Technical Bulletin

Monday, 3rd November 2014

Purpose of Announcement

On the 18th of December the Medicare Public Signing and Medicare Public Encryption certificates in your PKI store *will expire and need to be replaced*.

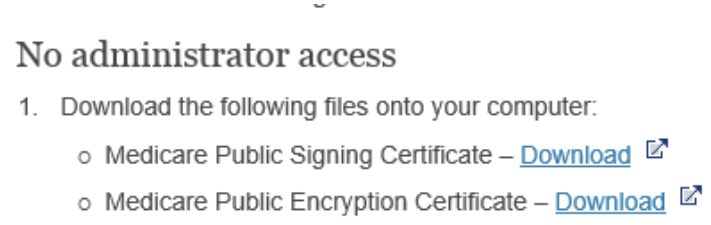
Depending on the version of the PKI Certificate Manager you have installed this may happen automatically. What this means to you: You will not be able to submit Medicare claims.

What you need to do now

The quickest way to pre-empt any problems that may be caused by certificate expiry is to download the latest PKI Certificate Manager (2.3.20) from the Medicare website (if you don't already have it). Please navigate to the following link:

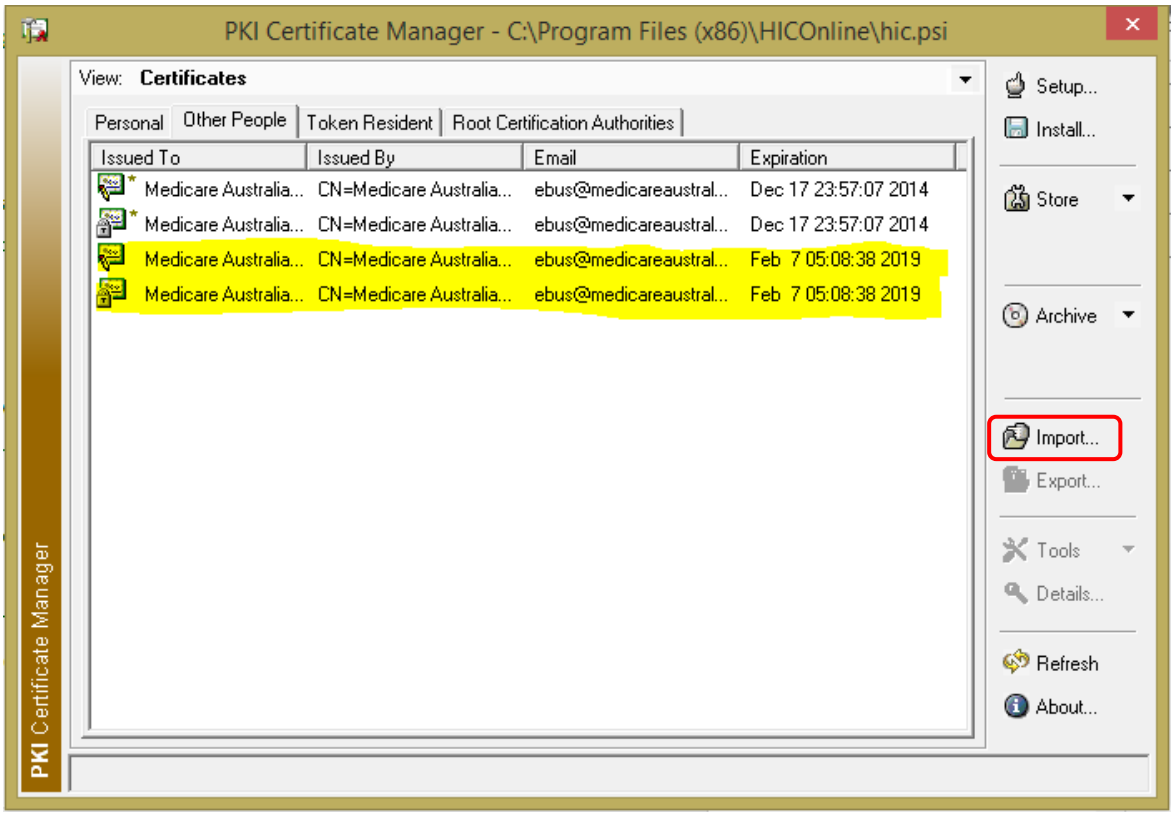
1. http://www.medicareaustralia.gov.au/provider/vendors/pki/index.jsp#N1047F
2. Scroll down to Download the Certificate Manager and download it. Extract the installer from the zip file and install the program.

A little further down the page there are also two links for the replacement certificates. Download these also.



3. Install the certificates by opening up the PKI Certificate Manager from control panel. On your PC (server) go to Window Control Panel. Open the *PKI Certificate Manager*.

You can then either use import to import them into the "Other People" tab OR drag and drop them into the tab. If the highlighted certificates already exist on your system there is no need to do anything.



4. Verify that the certificates are correctly installed by trying to retrieve a bulk bill payment report. If this works there is no need to do any further checking.

Help is on hand

If the above instructions are not able to be executed by yourself, or your IT services provider, please contact Medtech Support at support@medtechglobal.com to schedule one of our support team to install the new certificate as it is released by Medicare.