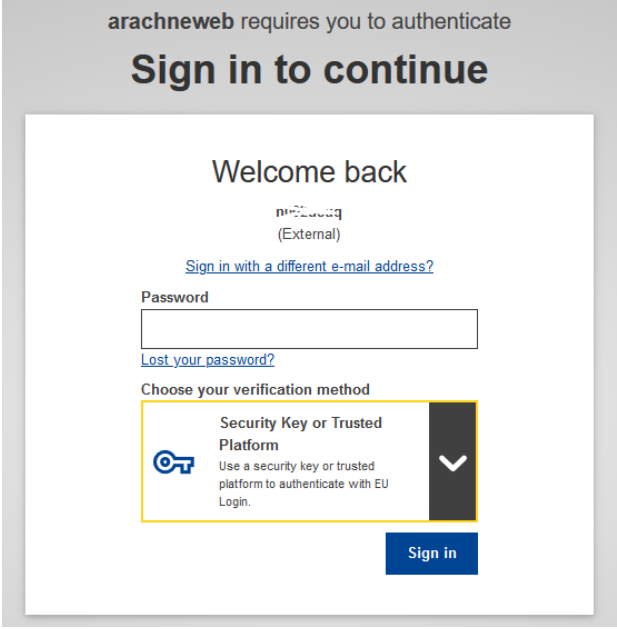
Prerequisite: Valid phone number should be registered via EU Login -> My Account details. If not yet done, the steps are described in detail in 3.2 ANNEX B : Install and initialize the EU Login mobile app.

Steps to perform:

1. Enter your password in the "Password" field and enter a previously registered mobile phone number in the "Mobile phone" field, starting with a plus sign and with the country code. Do not include dots, parenthesis or hyphens.
2. Enter your mobile phone number.
3. When clicking "Sign in", an SMS is sent to your mobile device. The SMS contains a challenge code made of nine characters (three blocks of three characters) separated with hyphens (minus sign).
4. Type the challenge you received in the "SMS text challenge" fields and click on "Sign in" to proceed to the service you requested to use.

2.4 Trusted Platform

User uses Windows Sign-in option, no need to use a mobile phone to authenticate using 2FA:



Prerequisite: User needs to set up one of the 'Windows Hello' options. If not yet done, the steps are described in detail in 3.3 ANNEX C : Activate Windows Hello.

Steps to perform:

1. Enter your password in the "Password" field, select "Security Key or Trusted Platform" as the verification method and click on "Sign in".
2. The system will detect which method you have activated using Windows Hello. Depending on the activated method you can key in your PIN code, scan your fingerprint or use your camera to authenticate.
3. You can now proceed to the service you requested to use.

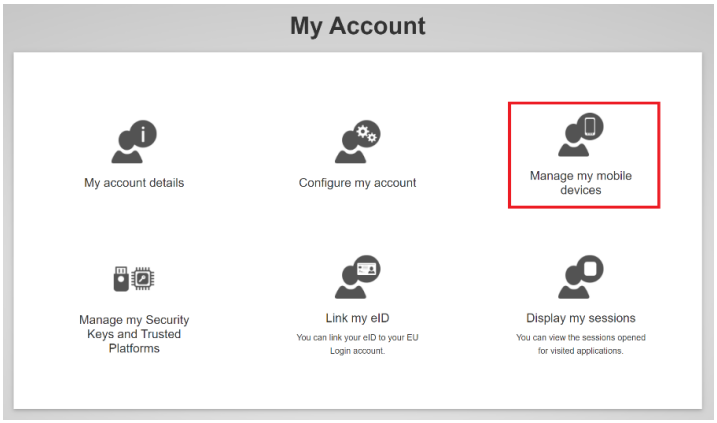
3 Annexes

3.1 ANNEX A : Install and initialize the EU Login mobile app

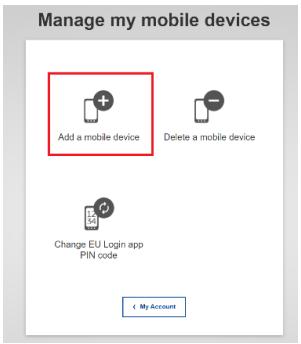
1. Go to the page https://webgate.ec.europa.eu/cas/login and connect with your EU Login.

2. Once successfully authenticated, move the mouse over the gear at the top right corner to display the menu and select "My Account".

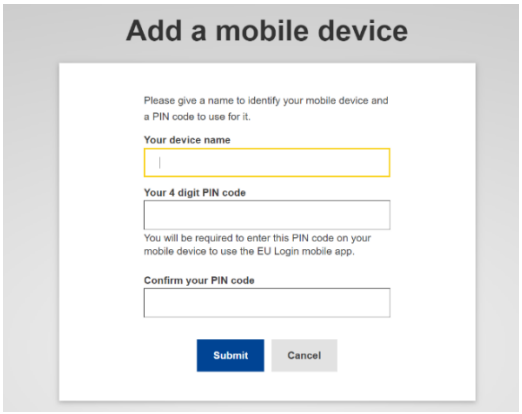
3. Select “Manage my mobile devices” in the menu.



4. Click on “Add a mobile device”.



5. Give the device a name and enter a 4 digit pin for linking the device to your EU Login account, confirm the pin code and click submit.



6. Scan the QR code with the EU Login mobile app that you want to install on your smartphone or tablet (Android or IOS).

7. In the EU Login mobile app:
   - Click 'Initialise'
   - Scan the QR code
   - Enter the same pin code that you entered in step 4
   - A notification pops up for a 'pending approval for device registration'. Tap it
   - You can choose to enable biometric authentication
   - Your device is registered and linked to your EU Login account.

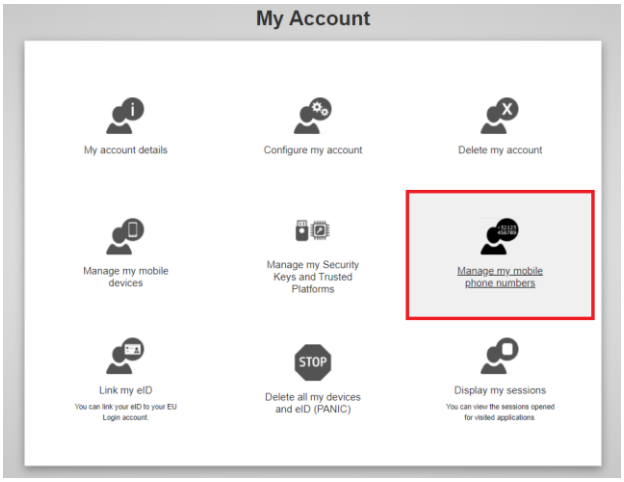
8. When the device is registered, you can go back to the application and authenticate using two-factor authentication.

3.2 ANNEX B : Install and initialize the EU Login mobile app

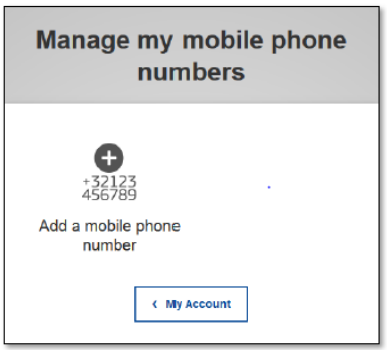
1. Go to the page https://webgate.ec.europa.eu/cas/login and connect with your EU Login.

2. Once successfully authenticated, move the mouse over the gear at the top right corner to display the menu and select "My Account".

3. Click on "Manage my mobile phone numbers".



4. Click on "**Add a mobile phone number**".



5. Enter your mobile phone number in the "Mobile phone number" field, starting with a plus sign and with the country code. Do not include dots, parenthesis or hyphens.

   When clicking "Add", an SMS is sent to your mobile device.
   The SMS contains a challenge code made of eight characters separated with a hyphen (minus sign).

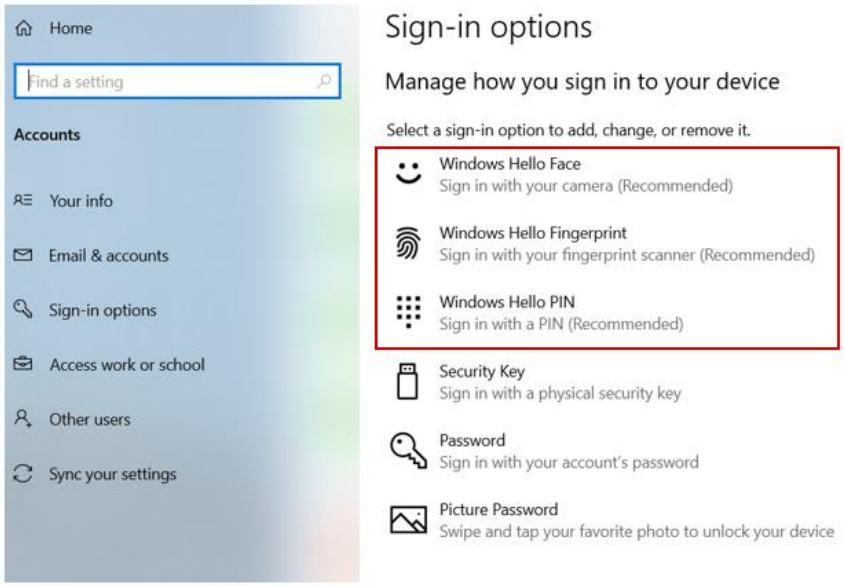
6. Type the challenge code you received in the "Text message challenge code" fields and click on "Finalise".

3.3 ANNEX C : Activate Windows Hello

In order to activate the Windows Hello option you need:

- to have local administrator rights on your laptop/pc
- to request your IT department to activate these options on you laptop/pc

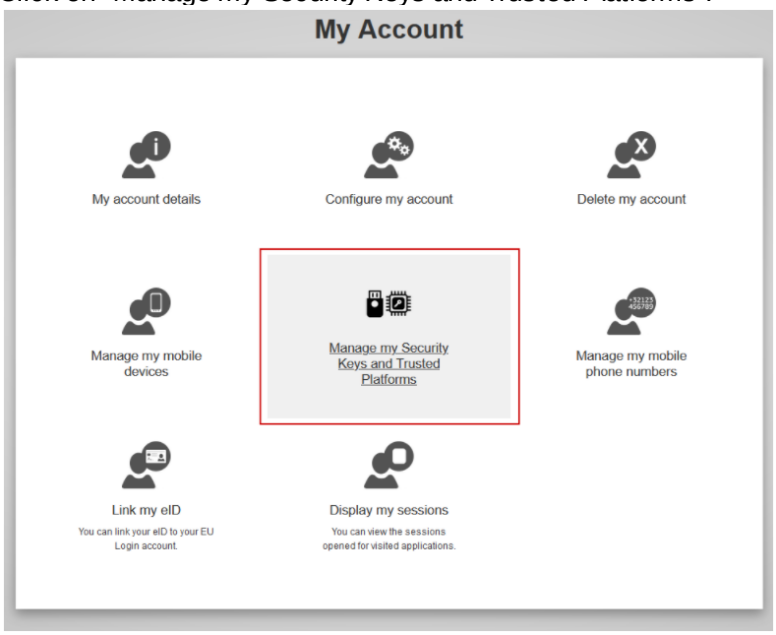
1. Set up one of the 'Windows Hello' options, by going to your Windows settings -> Sign-in Options and set up one of the below methods:



2. Go to the page https://webgate.ec.europa.eu/cas/login and connect with your EU Login.

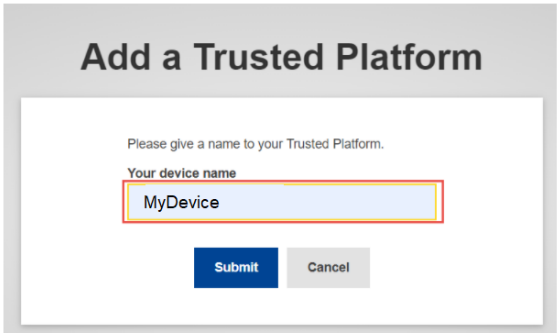
3. Once successfully authenticated, move the mouse over the gear at the top right corner to display the menu and select "My Account".

4. Click on "Manage my Security Keys and Trusted Platforms".

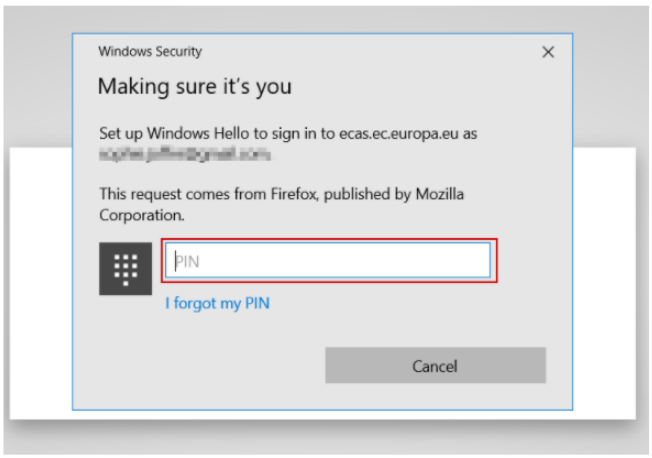


5. Select the option to 'Add a Trusted Platform'.

6. Give your device a name.



7. The system will detect which method you have activated using Windows Hello.



8. You have now finalized the set up to use Trusted Platform as your two-factor authentication method.