



COMMUNICATING ELECTRONICALLY WITH CUSTOMS.

This fact sheet deals with communicating electronically with Customs under the Integrated Cargo System (ICS).

The main elements covered by this fact sheet are:

- communication and connection options
- public key infrastructure (PKI)
- digital certificates
- evidence of identity (EOI)
- technical requirements for communicating with Customs.

COMMUNICATION AND CONNECTION OPTIONS

Legacy systems such as COMPILE, EXIT, Air Cargo Automation (ACA) and Sea Cargo Automation (SCA) operated through a closed communication gateway. With the implementation of the ICS, Customs now uses an open system based on Internet protocols. This provides clients with a number of options for communicating with Customs. As a result, a new security environment was required. The secure gateway to the ICS is known as the Customs Connect Facility (CCF).

There are two options for communicating with the ICS:

1. Customs Interactive

The Customs Interactive facility allows real time web-browser interaction with the ICS. This facility provides:

- a range of enhanced functions for lodging import and export declarations and cargo reports
- facilities to amend previous electronic data interchange (EDI) messages
- access to the diagnostic facility to verify the status of transactions in the ICS
- the ability to update the client register.

Advantages and disadvantages of Customs Interactive

Advantages

- Minimal software costs.
- Access to Customs online forms.
- Diagnostic facility available to check the status of cargo.
- Minimal training costs, as training support products are available from Customs.
- ICS client registration facility is only available through Customs Interactive.
- This facility includes a search function.

Disadvantages

- Internet service levels may require upgrading.
- Information cannot be held or saved in the system during work in progress for export reports.
- Electronic records cannot be stored on the users' system.
- No print functionality available for forms in the exports release; although a 'print screen' option may be utilised.

2. Electronic data interchange

Electronic data interchange (EDI) is a class of industry specific message formats used in electronic commerce. Customs Software Developers Guide details the messaging standards, specifications and the rules being applied by Customs to messages used by the ICS. There are many EDI software packages commercially available to industry; the Cargo Support website contains a list of relevant software developers.

Clients may connect via the Internet for EDI, or alternately, clients with high volumes may find it more cost effective to have a direct connection to Customs. Clients who are interested in a direct connection should read the Direct connections to Customs Connect Facility (CCF) fact sheet.

Those clients that arrange to purchase their own software through a software developer should seek advice on appropriate connection options either from the software developer or Customs.

Advantages and disadvantages of EDI

Advantages

- Ability to store records.
- Declarations and cargo reports can be held, saved, amended, printed and retransmitted.
- Ability to batch transactions.
- Option for other business enhancements to software, such as accounting and auditing functions.

Disadvantages

- Higher set-up and maintenance costs.
- Software reliability and impact of downtime.
- Potential costs of training staff.

PUBLIC KEY INFRASTRUCTURE

What is public key infrastructure?

In line with the Commonwealth Government's Gatekeeper strategy for supporting the security of online transactions with government, public key infrastructure (PKI) is being used to provide Customs and Customs clients with assurance that messages received from each other are genuine, and that the sender can be legally identified. PKI is the security mechanism for communications in a global and open network. It uses encryption to protect transmitted data from or to Customs. A digital certificate and associated 'keys' verify who is communicating and the integrity of the communicator's data. The digital certificate is the electronic equivalent of the hand written signature and sealed envelope process.

The security features of PKI include:

- authentication (knowing who the message is from)
- integrity (knowing it has not been tampered with)
- non-repudiation (knowing that the sender cannot deny having sent it)
- confidentiality (knowing that no unauthorised reading has occurred).

DIGITAL CERTIFICATES

What is a digital certificate?

A digital certificate should be considered as an electronic signature of either an individual and/or related entity. The digital certificate exists as a software file and is housed within web-browsers. A digital certificate creates a unique identifier that can be checked by the receiver of information to provide evidence of the sender's identity and confirm that the document (if signed) has not been altered or interfered with.

A digital certificate actually contains two separate certificate parts (each with public and private keys); one for signing (authenticating) and another for encrypting/decrypting electronic messages.

Who needs a digital certificate?

A digital certificate will be required by any organisation or person in the exporting, importing, brokering, forwarding, cargo reporting, cargo carrying/handling and related industries who will communicate directly with Customs electronically.

These include:

- service providers - for example brokerages, cargo reporters, freight forwarders and bureaus
- exporters, importers, and cargo reporters who communicate directly with Customs and who do not use service providers to communicate with Customs - if you use a service provider for some functions (for example to lodge import or export declarations) but intend to communicate directly with Customs for other functions (for example to use the diagnostic facility) you will still need to have a digital certificate
- software developers for the purpose of developing software
- Customs Interactive users.

How many digital certificates will be needed?

All direct electronic communicators will need at least one digital certificate. The number of certificates required by a business will be dependant on the IT setup and the method of communicating with Customs.

For those businesses that plan to use EDI, the software developers who supplied the EDI software will be able to provide advice and assistance.

Types of certificates

There are five types of certificates available from certification authorities (CAs) for communicating with Customs, depending on the nature of the communicator.

Type 1 - grade 2 individual certificates

For users who are operating as an individual, where the digital certificate identifies and authenticates them personally.

Type 2 - grade 2 non-individual certificates

For organisations without an Australian Business Number (ABN), where the digital certificate identifies the organisation and the individual.

Type ABN-DSC grade 2 certificates

For organisations with an ABN (including sole traders and government agencies). The initial certificate will be issued to an authorised officer in the organisation. The authorised officer can then organise for additional certificates to be issued for other individuals within the organisation. These certificates will then be issued by the CA.

Type 3 (device) certificates

The type 3 (device) certificate will not authenticate human entities. This is a device or server-based certificate for organisations whose communications are signed by a server. This will be of direct relevance to businesses that use EDI to communicate with Customs. To obtain a type 3 (device) certificate, an applicant must have an ABN and obtain a type ABN-DSC certificate. The applicant must already have an ABN-DSC certificate in order to apply to the CA for a type 3 certificate.

Type 3 Host (Device) certificates

A Type 3 Host (Device) certificate is for use where your organisation wants a device certificate to be hosted by another organisation, called a host bureau.

You will need a Type 3 Host (Device) certificate if you require a host bureau to:

- communicate import declarations to Customs on your behalf
- host your digital certificate and private keys.

To obtain a Type 3 Host certificate you must first obtain an ABN-DSC Authorised Officer certificate. You must also have registered your ABN DSC details with Customs.

For more information about Type 3 Host (Device) certificates, go to the 'bureaus' page on the Cargo Support website, located at <http://www.customs.gov.au/site/page.cfm?u=5608>.

Customs expects that most clients who communicate via EDI will use type 3 (device) certificates. As these clients will also be ABN holders they will require a nominated employee within the organisation to be an authorised officer and hold a type ABN-DSC certificate. For businesses that plan to lodge import declarations in the ICS, the authorised officer must be the owner of the consignment or a licensed broker. That person can then seek additional certificates for others in the organisation who are required to communicate with Customs via Customs Interactive.

In addition to Customs and its clients, the parties involved in the digital certificate process are:

- Certification Authority (CA) - the CA issues digital certificates. The only approved CA currently able to issue digital certificates for communicating with Customs is VeriSign. Further information about VeriSign certificates can be found at www.verisign.com.au
- Registration Authority (RA) - the RA processes evidence of identity. The RA for VeriSign purposes is Australia Post. Details of other Customs and Gatekeeper approved CAs and RAs will be posted on the Customs website as they become available.

EVIDENCE OF IDENTITY

Clients wishing to obtain a digital certificate may need to undertake an evidence of identity (EOI) check at a RA. An EOI check is required for type 1, type 2 and the authorised officer ABN-DSC certificates. To have an EOI check, clients will first need to complete an application for a digital certificate through a Customs approved CA. This will be done electronically. Clients will then need to take the application form and relevant identification documents to the RA (eg, an authorized Australia Post outlet).

A guide to the required identification documents appears at the end of this fact sheet. The application fee for type 1 and type 2 certificates will be paid to the RA at the time of the EOI check.

Getting the certificate

For type 1 and type 2 certificates, once the EOI is verified by the RA, the RA will notify the CA. The CA will then issue a digital certificate to the client via email. Once EOI has been completed, the digital certificate will be available within five working days.

Important: The CA will actually issue each digital certificate via two emails; one for the signature certificate part and another for the encryption/decryption certificate part. Both these digital certificate parts must be downloaded to complete the process. For those obtaining an authorised officer ABN-DSC, a subscriber agreement will need to be completed, signed and returned to the CA prior to the application and issue of digital certificates. The CA will send the subscriber agreement to the contact officer after receiving a request to establish an account (through their website).

Therefore, it is advisable that clients allow 10 working days to complete this process and obtain a digital certificate.

Important: You will be asked to provide the CA and RA with an email address. You must ensure this is the email address you wish to use in your communications with Customs. For a client to unlock an ICS email from Customs, the address used by Customs must match the email address in the certificate unlocking the email. It is also important to note that the digital certificate must be downloaded to the same computer/browser from which the enrolment form was originally downloaded from the CA. This is a necessary security requirement.

The certificate will be issued in the name of the applicant. For ABN holders, the initial certificate will be issued to the authorised officer in the ABN name of the organisation. Once a digital certificate has been issued to an authorised officer, that person is entitled to process EOI for subsequent members of the organisation. The authorised officer will forward the names of additional staff requiring certificates to the CA via the CA's website.

Registering the certificate

Important: Before a digital certificate can be used with the ICS, a registration process must be completed. For full details on how to complete this process refer to the Digital Certificate and Client Registrations - Revised Processes fact sheet available at www.customs.gov.au.

How long do certificates last?

All certificates must be renewed every two years, with the exception of type 3 (device) certificates. There will be the option with type 3 (device) certificates to purchase either a one year certificate or two year certificate. If a certificate is to be renewed in the same company or individual name, new EOI will only be required every six years. The CA will stipulate what is required when a change occurs in an organisation, for example when there is a new authorised officer, when issuing the certificate.

Important: Renewed digital certificates actually contain different data elements to their original version. Therefore, the renewed digital certificate details must be re-registered in the CCF.

Certificate costs

Certificate costs may vary depending on the CA. Listed below are the current costs of digital certificates that are available from VeriSign. All prices are inclusive of GST and are correct at time of printing.

Type	New	Renewal
Type 1 grade 2	\$126.50	\$93.50
Type 2 grade 2	\$137.50	\$93.50
ABN-DSC authorised officer (AO)	\$187.00	[\$126.50 for additional AO] \$93.50
ABN-DSC (non-AO)	\$93.50	\$93.50
Type 3 (device) - 1 year	\$319.00	\$319.00
Type 3 (device) - 2 year	\$594.00	\$594.00

TECHNICAL REQUIREMENTS FOR COMMUNICATING WITH CUSTOMS

Clients must have the following minimum IT requirements in order to communicate with Customs:

- Microsoft Windows 2000 or XP
- email which supports 'PKCS 12' format digital certificates (check this with the company you are using)
- Microsoft Internet Explorer 5.5 (Service Pack 2) or above
- 56 KBPS modem or better (Broadband connection recommended)
- 1024 x 768 or above screen resolution
- 16 bit colours screen setting.

CHECKLIST FOR DOING BUSINESS WITH CUSTOMS

1. Determine how you will communicate with Customs - via Customs Interactive and/or EDI.
2. If you are using EDI you should liaise directly with your software provider.
3. Determine how many digital certificates you or your business will need.
4. Contact VeriSign and complete the process (including EOI) for obtaining a digital certificate.
5. Complete the registration process with Customs including the signing of the User Agreement (see separate Digital Certificate and Client Registrations - Revised Processes fact sheet).

EVIDENCE OF IDENTITY REQUIREMENTS

Minimum EOI requirements to obtain certificates for type 1 grade 2 and type 2 grade 2 certificates are:

- EOI documentation to the value of 100 points in accordance with the Financial Transaction Reports Act 1998 Form 201 - Identification Record for a Signatory to an Account (Annex A). It is
- mandatory that one of the three listed primary documents be produced
- a face-to-face interview with the registration authority at the time the documents are presented
- a current photograph (if not provided with a primary document).

Where a name shown in one of the three listed primary documents differs from the name shown in any other document, proof of the reason for that name change must be provided. This proof does not count towards the 100-point check.

Minimum EOI requirements to obtain certificates for type ABN-DSC and type 3 certificates are:

- an original or certified copy of the notice issued by the Registrar of the Australian Business Register (ABR) bearing the business entity's name and the ABN. If either the owner, chief executive or other named officer or employee with clear capacity to commit the business entity, is named as the public officer on the document issued by the Registrar of the ABR, then this document will suffice, or
- if the notice issued by the Registrar of the ABR cannot be provided then: a legal or regulatory document binding either the authorized officer or the authoriser with a clear capacity to commit the business entity, to the business entity (in this case online verification with the ABR to link the organisation's ABN to its business name must be achieved), and
- EOI documentation to the value of 100 points using the Financial Transaction Reports Act 1998 Form 201 - Identification Record for a Signatory to an Account (Annex A). It is mandatory that one of the three listed primary documents be produced, and
- a face-to-face interview with the registration authority at the time the documents are presented, and
-
- a current photograph (if not provided with a primary document).

Where a name shown in one of the three listed primary documents differs from the name shown in any other document, proof of the reason for that name change must be provided. This proof does not count towards the 100-point check.

FOR MORE INFORMATION

Go to www.customs.gov.au, email cargosupport@customs.gov.au or phone 1300 558 099.