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)
16/F, 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 (2015/10)
(Revised on 2 October 2015)

(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:

(Please ✓ if appropriate)

Part II – Questions (<u>Answers to all questions are required</u>)

Q.1 Please advise whether the products as specified in Part I are designed or modified to use cryptography employing digital techniques performing cryptographic function? (□ Yes / □ No)
If the answer is not affirmative, please go to Part III.

Q.2 Please complete Annex 1 (page 4) with details of the cryptographic function of the products as specified in Part I.

Q.3 Please advise whether the products as specified in Part I are:

a) Items meeting all the Note 3(a) requirements as specified in Annex 2 (page 5). (□ Yes / □ No)

b) Hardware components or executable software of existing items meeting all the Note 3(b) requirements as specified in Annex 2. (□ Yes / □No)
If the answer to Q.3(b) is affirmative, please quote example(s) for the existing items: including brand, model and product descriptions.

Q.4 Please advise whether the products as specified in Part I meet all of the following: (□Yes / □ No)

a) The items are of potential interest to a wide range of individuals and businesses.

b) The price and information about the main functionality of the items are available before purchase.

Q.5 Please advise whether the products as specified in Part I are items meeting all the Note 4 requirements as specified in Annex 2. (□ Yes / □ No)

Q.6 Please advise whether ALL the cryptographic functions of the products as specified in Part I are ONLY used for authentication, digital signature or the execution of copy-protected software.
(□Yes / □ No)

Q.7 Please advise whether the products as specified in Part I are items/equipment mentioned in 5A002 Note in Annex 3? (□ Yes / □ No)
If yes, please advise the relevant paragraph letter (e.g. k) of 5A002 Note ______________________

Note: If answer to any of the above questions Q.3, Q.4, Q5, Q.6 or Q7 is “YES”, relevant details and supporting information such as a <u>letter from the Brand Owner may be required to confirm the fulfillment of the relevant criteria</u>.

Q.8 For the products originated from US, are they subject to the control of US EAR 740.17(b)(2) or US EAR 740.17(b)(3)(iii) ? (□Yes / □ No)
If yes, please provide the relevant copy of Commodity Classification Automated Tracking System (CCATS) issued by the Bureau of Information and Security of the US Government.

Part III – Temperature Information

In case the products as specified in Part I are general purpose integrated circuits, please provide the following information.

1. Please advise whether these integrated circuits are used for civil automobile or railway train applications? (□ Yes / □ No)
2. Please provide the temperature rated for operation over the entire ambient temperature range from ________℃ to ________℃.

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 (Please ✓ if appropriate)

Does the product contain the following cryptographic functions?

YES / NO

(1) A “symmetric algorithm”
If “yes”, please state the following: □ □
(i) Full name __________________________;
(ii) Key length ___________bits;
(iii) It is used for authentication only; □ □
(iv) It is used for digital signature only; □ □
(v) It is used for execution of copy-protected software only; □ □
(vi) It is used for encryption or decryption of data file (including image, voice or text etc.); □ □
(vii) Other application: ____.

(2) An “asymmetric algorithm” □ □
If “yes”, please state the basis of the algorithm in the following parts:
(a) Factorisation of integers (e.g., RSA); □ □
If “yes”, please state the following:
(i) Full name __________________________;
(ii) Key length ___________ bits;
(iii) It is used for authentication only; □ □
(iv) It is used for digital signature only; □ □
(v) It is used for execution of copy-protected software only; □ □
(vi) It is used for encryption or decryption of data file; □ □
(vii) Other application: _______________________________________.
(b) Computation of discrete logarithms in a multiplicative group of a finite field (e.g., Diffie-Hellman over Z/pZ); □ □
If “yes”, please state the following:
(i) Full name __________________________;
(ii) Key length ___________ bits;
(iii) It is used for authentication only; □ □
(iv) It is used for digital signature only; □ □
(v) It is used for execution of copy-protected software only; □ □
(vi) It is used for encryption or decryption of data file; □ □
(vi) Other application: _______________________________________.
(c) Discrete logarithms in a group other than mentioned in (2)(b) above (e.g., Diffie-Hellman over an elliptic curve); □ □
If “yes”, please state the following:
(i) Full name __________________________;
(ii) Key length ___________ bits;
(iii) It is used for authentication only; □ □
(iv) It is used for digital signature only; □ □
(v) It is used for execution of copy-protected software only; □ □
(vi) It is used for encryption or decryption of data file; □ □
(vi) Other application: _______________________________________.

(3) Others (Please use separate sheet if required.)
Please state the details of other cryptographic functions together with their key length in bits, and describe how the algorithms are used.

Annex 2

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

<u>Note 3</u> <u>Cryptography Note:</u>

5A002 and 5D002 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.

<u>Note 4</u>

Category 5-Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:

(a) The primary function or set of functions is not any of the following:

(1) Information security;

(2) A computer, including operating systems, parts and components of the computer;

(3) Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management);

(4) Networking (includes operation, administration, management and provisioning);

(b) The cryptographic functionality is limited to supporting their primary function or set of functions;

(c) 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) and (b) above.

Annex 3

Note

5A002 does not include any of the following:

(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 is restricted for use in equipment or systems excluded from 5A002 by Note 4 in Annex 2 or paragraphs (d), (e), (f), (g) and (i) of this Note, and 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, personalized 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 by 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) Deleted;

(c) Deleted;

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

Technical Note:

"Money transactions" in this paragraph includes the collection and settlement of fares or credit functions.

(e) Portable or mobile radiotelephones for civil use (e.g. for use with commercial civil cellular radiocommunications 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));

(f) 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 basestation) is less than 400 metres according to the manufacturer's specifications;

(g) 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 paragraph (a)(2) to a(5) of Note 3 in Annex 2 , that have been customized for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customized devices;

(h) Deleted;

(i) Wireless "personal area network" equipment that implements only published or 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, or not exceeding 100 metres according to the manufacturer’s specifications for equipment that cannot interconnect with more than 7 devices;

(j) Equipment, having no functionality specified by 5A002(a)(2), 5A002(a)(4), 5A002(a)(7), or 5A002(a)(8), where all cryptographic capability specified by 5A002(a) meets any of the following:

(1) It cannot be used;

(2) It can only be made usable by means of "cryptographic activation";

(k) Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, which also meets the provisions of paragraph (a)(2) to (a)(5) of Note 3 in Annex 2, having an RF output power limited to 0.1 W (20 dBm) or less, and supporting 16 or fewer concurrent users.