



Singapore Customs,
Tariffs & Trade Services Branch,
55 Newton Road #07-01,
Revenue House
Singapore 307987
Tel No. : 6256 1281
Fax No. : 6337 6361
Email: customs_ttsb@customs.gov.sg

ANNEX A - PRODUCT QUESTIONNAIRE A-1 CRYPTOGRAPHY

SECTION A BASIC PRODUCT INFORMATION

(1) Name of the Manufacturer:

(2) Brand:

(3) Model No./Part No.:

(4) Country of Origin:

(The country of origin may not necessarily be the manufacturing or exporting country. For example, the product will be regarded as of US origin if they are made of US-origin technology or software, regardless of the country of manufacturing.)

SECTION B CRYPTOGRAPHY NOTE

(5) Is the item available and sold from stock at retail selling points without restriction, to the general public through any of the following means?

(‘Retail selling points’ are places where the cryptographic item(s) are readily available for sale and that any person can order with reference to available catalogues and advertisements. For example, computer shops easily accessible by buyers, sales via mail order, telephone, fax or online transactions.

‘Without restriction’ means that any person may acquire the products by paying the standard price to the seller without being subjected to any additional conditions, other than those normally arising from copyright (e.g. conditions imposed in a software licence).

(a) Over-the-counter transactions

Yes No

If ‘Yes’, please provide contact details of seller:

(b) Mail order transactions

Yes No

If ‘Yes’, please provide contact details of seller:

(c) Electronic transactions

Yes No

If ‘Yes’, please provide contact details of seller:

(d) Telephone call transactions

Yes No

If ‘Yes’, please provide contact details of seller:

(6) Can the user easily change the cryptographic functionality of the item from what is specified in the manufacturer's specification? (i.e. the cryptographic functionality in the product can only be used according to the manufacturer specification. Specific function such as user selection on the key length, etc., is not considered as "easily change".)

Yes No

If 'Yes', please provide details:

(7) Is the item designed for installation by the user without further substantial support by the supplier? (This does not include nominal installation support, such as telephone or e-mail help-lines to resolve user problems.)

Yes No

If 'No', please provide details:

SECTION C FUNCTIONALITY OF PRODUCT

If any of your answers to (8) to (15) are 'Yes', please provide the relevant details and supporting information.

(8) Is the primary function or set of functions not the following:

(a) 'Information Security'

('Information security' means all the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. It includes 'cryptology', 'cryptanalysis', protection against compromising emanations and computer security.

'Cryptology' means the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorised use.

'Cryptanalysis' means analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text.)

Yes No

(b) A computer, including operation systems, parts and components of the computer therefor

Yes No

(c) Networking (includes operation, administration, management and provisioning)

Yes No

(d) Sending, receiving or storing information

Yes No

If 'No', is it in support of entertainment, mass commercial broadcasts, digital rights management or medical records management?

Yes No

(9) Is the cryptography functionality limited to supporting their primary function or set of functions?

Yes No

(10) Is it a 'personalised smart card'?

('Personalised smart card' means a smart card or an electronically readable personal document (e.g. e-passport), containing a microcircuit which has been programmed for a specific application and cannot be reprogrammed for any other application by the user.)

Yes No

If 'Yes', please state the following:

(a) Is the cryptographic capability restricted for use in equipment or systems stated in (11) to (15) of this Section?

Yes No

(b) Is the application for general public-use where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of personal data stored within?

Yes No

(11) Is it a cryptographic equipment specially designed and limited to banking use or 'money transactions'?

('Money transactions' include the collection and settlement of fares or credit functions.)

Yes No

(12) Is it a portable or mobile radiotelephones for civil use (e.g. for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g. Radio Network Controller (RNC) or Base Station Controller (BSC))?

Yes No

(13) Is it a cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e. a single, unrelayed hop between terminal and home base station) is less than 400 metres according to the manufacturer's specifications?

Yes No

(14) Is it a portable or mobile radiotelephones and similar client wireless device for civil use, that implements only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published), that have been customised for a specific civil industry applications with features that do not affect the cryptographic functionality of these original non-customised devices?

Yes No

(15) Is it a wireless 'personal area network' equipment that implement only published commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 metres according to the manufacturer's specifications?

('Personal area network' means a data communication system having all of the following characteristics:

- a. *Allows an arbitrary number of independent or interconnected 'data devices' to communicate directly with each other; and*
- b. *Is confined to the communication between devices within the immediate vicinity of an individual person or device controller (e.g. single room, office or automobile).*

'Data devices' means equipment capable of transmitting or receiving sequences of digital information.)

Yes No

SECTION D TECHNICAL QUESTIONS

If your answers to any of the following is 'Yes', please provide the details and technical literature in that particular respect.

Does the item contain the following cryptographic functions?

(16)A "symmetric algorithm"

Yes No

If 'Yes', please state the following:

(a) Full name:

(b) Key length:
bits

(c) Is it used for authentication?

Yes No

(d) Is it used for digital signature?

Yes No

(e) Is used for encryption?

Yes No

If 'Yes', please specify what is being encrypted:

files text communication

Others, please specify:

(17)An "asymmetric algorithm" where the security of the algorithm is based on any of the following:

(a) Factorisation of integers (e.g. RSA)

Yes No

If 'Yes', please state the following:

(i) Full name:

(ii) Key length:
bits

(iii) Is it used for authentication?

Yes No

(iv) Is it used for digital signature?

Yes No

(v) Is it used for encryption or decryption?

Yes No

If 'Yes', please specify what is being encrypted:

files text communication

Others, please specify:

(b) Computation of discrete logarithms in a multiplicative group of a finite field (e.g., Elliptic curve, Diffie-Hellman over Z/pZ)

Yes No

If 'Yes', please state the following:

(i) Full name:

(ii) Key length:

bits

(iii) Is it used for authentication?

Yes No

(iv) Is it used for digital signature?

Yes No

(v) Is it used for encryption or decryption?

Yes No

If 'Yes', please specify what is being encrypted:

files text communication

Others, please specify:

(c) Other public key primitives (e.g. Diffie-Hellman over an elliptic curve)

Yes No

If 'Yes', please state the following:

(i) Describe briefly the primitives used:

(ii) Full name:

(iii) Key length:

bits

(iv) Is it used for authentication?

Yes No

(v) Is it used for digital signature?

Yes No

(vi) Is it used for encryption?

Yes No

If 'Yes', please specify what is being encrypted:

files text communication

Others, please specify:

(18) Does the item contain special mechanisms to detect tampering or intrusion?

Yes No

(19) Are the cryptographic algorithms implemented in hardware (ASIC/ASSP/gate array) or software (microprocessor/DSP code)?

SECTION E DECLARATION

I/We declare that all the information provided is true and correct, to the best of my/our knowledge.

(20) Name:

(21) NRIC/Passport No.:

(22) Designation:

(23) Contact No.:

(24) Email:

(25) Fax No.:

(26) Signature:

(27) Date(dd/mm/yyyy):