nehta

NASH Organisation Certificate Tracker Installation and User Guide v1.0.1

6 May 2016

Approved for external use

Document ID: NEHTA-2295:2016

National E-Health Transition Authority

National E-Health Transition Authority Ltd
Level 25, 56 Pitt Street
Sydney, NSW 2000
Australia
www.nehta.gov.au

Acknowledgements

Council of Australian Governments
The National E-Health Transition Authority is jointly funded by the Australian Government and all State and Territory Governments.

Document information

Key information

Owner	Head of Strategy, Architecture & Informatics Group
Contact for enquiries	NEHTA Help Centre t: 1300 901 001 e: help@nehta.gov.au

Product version history

Product version	Date	Release comments
1.0	17 March 2016	Initial release
1.0.1	6 May 2016	Minor update

Table of contents

1 Introduction

1.1 Product overview

The *NASH*[1] *Organisation Certificate Tracker* (hereafter: the Certificate Tracker) is a simple tool for reporting on installed NASH certificates and their expiry dates. This document describes the installation and use of this tool.

Healthcare provider organisations need active NASH PKI certificates to access the My Health Record system and securely send and receive health information. NASH PKI certificates expire after two years, and therefore need to be renewed to ensure ongoing access to the My Health Record system.

The Certificate Tracker tracks the NASH Public Key Infrastructure (PKI) certificates held by your organisation, and lets you identify which are due to expire soon.

The following points should be noted about this tool:

- The Certificate Tracker also uses Medicare PKI certificates but does not track them. Your organisation's Medicare PKI certificate needs to be installed and valid for the Certificate Tracker to access the Healthcare Identifiers (HI) Service, which provides details associated with the NASH PKI certificates.
- The Certificate Tracker is *not* a certificate management tool: it does not let you remove old certificates or install new ones. These tasks should be undertaken by a suitably skilled IT professional.

1.2 Audience

This document is intended for end users of the Certificate Tracker, as well as system administrators charged with the task of installing and managing the tool and digital certificates.

1.3 Disclaimer

This document does not provide advice on legal or regulatory requirements for obtaining any certificates or any other compliance with legal and regulatory requirements, including in relation to NASH certificates, and end users must not rely on this document for any such purpose. End users must obtain their own independent advice on these matters.

[1] National Authentication Service for Health

2 Installing, removing or updating the Certificate Tracker

2.1 System requirements

The Certificate Tracker runs on Windows and requires .NET 4.0 client or higher. As a general rule, systems capable of running Windows XP or later should be compatible. For details, see the following link:

https://msdn.microsoft.com/library/8z6watww(v=vs.100).aspx

2.2 Installation

The Certificate Tracker installer is called **CertificateTrackerSetup.exe**. Please note the following points at the outset:

- Administrator rights are needed to install the application.
- The Certificate Tracker uses locally stored Medicare and NASH certificates to pre-populate parts of the interface. Accordingly, the Certificate Tracker needs to be installed on the same machine as these certificates. (Check with your IT support if you are unsure about this.)
- The Certificate Tracker must be installed on a machine with internet access. Additional configuration is needed for machines that connect to the internet via proxy servers: see Appendix A for details.
- We recommend that you first copy the installer into a local directory before starting the installation.

Double-click on the installer to run it. This will display an installation "wizard" screen.

Figure 1: Installation wizard welcome screen

Installation is very simple; settings are pre-determined and cannot be changed.

1 Click **Next** in the screen in Figure 1, and the installation details will be displayed in the next screen.

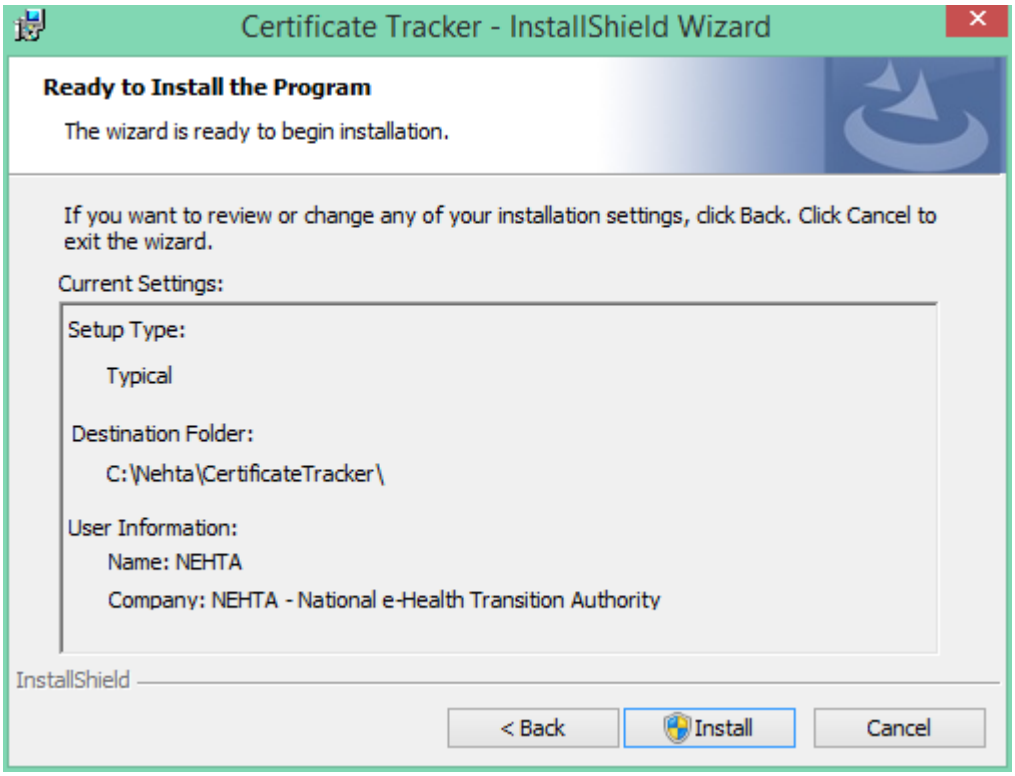

Figure 2: Installation details

2 The screen in Figure 2 displays the settings for your installation, and prompts you to proceed by clicking **Install**.

Depending on your system configuration, the next screen may ask you to confirm that the installer is allowed to make changes to your computer.

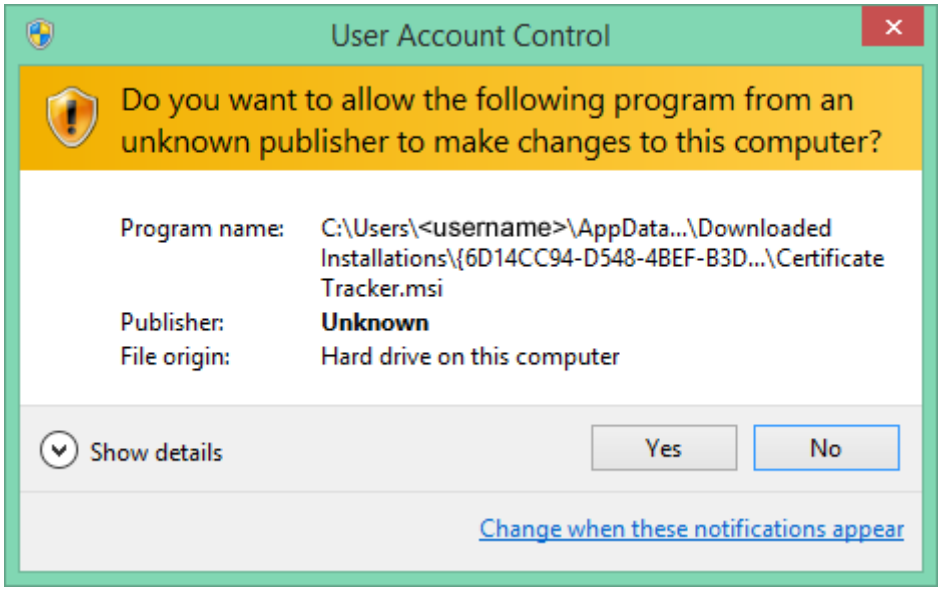

Figure 3: Confirming system changes

3 Click **Yes** to allow installation to proceed. The installation should then complete without further intervention on your part.

4 Click **Finish** on the final screen to exit the installer.

You should now see a shortcut on your desktop named *NASH Organisation Certificate Tracker*; the tool can also be accessed via the **Start** menu like any other application. See Figure 4 below.

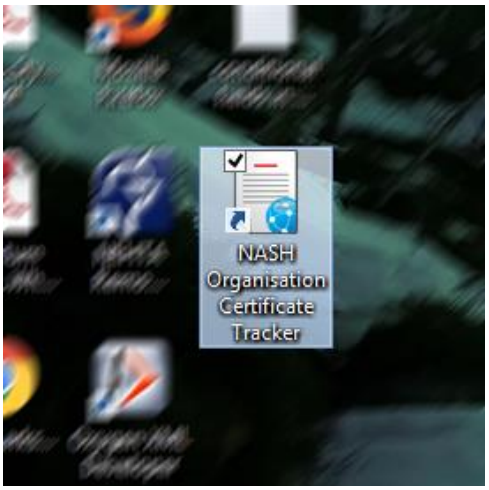

Figure 4: Certificate Tracker desktop shortcut

Installation of the Certificate Tracker is now complete. Please go to Section 3 for information about using the Certificate Tracker.

2.3 Repairing or removing the Certificate Tracker

Double-click on the installer if you need to repair or remove the Certificate Tracker. The welcome screen once again displays as per Figure 1 on page 7, but clicking **Next** in this instance will display the Program Maintenance screen, as shown below.

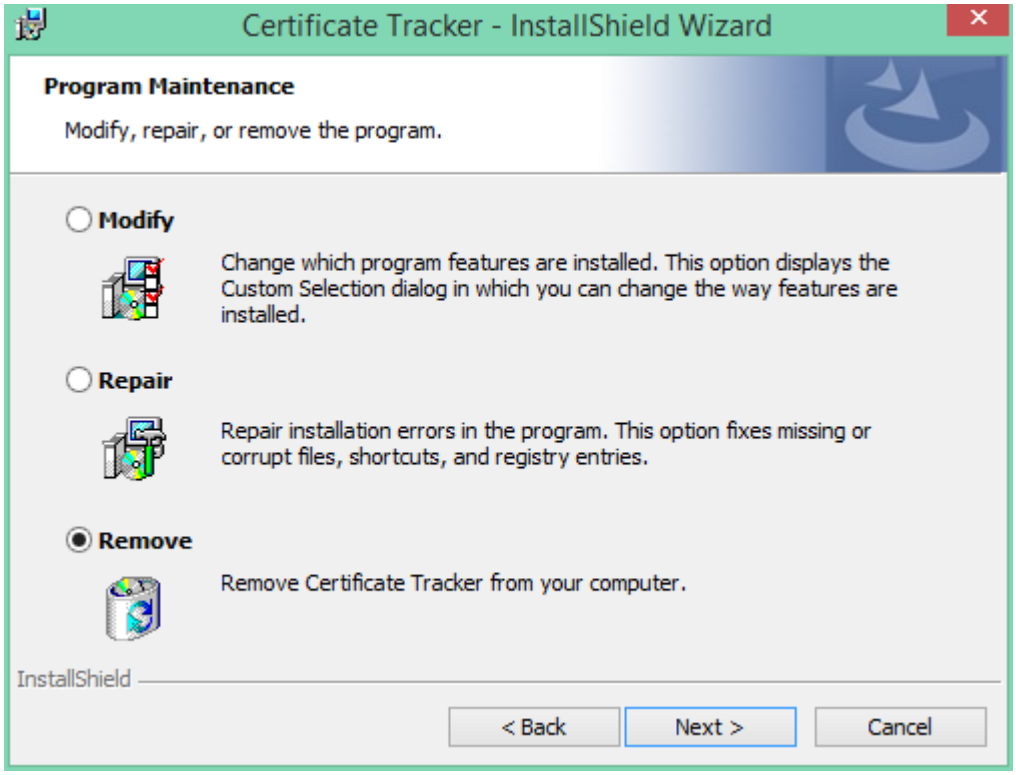

Figure 5: Program Maintenance screen

- The **Modify** button in this screen is not applicable, since the Certificate Tracker installation does not provide any modification options.
- The **Repair** button essentially reinstalls the Certificate Tracker. Selecting this option and clicking **Next** displays a screen similar to Figure 2 on page 7. Click **Install** in this latter screen to complete the reinstallation without further intervention.
- The **Remove** button uninstalls the Certificate Tracker. Click **Next** to proceed from this screen, and **Remove** in the following screen to confirm that you wish to uninstall the Certificate Tracker. The ensuing sequence directly parallels the installation process.

2.4 Updating the Certificate Tracker

If you already have the Certificate Tracker installed and attempt to install a new version, you may see an error message like the one below.

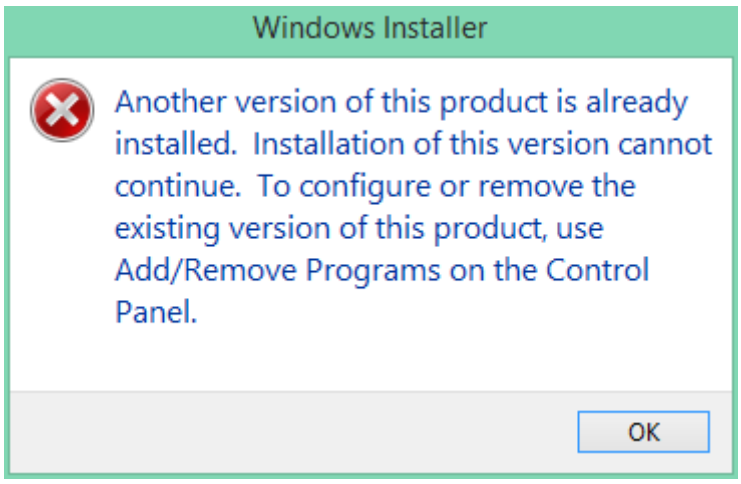

Figure 6: Error generated by updating the Certificate Tracker

Just as the error message recommends, you need to remove the old version via the Windows Control Panel. Or, if you still have the installer that was used to install this version of the Certificate Tracker, you could use that to uninstall it, as per Section 2.3.

The way you locate the **Add/Remove Programs** function depends on your version of Windows. The best way to find this function is to search for "remove program" from the Control Panel window, as shown in Figure 7.

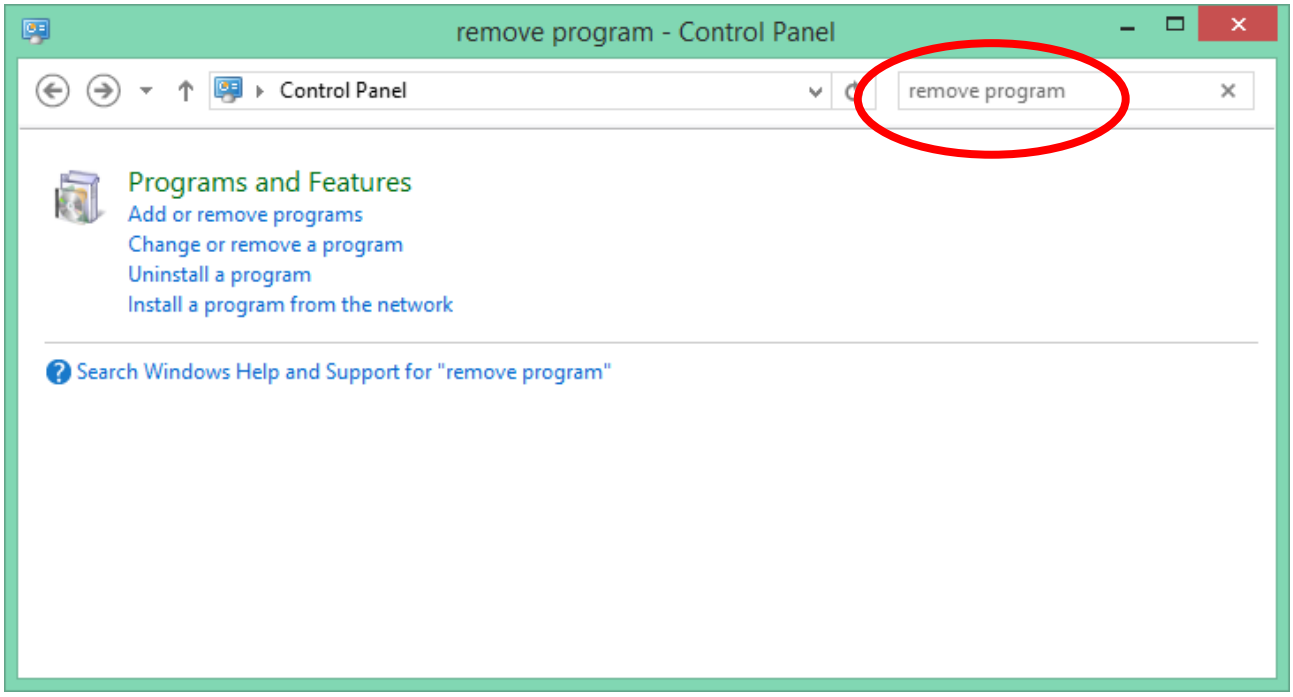

Figure 7: Searching for "remove program" in the Control Panel

Any of the links to remove or uninstall a program (that is, the first three links shown above) will take you to the utility you need. Click on one of these links, select the Certificate Tracker, and click **Uninstall**, as shown below.

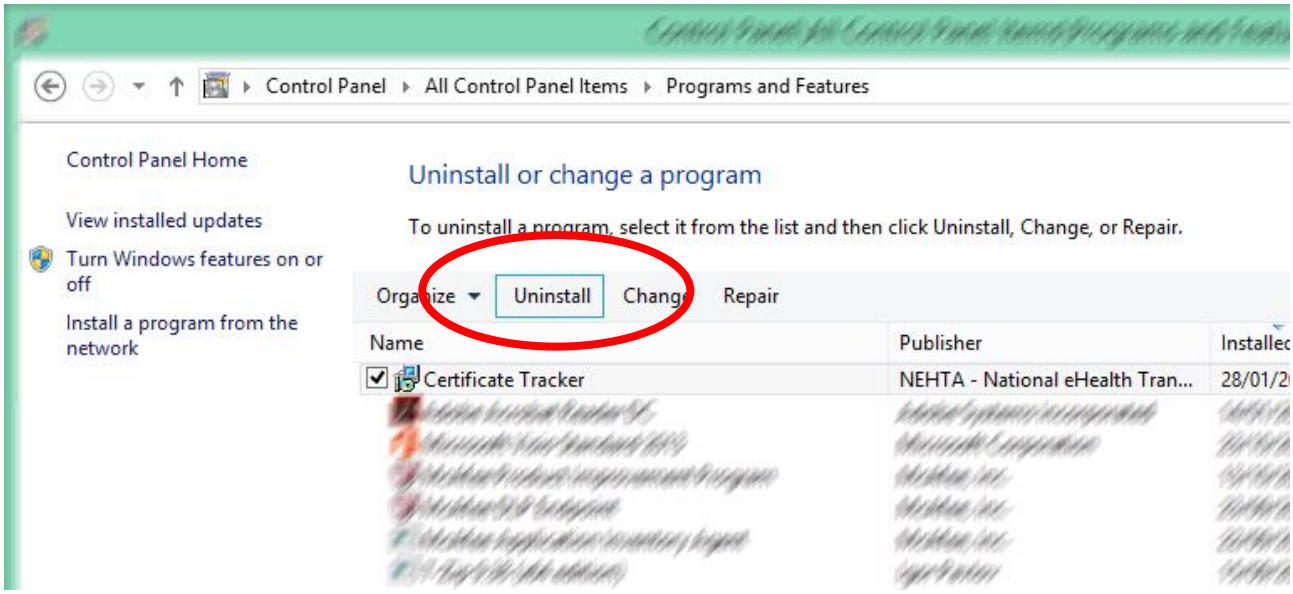

Figure 8: Uninstall utility

Depending on your system's security settings, you may need to confirm this action one or two times. Once you have removed the old version of the Certificate Tracker, install the new version as per the instructions above.

3 Using the Certificate Tracker

3.1 Launching the Certificate Tracker

The Certificate Tracker should be accessible via a desktop shortcut (see Figure 4 on page 8) or via the **Start** menu. It displays in a single window, as shown in Figure 9 below.

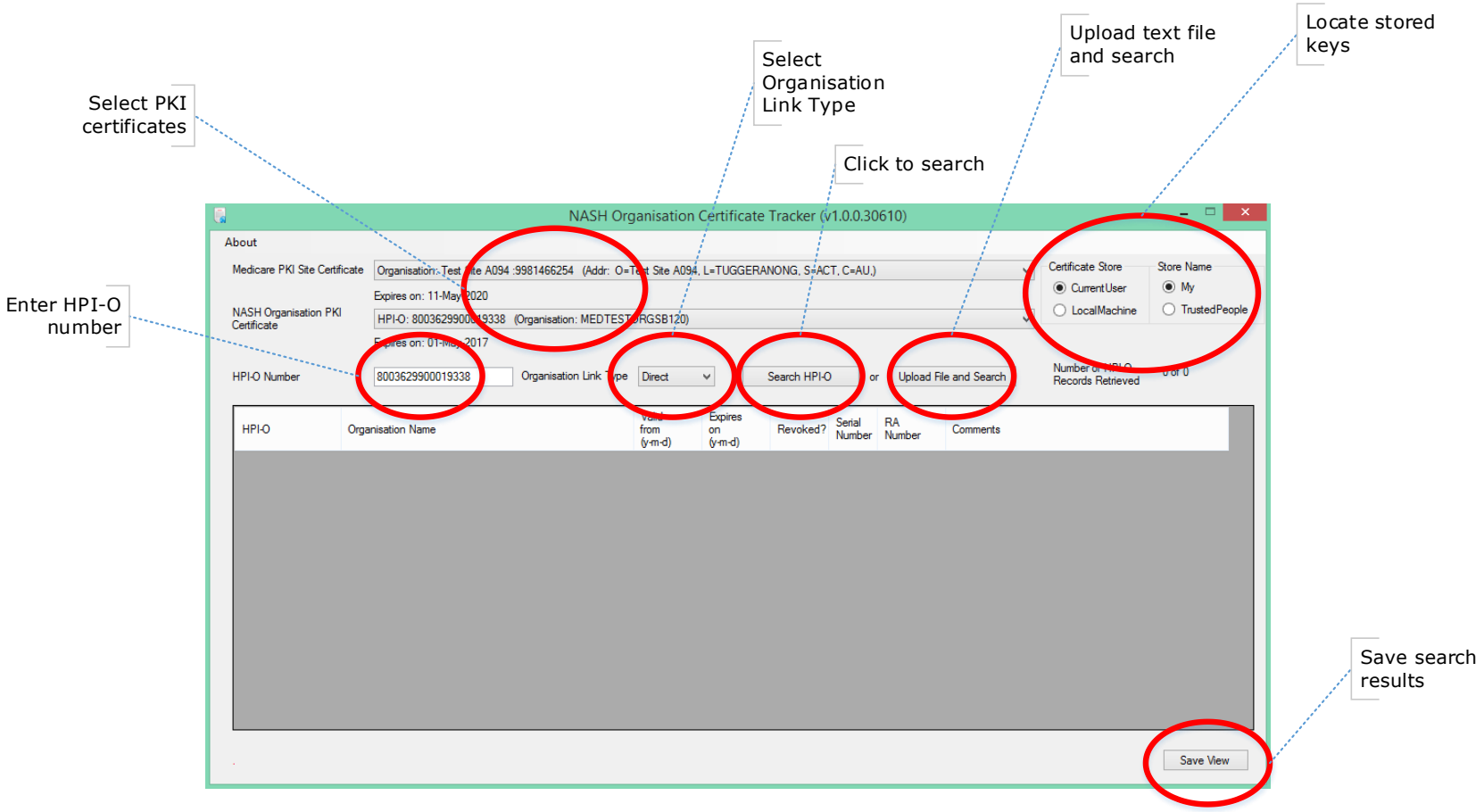

Figure 9: Certificate Tracker window, annotated

3.2 How to use the Certificate Tracker

There are three different ways to use the Certificate Tracker, as detailed below:

- Inspect a single NASH certificate
- Search based on a single HPI-O number
- Search based on a list of HPI-O numbers

3.2.1 Inspect a single NASH certificate

If your organisation only has a single NASH certificate, you can determine its expiry date by simple inspection.

Select your NASH certificate from the **NASH Organisation PKI Certificate** drop-down list (Section 3.3.2) and note the expiry date immediately displayed below it.

If the list of NASH certificates is not populated, explore different configurations of the keystore radio buttons (Section 3.3.6).

3.2.2 Search based on a single HPI-O number

You can search based on a single HPI-O number, and the Certificate Tracker will automatically return details of linked HPI-Os as well. This method is recommended for organisations with a single seed organisation.

1 Confirm that the PKI certificate drop-downs are populated. If not, different configurations of the keystore radio buttons (Section 3.3.6) should be explored.

2 Select active certificates from both of the PKI certificate drop-downs (Section 3.3.2).

The **HPI-O Number** field will be pre-populated with the selection in the **NASH Organisation PKI Certificate** drop-down list. Manually overwrite this number if necessary.

3 Determine the scope of the search via the **Organisation Link Type** drop-down list (Section 3.3.3).

4 Click on the **Search HPI-O** button to execute the search.

The Certificate Tracker first accesses HPD records and then NASH records. The number and type of records retrieved are displayed in a counter on the right of the screen.

5 View details of the certificates.

a If you only have a few certificates, you can inspect the certificate details in the table of results. If necessary, you can sort the results by clicking on any of the table headings to sort by that factor. Click once to sort ascending; click again to sort descending.

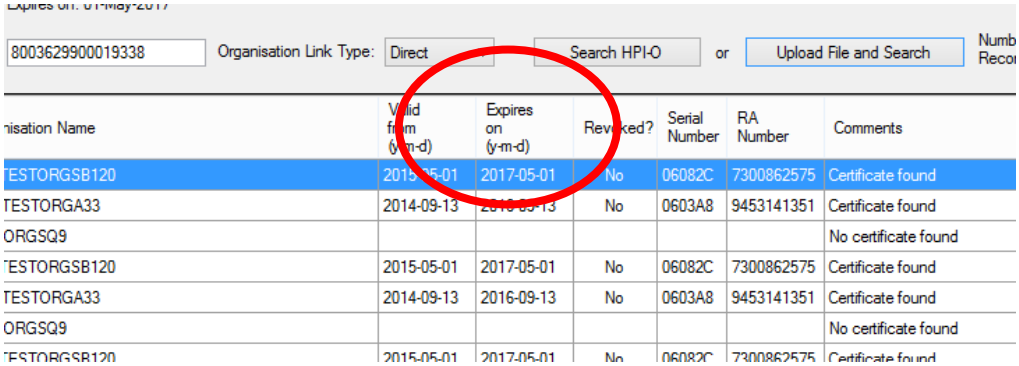

Figure 10: Click headings to sort results

b The Certificate Tracker will return HPI-Os linked to the entered HPI-O, regardless of whether or not the linked organisations have a NASH certificate. So there may be a number of rows in the results table without any details for the HPI-O.

c Most of the headings in the table of results should be self-explanatory. The two exceptions are the **Serial Number** and **RA Number**, both of which are used to correctly identify the NASH certificate. In addition, the RA (Registration Authority) number can be reconciled with the RA number cited on the CD that supplies your organisation's NASH certificates.

6 If desired, save your search results by clicking on the **Save View** button (Section 3.3.7).

3.2.3 Search based on a list of HPI-O numbers

The Certificate Tracker has a facility for searching lists of HPI-O numbers. This method is recommended for organisations with multiple seed organisations.

To use this method, you will first need to prepare a text file with your organisation's HPI-O numbers on separate lines.

1 Confirm that the PKI certificate drop-downs are populated. If not, different configurations of the keystore radio buttons (Section 3.3.6) should be explored.

2 Select active certificates from both of the PKI certificate drop-downs (Section 3.3.2).

The **HPI-O Number** field is not relevant to this procedure.

3 Determine the scope of the search via the **Organisation Link Type** drop-down list (Section 3.3.3).

4 Click on the **Upload File and Search** button (Section 3.3.5). You will be prompted to locate the text file of HPI-O numbers. Once you have done so, the search will commence immediately.

The Certificate Tracker first accesses HPD records and then NASH records. The number and type of records retrieved are displayed in a counter on the right of the screen.

5 View details of the certificates.

a You may find it helpful to sort the results by clicking on any of the table headings to sort by that factor. Click once to sort ascending; click again to sort descending. See Figure 10 above.

b Most of the headings in the table of results should be self-explanatory. The two exceptions are the **Serial Number** and **RA Number**, both of which are used to correctly identify the NASH certificate. In addition, the RA (Registration Authority) number can be reconciled with the RA number cited on the CD that supplies your organisation's NASH certificates.

6 If desired, save your search results by clicking on the **Save View** button (Section 3.3.7).

3.3 Certificate Tracker features

Key features of the Certificate Tracker are annotated in Figure 9 (page 12), and described in the following sub-sections.

3.3.1 HPI-O Number field

This field is pre-populated by your selection in the **NASH Organisation PKI Certificate** drop-down, but it can be overridden by entering a different HPI-O number. The content of this field becomes the subject of the search when you click on the **Search HPI-O** button.

3.3.2 PKI certificate drop-downs

The Certificate Tracker needs to connect to the HI Service Health Provider Directory (HPD), which requires an active Medicare PKI Site certificate. Similarly, it needs to connect to the NASH directory, which requires an active NASH certificate.

The expiry date for the selected certificate is displayed immediately below the drop-down list. Any active (non-expired) certificate will suffice to make the connection. Conversely, expired certificates will not work. They will be clearly labelled with "EXPIRED" before their name.

The selection in the **NASH Organisation PKI Certificate** drop-down pre-populates the **HPI-O Number** field, but you can override this by entering a different number in this field.

3.3.3 Organisation Link Type drop-down

The Certificate Tracker displays NASH certificates that are related to the HPI-O that you searched for. This list controls the scope of these related certificates that are returned. The default setting is "Direct". The options on this list are as follows.

Table 1: Organisation Link Type list options

List Option	Meaning
Direct	The organisations immediately above or below this organisation in the hierarchy (default option).
Children	All organisations beneath this organisation in the hierarchy.
Parents	All organisations above this organisation in the hierarchy.
All	All results.

If the meanings of these list options are still unclear, the following diagram may help. It depicts the different search results relative to an organisation (B) at the second level of its organisational hierarchy.

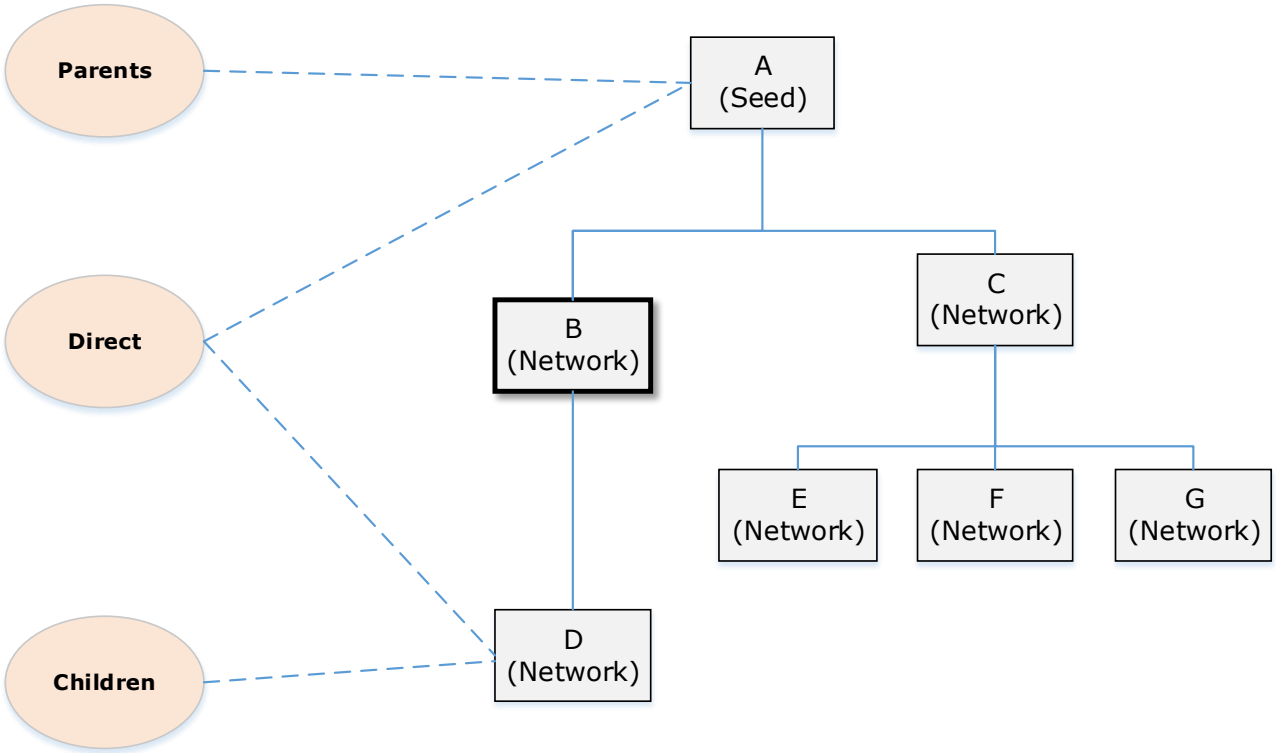

Figure 11: Search results relative to "Organisation B"

In the context of the organisational hierarchy depicted in Figure 11, a search for B's HPI-O number will yield the following results, depending on the **Organisation Link Type** list selection.

Table 2: Search results relative to Figure 11

Organisation Link Type	Results
Direct	A, B, D
Children	B, D
Parents	A, B
All	A, B, C, D, E, F, G

3.3.4 Search HPI-O button

Click this button to execute a search for the HPI-O number in the **HPI-O Number** field as well as any associated organisations as determined by the **Organisation Link Type** drop-down.

3.3.5 Upload File and Search button

If you have a text file with your organisation's HPI-O numbers on separate lines, upload and search it by clicking on this button. A standard Windows dialog will prompt you to locate the text file. Once you have done so, the search will execute immediately.

3.3.6 Keystore radio buttons

The **Certificate Store** and **Store Name** radio buttons tell the Certificate Tracker where it should look for stored certificate keys on your system. Certificates should be visible in both the **Medicare PKI Site Certificate** and **NASH Organisation PKI Certificate** drop-down lists. If either or both of these lists are blank, that may be a result of the selections here.

The most appropriate settings for most environments have been preselected, but since there are only four possible configurations, you can easily explore each one. The configuration you select will be retained, so you will not need to repeat this step the next time you use the Certificate Tracker.

If you are still unable to display certificates in one or both lists, contact your IT service provider.

3.3.7 Save View button

You can save the results of your search (in CSV[2] format) by clicking on **Save View**, and saving the file to a convenient location. CSV files can be read by Excel and other applications, so you can use the information in this file in your office management software to monitor certificate expiry dates.

[2] CSV = "Comma Separated Value", a common format for tabular data.

Appendix A Configuring the Certificate Tracker to use a proxy server

If your organisation uses a proxy server to connect to the internet, the Certificate Tracker configuration file will need to be modified to support this. The procedure to do this is as follows.

1 Locate the following file on your computer: **C:\Nehta\CertificateTracker\CertificateTracker.exe.config**. Right click on it, and open it with the Windows Notepad utility.

2 Locate the section that references a proxy server (it should be line 31):

```
<system.net>
  <defaultProxy enabled="false" useDefaultCredentials="true">
    <proxy proxyaddress="http://proxyname:8080" bypassonlocal="True"/>
  </defaultProxy>
</system.net>
```

3 Set **enabled="true"**.

4 Set the **proxyname** to the name of your proxy server.

5 Set the port (currently **8080**) to the port used for your proxy server.

For example, a proxy server named **myproxy** connecting through port **1234** would be accommodated as follows.

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://myproxy:1234" bypassonlocal="True"/>
  </defaultProxy>
</system.net>
```

This should enable the use of your proxy server using the default credentials used by the computer when browsing the internet.

Acronyms

Acronym	Description
CSV	comma separated value
HI	healthcare identifiers
HPD	Healthcare Provider Directory
HPI-O	Healthcare Provider Identifier – Organisation
NASH	National Authentication Service for Health
PKI	public key infrastructure
RA	registration authority