Australian Government
Australian Customs Service

CUSTOMS TYPE 3 CERTIFICATE 2012 INSTALLATION GUIDE

The Type 3 digital certificate used by the Australian Customs and Border Protection is due for a renewal.

This means that users who send messages to the Integrated Cargo System (ICS), using electronic data interchange (EDI) software, will need to rollover to the new Customs Type 3 certificate.

This rollover does not affect any digital certificates that you or your organisation have purchased.

The rollover will occur on Wednesday 27 June 2012 at **00:01 am,** with a scheduled outage between **00:01am and 04:00 am**.
You must configure your Secure EDI application (SEDI) to accept the new Customs certificate on or after this time.

I do not use the Customs version of SEDI
Although Customs cannot provide advice on how to make these changes in applications other than SEDI, the following instructions should provide users with the general information they need.
For support of these applications, clients are advised to contact their software supplier.

What do I need to do?
Users of Type 3 certificates for system-to-system communication will need to configure their SEDI application to replace the Customs certificate with a new one.

The new certificate can be downloaded from the Cargo Support website as a Zip file:
http://www.cargosupport.gov.au/site/page5952.asp

The .zip file contains the .cer file:

- CCFEmailGateway20140530_PEM – the new Customs Type 3 certificate

How do I replace the Customs Certificate in my SEDI?
The SEDI application can be used in either Graphical User Interface (GUI) mode or via a Command Line Interface (CLI) mode.
The following instructions will guide you through the rollover process for either method of operation.

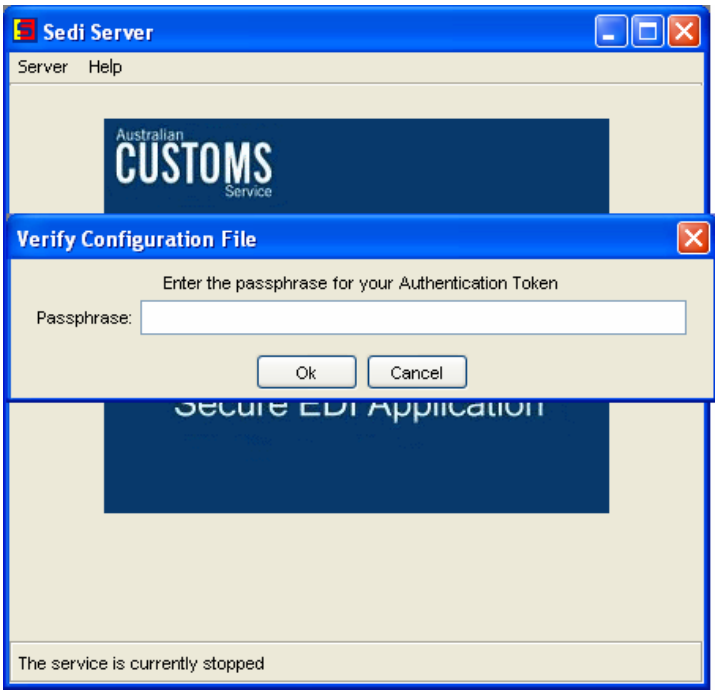
Rollover of the Customs Type 3 Certificate using GUI

1. Ensure that the new Customs Type 3 certificate has been saved to a location that is accessible from the machine where you have SEDI installed. Place the new certificates into the following directory:

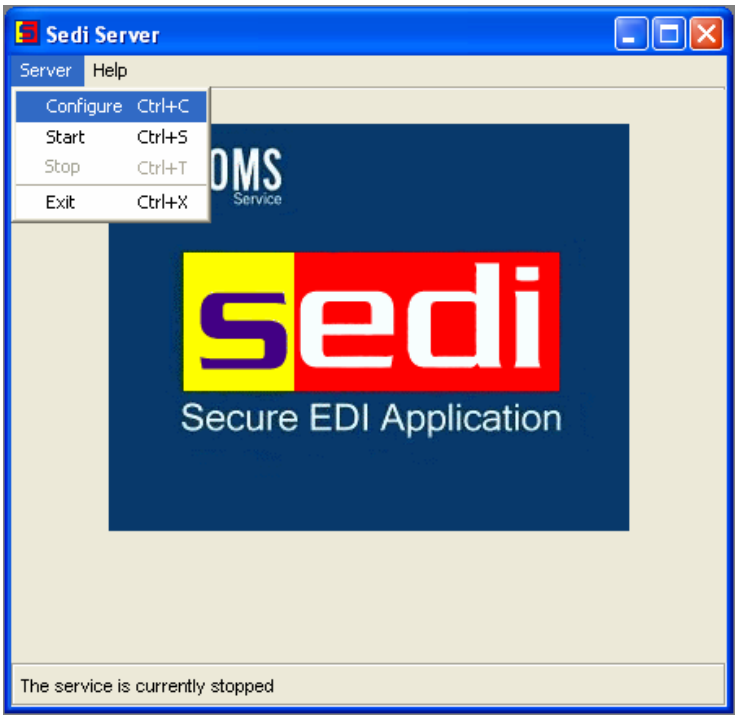
   C:\Program Files\Customs SEDI\CertsAndKeys.

   Note: This is the default location. If you have not installed SEDI into the default location you will need to locate your SEDI installation directory.

2. Access the SEDI Server. You may be prompted to enter your SEDI passphrase.
   If it is already processing messages then you will have to stop it by selecting from the menu 'Server' → 'Stop'.

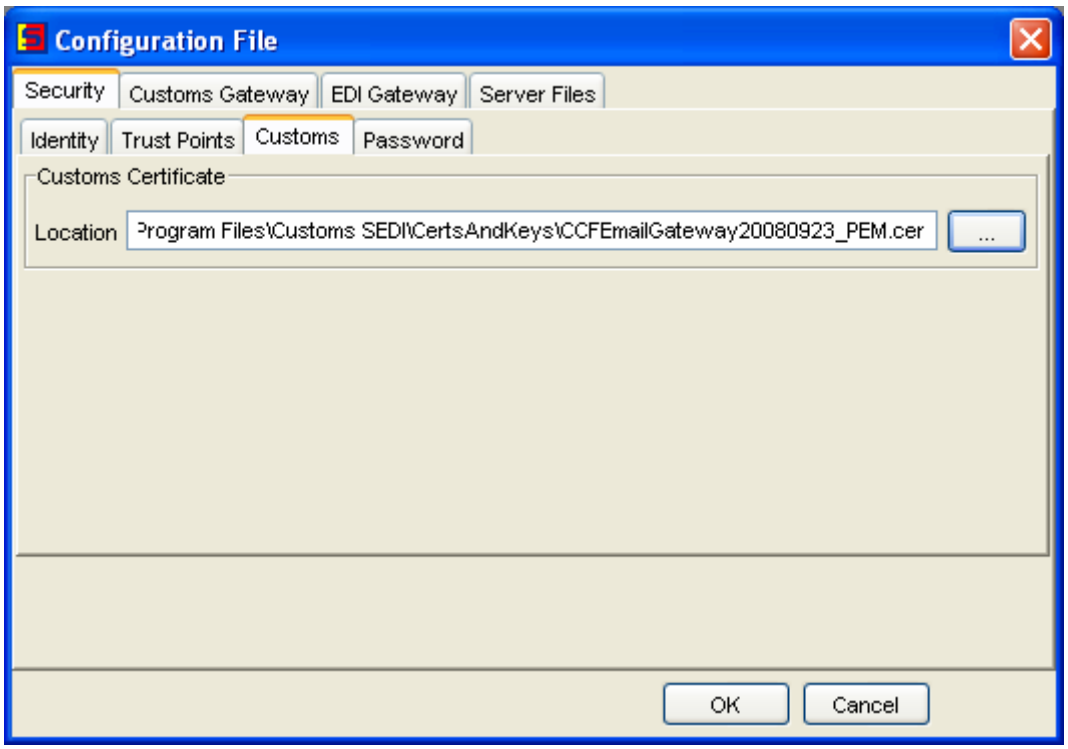


3. Enter the SEDI passphrase and click the OK button.
4. From the menu select 'Server' → 'Configure'.



5. You may be prompted to enter your SEDI passphrase again.
   Note that the 'Configure' menu item is not accessible if the server is still running and processing messages.

The Configuration File window displays.



6. Click on the 'Security' tab, then click on the 'Customs' tab.
7. Use the  (browse) button and navigate to the location of the new Customs certificate file.
8. Select the file and click 'Open'. You will be returned to the Customs tab with the new certificate listed in the Location field.

You will now be able to start the SEDI server and send EDI messages to Customs.
Repeat the above process for all instances of SEDI.

Rollover of the Customs Type 3 Certificate for CLI users of SEDI.

1. Obtain the new Customs Type 3 certificate. It can be obtained from the Customs website at **http://www.cargosupport.gov.au/site/page5952.asp**

2. Extract the new certificates from the .zip file. The .zip file contains the .cer file:
   - CCFEmailGateway20140530_PEM.cer – the new Customs Type 3 certificate

3. Place the new Customs Type 3 certificate into the following directory:

   C:\Program Files\Customs SEDI\CertsandKeys.

   Note: This is the default location. If you have not installed SEDI into the default location you will need to locate your SEDI installation directory.

4. Stop the SEDI Server and open the file sedi.xconf with a simple text editor such as Notepad.

5. Edit the following lines in the configuration file:

   <confidentialityCertificate file="CertsandKeys**Insert New Customs certificate file name here**"

   This line is located about 7 lines up from the bottom of the sedi.xconf file.
   Only change the section in bold. Do not confuse this with the line that begins: <confidentiality key

pair.>

For Example:
Replace “CCFEmailGateway20120529_PEM.cer” with “CCFEmailGateway20140530_PEM.cer”.

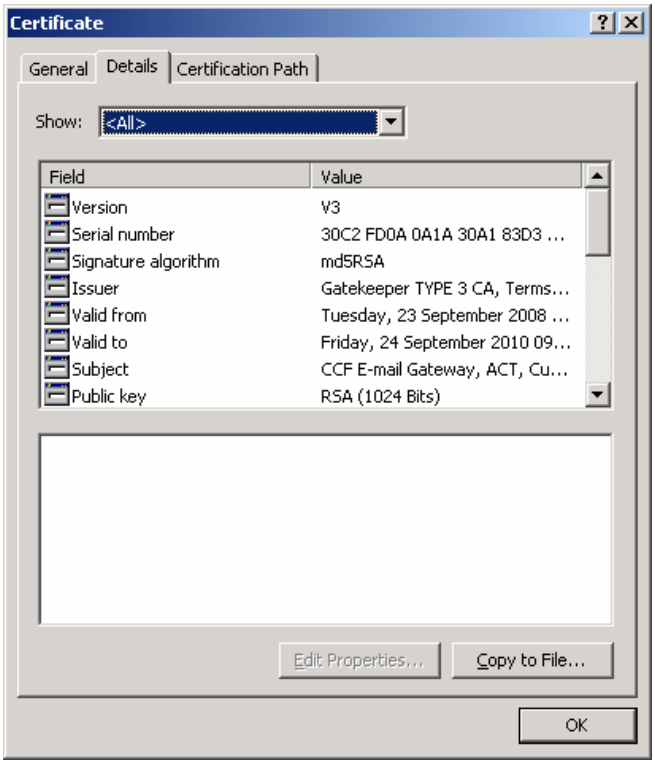
6. Save and close the file. You will now be able to start the SEDI server and send EDI messages to Customs.

Need help or further information?
Contact Cargo Systems Support via email on cargosupport@customs.gov.au or phone 1300 558 099.

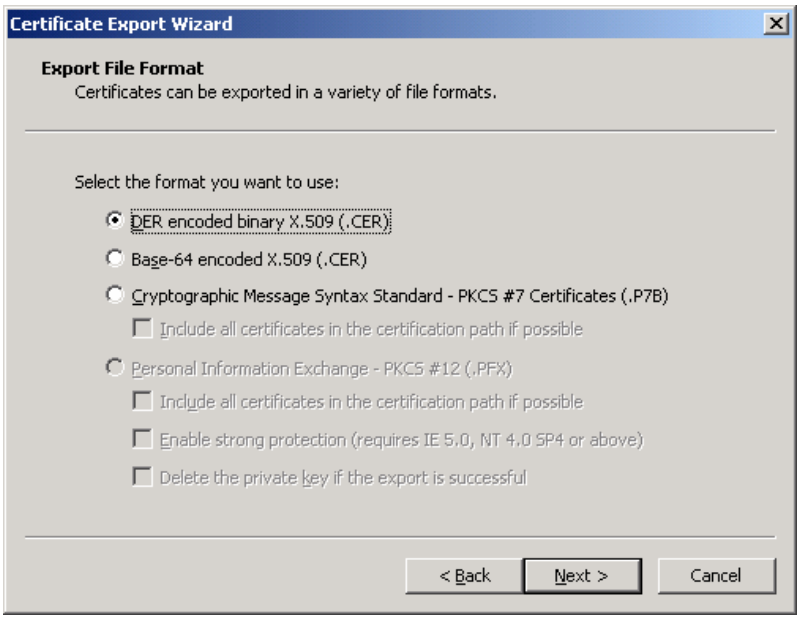
Need a different certificate format for your own EDI application?

Some EDI applications may require a certificate file that is in a different format. The format of the certificate supplied by Customs is what is known as a “PEM” or “base64” format and will work with Customs version of SEDI.
If you require a “DER” format, which is also known as a binary format, then follow the steps below to convert the certificate format.

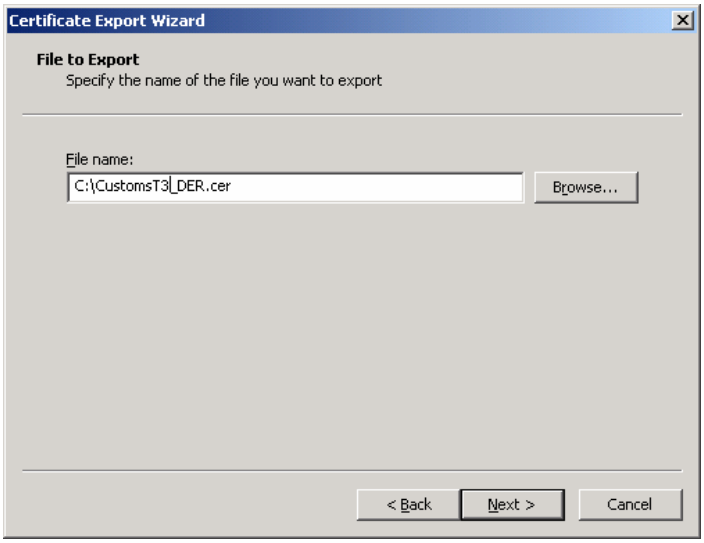
1. Copy the original Customs Type 3 certificate file on to a computer running Windows 2000/XP/Vista and double-click the file. A certificate dialog box will pop up. Select ‘Details’ tab and press the ‘Copy to File…’ button.



2. The ‘Certificate Export Wizard’ will pop up. Follow the prompt.
In the ‘Export File Format’ screen select ‘DER encoded binary X.509 (.CER)’ then press ‘Next’.



3. In the ‘File to Export’ screen enter the path and filename to where you would like to save your DER format Customs Type 3 certificate then press ‘Next’.



4. Press ‘Finish’.

The new file can now be copied to your EDI application for use.