PKI – Customs and PKI Technology

This fact sheet explains Public Key Infrastructure (PKI) technology and its use with the Integrated Cargo System (ICS).

This fact sheet is relevant for the following clients:

- exporters, importers and cargo reporters;
- service providers, such as customs brokers and freight forwarders; and
- bureaus (who may create and/or transmit messages on behalf of the above groups).

Customs and PKI

Clients who intend to communicate electronically with Customs through the ICS are required to use PKI technology.

The Customs PKI framework is established under the Government's 'Gatekeeper Strategy'. This means that Customs will only accept certificates issued by Certifying Authorities accredited under Gatekeeper and which also meet Custom's service level standards. Currently the only Gatekeeper accredited Certifying Authority recognised by Customs is VeriSign Australia.

What is PKI?

PKI is the mechanism for ensuring the integrity, confidentiality and security of electronic communications conducted in a global and open network.

PKI is designed to ensure the authenticity of both the message content and sender's identity in electronic communications to and from the ICS. For businesses, the Gatekeeper Strategy evidence of identity requirements are designed to ensure that the person who receives the certificate is legally able to commit a business entity to electronic transactions with relying parties, for example Customs.

PKI delivers:

- **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).

This is achieved through a framework of administrative, legal and technical arrangements, including:

- asymmetric encryption involving public and private keys used in association with the digital certificate;
- registration and certification processes for each certificate holder and communicator; and
- a set of legally binding contracts governing the obligations and responsibilities of the certificate holders, such as the Certificate Policy of the Certificate Issuing Authority and the users agreement with Customs.

In effect, a digital certificate used in communication with Customs is equivalent to a hand written signature for the purposes of the *Electronic Transactions Act 1999* with the added consequence that the Customs Act holds the signing party liable for all transactions made under their signature unless they can prove otherwise.

Responsibility for Signatures

The client whose electronic signature appears on the communication will therefore be considered to have made the statement to Customs. They will be regarded as being responsible for the content of the communication unless they can prove otherwise.

It is therefore imperative for the certificate holder to ensure that they meet the obligations under the User Agreement (also known as the Customs Connect Facility Conditions of Use) and Certificate Policy issued by VeriSign Australia. The User Agreement is signed when the certificate holder registers with Customs to gain access to Customs IT systems. Agreeing with the obligations in the Certificate Policy is part of the process in acquiring a digital certificate.

For more Information

Further information about PKI and the use of digital certificates can be found in the following fact sheets:

- *PKI – Bureaus and Wholesaler/ Co-load Arrangements;* and
- *PKI – False and Misleading Statements*.

Additionally, Chief Executive Officer Determination Number 1 of 2006 details the information technology requirements for signing electronic communications to Customs.

Go to www.customs.gov.au
Email cargosupport@customs.gov.au
Phone 1300 558 099