

Digital Certificates are used to ensure secure communications when using Internet Mail. 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. VeriSign is the only one approved by Customs. The requirements for EDI Messaging as defined by Customs are.

- ABN-DSC (AO)
- Device Type3 Certificates (What 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 verisign (see step 1 below).

In short - the following steps will need to be followed to use Digital Certificates in Edisoft.

### **Step 1 - Apply to VeriSign for Digital Certificates & Install into Windows.**

Your Authorised Officer (AO) will need to apply (or reapply) to VeriSign for the ABN-DSC (AO) certificate. Once you have this, the authorised officer will be able to apply (or reapply) for the Device Type 3 digital certificate. These digital certificates are independent of edisoft - and will need to be installed into your Windows Certificate Storage first, before edisoft can use them.

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

**Note: When installing the digital certificates from Verisign - 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.

**Password**

To maintain security, the private key was protected with a password.

---

Type the password for the private key.

Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

For assistance installing digital certificates into windows (Step 1), please contact Verisign on 03 9674 5500.

### **Step 2 - Informing Customs of your Digital Certificate**

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 fill out the customs B323 Digital Certificate Registration form (which can be downloaded from: [http://www.customs.gov.au/webdata/resources/files/B323\\_CCF\\_digital\\_certificate\\_and\\_client\\_registrations.pdf](http://www.customs.gov.au/webdata/resources/files/B323_CCF_digital_certificate_and_client_registrations.pdf))

Your serial number can be obtained by the following:

Open up Internet Options from your computers Control Panel.

Click on the Content Tab, and press the **Certificates** button.

Locate your **current** Type 3 digital certificate (using the expiration date so you don't go to an expired one), and click on the VIEW button. Then click on the DETAILS tab. Your serial number will be provided in this windows.

After faxing this form to Customs, you should receive an email response, confirming your digital certificate has been updated in their database.

### **Step 3 - Linking Edisoft to the digital certificate.**

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 should give you a clue). Make sure that you take note of the expiry date, so you don't accidentally import the wrong digital certificate. (The digital certificate you choose must be a Type 3, 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 will be linked to your digital certificate, and 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 type 3 digital certificate**

Edisoft requires it's own unique email address. The 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.

### **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 <http://www.customs.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 a ABN - DSC certificate or higher.
4. Organisations with a ABN - DSC certificate may hold a Type 3 certificate, for server to server

communications.