Digital signatures—passport to Customs Integrated Cargo System

By Jennifer Stonebridge

Customs Legislation Amendment and Repeal (International Trade Modernisation) Bill 2000 is currently before Parliament. It will put in place the legal framework for Customs new cargo management system.

Maintaining confidentiality within the open communication system is a vital part of its development.

To ensure confidentiality, all users of Customs Integrated Cargo System will need digital certificates and keys to operate in the new cargo management environment.

The digital certificate must meet Government requirements for public key infrastructure (PKI). They will become the clients' passports to Customs providing instant recognition, enabling them to conduct their business transactions securely.

Public key encryption uses two digital cryptographic keys - one to encrypt information, the other to decrypt it, and vice-versa.

The public key is freely available to traders, allowing them to identify themselves to each other and establish electronic trading relationships. The private key is kept secret by its owner to decrypt the messages. No other key can decrypt them.

The digital certificates and keys will be issued commercially by accredited certificate authorities under the Government Gatekeeper framework. For enterprises they will link to the Australian Business Number and be used to digitally sign each electronic message sent to Customs.

The Gatekeeper Policy Advisory Committee will ensure digital certificates comply with international and Australian standards, streamlining ongoing participation in international trade.

Certificates will be issued for a specific period, expected to be between one and two years. They will cost approximately $50 and Customs will work with software developers to find the best way of incorporating automatic use of digital keys and certificates in "standard" Customs message software.

Customs Director Electronic Commerce Garry Grant said PKI is the only viable way of providing users with the required level of confidentiality, message integrity and recognition by Customs when using open communication systems such as the Internet.

"Customs internal systems will use PKI to ensure documents are not altered following dispatch by the sender. Mr Grant said: "The use of digital signatures will ensure only authorised users access the Integrated Cargo System."

"It is important that Customs and its clients can ensure messages received from another party are genuine and senders can be legally identified.

"CMR's Customs Connect Facility will validate digital signatures and certificates checking data to confirm users' access privileges.

"The whole process occurs instantly as part of the transaction process and is designed to meet international security standards."

With the increasing take-up of digital certificates in our APEC region, PKI is almost universally accepted.

"Now it is not just a question of being leading edge but simply "keeping up with the Joneses," Mr Grant said.

"An alliance is being set up between e-commerce bodies in Singapore, Korea, Malaysia, Chinese Taipei, Hong Kong, China and Australia. There are also Memoranda of Understanding between digital certification authorities in Malaysia, United Kingdom, Singapore and Hong Kong.

"As well, the international banking sector's PKI process, Identrus, has links with a parallel PKI system used by the international association of merchant banks. Australian banks are also participating in Identrus, ensuring the secure exchange of financial information.

"The need is the same - to create mutually recognisable and inter-operable digital certification processes to facilitate cross-border commerce."

Additional information, including a new range of CMR fact sheets, is available on the Customs web site www.customs.gov.au or by contacting Director Electronic Commerce, Garry Grant: phone 02 6275 6186 or e-mail garry.grant@customs.gov.au .

How PKI works

To import some books Alice (the importer) must complete the following five steps:

1. Get a digital certificate with a key pair (her public and private keys) to identify herself to Customs. Alice will be guided to a Gatekeeper registered certification authority by the Customs website.

2. Complete and digitally "sign" an import declaration using her private key, ensuring information is from her and not altered along the way.

3. Encrypt the import declaration with Customs public key, ensuring only Customs can access the information.

4. Transmit the import declaration over the Internet to Customs.

5. Receive approval from Customs to import books.

Once the import declaration is transmitted, the approval process will be completed automatically in seconds. Customs will decrypt Alice's declaration with its private key. The validity of Alice's digital certificate will be checked with the certification authority and her digital signature verified. Once processed by the Integrated Cargo System, Alice will be given approval to import her books.