Encryption systems: Issues arising from import to, and use in, Australia

Rob Nicholls, Partner (Professional Engineer), Gilbert & Tobin

1. INTRODUCTION

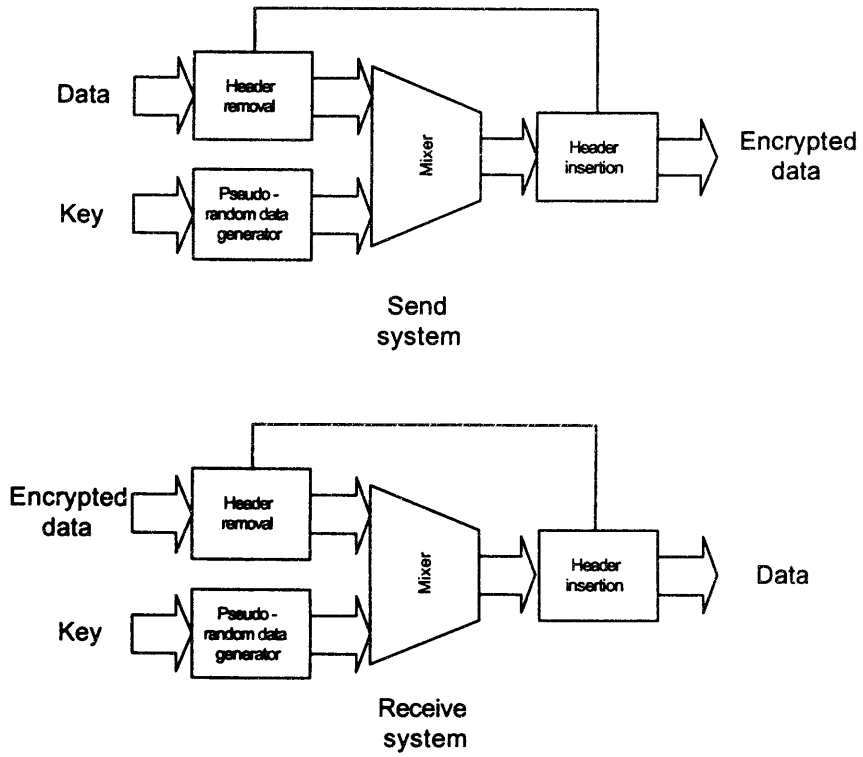
As the levels of both electronic commerce and electronic banking increase in Australia, there is heightening interest in acquiring encryption technologies as part of a solution to maintaining security of funds in any transaction. This paper examines some of the issues that arise out of the importation and use of encryption systems where the encryption system originated outside of Australia.

The issues raised in the paper are of particular importance to multinational corporations adopting a common system with the parent company and to the importation of "system in a box" solutions designed to allow the rapid deployment of e-commerce systems.

The paper commences with an outline of the processes associated with encryption and cryptography and then moves on to describe the relevant legislative aspects in Australia. The paper uses as a premise the concept that those people providing electronic commerce solutions are likely to be carriage service providers (rather than content service providers) as those terms are defined under the *Telecommunications Act* 1997 (Cth).

2. CRYPTOGRAPHY

In order to understand the restriction on use of cryptographic software and systems, it is useful to gain an appreciation of the basics of the systems. Figure 1 sets out the send and receive portions of a typical secure network.



Data is encrypted by mixing it with pseudo-random data. This works by chopping the data into blocks of a given length before mixing with a pseudo-random data of the same length. The result is fed onto a normal transmission network. On the receive side, the blocks of data are mixed with the same pseudo-random data blocks to recover the original signal. There are two essentials from this model:

(a) The key must be the same in the send system and the receive system to be able to generate identical blocks to recover the original data; and

(b) the longer the blocks of data, the stronger the encryption.

There are practical limits to encryption block lengths. When early military systems were developed in the mid-seventies, it was felt that 56 bit blocks were very secure. These days, 128 bit is standard for personal use in the USA, 40 bit in other countries. It is worth noting that an Australian amateur team decrypted 56 bit-encrypted data in 22 hours early in 1999. The capability to decrypt shorter blocks has lead to calls for longer code lengths to be exported from the USA to avoid the restrictions that limit network security.

3. INTERNATIONAL FRAMEWORK

The distribution of software, which has a function to encrypt a communication, has traditionally been controlled by agreements on export control. During the cold war years, this control was an arrangement by the 17 members of the Coordinating Committee for Multilateral Export Controls, (COCOM) (most NATO countries, Australia and Japan). The list of materials prohibited from export from member countries was extensive and

included encryption technology as "high-level munitions".

The COCOM agreement has been replaced by the Wassenaar Arrangement. Twenty-eight countries agreed, in 1995, to establish the Wassenaar Arrangement on *Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. These controls form a global multilateral regime covering both armaments and sensitive dual-use goods and technology. The arrangement aims to respond to the new security threats of the post Cold War by providing greater openness through information sharing about arms and technology transfers worldwide.

In addition, the Organisation for Economic Cooperation and Development (**OECD**) has developed policy with respect to the use of cryptography in the promotion of trade. The OECD has also investigated the privacy implications of both cryptography and the digital economy. The privacy investigations have not lead to binding policy. However, the OECD has developed a cryptography policy. This policy has been endorsed by Australia, in preference to earlier controversial recommendations of the Walsh Report[1].

The requirement to deploy an ability to intercept telecommunications traffic is also derived from international agreement. In general terms, unless exempted, all carriers and carriage service providers must provide facilities that enable them to execute a warrant for interception and to provide special assistance to law enforcement and security agencies. The substance of the obligations is drawn from an *International User Requirement* agreed to by Australia, North America and the European Union countries

4. AUSTRALIAN IMPLEMENTATION

Import and export of goods (including software) into and out of Australia is regulated by the *Customs Act 1901*, the *Customs (Prohibited Imports) Regulations* and *Customs (Prohibited Exports) Regulations* in force under that Act.

Essentially, the legislation works by way of exemption: goods may be imported or exported into Australia unless goods are referred to in the relevant schedules to the Regulations. If goods are so referred to, they may only be dealt with in accordance with such restrictions as are imposed in the regulations.

Encryption and cryptographic technology is not dealt with in the *Customs (Prohibited Imports) Regulations* and accordingly importation of non-military encryption or cryptographic technology into Australia is not restricted or prohibited. This is typical in the implementation of the Wassenaar Arrangement. Some countries (notably France) restrict imports of cryptographic technology.

By contrast, the *Customs (Prohibited Exports) Regulations*, by item 43 of Schedule 13 to those regulations, list:

(a) *"complete or partially complete cryptographic equipment designed to ensure the secrecy of communications (including data communications and communications through the medium of telegraphy, video, telephony and facsimile) or stored information;*

(b) software controlling, or computers performing the function of, cryptographic equipment referred to in paragraph (a);

(c) parts designed for goods referred to in paragraphs (a) or (b);

(d) applications software for cryptographic or cryptanalytic purposes including software used for the design and analysis of cryptlogics;

(h) information security systems, equipment, software, applications specific assemblies, modules or integrated circuits, designed or modified to provide certified or certifiable multi-level security or user-isolation at a level exceeding Class 4 of the Information Technology Security Evaluation Criteria (**ITSEC**) or equivalent in force at the commencement of these Regulations;

(i) Software designed or adapted for the purpose of demonstrating that the information securities features referred to in paragraph (h) provide a multi-level security or user-isolation function."

"Software" is defined in Regulation 13(7) as "a collection of one or more computer programs or microprograms fixed in any tangible medium of expression".

Where goods fall within Schedule 13, Regulation 13B applies. Set out below are relevant parts of Regulation 13B below:

"13B (2) The exportation from Australia of goods specified in Schedule 13 is prohibited unless sub-regulation (3), (3A) or (3B) applies to those goods."

(3) This sub-regulation applies to goods if:

(a) a permission in writing to export the goods has been granted by the Minister for Defence or an authorised person; and

(b) the permission is produced to the Collector.

(3A) This sub-regulation applies to goods if:

(a) the person exporting the goods is the holder of a licence to export the goods granted by the Minister for Defence or an authorised person; and

(b) the licence is produced to the Collector.

[Sub-regulation 3B refers to goods imported and exported by defence forces of friendly countries, including the United States of America.]

(4) A permission or licence granted under this regulation may specify conditions, or requirements, to be complied with by the holder of the permission or licence and may,

in respect of any such condition or requirements, specify a time (being a time before or after the exportation of the goods to which the permission or licence relates) at or before which the condition or requirement shall be complied with by the holder.

(5) *The Minister for Defence may revoke a permission or licence granted under this regulation if the holder of the permission or licences fail to comply with the conditional requirements specified in the permission or licence".*

This means that encryption systems imported into Australia may not be re-exported. If a person wished to export any encryption system previously imported by itself or others, it is likely that an export licence would be required and this may also require permission from the US (or an amendment to an existing US export licence). That is, the restriction in relation to export of encryption technology is not specific to technology developed in Australia and would apply to technology developed in the USA, imported into Australia and subsequently re-exported.

5. RESTRICTIONS DERIVED FROM THE USA

On December 31 1998, the U.S. Department of Commerce Bureau of Export Administration (**BXA**) amended the regulations governing the export of encryption software and commodities, commonly referred to as "encryption items" (**EI**). These amendments are designed to loosen EI controls to respond to criticisms of U.S. export controls.

On December 30 1996, the BXA first amended the Export Administration Regulations (**EAR**), formally transferring EI controls from the U.S. Munitions List to the Commerce Control List. This amendment permitted the mass market export of weak, non-recoverable encryption products (no greater key length than 40-bit) and some stronger encryption products (56-bit) provided the exporter agreed to institute development of key recovery elements into their products. All strong encryption required a licence or licensing arrangement from BXA.

On September 22, 1998, the EAR was amended a second time to permit the export (under a licence exception) of non-recoverable strong encryption for "financial-specific software". Financial-specific software included software that was restricted by design for financial applications to secure financial communications and transactions for end users. Examples of such software include components of the SET™ protocol introduced by Visa and MasterCard. General use non-recoverable encryption software for use by banks and financial institutions was also authorised. The amendment clarified that encryption loaded onto lap-tops and similar devices could be exported for temporary business-specific and/or personal use provided the device stayed within a person's "effective control".

The latest amendments represent the Administration's most recent attempt to balance the competitive and technological needs of electronic commerce with U.S. national security interests. Principally, the amendments create a host of additional exceptions for the use of stronger non-recoverable encryption for specific industry sectors: U.S. subsidiaries, medical and health care institutions, insurance companies and on-line merchants. Additionally, the threshold for the export of non-recoverable mass-market encryption items has been raised to 56-bit.

6. CARRIAGE SERVICE PROVIDERS

There are further restrictions if the encryption system is used by a carriage service provider under the Telecommunications Act 1997 (**Act**).

The Act was amended in late 1997 by the *Telecommunications Legislation Amendment Act 1997*, which introduced a new legislative framework for dealing with law enforcement. This framework makes it mandatory for carriage service providers to provide interception capabilities.

Section 324 is as follows:

Obligations of persons not covered by a determination in relation to particular carriage service

(1) This section applies to a carriage service that involves, or will involve, the use of a controlled network or controlled facility of a person who is a carrier or carriage service provider if the service is not covered by any determination under section 322 that is expressed to be a determination in relation to:

(a) interception capability only; or

(b) both interception capability and special assistance capability.

(2) The person must ensure that the network or facility has the interception capability to enable a communication passing over the network or facility to be intercepted in accordance with a warrant issued under the *Telecommunications (Interception) Act 1979*.

(3) Without limiting subsection (2), the obligation under that subsection in relation to the possession of an interception capability includes the obligation to ensure that that capability is developed, installed and maintained.

Note 1: A person may be exempted from the requirements of this section under a provision of Subdivision C.

Note 2: A person may be required to comply with the special assistance capability requirements under a determination made under section 322 as well as the interception capability requirements under this section.

To date, there have been no determinations by the Attorney-General as to either:

- nominated carriage service providers; or

- interception capabilities or special assistance capabilities.

It is reasonable to assume that such determination will be made at some point in the future.

7. SERVICE LIMITATIONS

There may be some service limitations for users of encryption systems that wish to operate a virtual private network (**VPN**) to countries outside of the USA and Australia. In particular, there may be encryption export problems to any country that has political stability issues. The normal solution to this type of problem is the reduction of access rights to those sites, which are in less secure areas. It may be possible to offer this type of configuration as a service option.

A person's liabilities as a service provider and as a potential exporter are not affected by whether the encryption system is bought or leased. Further, an exemption from providing an interception capability is not automatically given to providers of raw bandwidth services.

8. SUMMARY

There is no relevant restriction under Australian law on the import into Australia of software for encryption or cryptographic technology as encryption technology fall outside of the *Customs (Prohibited Imports) Regulations*.

Carriage service providers have obligations to provide interception capability and this leads to a requirement to have the ability to intercept data in certain circumstances. This includes the interception of encrypted data.

A carriage service provider must ensure that the network or system has the interception capability to enable a communication passing over the network or system to be intercepted in accordance with a warrant issued under the *Telecommunications (Interception) Act 1979*. This obligation in relation to the possession of an interception capability includes the obligation to ensure that the capability is developed, installed and maintained.

There are restrictions under Australian law on the export from Australia of cryptographic technology. These restrictions are not limited by reference to the origin of the cryptographic technology. That is, the restrictions apply regardless of whether the technology was developed in Australia or was developed elsewhere and imported into Australia.

There are no relevant restrictions under Australian law on the use of strong encryption over (otherwise legal) communications traffic either wholly within Australia or to and from Australia.

In the case of private key encryption systems operated within organisations, the ability of the controller of information systems and services within that organisation to decrypt communications (when intercepted at the request of law enforcement agencies pursuant to the issue of a warrant) would suffice to meet this requirement. It is not necessary for the key to be placed in the hands of law enforcement agencies or for the system to otherwise be capable of interception by law enforcement agencies.

Restrictions apply as to the use of communications networks for or in relation to the commission of offences. A carriage service provider must, as set out in the Act, "do its best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth [of Australia], a State and Territories [of Australia]".

1 The report, entitled "Review of policy relating to encryption technologies" was the outcome of a study conducted in 1996 by Gerard Walsh, a former deputy director-general of the Australian Security Intelligence Organisation. Publication of the report was eagerly awaited by members of the law enforcement community, other government departments, commerce and the online community. It was expected that the report would examine the various issues in the cryptography debate and encourage further comment and consultation. The report was listed for sale by the Australian Government Publishing Service in January 1997, but was hurriedly withdrawn from the list 3 weeks later.