PKI Certificate Renewal Guide

How to Install Medicare Australia's Public Certificate

Version 3.0

Important information for:

Medicare Online Claiming – Eclipse,

Aged Care Online Claiming, and

PBS Online Claiming

Release Date: March 2011

Use of the Medicare Australia eSignature API Version V 2.1+ is subject to the terms of the

Medicare Australia eSignature API Licence Agreement.

Copyright © 2007- Medicare Australia - Canberra Australia

This product uses software from the OpenSSL and SQLite toolkits.

OpenSSL:
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit
(http://www.openssl.org/) Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.
This product includes cryptographic software written by Eric Young. (eay@cryptsoft.com)

SQLite:
This product includes software developed by Hwaci - Applied Software Research. (http://www.sqlite.org/)
This product was written by Dr. Richard Hipp (drh@hwaci.com) and is unrestricted open source.

Table of Contents

Table of Figures

Introduction

The Medicare Australia PKI certificate is used when you use the Medicare Australia's Online Claiming channels. The current Medicare Australia PKI certificate expires on 23 April 2011, and is being replaced with a new Medicare Australia PKI certificate.

The 'How To' instructions in this document will help you make the changes on your system software using the latest version of the Medicare Australia PKI Certificate Manager V2.3.15.

IMPORTANT NOTE:

Before proceeding to install the new Medicare Australia public certificates check if your software vendor has communicated with you about this certificate change. If provided follow your Software Vendor instructions.

This document contains the following information to assist with the renewal process of the Medicare Australia Certificates:

- Contact details

- Frequently asked questions

- Installing the latest version of Medicare Australia PKI Certificate Manager

- Installing Medicare Australia Certificates.

Contact details
For enquiries and assistance contact:

Medicare Australia eBusiness Service Centre – 1800 700 199

or by email

onlineclaiming@medicareaustralia.gov.au

Frequently Asked Questions

Why do I need to update the certificates?

Valid Medicare Australia certificates are required by customers who communicate electronically with Medicare Australia when using PKI. Replacement of expired certificates is a normal operational procedure. Renewing your Medicare Australia certificates will allow online operations to continue uninterrupted.

Am I impacted by this change?

If you are using one of the following programs, Medicare Online Claiming, PBS Online Claiming or Aged Care Online Claiming you may be affected by this change. Clients on Client Adaptor 6 or higher software may find the update has occurred seamlessly by the newer version of software.

How is Medicare Australia managing this PKI certificates change?

By placing the new version of the Medicare Australia PKI Certificate Manager on our web page. It is supported by documentation with step by step instructions.

How can I get the PKI Certificate Manager?

The PKI Certificate Manager is available on the Medicare Australia site. To download the latest version, go to the "Installing PKI Certificate Manager" section of this document on how to proceed.

Can I install this new version of the PKI Certificate Manager on top of my current version?

Yes. It will overwrite the older version and will open up with the same view of the certificates as before. Ensure you have installed to the correct PC that manages the certificates within a network.

My system is not allowing me to install the PKI Certificate Manager

Contact Medicare Australia eBusiness Service Centre for assistance.

When do I change/update the certificates?

You can make the change whenever it suits you depending on the version of your software. We will commence pushing out the new certificate on 19 March 2011. You may want to check your certificate store to see if you have already received the certificate appearing under the 'Other People' tab view of the PKI Certificate Manager. You do not need the latest PKI Certificate Manager to view certificates in the certificate store.

How do I make this change to my certificate store?

You should check the PSI store – it may have update already from 20 March 2011. Please refer to "Installing Medicare Australia PKI Certificate Manager" and "Installing Medicare Australia Certificates" in this document if you need to make the change.

What if I updated my certificate store early?

It is never too early to update your certificate store.

What if I am unsure about updating my certificate store?

Contact Medicare Australia eBusiness Service Centre for assistance.

I have two names in my store, for Medicare Australia.

Medicare Australia has supplied two pair of certificates – each pair carrying a different email address. Either email address can be selected to send secure transmissions to Medicare Australia. It will depend on your software which certificate is selected.

ebus@medicareaustralia.gov.au. The certificate we are updating carries the email address of ebus@hic.gov.au. This is the certificate we will use to sign outbound messages from mid April 2011.

Who can tell me the password to the PSI store?

It could be one of the following:

- The practice manager
- The person who manages your system
- Your Software Vendor
- Your IT support person.

If the password to the store cannot be found is there another solution?

Replacing the store would not be recommended unless you are experiencing transmitting errors. The older store can be replaced but you should contact your vendor to assist with the store replacement.

Can I build a new store over the top of the older store?

No.

Installing PKI Certificate Manager

You will need to know your PSI store password to make changes to your PSI store.

This password was set when your PKI certificate was first installed. Your practice manager or software vendor might know this password. You will need this store password if you want to update the PSI store with the new PKI Certificate Manager.

Note: If your Software Vendor has contacted you about the Medicare Australia's PKI certificate renewal, please follow the instructions they supplied.

Procedure for installing PKI Certificate Manager

1. Establish a connection to the Internet.

2. Copy http://www.medicareaustralia.gov.au/provider/vendors/pki/cert-manager.jsp into the Address area of your web browser and press the Enter key. The Medicare Australia PKI Utilities web page will be displayed, as shown in Figure 2.

Note: Ensure you choose the download carefully. The Windows version is listed first followed by the MAC version. There are two MAC versions. There is a new utility for MAC 10.6 and an earlier version for MAC 10.5

Downloads:

- Certificate Manager Installer Application (Windows) (ZIP, 200Kb)
- PKI Certificate Manager Installer Application (MAC) ZIP, 2.0Mb)
- PKI Certificate Manager Users Guide (Windows) [PDF, Kb]
- Mac PKI Certificate Manager User Guide [PDF, Kb]
- Button
- PSI Applet Programmers Guide [PDF, 1.3Mb]
- Platform Reference Guide [PDF, 521Kb]
- PKI API Glossary [PDF, 413Kb]
- PKI Certificate Renewal Guide [PDF, 553Kb]
- Medicare Australia new certificate for PKI CM

Figure 1.   PKI Utilities Web Page

3. Download PKI Certificate Manager by clicking on the PKI Certificate Manager Utility (Windows). The 'File Download' dialog box will open, as shown in Figure 3. Choose to save it to your desktop
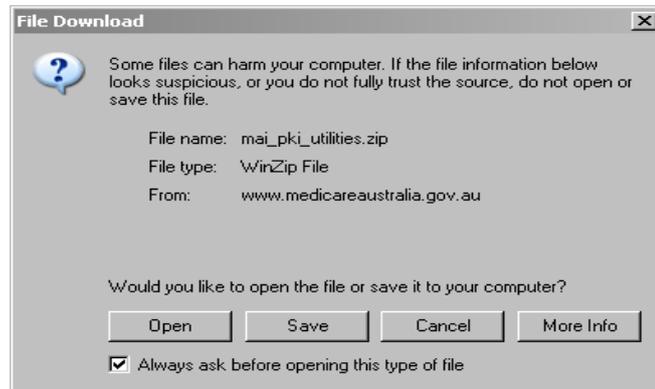

Figure 2.   File Download Dialog Box

Note: Before proceeding to the next step ensure the installation is done on the server or the main PC or on any PC that has a PSI store.

4. Double click on the "PKI Certificate Manager Installer.exe" icon (refer Figure 4) on your Desktop, and follow the prompts to install. Once installed, this utility can be accessed via the Control Panel.

PKI Certificate Manager Installer.exe

Figure 3.   PKI Certificate Manager Installer icon

You have successfully installed the latest version of the Medicare Australia Certificate Manager (Version 2.3.15). You can view your PSI store and if necessary proceed to install the Medicare Australia Certificates.

Installing Medicare Australia Certificates

These certificates are required to be imported into your PSI store to communicate successfully with Medicare Australia electronically. To install the Medicare Australia Certificates, follow the steps shown below.

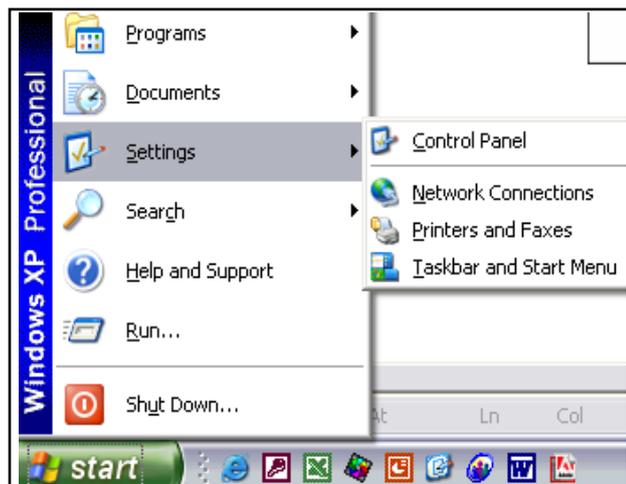1. Click START and navigate to the Control Panel as shown in Figure 5.

Figure 4.   Navigation to the Control Panel

2. Double click on the PKI Certificate Manager Icon, as shown in Figure 5.

Figure 5.   PKI Certificate Manager Icon

Click the About button to confirm the version.

3. The following screen shown in Figure 7 will appear if the PSI store has been located. You can view your certificate in the "Personal" tab. Go directly to Step 5.
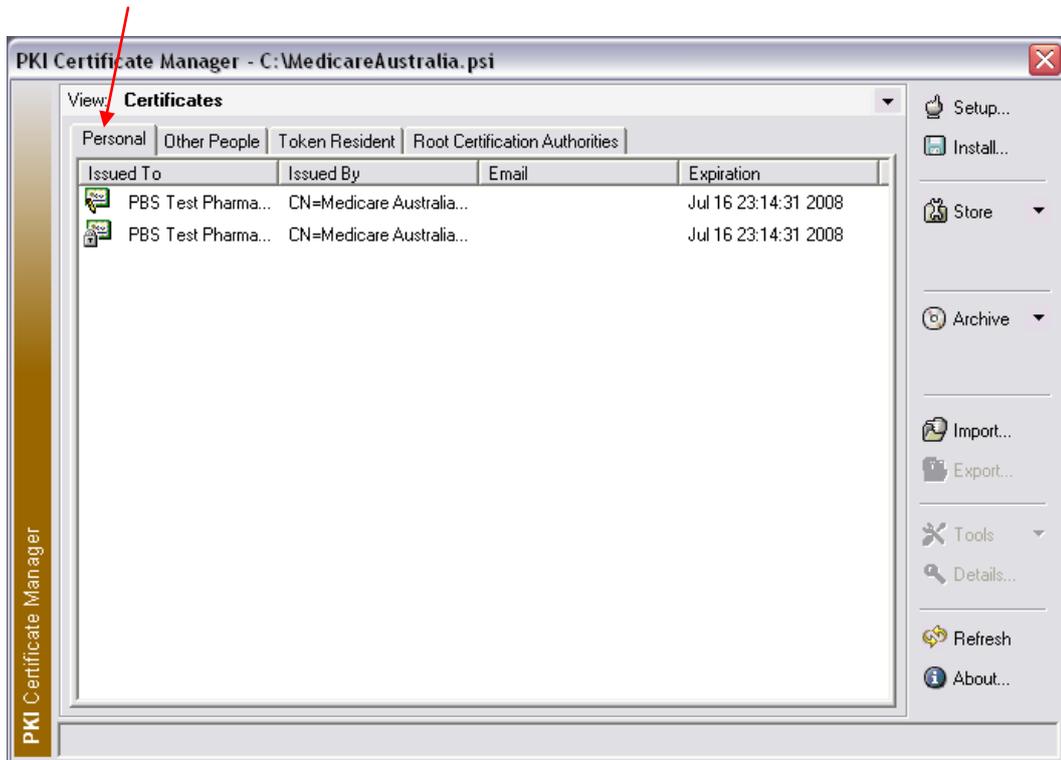

Figure 6.   PKI Certificate Manager – Main Window

4. The following screen shown in Figure 7 will appear **if** the PSI store cannot be located. For further assistance contact your Software Vendor.
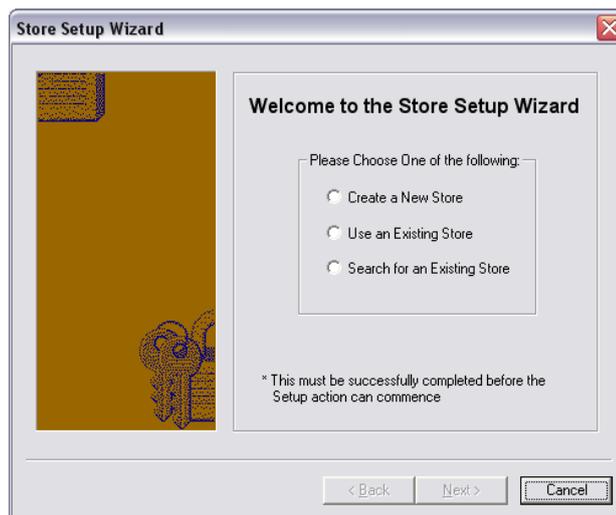

Figure 7.   Store Setup Wizard

5. To view the current Medicare Australia certificates select "Other People" tab, as shown in Figure 8.

Figure 8.   PKI Certificate Manager – "Other People" Tab

6. Click on the 'Store' button and from the drop down menu select 'Initialise Defaults', as shown in Figure 9.

Figure 9.   PKI Certificate Manager – Initialise Store Defaults

7. Enter your store password when prompted, as shown in Figure 10.

Figure 10.   Store Initialization Wizard – Password Screen

Note: The store password was set when you first installed your certificate.

8. Click finish for the certificates to be imported into your PSI store when the confirmation screen appears, as shown in Figure 11.
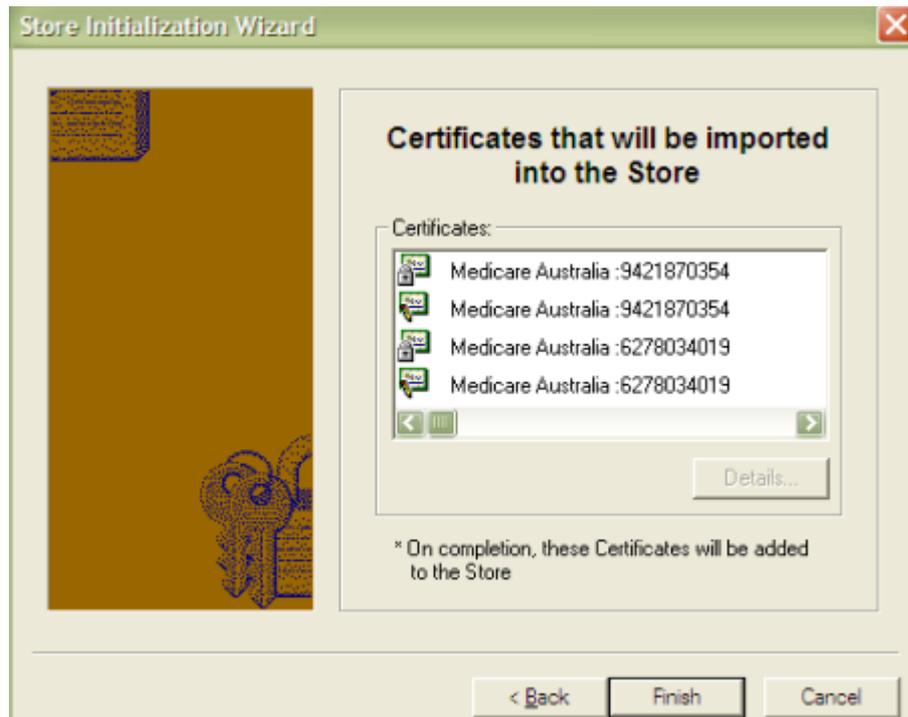

Figure 11.   Store Initialization Wizard – Confirmation Screen

9. Click on the 'Other People' Tab to see the two Medicare Australia certificates, as shown in Figure 12. You have now completed the task successfully.
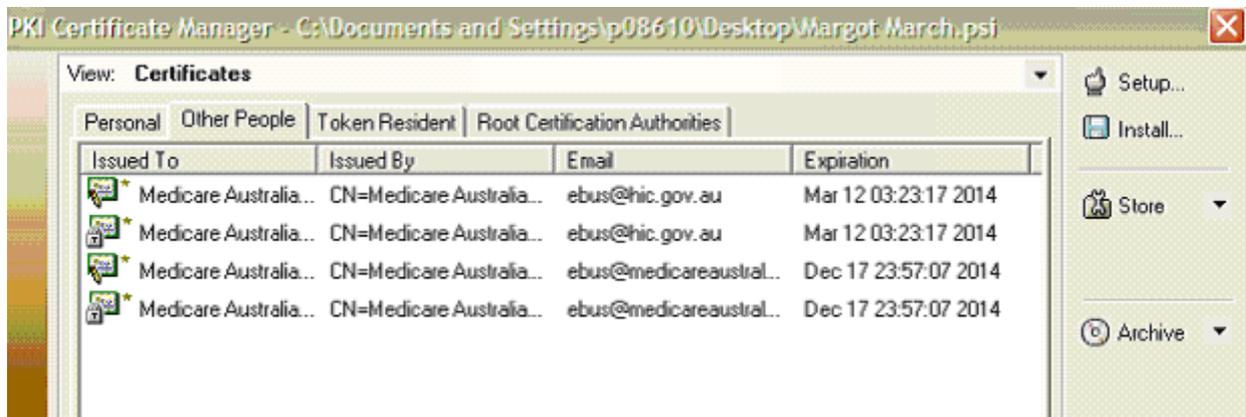

Figure 12.   PKI Certificate Manager – Medicare Australia Certificates after Initialisation

10. Click on the "Personal" tab to return to the original screen to see your certificates.

11. To remove old certificates from the store click on the certificate name. Select Tools and Remove. Follow the prompts.

12. Close out of the PKI Certificate Manager by clicking on the Close, [X], button located top right of the screen.

IMPORTANT NOTE:

Before resuming your online transmissions close down your claiming software and reopen again to ensure you are using the certificates that have just been imported into the store.