

## Digital Certificate

Upon your first login as a healthcare professional to the National Contact Point (NCP) platform, it is necessary to issue and install a digital certificate, which can only be stored on the specific computer where the login is performed. The certificate is valid for two (2) years and is essential for secure access to medical data of citizens from other participating European countries.

Its installation is a prerequisite for the secure Cross-Border exchange of health information, as part of the operation of the NCP through the National Contact Point for eHealth (NCPeH) of Cyprus (CY).

Depending on the operating system, you must follow the corresponding recommended procedure.

### Digital Certificate Installation Process on MacOS

1. Locate and open the application "Keychain Access" either by using Spotlight Search or by navigating to Applications > Utilities in Finder.

**Note:** In newer versions of macOS, such as macOS Sequoia, when you try to open the Keychain Access application, the system may first launch the Passwords app and display a message with options. In this case, select "Open Keychain Access" to proceed to the correct application.

In this case, we select 'Open Keychain Access' to proceed to the correct application.

2. In the pop-up window that will appear with title "Manage your passwords" in "System Settings", click on the "Open Keychain Access" button.
3. While you are in the application "Keychain Access", navigate to the menu bar and click on File > Import Items.
4. Click the "Show Options" button.
5. Under "Destination Keychain" drop down, select "System".
6. Locate and select the .pfx file that you just downloaded from the NCP platform.

**Note:** Most likely to be found in "Downloads".

7. Click "Open".
8. Enter your user account password and click "Modify Keychain".  
  
**Note: This won't be needed, in case you entered your credentials while the application was launched.**
9. Enter the password you received on your mobile phone when you requested a new certificate.
10. Click "Ok" button.
11. Enter your user account password and click "Modify Keychain".
12. Locate and select the certificate in the "System list".
13. Navigate to File > Get Info. To navigate to "Get Info" you can either use the menu bar or right click on the file .pfx.
14. Expand the "Trust" section.
15. Under the field "When using this certificate" drop down select "Always Trust".
16. Close the window and re-enter your user account password to save changes.
17. Click "Update Settings" for changes to be applied.
18. Navigate to File > Close to close the "Keychain Access" window.

### Installation on Windows

1. Find your new certificate file and double click on it.
2. Select Current User and click "Next"
3. Browse to certificate file.
4. Αλλάξτε τον τύπο αρχείου από \*X.509 Certificate (\*.cer, \*.crt) σε Personal Information Exchange (\*.pfx, \*. p12).

5. Select the certificate file and click "Open".
6. Click «Next».
7. Enter the password you received on your mobile phone when you requested a new certificate.
8. Deselect Enable strong private key protection.
9. Click «Next».
10. Select Automatically select the certificate store on the type of certificate and click "Next".
11. Click «Finish».
12. Click "OK" to close the import was successful message.