

TIPS FOR MAKING PKI EASY TO INSTALL

Background:

The following tips have been developed by SEA-GP (Brisbane) Information Management Working Group based on experience with installing and using digital certificates linked to health care users via a public key infrastructure (PKI).

Introduction:

Digital certificates come in two main types.

- The first type is a **location based certificate** which is used by a single health care business (eg General Practice, Pharmacy, Allied Health practice) to:
 - Electronically send documents to another health care business or individual, and
 - Receive electronic messages securely.

Pathology and radiology results have been sent to GP practices electronically over the past 10 years, ie. the pathology company uses its location certificate to securely send the pathology result to the General Practice's location certificate.

The practice "binds" their location certificate to the practice's email address, allowing the practice to send a secure, encrypted email.

- The second type is an **individual certificate** which is used by an individual health care provider to:
 - Electronically sign and send documents to another health care business or individual health care provider (eg. Specialist referral letter or pathology referral); and
 - Receive electronic messages securely.

The individual certificate binds the individual to the public key (which is used to encrypt the message).

The individual health care provider "binds" his/her individual certificates to his/her email address, allowing him/her to send a secure, encrypted, and **signed** email. The individual certificate allows the secure email to be "signed", ie. verified that the email came from that particular individual, just like signing a written document.

Sending a secure email requires installation onto your computer of both the sender's private certificates, and also the recipient's public certificates.

It is important to consider how you will possibly use your location or individual certificate as this will influence your PKI installation set-up. The ability to use email to send information securely to other health providers and vice versa is a useful option to consider. This relies on having a location (practice) based email address "bound" to a location certificate, or an individual email address "bound" to an individual certificate. To send messages securely to another health provider is possible by requesting the recipients public key from the recipient, or downloading the recipient's key from the Certificates Australia Public Directory. Changing the email address linked to your digital certificate is possible, but can only be done by reapplying in writing to Medicare Australia. Getting it right the first time will save you time and mental energy.

WHEN APPLYING FOR YOUR PKI CERTIFICATES FROM MEDICARE

So with the above in mind, when applying for a **location certificate**, make sure you link it to an email address at your practice. This will ensure you have the option to use the location certificate to send and receive secure emails if you so desire, eg. admin@gppractice.com.au. If you do not supply a valid email address when initially applying for a location certificate, Medicare will assign an invalid email address to your location certificate, preventing you from using it for secure email. Practice processes also need to

reflect the setting up of a location based digital certificate in that a staff member must be delegated to open the email account on a regular basis to read and process the mail, ensuring that incoming emails are acted upon.

Similarly, when applying for an individual certificate, ensure that you supply an email address that you can access from your workplace. This allows you to use that email address to send and receive secure, encrypted and signed emails.

INSTALLING CERTIFICATES ONTO YOUR COMPUTER

Part 1. (Installing your own location or individual private certificates)

You should receive instructions on how to install your certificates when you receive your individual token, individual smart card, or practice location certificate CD.

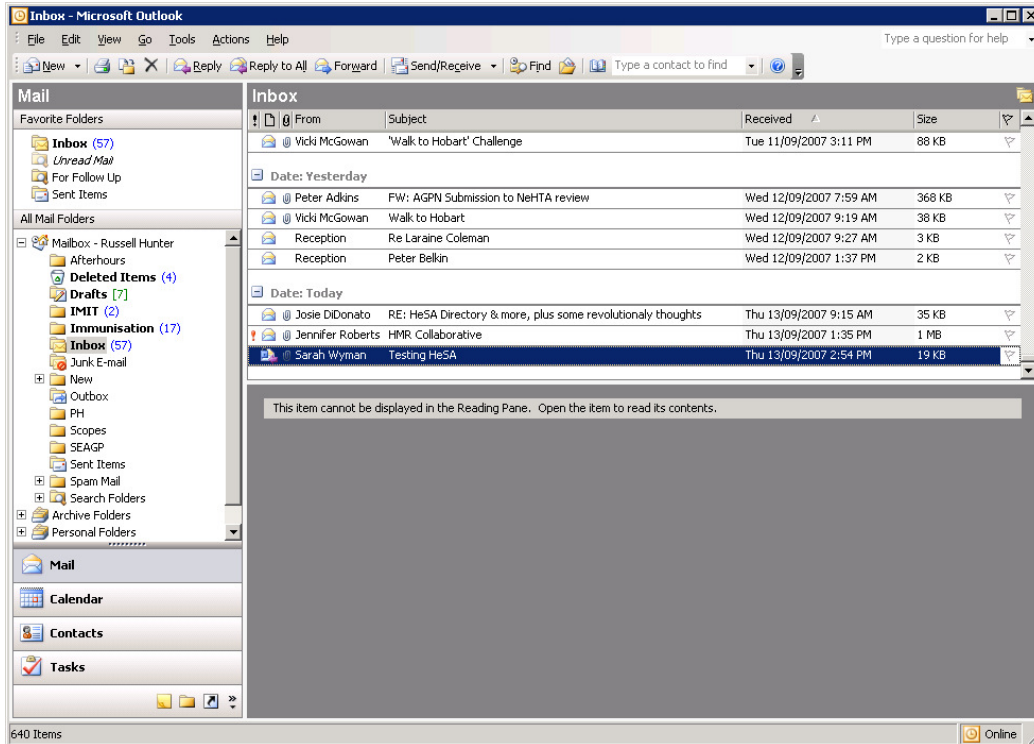
CONFIGURING YOUR EMAIL PROGRAM TO USE THESE CERTIFICATES TO SEND AND RECEIVE SECURE EMAILS

Medicare Australia has a comprehensive list of instructions for Outlook Express and various versions of Outlook on the Medicare Australia website:

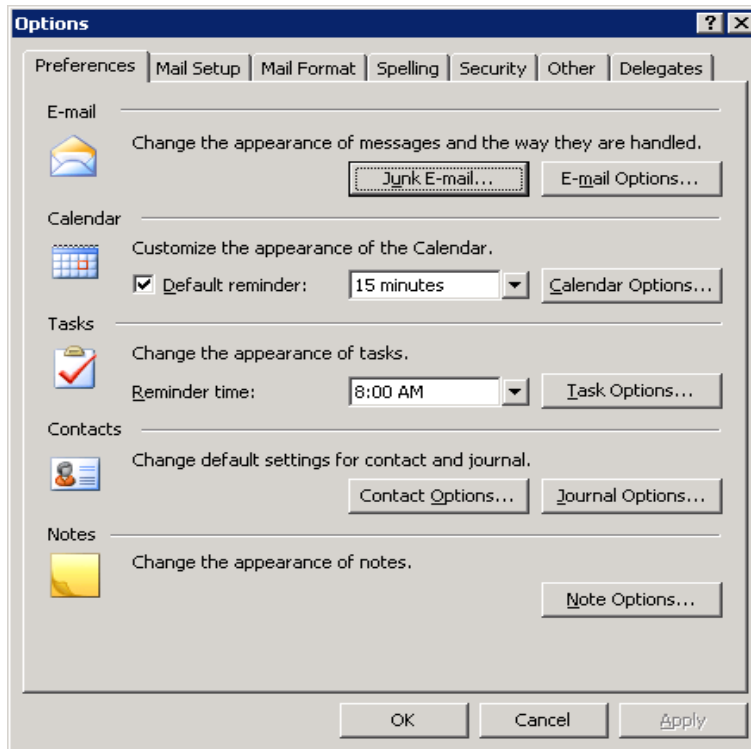
1. [PKI procedures - Medicare Australia](#)

CONFIGURE YOUR EMAIL PROGRAM TO SEND AND RECEIVE SECURE EMAILS.

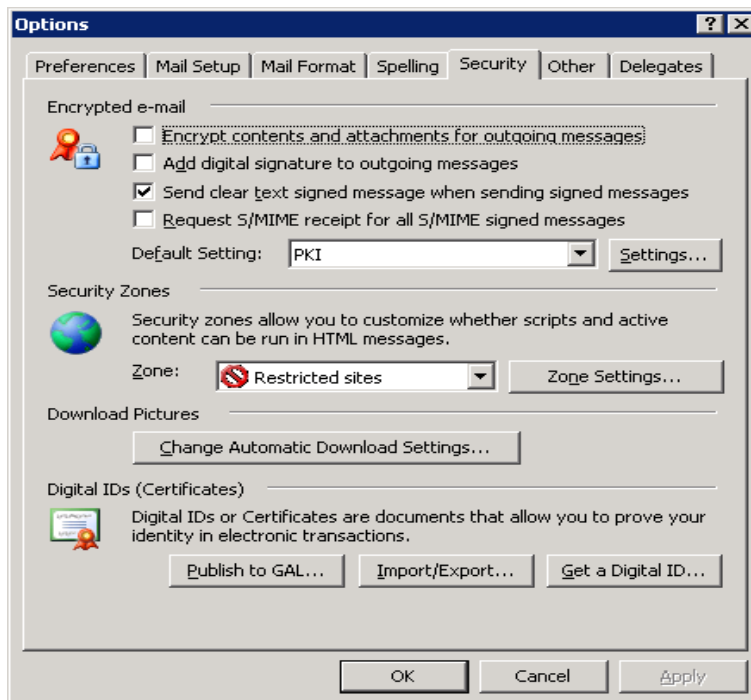
These instructions are for Outlook 2003. Use the link above to get specific instructions for other versions of Outlook.



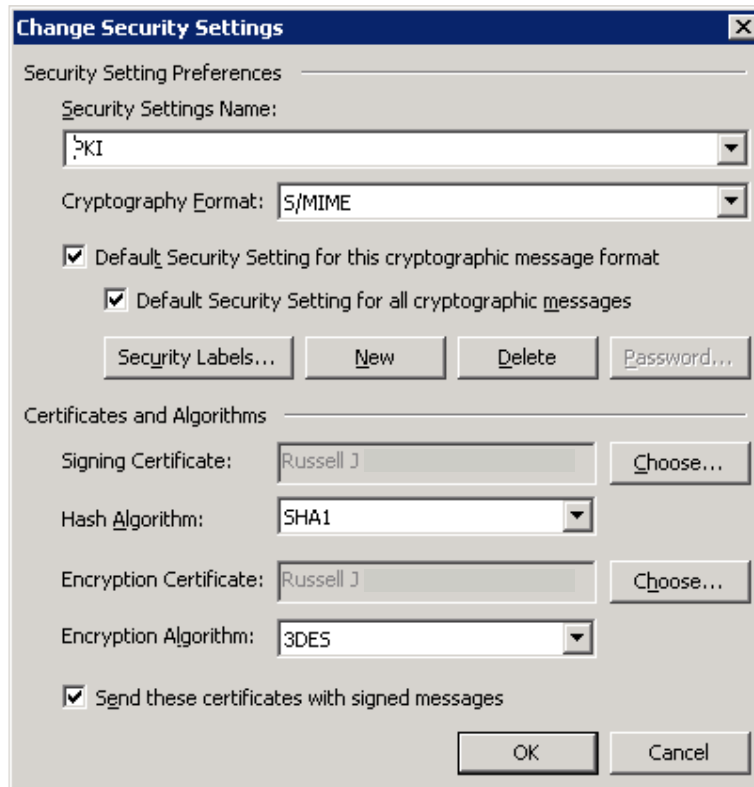
In Outlook 2003, click Tools, Options.



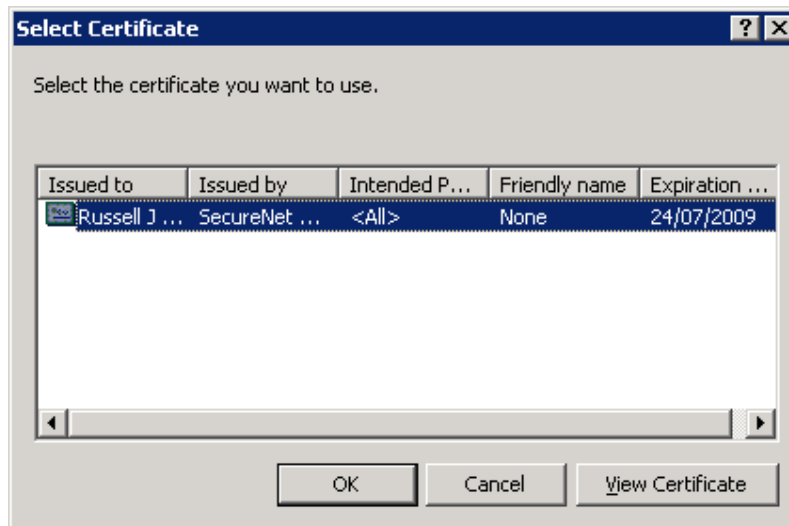
Click the Security tab.



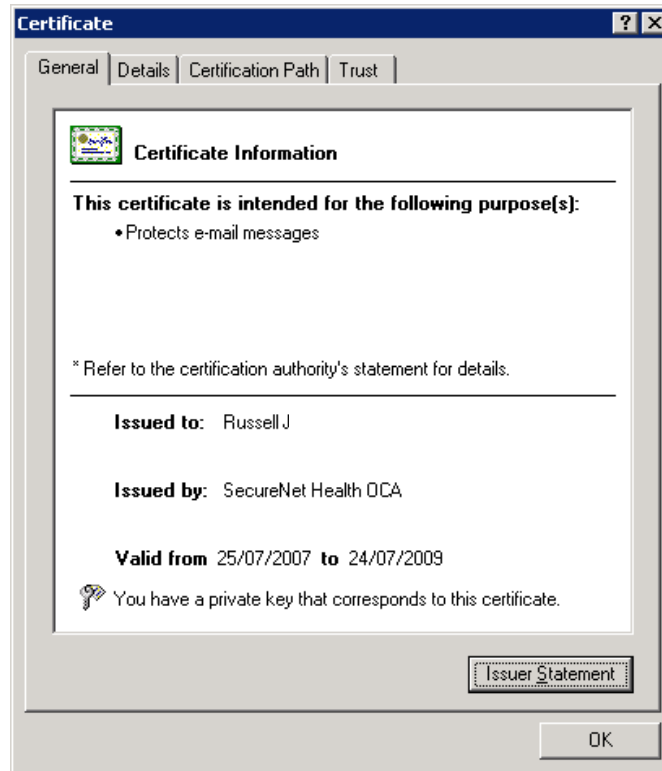
Tick the boxes “Encrypt contents and attachments for outgoing messages”, and “Add digital signature to outgoing messages”. Then click “Settings”.



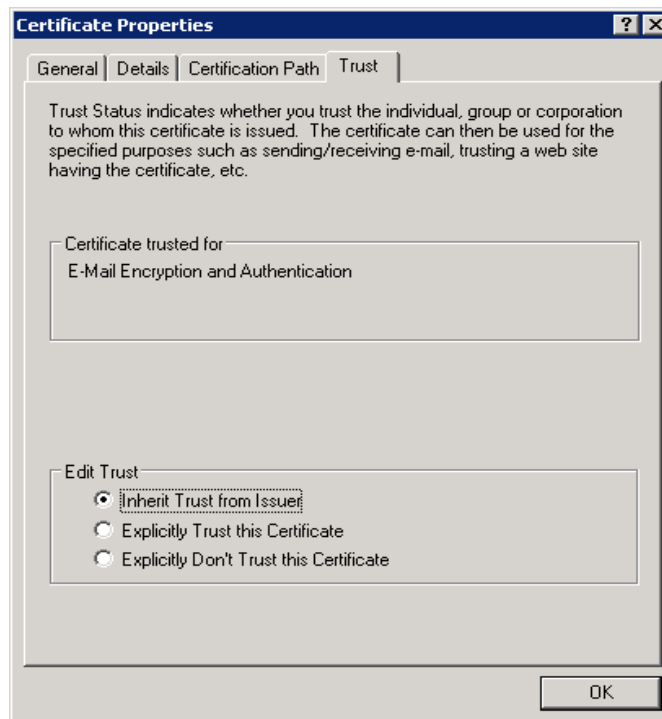
If the certificates and algorithm boxes look like the above, then it is configured properly. Click OK. If the Signing Certificate box is empty, click Choose. The window below will appear. Click on the certificate with your name (if there is more than one, choose the one with the latest expiry date).



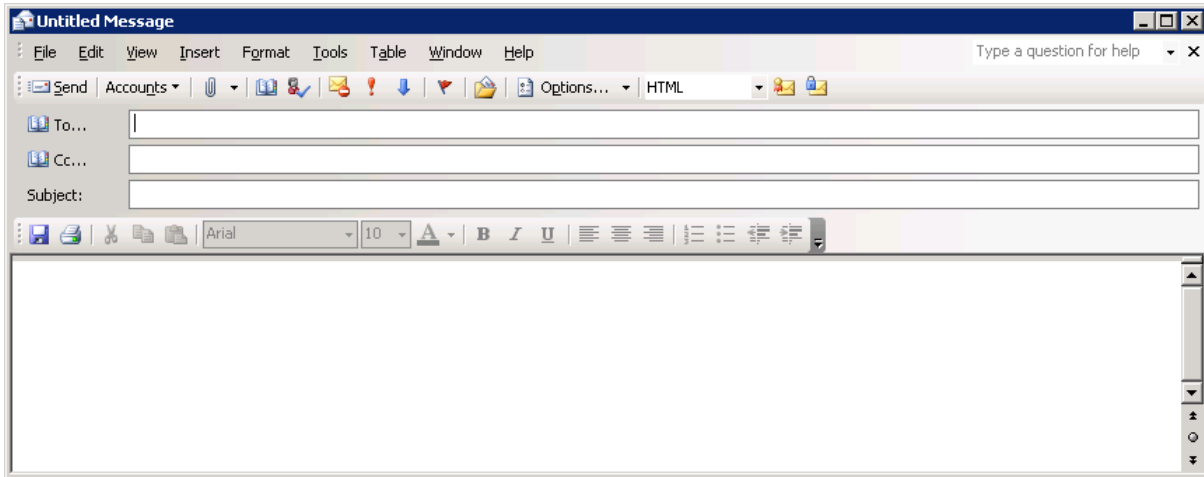
Click the View Certificate button.



Click the Trust tab.



Make sure the "Inherit trust from Issuer", button is selected. Click OK on all the opened windows. You should now be able to use your certificates to send encrypted and signed emails.



Emails will continue to be sent unencrypted by default. To send an encrypted and/or signed email, click the encrypt and/or sign icons on the right hand side of the toolbar above the addressee box as above.

Medicare Australia has more helpful information at [PKI frequently asked questions \(FAQ\) - Medicare Australia](#).

The “support toolkit” link in this webpage has more helpful information.

TROUBLESHOOTING

When your email program (eg Outlook) uses your certificates to encrypt and/or sign an email, the program has to be certain that the certificates are actually yours, ie. it has to “trust” them. Outlook has to be sure that your certificates are not being used illegally by someone else. Outlook can automatically trust your certificate when it trusts the “root” or “parental” certificate that validated and issued your certificate. If that root certificate is already installed in Outlook, your certificate (and any other certificate issued by that root certificate) will automatically be trusted.

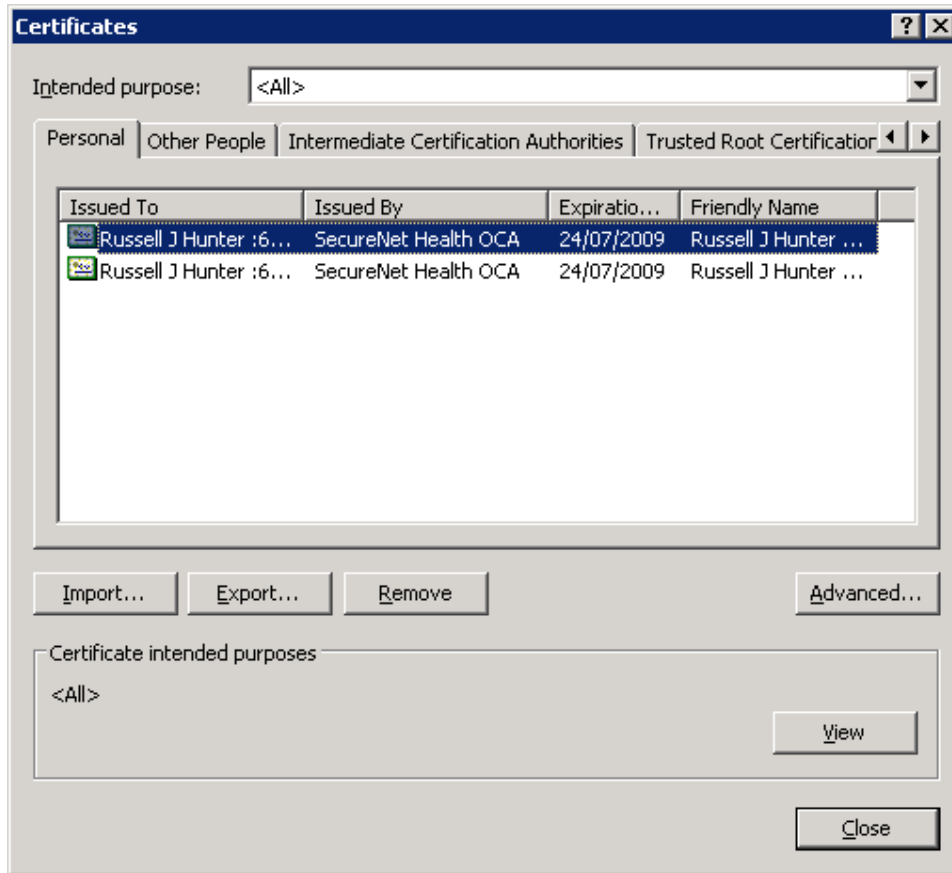
However, sometimes the root certificate is not installed automatically, resulting in Outlook not trusting individual certificates. If so, when you attempt to send a signed or encrypted email, this error message will appear:



This indicates that outlook does not “trust” your certificate. **TO FIX THIS**, you need to download and install the root certificate from the authority that issued the certificate so that your computer will trust your certificates.

First, find out which authority issued your certificate by

- clicking Start, Control Panel, Internet Options, Content, Certificates, Personal.



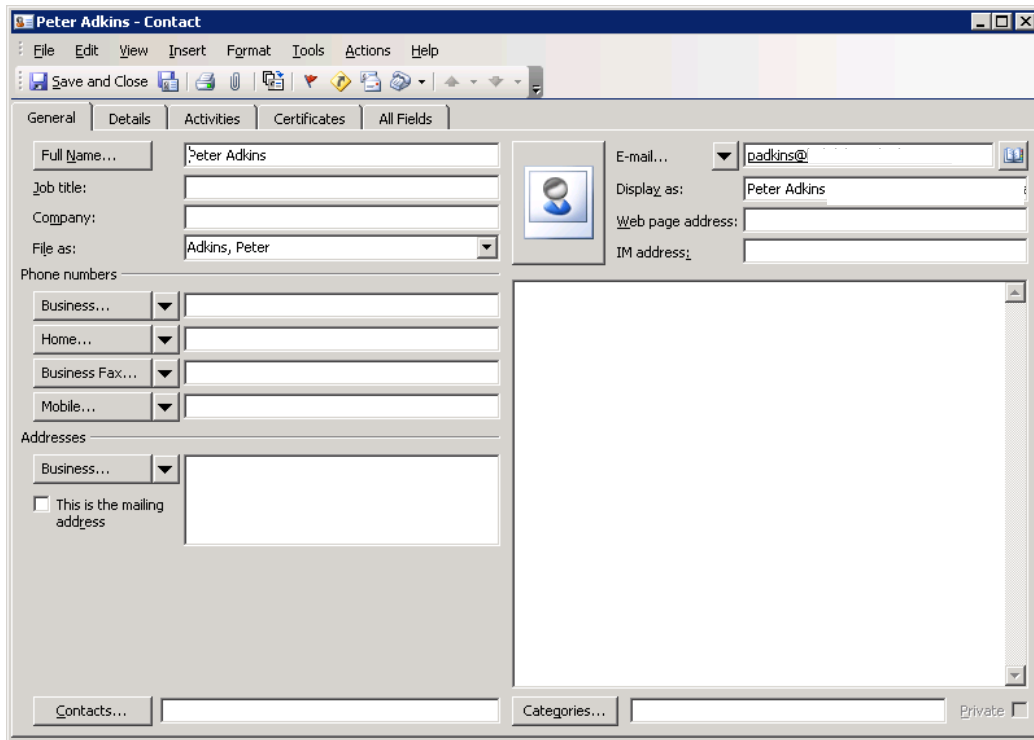
You will see from this example that Russell Hunter’s individual keys were issued by SecureNet Health OCA.

Click the “Intermediate Certification Authorities” tab, and check that “SecureNet Health OCA” is listed there. If the issuing authority is not listed here, download the appropriate certificate from the Public Directory website, as detailed below in Appendix A.

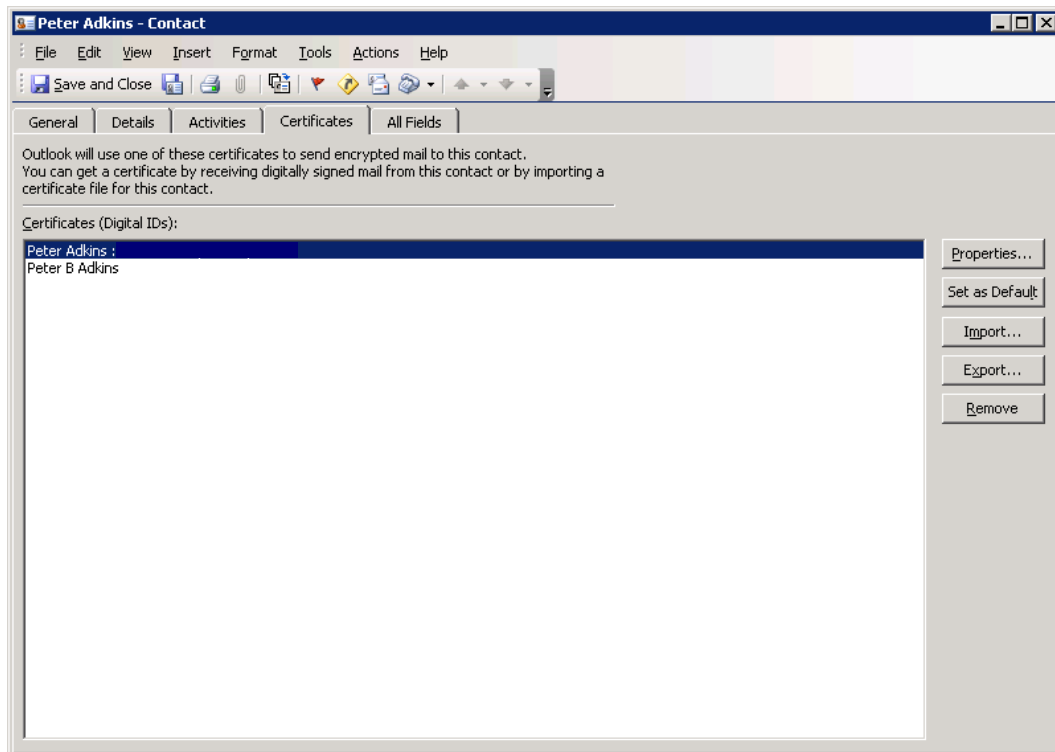
(Note: As at late 2007, individual and location certificate appear to be issued by two separate Intermediate Certification Authorities – SecureNet Health OCA and Medicare Australia Organisation Root Authority. It is worth installing both these root certificates so that all individual certificates are automatically trusted.)

PART 2. Installing a Contact's individual encryption and signing certificates.

- Open the contacts entry in Outlook.



Click Certificates. If two certificates are listed under the Certificates tab, it is likely that their encryption and signing keys are already installed.



If no certificates are installed, go to the Public Directory website, to locate and download your contact's certificates –

[Certificates Australia Certificate Search - Healthcare Public Directories](http://www.certificates-australia.com.au/general/cert_search_health.shtml)

The screenshot shows the 'Certificates Australia - Healthcare Public Directory Search' page. The browser title is 'Verizon Business / Cybertrust : Certificates Australia - Microsoft Internet Explorer provided by SEAGP (Brisbane)'. The address bar shows 'http://www.certificates-australia.com.au/general/cert_search_health.shtml'. The page features a Verizon Business logo and navigation links for PRODUCTS, CUSTOMER SERVICE, and ABOUT US. A 'Quick Links' sidebar on the left lists various certificate categories like 'Certificate Search', 'Medicare Australia PKI', 'SecureNet Limited PKI', 'SecureNet Trusted Services VPN CA', 'Certificates Australia PKI', and 'General'. The main content area is titled 'Healthcare Public Directory Search' and contains a search form with fields for 'First Name', 'Surname / RA Number', 'Email address', and 'Organisation name'. There is also a dropdown for 'An Australian State' set to 'Any' and a 'Search!' button. Below the form, there is a link for 'Click here for search tips'. A section titled 'What this page provides' explains that users can search for registered persons and download their public digital certificates. A 'How to use this page' section provides instructions on how to enter search criteria and use the search button. A 'Note' at the bottom advises users to choose the appropriate link in the left column for downloading certificates or CRLs.

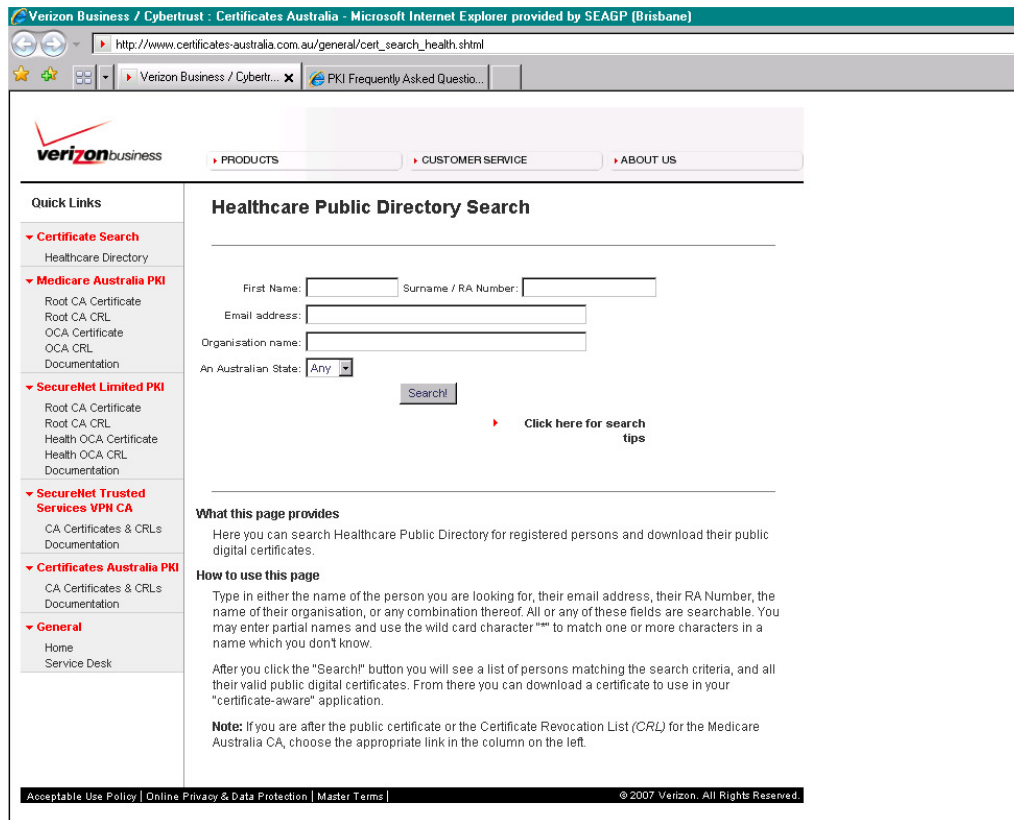
Enter your contact's details, click Search.

The screenshot shows the 'Certificates Australia - Matching Certificates' page. The browser title is 'Verizon Business / Cybertrust : Certificates Australia - Microsoft Internet Explorer provided by SEAGP (Brisbane)'. The address bar shows 'http://www.certificates-australia.com.au/cgi-bin/ldapnsearch_health.pl'. The page features the same Verizon Business logo and navigation links as the search page. The 'Quick Links' sidebar is identical. The main content area is titled 'Matching Certificates' and includes a note: 'Note: A maximum of 50 entries will be displayed.' Below this, the search results for 'cn=Peter Adkins : padkins@' are shown. Two certificate entries are listed, both valid from 19 Sep 2007 to 19 Sep 2012. The first is a 'Non-Repudiation Certificate' and the second is an 'Encryption Certificate'. A question is asked: 'What MIME-type should we use when transmitting the end-user certificate?' with two radio button options: 'application/pkix-cert' (selected) and 'application/x-x509-email-cert'. A 'Get certificate' button is located below the options.

You will note that there are two certificates to be downloaded – a signing certificate and an encryption certificate. Click Get Certificate. Save the signing file to an appropriate folder on your computer, then click the next radio button in the screen above, to select the encryption certificate. Again click Get Certificate to download and save the encryption file to the same folder. Return to the certificate window of the contact. Double click the Import button, open the folder where these files have been saved, and double click both those files separately to install both the encryption and signing keys of your contact. You should now be able to send secure emails to that contact.

Appendix A: Downloading and Installing Intermediate Certification Authority Certificates.

Go to [Certificates Australia Certificate Search - Healthcare Public Directories](http://www.certificates-australia.com.au/general/cert_search_health.shtml)



Verizon Business / Cybertrust : Certificates Australia - Microsoft Internet Explorer provided by SEAGP (Brisbane)

http://www.certificates-australia.com.au/general/cert_search_health.shtml

Verizon Business / Cybertrust... x PKI Frequently Asked Questio...

verizonbusiness PRODUCTS CUSTOMER SERVICE ABOUT US

Quick Links

- ▼ Certificate Search
 - Healthcare Directory
- ▼ Medicare Australia PKI
 - Root CA Certificate
 - Root CA CRL
 - OCA Certificate
 - OCA CRL
 - Documentation
- ▼ SecureNet Limited PKI
 - Root CA Certificate
 - Root CA CRL
 - Health OCA Certificate
 - Health OCA CRL
 - Documentation
- ▼ SecureNet Trusted Services VPN CA
 - CA Certificates & CRLs
 - Documentation
- ▼ Certificates Australia PKI
 - CA Certificates & CRLs
 - Documentation
- ▼ General
 - Home
 - Service Desk

Healthcare Public Directory Search

First Name: Surname / RA Number:

Email address:

Organisation name:

An Australian State:

► [Click here for search tips](#)

What this page provides

Here you can search Healthcare Public Directory for registered persons and download their public digital certificates.

How to use this page

Type in either the name of the person you are looking for, their email address, their RA Number, the name of their organisation, or any combination thereof. All or any of these fields are searchable. You may enter partial names and use the wild card character "*" to match one or more characters in a name which you don't know.

After you click the "Search!" button you will see a list of persons matching the search criteria, and all their valid public digital certificates. From there you can download a certificate to use in your "certificate-aware" application.

Note: If you are after the public certificate or the Certificate Revocation List (CRL) for the Medicare Australia CA, choose the appropriate link in the column on the left.

Acceptable Use Policy | Online Privacy & Data Protection | Master Terms | © 2007 Verizon. All Rights Reserved.

Scroll down in this window, then click and download and save both the Medicare Australia Organisation CA Certificate, and the Medicare Australia Root CA Certificate.



Medicare Australia Root CA Public Certificate

What MIME-type should we use when transmitting the CA certificate?

application/pkix-cert (usually accepted by Internet Explorer and 3rd Party PKI Applications)

application/x-x509-ca-cert (usually accepted by Netscape)



Install both of these certificates by double clicking on the downloaded file, then click Open and then click Install Certificate. Windows will automatically insert them in the correct place on your computer.

All individual certificates issued by Medicare will now be automatically trusted by your computer.

Glossary:

Public Key Infrastructure (PKI) is an arrangement that binds public keys with respective user identities by means of a certificate authority.

Certificate authority (CA) is an entity which issues digital certificates for use by other individuals or organisations.

Root Certificate A Certificate Authority can issue multiple certificates in the form of a tree structure. A root certificate is the top-most certificate of the tree. All certificates below the root certificate inherit the trustworthiness of the root certificate.

Public Key The public key encrypts the message and only allows the holder of the Private key to decrypt it. The public key combines the user token (smart card or i-key) and the pass phrase typed in by the user to send the message.

Private Key The private key decrypts the encrypted message (ensuring confidentiality), ensures that the message has not been tampered with and allows the message to be electronically signed to ensure authenticity and also proof that the message has been sent.

Public Directory Found at [Certificates Australia Certificate Search - Healthcare Public Directories](#)
The public directory allows users to look up and download other health provider's public key (digital certificate). The directory search facility has a number of practical limitations and improvements to the directory are being sought by SEA-GP (Brisbane).

March 2009