Integrated Cargo System

New dates for exports rollout

The export component of Customs new IT system, the Integrated Cargo System (ICS), went live for industry testing on Monday 18 August.

To ensure that industry has the full six months of testing that it has been asking for, Customs has postponed the cutover date, from 1 December 2003 to 1 March 2004.

This will minimise disruption to the trading community and ensure the ICS's robustness.

This postponement will allow Customs clients more time to replace or update their computer software and review their business processes to align with new requirements.

To ensure that industry has a full six months of testing, Customs has postponed the cutover date of the ICS from 1 December 2003 to 1 March 2004.

Customs clients involved in the export chain will now be able to report via the new system from 16 February. It will be mandatory for exporters to report via the ICS from 1 March.

Clients who will be communicating directly with Customs should be looking at the options available for connecting to the ICS. It is also important for clients to understand the new rules and regulations that will be introduced in February. It is critical that individuals and businesses in the export chain ensure they can continue exporting once the ICS becomes operative.

Many clients are already looking at their software requirements to ensure they will be ready for the changes. Individuals and businesses in the trading community, who are not using service providers, can communicate directly with Customs via electronic data interchange (EDI) and/or through the Internet.

Accessing the ICS via the Internet will involve logging onto the Customs website and following the prompts. In comparison, EDI batch transmission communicates either through an Internet service provider or a direct line to Customs. The EDI option will require users to develop their own software or purchase an off-the-shelf product.

A list of developers creating software packages can be found at www.customs.gov.au. Select 'cargo management re-engineering' from the navigation bar and follow the links. Another alternative is to use the services of a bureau or value added network.

The security built into Customs new reporting system requires that any individual or company registering as a user will have to purchase a digital certificate from a Customs Gatekeeper approved certification authority.

Digital certificates

Clients will have to buy a digital certificate from an approved certification authority before registering. Clients who report the movement of goods through a customs broker, service provider or bureau may not need to register. Service providers and bureaus may register clients on their behalf.

A variety of digital certificates exist to suit different client circumstances (see box below).

To obtain a digital certificate, Customs clients must contact the certification authority directly via its website.

After enrolment, the certification authority will send the client a subscriber agreement that must be completed, signed and returned to the certification authority (see below).

Once the certification authority has received the agreement, the client can then order the required digital certificate.

In some cases, an evidence of identity (EOI) check will be required. In these cases, clients must take their completed application form and EOI requirements (see next column) to the registration authority (RA) - Australia Post - for an EOI check.

Australia Post will notify the certification authority that applicants have met EOI requirements. Applicants will then be issued with a digital certificate within five working days of completing the EOI check. It is important to remember that an ABN-DSC must have been received by an organisation before applying for a type 3 device certificate.

Currently, the only approved certification authority that can issue digital certificates to Customs clients is VeriSign.

For more information and instructions on how to purchase a digital certificate go to www.verisign.com.au, select 'Gatekeeper' and click on Australian Customs Service.

When additional certification authority providers become approved, their details will be posted on the Customs website.

Evidence of identity check

The security built into the Customs Integrated Cargo System ensures that all messages sent between Customs clients and Customs are authentic and confidential and that their integrity cannot be questioned or repudiated. This process rests on the proof of identity that is established through an EOI check.

Before completing registration or obtaining a digital certificate, users may need to go to a 'KeyPOST' or any other Australia Post corporate outlet and complete an EOI check. The certification authority will advise you of this requirement upon application. This process, similar to the 100-point check conducted when opening a bank account, involves producing documentation to prove identity so that users can be issued with a digital certificate.

EOI for an individual

Individuals will have to provide identification based on the 100-point check. A list of the required documentation is available on the *Communicating electronically with Customs* fact sheet at www.customs.gov.au.

EOI for an organisation

To obtain a digital certificate for an organisation, whether it has an ABN or not, the company's representative will need to pass the 100-point check and also provide evidence of the organisation's existence (for example, a company-related document such as a Certificate of Incorporation or Certificate of Business Name Registration).

Information particular to Customs clients is available on the VeriSign website at www.verisign.com.au/gatekeeper/customs.

Service provider's provision of EOI

Customs does not formally require service providers to obtain EOI from their clients. However, it will be extremely important that service providers can prove to Customs the identity of their clients for legal purposes, should the situation arise.

Specific certificates exist for:

- users who are operating as individuals where the digital certificate identifies and authenticates them personally (a type 1 - grade 2 certificate)
- organisations without an ABN where the digital certificate identifies the organisation and the individual (a type 2 - grade 2 certificate)
- organisations with an ABN (including sole traders and government agencies). The initial certificate will be issued to an authorised officer in the organisation. That authorised officer can then conduct EOI checks for other individuals in the organisation who require certificates (a type ABN-DSC - grade 2 certificate)
- organisations who will be communicating to the ICS via EDI require a type 3 device certificate. This certificate is to be loaded onto a server for signing system-to-system communications. To obtain this certificate, users must have an ABN and must already have a type ABN-DSC (a type 3 certificate - device certificate).

Each digital certificate will contain the:

- certificate owner's details
- certificate issuer's details
- owner's public signing and encryption keys, and validity and expiration dates.

Registration

Customs clients who are ABN holders and have dealt with Customs, using their ABN, on more than one occasion in the past financial year, will be automatically registered in the ICS by Customs. Businesses who do not fit into this category and wish to communicate directly with Customs will need to register before reporting in the ICS.

It is suggested that clients read Customs *Registering for exports* fact sheet before registering. All fact sheets are available at www.customs.gov.au.

For more information go to www.customs.gov.au and select 'cargo management re-engineering' from the navigation bar, email cmr@customs.gov.au, or telephone 1800 022 267.

Public key infrastructure

An open Internet-based system, such as the Integrated Cargo System, provides users with a variety of choices which can lead to cost savings as businesses and individuals tailor their communications to suit their needs.

However, this open system requires greater security. Customs is ensuring the ICS's security environment by using public key infrastructure (PKI).

This security mechanism is widely used for global and open communication networks and:

- encrypts messages to protect data
- uses digital certificates to ensure only registered users can access the system
- uses 'keys' which verify who is communicating as well as the integrity of the communicator's data.

PKI manages the digital certificates and keys that replace hand-written signatures and sealed envelopes in its electronic equivalent.

Sending an email through the Internet is similar to mailing a postcard, since the postcard can be read by anyone along the way and may or may not end up with the right addressee.

Similarly, anyone can change the postcard's content along the way, making it hard to verify who really wrote and posted it.

PKI, on the other hand, is like a courier service which secures every aspect of the communication chain. Because all messages are encrypted, their confidentiality and integrity are guaranteed. The addressee can be confident that the message has not been tampered with or accessed by unauthorised parties.

The use of PKI 'keys' means that the sender's identity can always be authenticated. The addressee will always know who sent the message and the sender will not be able to repudiate sending it.

Training sessions

Australia's business community will face a number of challenges over the next 12 months as Customs updates its export and import reporting systems. The introduction of new legislation and the ICS will impact on all individuals and businesses involved in the export and import chains.

Industry must start preparing for these changes now. The ICS will be introduced for exports on 16 February 2004 and the current export reporting system (EXIT) will be switched off on 1 March 2004.

The ICS will be introduced for importers in mid-2004.

To assist industry to prepare for these changes, Customs is holding a variety of training sessions and workshops to address Customs clients' different needs.

Workshops and information sessions

Export business changes

This workshop will contain detailed information on the changes that will occur with the introduction of the ICS as well as a review of the information required to convert to the new system.

Key topics:

- overview on options for communicating with Customs, including digital certificates and client registration
- transition rules and cut-over arrangements from EXIT to the ICS
- business changes and new rules for export that will be introduced from 16 February.

Export workshop

This workshop will focus on changes to export reporting with the introduction of the ICS. Transition arrangements will also be included.

Key topics:

- export declaration
- export cargo report
- cargo terminal operator (CTO)/stevedore gate receipt
- withdrawal/amendment of export entries
- delivery of export goods without authority.

This workshop will be run in conjunction with the Customs Brokers and Forwarders Council of Australia (CBFCA).

For further information on the changes, which are part of the Customs Cargo Management Re-engineering (CMR) project, including information session locations, dates and times, go to www.customs.gov.au and select 'cargo management re-engineering'.