Digital Certificates

Digital Certificates are required if you wish to send EDN's and communicate with Customs from EdiSoft.

When a message is signed and encrypted using this method, nobody but the intended recipient can access the message. This protects the integrity of the information as well as preventing any tampering by viruses.

Before applying for Digital Certificates, you should configure EdiSoft to use Internet Mail. This is done in 'Setup' using the 'Internet Setup' tab. **Make sure this is working properly**. The e-mail address you use for EDI Messaging will be associated with the Digital Certificates issued to you and changing it later will require changes to your registration. Much messing around and expense.

Digital Certificates are obtained from a 3rd party issuing authority. Digicert is the only one approved by Customs. The requirements for EDI Messaging as defined by Customs are.

- ABN-DSC (AO) / Signing Certificate
- Device/Type3 Certificates (This is the cert that EdiSoft will use)

EdiSoft uses 2 separate Digital Certificates. The first Certificate (the ICS Digital Certificate) will be supplied with EdiSoft. This Certificate is common for all users. Any changes to this will be included in future updates of EdiSoft. Under normal circumstances you should not have to worry about the ICS Digital Certificate.

The second Digital Certificate is the user Digital Certificate. This Digital Certificate is unique for each site - which you will need to apply for from DigiCert (see step 1 below).

In short - the following steps will need to be followed to use Digital Certificates in EdiSoft. **Please note that Steps 1 and 2 are independent of EdiSoft. You will need to consult either DigiCert or Customs if you have questions regarding these instructions.** Applying for and installing the Digital Certificates can be a daunting task, as can adding the Certificates to the customs web-based system. We have received a number of concerns from users as to the complexity of this task and we can emphasize with you. Unfortunately, these two tasks are requirements from Customs and outside of our control. We recommend that you use an IT Consultant or someone who is tech-savvy to complete these first two steps.

Step 1: Apply and Purchase Digital Certificates from DigiCert

1) Navigate to the following website: - https://gatekeeper.digicert.com/customs

2) Enter your ABN into the field they provide and click 'Begin'.

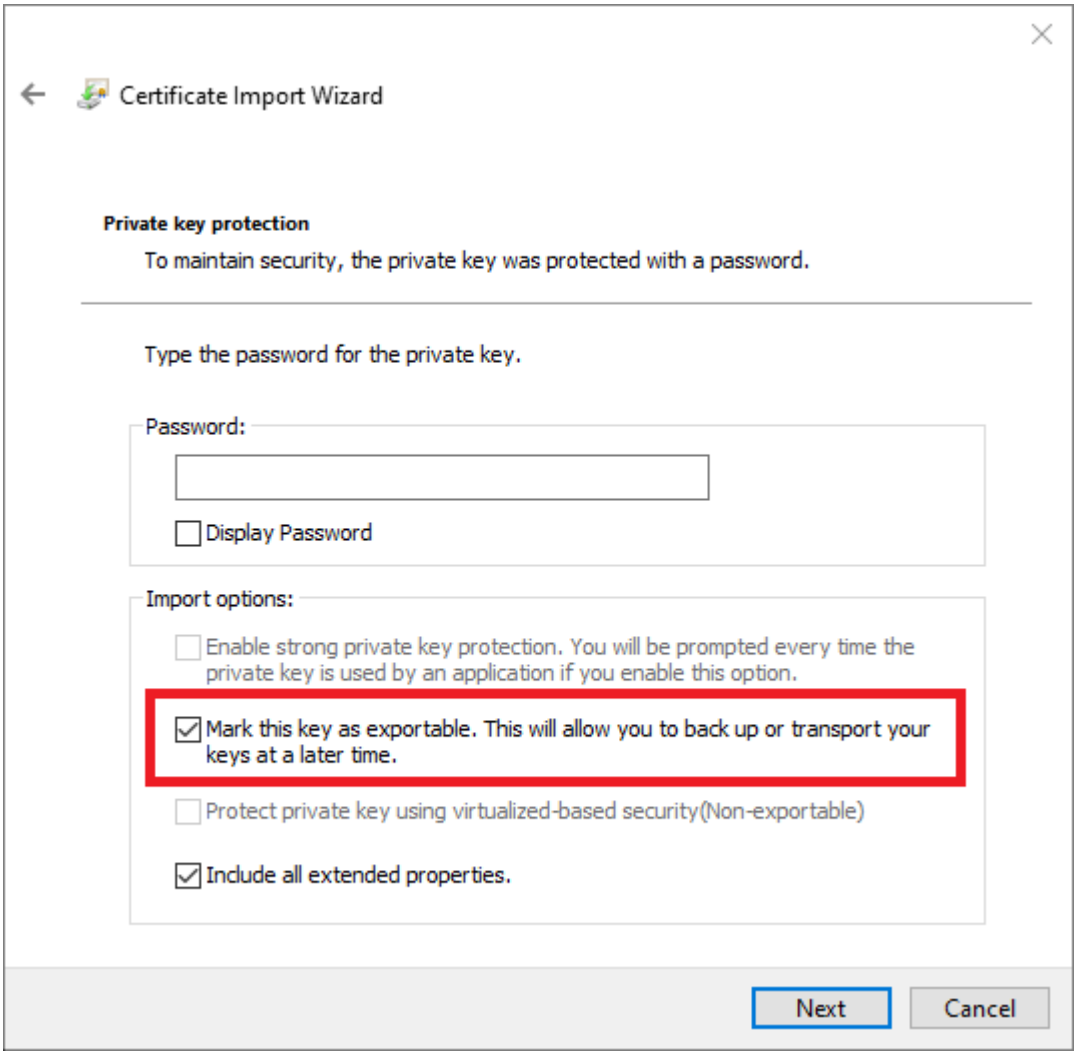
From here you should be able to apply for a Manager Certificate (required to obtain a Device Certificate) and a Device Certificate. If your Certificate's just need renewing rather than creating a new account, this should also be possible from this website.

Note: '*Manager' Certificates are sometimes called 'Signing' or 'DSC ABN' Certificates. 'Device' Certificates are often called 'Type 3' or 'Type III' Certificates.*

When you receive the Certificates from DigiCert they will be saved into the Windows Certificate Store on the workstation that downloaded them.

Note: When installing the Digital Certificates from DigiCert - make sure you tick the field 'Mark this key as exportable', as shown below! (By default - this will **not** be turned on). This will allow you to export your entire Certificate to another computer if upgrading computers in the future. You will also require the private key to encrypt and decrypt messages!

Note: Make sure that you install the Certificates onto a work station that has EdiSoft installed (as you will use EdiSoft on this workstation to link to later). This is only necessary while doing the setup. After you link to EdiSoft (step 3) any workstation will be able to utilise the Digital Certificate that has been linked to EdiSoft.



Note: After your Certificates are installed, we recommend backing them up on another device or share drive in case your computer crashes. To do this, use the 'Export' option in the Windows Certificate Store and use the option to ***include*** the private keys.

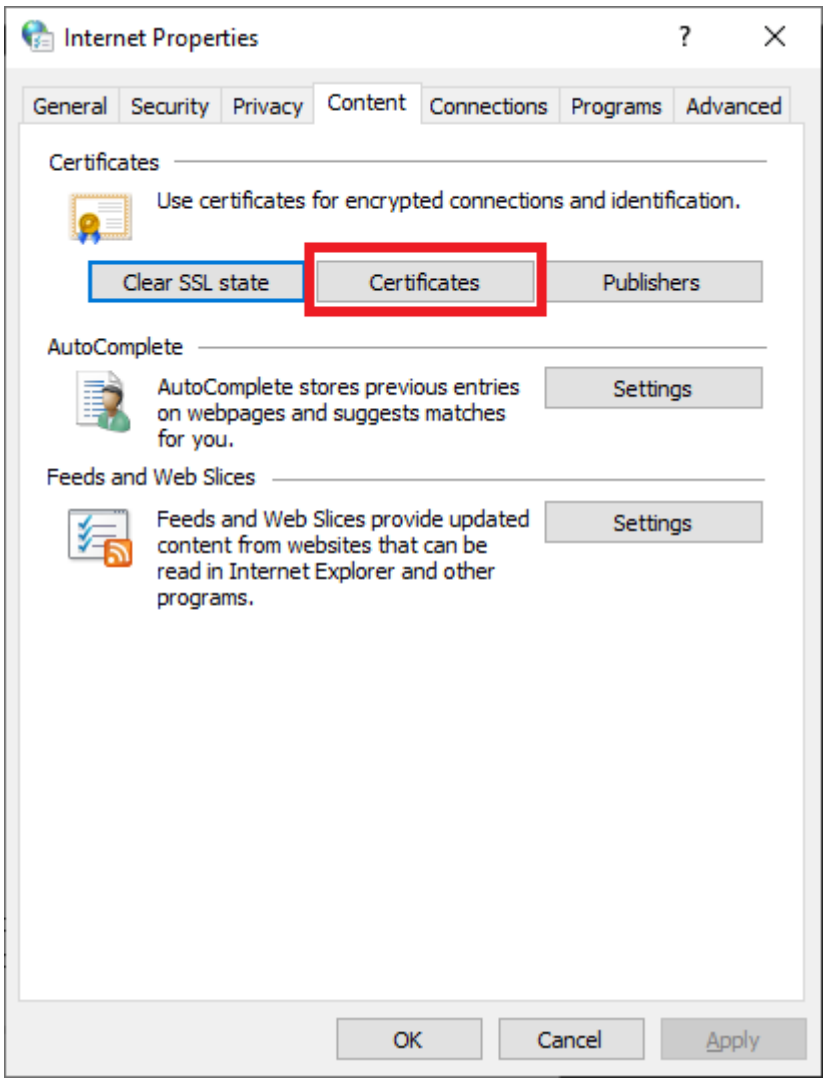
Step 2: Upload the Device Certificate to Customs

Now that you have your user Digital Certificate installed on your workstation (it has not yet been installed into EdiSoft) - you will need to advise customs of your new Certificate. To do this, you will need to use the Customs ICS Webpage to add your Certificate and details. This process is quite complex and can change. You may need to contact Customs for more information on how to do this and to obtain the relevant instructions.

The Instructions as per when this document was last updated are below:

1) Navigate to the Windows Certificate Store. (found in Internet Explorer -> Tools -> Internet Options)

2) When in Internet Options, navigate to the 'Content tab' then click on 'Certificates'. (shown below)



4. From there, you should be able to find your updated Certificate and export this to your workstation anywhere. This time however, you will export the Certificate **without** ticking 'include private key'. (export the certificate as a **".cer"** file)

5. Remember where you saved the Certificate file, and navigate to the 'Customs Interactive' website. (https://www.ccf.customs.gov.au/)

6. Sign in using your 'Signing / Manager / ABN DSC' Certificate when prompted.

7. Navigate to ‘Identity Manager’ and find the ‘Add a User or Device’ Certificate Upload option.

8. Browse and find your **“.cer”** file recently created and Upload this Certificate to Customs. You should now be ready to Install the Certificate into EdiSoft.

Note: Your Digital Certificate MUST be correctly registered with Customs before you will be able to use it within EdiSoft. Failure to do this will lead to error messages such as unknown crypto errors, unable to find a matching Digital Certificate, or potentially fatal error messages on your EDNs.

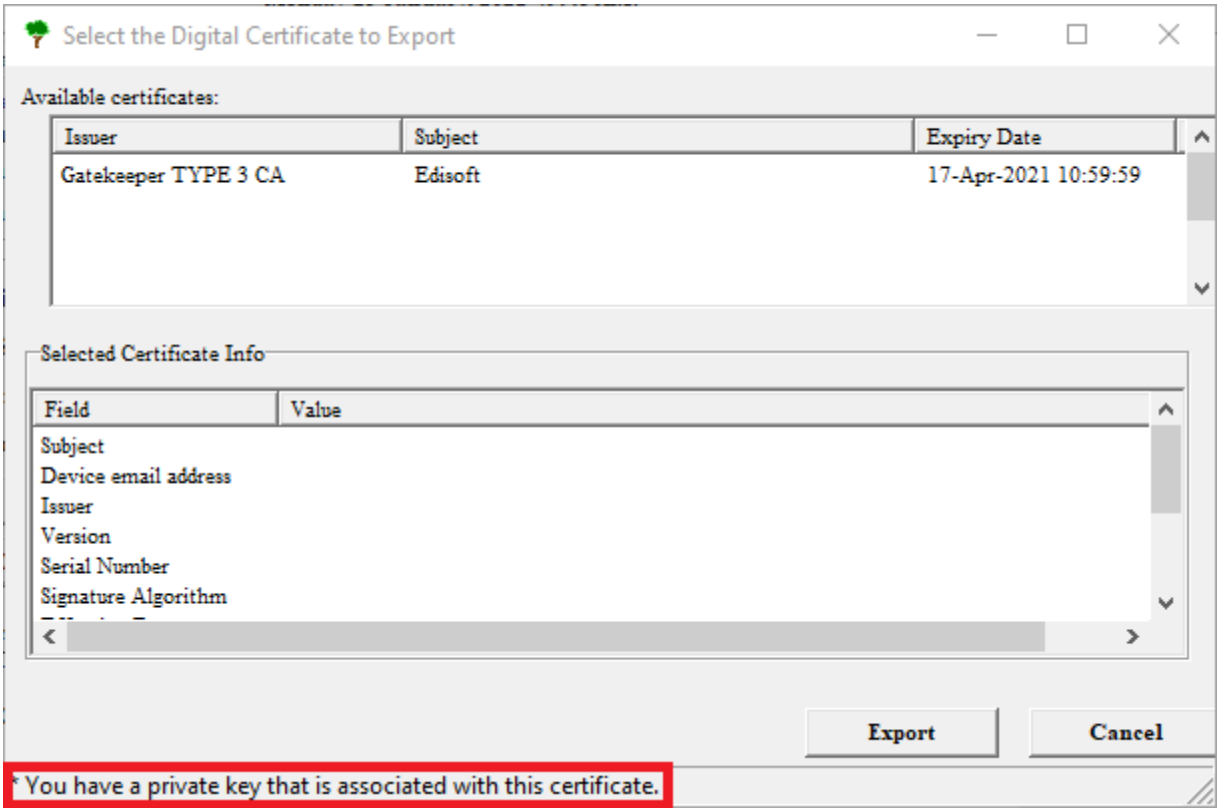
Step 3: Installing the Certificate into EdiSoft

The final step, is to link EdiSoft to the Digital Certificate, so EdiSoft can use this to send messages to customs. To do this:

1. Open EdiSoft, and click on the SETUP menu item. Navigate to the ICS tab.

2. Click on the "Export Certificate from Windows Certificate Store" button in the ‘Setup’ -> ‘ICS’ tab. A list of Certificates will be displayed.

3. Select the Device/Type 3 Certificate that relates to EdiSoft. (The subject will give you a clue). Make sure that you take note of the expiry date, so you don't accidently import the wrong Digital Certificate. (The Digital Certificate must include the ‘private key’, and must not be expired)



4. Click on the Export Button. You may need to provide a password that you use for this Digital Certificate. Once entered - EdiSoft should be linked to your Digital Certificate, and should be ready for use.

Common Problems:

After renewing your Digital Certificate, you may find that Customs is not receiving your emails. If this is the case, one of the following has most likely occurred:

The wrong serial number has been inserted at Customs:

This can occur, as the form that you send to customs is a fax form. Human errors can be made either while filling in the form, or when Customs types in the serial number at their end. Either way, this can be corrected by copying and pasting your serial number from Windows into an email, and sending to Customs asking them to confirm that they have the correct Certificate installed. (Because you can copy and paste it into an email, and they can copy it from your email into their system, it eliminates human error)

The wrong Certificate has been installed/linked to EdiSoft:

Repeat step 3 above, to make sure that you have installed a Type 3 Digital Certificate that is valid, and that the Certificate you installed into EdiSoft matches the Certificate that you informed customs of in step 2.

An incorrect email address was used for your Device/Type 3 Digital Certificate:

EdiSoft requires its own unique email address. The Device/Type 3 Digital Certificate should be registered to the same email address. It is also helpful to verify with customs that they have the same email address in their system that you use for EdiSoft.

An uncollected response from Customs exists on the old Certificate:

It may be possible that a reply Customs ICS have sent could be using the previous Digital Certificate, and EdiSoft on the latest Certificate is now not able to decrypt it. To fix this issue, you could try the following the below steps:

1. Go to 'setup' -> 'internet setup' -> then click 'Test POP3 Connection'

2. From here you should see all the replies that EdiSoft is waiting to receive, clear all the messages out that are from @ccf.border.gov.au addresses

3. Once all the messages have been cleared, try duplicating the failed EDN and sending the new one.

4. Wait a few minutes and then try running another 'Test POP3 Connection' to see if you have received any replies from the recently sent EDN. If so, try running another 'Transmit & Receive' to see if the error is resolved

More information about the ICS Digital Certificate

You will also need to use the Public Key Certificate from Customs. This is the Certificate that is installed for you automatically in the **...\Woodwind\Data\Digital Certs** directory when you do an update but if necessary, this Certificate can be downloaded from the Customs website (https://www.homeaffairs.gov.au/) and copied to the **...\Woodwind\Data\Digital Certs** directory. When you need to link the Customs Public Key Certificate (also a Device / Type 3) then click on the **"ICS Digital Certificate**" in the Setup/ICS tab. Use this same procedure when the Customs Public Key expires and you need to "roll-over" to the new one.

All these Certificates should be installed in the **...\Woodwind\Data\Digital Certs** directory, that is where EdiSoft expects to find them. You should also copy them onto a diskette or CD and put them in a safe place where you can find them. If you have a hardware crash, they will be needed.

When this has been done EdiSoft will use these Certificates to Sign and Encrypt the messages going to Customs ICS and EdiSoft will also Decrypt messages coming back from Customs ICS. It is all done for you.

PKI Business Rules (as defined by Customs)

Batch use of CMR Systems

Any client who registers with Customs to use the ICS via EDI must have a Digital Certificate.

1. Digital signature and encryption of interchanges shall conform to Customs & Gatekeeper standards and be issued by a Gatekeeper Accredited Certification Authority (CA).

2. All interchanges are to be Digitally signed and encrypted by the creator, using a valid Customs & Gatekeeper-compliant Certificate.

3. Organisations with an ABN will use an ABN - DSC Certificate or higher.

4. Organisations with an ABN - DSC Certificate may hold a Device / Type 3 Certificate, for Server-to-Server communications.

RESOURCES:

EDISOFT HELPDESK
Website: www.woodwindsys.com.au
Email: helpdesk@edisoft.com.au

DIGICERT HELPDESK
Website: https://gatekeeper.digicert.com/support
Email: gk_validation@digicert.com
Phone: 03 9914 5600

CUSTOMS – CARGO SUPPORT
Website: https://www.abf.gov.au/help-and-support/ics/integrated-cargo-system-(ics)/using-the-ics/contact-cargo-systems-support
Email: cargosupport@border.gov.au
Phone: 1300 558 099