可輸入資料 Fillable Form 列印 Print 重設 Reset

Director-General of Trade and Industry
(Attn.: Classification Section)
Strategic Trade Controls Branch
Trade and Industry Department
Trade and Industry Tower
3 Concorde Road, Kowloon City
Hong Kong
Fax No.: +852 3525 1526

TRADE AND INDUSTRY DEPARTMENT
CRYPTOGRAPHY QUESTIONNAIRE
Classification of Encryption Products
SC037 (2023/11)

(Please ✓ if appropriate)

Part I – Product Information

a) Name of the Brand Owner: _____

b) Brand: _____

c) Model Number / Part Number:

_____

(Remark: If more than one model number/part number are to be covered in this form, please list all relevant Model Numbers/Part Numbers in separate sheet(s).)

d) Product Description(s):_____

e) Type: ☐ Integrated Circuits / ☐ Modules / ☐ Electronic Assemblies / ☐ Equipment / ☐ Systems / ☐ Software / ☐ Others _____

f) Control Status in the Exporting Country (Place) : ☐ Controlled / ☐ Not Controlled
Export Control Information (if available) :

_____

(Example: ECCN and CCATS for US encryption products)

g) Origin: _____ (Note: "Origin" of the goods may not necessarily be the manufacturing or exporting country/ place. For example, in general, goods will be regarded as of US origin if they are made of US-origin technology or software, irrespective of the country/ place of manufacturing.)

h) Other Supplementary Information:

Part II – Information of the product in Part I (Answers to all questions are required)

(Please ✓ if appropriate)

		Yes	No
Q.1	Please advise whether the product as specified in Part I is designed or modified to use cryptography employing digital techniques performing cryptographic function? If 'No', please go to Part III.	☐	☐
Q.2	(1) Please advise whether the product as specified in Part I is an item meeting all the Note 3(a) requirements as specified in Annex 1 (page 6).	☐	☐
	(2) Please advise whether the product is of potential interest to a wide range of individuals and businesses.	☐	☐
	(3) Please advise whether the price and information about the main functionality of the product is available before purchase.	☐	☐
Q.3	Please advise whether the product as specified in Part I is Hardware component or executable software of existing item meeting all the Note 3(b) requirements as specified in Annex 1 (page 6). If 'Yes', please quote example(s) for the existing item: including brand, model and product descriptions. _____	☐	☐
Q.4	Please advise whether the product is designed or modified to use 'cryptography for data confidentiality' having a 'described security algorithm', where that cryptographic capability is usable, has been activated, or can be activated by means of "cryptographic activation" not employing a secure mechanism, as follows:		
	(a) Items having "information security" as a primary function;	☐	☐
	(b) Digital communication or networking systems, equipment or components, not specified in Q.4(a);	☐	☐
	(c) Computers, other items having information storage or processing as a primary function, and components therefor, not specified in Q.4(a) or Q.4(b);	☐	☐
	(d) Items, not specified in Q.4(a) to Q.4(c), where the 'cryptography for data confidentiality' having a 'described security algorithm' meets all of the following:		
	(i) It supports a non-primary function of the item;	☐	☐
	(ii) It is performed by incorporated equipment or "software" that would, as a standalone item, be specified by Category 5 – Part 2.	☐	☐
	If the answer to Q.1 is 'Yes' and Q.4(d)(ii) is also 'Yes', please provide relevant details (e.g. brand, model and product descriptions) of the standalone item performing cryptographic function. _____		

Q.5	Please advise whether the product as specified in Part I is item/equipment mentioned in 5A002 Note in Annex 2 (page 7-8). If 'Yes', please advise the relevant paragraph letter (e.g. h) of 5A002 Note _____	☐	☐
Q.6	Please advise whether the usage of the cryptographic functions of the product is : (a) Encryption or decryption of data file (including image, voice or text, etc.) (b) Others, please specify:_____	☐ ☐	☐ ☐
Q.7	If the answer to Q.6 is 'Yes', please state the following: (a) A "symmetric algorithm" Full name : _____ Key length : _____ bits (b) An "asymmetric algorithm" (i) Factorisation of integers (e.g., RSA); Full name : _____ Key length : _____ bits (ii) Computation of discrete logarithms in a multiplicative group of a finite field (e.g., Diffie-Hellman over Z/pZ); Full name : _____ Key length : _____ bits (iii) Discrete logarithms in a group other than mentioned in (b)(ii) above (e.g., Diffie- Hellman over an elliptic curve); Full name : _____ Key length : _____ bits (iv) Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium); Full name : _____ Key length : _____ bits (v) Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); Full name : _____ Key length : _____ bits (vi) Decoding random codes (e.g., McEliece, Niederreiter). Full name : _____ Key length : _____ bits	☐ ☐	☐ ☐
Q.8	Please advise whether the usage of the cryptographic functions of the product is (check all that apply): (a) Authentication (b) Digital signature (c) Data integrity (d) Non-repudiation (e) Digital rights management, including the execution of copy-protected software (f) Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management (g) Key management in support of any function described in (a) to (f) above	☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐
Q.9	If the answer to Q.8 is 'Yes', please advise the security algorithm: (a) A "symmetric algorithm" Full name : _____ Key length : _____ bits (b) An "asymmetric algorithm" (i) Factorisation of integers (e.g., RSA);	☐ ☐	☐ ☐

	Full name : _____ Key length : _____ bits (ii) Computation of discrete logarithms in a multiplicative group of a finite field (e.g., Diffie-Hellman over Z/pZ); Full name : _____ Key length : _____ bits (iii) Discrete logarithms in a group other than mentioned in (b)(ii) above (e.g., Diffie- Hellman over an elliptic curve); Full name : _____ Key length : _____ bits (iv) Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium); Full name : _____ Key length : _____ bits (v) Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); Full name : _____ Key length : _____ bits (vi) Decoding random codes (e.g., McEliece, Niederreiter). Full name : _____ Key length : _____ bits	

Note:
Details and supporting information such as a letter from the Brand Owner may be required to confirm the fulfillment of the relevant criteria.

Part III – Other Information of the product in part I

		Yes	No
Q.10	For the product originated from US, is it subject to the control of US EAR 740.17(b)(2) or 740.17(b)(3)(iii) ? If yes, please provide the relevant copy of Commodity Classification Automated Tracking System (CCATS) issued by the Bureau of Industry and Security of the US Government.	☐	☐
Q.11	**(For general purpose integrated circuits)** The temperature rated for operation over the entire ambient temperature range from _____to _____ ºC. Please advise whether the integrated circuits is designed for civil automobile or railway train applications.	☐	☐

Part IV – Declarations

I declare that I am the **Brand Owner** of the products as specified in Part I and it is to the best of my knowledge and belief the information given above is true and correct.

Name of Signatory : _____
(in block letters)

Position of Signatory in the Company : _____

Name of Company : _____
(Remark: name of company shall be consistent with the name of Brand Owner)

Signature & Company Chop : _____

Company Phone Number: _____

Company Email Address : _____

Company Homepage : _____

Date : _____

Important Note : The data collected in this form will be kept in confidence. They may however be disclosed to other government departments, or to third parties in Hong Kong or elsewhere, if such disclosure is necessary to facilitate consideration of the related application, is in the interests of Hong Kong, is authorised or required by the law; or if explicit consent to such disclosure is given by the applicant/data subject.

The Director-General of Trade and Industry at all times reserves the right to request additional information and further documentary proof to substantiate the classification applications. Questionnaires that are not properly completed or not accompanied by all the necessary documentation will be deferred/ rejected.

For other information concerning the handling of personal data by the Department, please refer to a relevant Note issued by the Department on the subject, copy of which is obtainable from the Strategic Trade Controls Branch on 16/F, Trade and Industry Tower, 3 Concorde Road, Kowloon City, Hong Kong.

Annex 1

Part 2 "Information Security" of Category 5 "Telecommunications and Information Security" of the Import and Export (Strategic Commodities) Regulations, Chapter 60G

Note 3 Cryptography Note:

5A002, 5D002(a)(1), 5D002(b) and 5D002(c)(1) do not apply to items as follows:

(a) Items meeting all of the following:
  (1) Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
    (a) Over-the-counter transactions;
    (b) Mail order transactions;
    (c) Electronic transactions;
    (d) Telephone call transactions;
  (2) The cryptographic functionality cannot easily be changed by the user;
  (3) Designed for installation by the user without further substantial support by the supplier; and
  (4) When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs (a) (1), (2) and (3) above;

(b) Hardware components or 'executable software' of existing items described in paragraph (a) of this Note, that have been designed for these existing items, meeting all of the following:
  (1) Information security is not the primary function or set of functions of the component or 'executable software';
  (2) The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;
  (3) The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification; and
  (4) When necessary as determined by the appropriate authority in the exporter's country, details of the component or 'executable software' and relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described in paragraph (b)(1), (2) and (3).

Technical Note:

For the purposes of Note 3, 'executable software' means 'software' in executable form, from an existing hardware component excluded from 5A002 by Note 3.

Note:

'Executable software' does not include complete binary images of the 'software' running on an end-item.

Annex 2

Note

5A002(a) does not control any of the following items, or specially designed "information security" components therefor:

(a) Smart cards and smart card 'readers/writers' as follows:

(1) A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:

(a) The cryptographic capability meets all of the following:

(1) It is restricted for use in any of the following:

(a) Equipment or systems not described by 5A002(a)(1) to 5A002(a)(4);

(b) Equipment or systems not using 'cryptography for data confidentiality' having a 'described security algorithm';

(c) Equipment or systems, excluded from 5A002(a), by paragraphs (b) to (f) of this Note;

(2) It cannot be reprogrammed for any other use;

(b) Having all of the following:

(1) It is specially designed and limited to allow protection of 'personal data' stored within;

(2) Has been, or can only be, personalised for public or commercial transactions or individual identification;

(3) Where the cryptographic capability is not user-accessible;

Technical Note:

'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for "authentication".

(2) 'Readers/writers' specially designed or modified, and limited, for items specified in paragraph (a) (1) of this Note.

Technical Note:

'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network.

(b) Cryptographic equipment specially designed and limited for banking use or 'money transactions';

Technical Note:

'Money transactions' in 5A002(a) Note 2(b) includes the collection and settlement of fares or credit functions.

(c) 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));

(d) 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;

(e) Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs (a)(2) to (a)(4) of the Cryptography Note (Note 3 in Annex 1), that have been customised for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customised devices;

(f) Items, where the "information security" functionality is limited to wireless "personal area network" functionality, implementing only published or commercial cryptographic standards;

(g) Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meet the provisions of paragraphs (a)(2) to (a)(4) of the Cryptography Note (Note 3 in Annex1), having an RF output power limited to 0.1 W (20 dBm) or less, and supporting 16 or fewer concurrent users.

(h) Routers, switches, gateways or relays, where the "information security" functionality is limited to the tasks of
"Operations, Administration or Maintenance" ("OAM") implementing only published or commercial cryptographic standards;

(i) General purpose computing equipment or servers, where the "information security" functionality meets all of the following:
  (1) Uses only published or commercial cryptographic standards;
  (2) Is any of the following:
    (a) Integral to a CPU that meets the provisions of Note 3 to Category 5–Part 2;
    (b) Integral to an operating system that is not specified in 5D002;
    (c) Limited to "OAM" of the equipment.

(j) Items specially designed for a 'connected civil industry application', meeting all of the following:
  (1) Being any of the following:
    (a) A network-capable endpoint device meeting any of the following:
      (1) The "information security" functionality is limited to securing 'non-arbitrary data' or the tasks of "Operations, Administration or Maintenance" ("OAM");
      (2) The device is limited to a specific 'connected civil industry application';
    (b) Networking equipment meeting all of the following:
      (1) Being specially designed to communicate with the devices specified by paragraph (j)(1)(a) above;
      (2) The "information security" functionality is limited to supporting the 'connected civil industry application' of devices specified by paragraph (j)(1)(a) above, or the tasks of "OAM" of this networking equipment or of other items specified by paragraph (j) of this Note;
  (2) Where the "information security" functionality implements only published or commercial cryptographic standards, and the cryptographic functionality cannot easily be changed by the user.
  Technical Notes:
    1. 'Connected civil industry application' means a network-connected consumer or civil industry application other than "information security", digital communication, general purpose networking or computing.
    2. 'Non-arbitrary data' means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location etc.), that cannot be changed by the user of the device.