

iOS Client Certificates

Overview

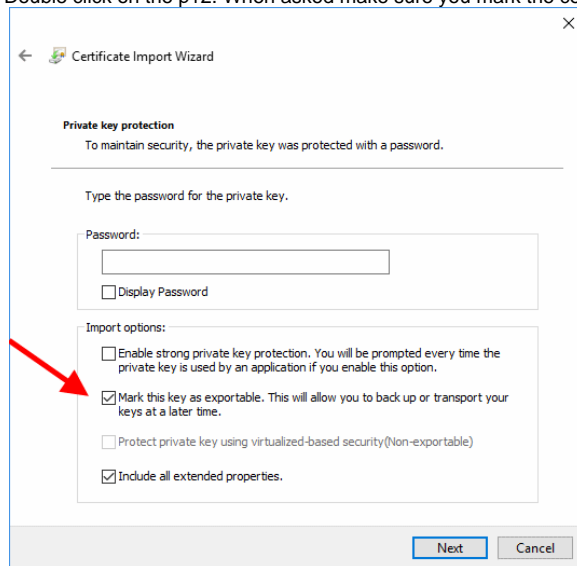
This article is to inform users how to prepare p12 certificates for use with iOS.

- 1 [Overview](#)
- 2 [Steps\(Windows\)](#)

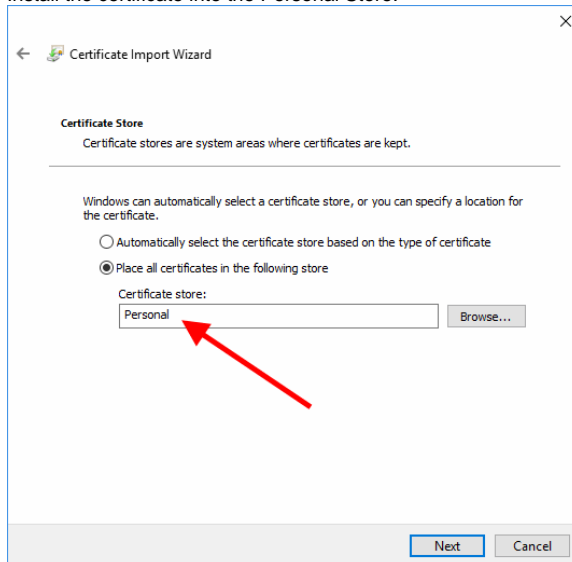
Steps(Windows)

This should not be required for newer versions of iOS. Medical Objects p12 should work without needing conversion via Windows.

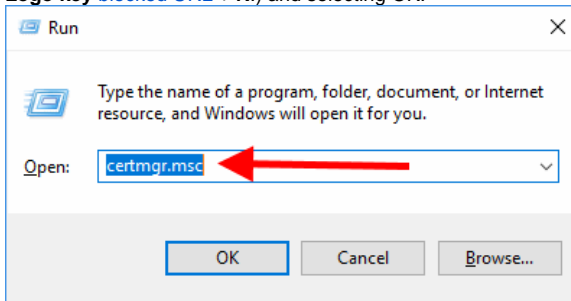
1. You should have a p12 either supplied by Medical Objects or generated using the Client Certificate Wizard [here](#)
2. Import the certificate into your Windows Certificate Store.
 - a. Double click on the p12. When asked make sure you mark the certificate as exportable.



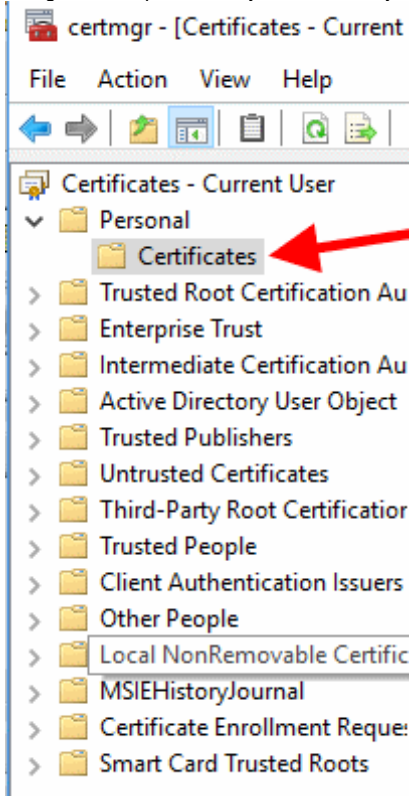
- b. Install the certificate into the Personal Store.



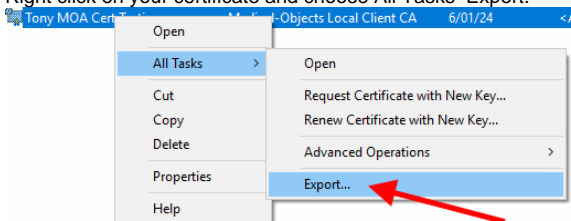
3. Open the certificate manager by typing certmgr.msc into a run dialog (Press the **Windows Logo key** **blocked URL** + **R**.) and selecting OK.



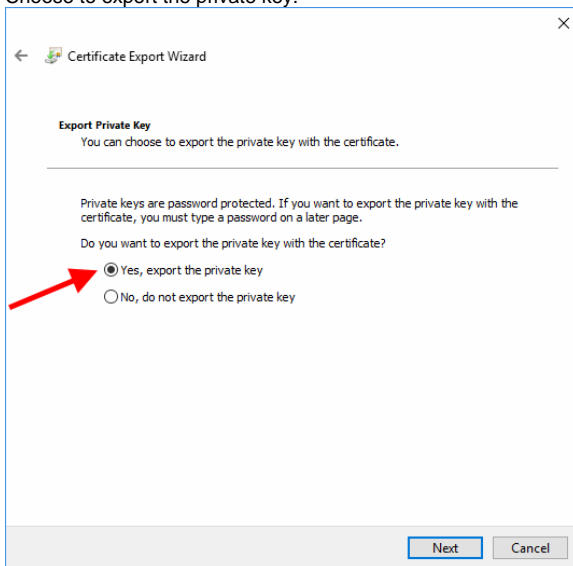
4. Navigate to the personal keystore and find your key.



5. Right click on your certificate and choose All Tasks > Export.

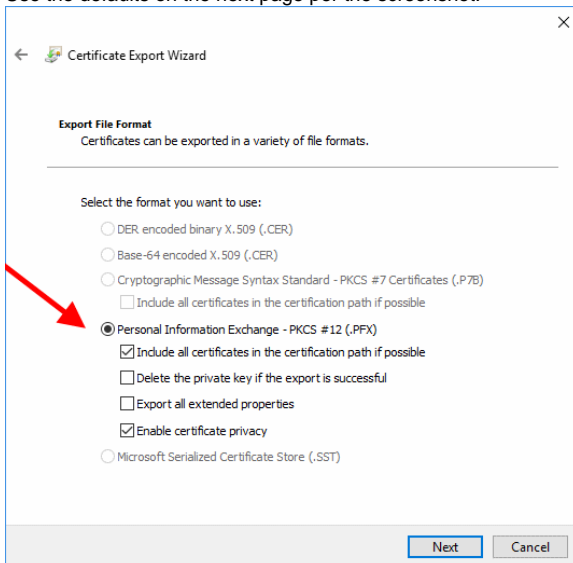


6. Choose to export the private key.



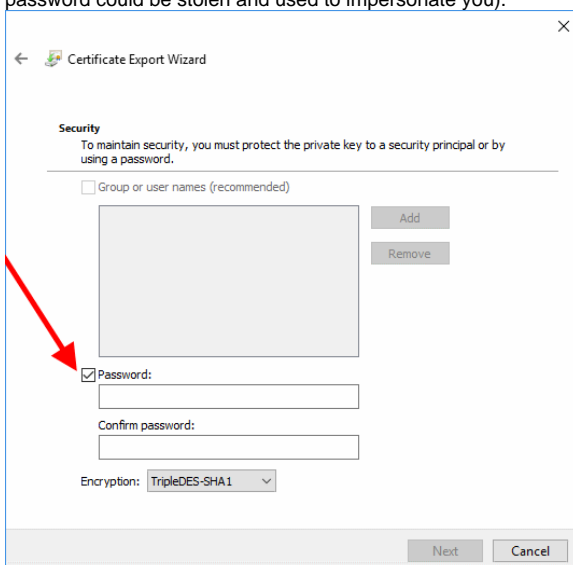
The screenshot shows the 'Export Private Key' step of the Certificate Export Wizard. The title bar says 'Certificate Export Wizard'. Below the title bar, there's a back arrow and the text 'Certificate Export Wizard'. The main heading is 'Export Private Key' with a subtitle 'You can choose to export the private key with the certificate.' Below this, a note states: 'Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.' The question is 'Do you want to export the private key with the certificate?'. There are two radio buttons: 'Yes, export the private key' (which is selected and pointed to by a red arrow) and 'No, do not export the private key'. At the bottom right are 'Next' and 'Cancel' buttons.

7. Use the defaults on the next page per the screenshot.



The screenshot shows the 'Export File Format' step of the Certificate Export Wizard. The title bar says 'Certificate Export Wizard'. Below the title bar, there's a back arrow and the text 'Certificate Export Wizard'. The main heading is 'Export File Format' with a subtitle 'Certificates can be exported in a variety of file formats.' Below this, the instruction is 'Select the format you want to use:'. There are five radio button options: 'DER encoded binary X.509 (.CER)', 'Base-64 encoded X.509 (.CER)', 'Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)', 'Personal Information Exchange - PKCS #12 (.PFX)' (which is selected and pointed to by a red arrow), and 'Microsoft Serialized Certificate Store (.SST)'. Under the 'Personal Information Exchange - PKCS #12 (.PFX)' option, there are four checkboxes: 'Include all certificates in the certification path if possible' (checked), 'Delete the private key if the export is successful' (unchecked), 'Export all extended properties' (unchecked), and 'Enable certificate privacy' (checked). At the bottom right are 'Next' and 'Cancel' buttons.

8. Set a password for the file you're about to generate (If you're emailing the final certificate to your iOS device don't email it with the password in the email as the combination of certificate and password could be stolen and used to impersonate you).



The screenshot shows the 'Security' step of the Certificate Export Wizard. The title bar says 'Certificate Export Wizard'. Below the title bar, there's a back arrow and the text 'Certificate Export Wizard'. The main heading is 'Security' with a subtitle 'To maintain security, you must protect the private key to a security principal or by using a password.' Below this, there's a checkbox for 'Group or user names (recommended)' which is unchecked. To the right of this checkbox are 'Add' and 'Remove' buttons. Below the checkbox is a large empty rectangular box. Below this box are two checkboxes: 'Password:' (which is checked and pointed to by a red arrow) and 'Confirm password:'. Below these checkboxes are two empty text input fields. At the bottom left, there's an 'Encryption:' label followed by a dropdown menu showing 'TripleDES-SHA1'. At the bottom right are 'Next' and 'Cancel' buttons.

9. Supply the resulting .pfx file to your iOS device (Email is useful for this. Itunes file sharing will not give you an option to install the certificate so that won't be useful). Open the file and follow the installation instructions. Note you may have to use your passcode to get to the point of installing the certificate before you are asked for the password for the certificate itself so if it's failing it may be because you're using the wrong password.
10. Note Safari may need restarting for the certificate you have just installed to become available. Instructions from Apple on this can be found [here](#).