Singapore Customs
55 Newton Road #06-01
Revenue House
Singapore 307987
Tel No.: 6355 2000
Email: customs_classification@customs.gov.sg
Form reference: SC-A-064A (Ver 10 – 11/20)

ANNEX A - PRODUCT QUESTIONNAIRE
A-1 CRYPTOGRAPHY
(Based on SGCO 2020)

Clear Form

SECTION A BASIC PRODUCT INFORMATION

(1) Name of the Manufacturer:

(2) Brand:

(3) Model No. / Part No.:

SECTION B CRYPTOGRAPHY NOTE

(4) 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 is readily available for sale and that any person can order with reference to available catalogues and advertisements. (e.g. computer shops that are 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 subject to any additional conditions, other than those normally arising from copyright (e.g. conditions imposed in a software licence). The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price enquiry is not considered to be a consultation.

Being available and sold from stock to the 'general public' means that the item is of potential interest to a wide range of individuals and businesses.)

(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:

(5) 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's 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:

(6) 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:

(7) Is the item a hardware component or 'executable software' designed for a higher assembly?

('Executable software' means software in executable form, from an existing hardware component. It does not include complete binary images of the software running on an end-item.)

☐ Yes ☐ No

If 'Yes', please state the following:

(a) Provide details of the higher assembly and submit the relevant product information (product brochure / technical specification):

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

(i) Over-the-counter transactions

☐ Yes ☐ No

If 'Yes', please provide contact details of seller:

(ii) Mail order transactions

☐ Yes ☐ No

If 'Yes', please provide contact details of seller:

(iii) Electronic transactions

☐ Yes ☐ No

If 'Yes', please provide contact details of seller:

(iv) Telephone call transactions

☐ Yes ☐ No

If 'Yes', please provide contact details of seller:

(c) Can the user easily change the cryptographic functionality of the higher assembly 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's 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:

(d) Is the higher assembly 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:

(e) Does the hardware component or 'executable software' change any cryptographic functionality of the higher assembly, or add new cryptographic functionality to the higher assembly?

☐ Yes ☐ No

(f) Is the feature set of the hardware component or 'executable software' fixed and not designed or modified to the customer's specification?

☐ Yes ☐ No

SECTION C FUNCTIONALITY OF PRODUCT

If any of your answers to (8) to (31) are 'Yes', please provide the relevant details and supporting information.

(8) Is the cryptographic capability usable, has been activated or can be activated by means of "cryptographic activation" not employing a secure mechanism?

("Cryptography activation" means any technique that activates or enables cryptographic capability of an item, by means of a secure mechanism implemented by the manufacturer of the item, where this mechanism is uniquely bound to a single instance of the item or one customer, for multiple instances of the item.)

☐ Yes ☐ No

(9) Is it an item having "information security" as a primary function?

("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 "cryptography", "cryptographic activation", 'cryptanalysis', protection against compromising emanations and computer security.

"Cryptography" 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.

"Cryptography activation" means any technique that activates or enables cryptographic capability of an item, by means of a secure mechanism implemented by the manufacturer of the item, where this mechanism is uniquely bound to either a single instance of the item or one customer, for multiple instances of the item.

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

☐ Yes ☐ No

(10) Is it a digital communication or networking system, equipment or component?

☐ Yes ☐ No

(11) Is it a computer, or item having information storage or processing as a primary function, or its component therefor?

☐ Yes ☐ No

(12) Is it an item where the cryptographic functionality supports a non-primary function of the item?

☐ Yes ☐ No

(13) Is it an item where the cryptographic functionality is performed by incorporated equipment or "software" that would, as a standalone item, be specified in Category 5 – Part 2?

(*"software" means a collection of one or more 'programs' or 'microprograms' recorded, stored or embodied in any device;*

'Program' means a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer.

'Microprogram' means a sequence of elementary instructions maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register.)

☐ Yes ☐ No

(14) Is it a smart card or an electronically readable personal document (e.g. token coin, e-passport)?

☐ Yes ☐ No

If 'Yes', please state the following:

(a) Is the cryptographic capability restricted for use in equipment or systems that are <u>not</u> stated in (9) to (12)?

☐ Yes ☐ No

(b) Is the cryptographic capability restricted for use in equipment or systems <u>not</u> using 'cryptography for data confidentiality'?

('Cryptography for data confidentiality' means "cryptography" that employs digital techniques and performs any cryptographic function other than any of the following:

(i) "Authentication";

(ii) Digital signature;

(iii) Data integrity;

(iv) Non-repudiation;

(v) Digital rights management, including the execution of copy-protected software;

(vi) *Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management; <u>or</u>*

(vii) Key management in support of any function described in paragraphs (i) to (vi) above.

"Authentication" means verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system. This includes verifying the origin or content of a message or other information, and all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.)

☐ Yes ☐ No

(c) Can it be reprogrammed for any other use?

☐ Yes ☐ No

(d) Has the application been, or can only be, personalised for public or commercial transactions or individual identification where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of 'personal data' stored within?

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

☐ Yes ☐ No

(15) Is it a 'reader/writer' specially designed or modified, and limited, for items fulfilling (14) (a) to (14) (c), or (14) (d)?

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

☐ Yes ☐ No

(16) 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

(17) 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

(18) 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 m according to the manufacturer's specifications?

☐ Yes ☐ No

(19) 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) and also meet the provisions stated in (5) and (6), 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?

☐ Yes ☐ No

(20) Is the "information security" functionality limited to wireless "personal area network" functionality that implement only published or commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 m according to the manufacturer's specifications, or not exceeding 100 m according to the manufacturer's specifications for equipment that cannot interconnect with more than seven devices?

("Personal area network" means a data communication system having both 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 and their nearby surrounding spaces).

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

☐ Yes ☐ No

(21) Is it a mobile telecommunications Radio Access Network (RAN) equipment designed for civil use, and also meet the provisions stated in (5) and (6), having an RF output power limited to 0.1 W (20 dBm) or less, and supporting 16 or fewer concurrent users?

☐ Yes ☐ No

(22) Is it a router, switch or relay, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance" ("OAM") implementing only published or commercial cryptographic standards?

("OAM" means performing one or more of the following tasks:

a. Establishing or managing any of the following:

1. Accounts or privileges of users or administrators;

2. Settings of an item; or

3. Authentication data in support of the tasks described in paragraphs a.1. or a.2.;

b. Monitoring or managing the operating condition or performance of an item; or

c. Managing logs or audit data in support of any of the tasks described in paragraphs a. or b.

"OAM" does not include either of the following tasks or their associated key management functions:

a. Provisioning or upgrading any cryptographic functionality that is not directly related to establishing or managing authentication data in support of the tasks described in paragraphs a.1. or a.2. above; or

b. Performing any cryptographic functionality on the forwarding or data plane of an item.)

☐ Yes ☐ No

(23) Is it a general purpose computing equipment or server?

☐ Yes ☐ No

If 'Yes', please state the following:

(a) Does the "information security" functionality use only published or commercial cryptographic standards?

☐ Yes ☐ No

(b) Is the "information security" functionality integral to a Central Processing Unit (CPU)?

☐ Yes ☐ No

If 'Yes', please state the following:

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

(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:

(ii) Can the user easily change the cryptographic functionality of the CPU 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:

(iii) Is the CPU 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 'Yes', please provide details:

(c) Is the "information security" functionality integral to an operating system?

☐ Yes ☐ No

If 'Yes', please state the following:

(i) Is the operating system specially designed or modified for the "development", "production" or "use" of an "information security" equipment?

("development", in relation to any goods, means any stage prior to the serial production of the goods, including design, design research, design analysis, development of a design concept, assembly and testing of a prototype, pilot production, generation of design data, the process of transforming design data into a product, configuration design, integration design, and layout;

"production", in relation to any goods, means any stage of production of the goods, including construction, production engineering, manufacture, integration, assembly, mounting, inspection, testing, and quality assurance;

"use", in relation to any goods, means the operation, installation, maintenance, inspection, repair, overhaul or refurbishing of the goods.)

☐ Yes ☐ No

(ii) Is the operating system having the characteristics of a cryptographic activation token stated in (25)?

☐ Yes ☐ No

(d) Is the "information security" functionality limited to "OAM" of the equipment?

☐ Yes ☐ No

(24) Is it specially designed for a 'connected civil industry application'?

('*connected civil industry application' means a network connected consumer or civil industry application other than "information security", digital communication, general purpose networking or computing.*)

☐ Yes ☐ No

If 'Yes', please state the following:

(a) Is it a network-capable endpoint device where the "information security" functionality is limited to securing 'non-arbitrary data' or the tasks of "OAM"?

(*'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.*)

☐ Yes ☐ No

(b) Is it a network-capable endpoint device limited to a specific 'connected civil industry application'?

☐ Yes ☐ No

(c) Is it a networking equipment specially designed to communicate with the devices stated in (24) (a) and (24) (b)?

☐ Yes ☐ No

(d) Is it a networking equipment where the "information security" functionality is limited to supporting the 'connected civil industry application' of devices stated in (24) (a) and (24) (b), or the tasks of "OAM" of this networking equipment or of other items stated in (24)?

☐ Yes ☐ No

(e) Is the item's "information security" functionality implements only published or commercial cryptographic standards, and the cryptographic functionality cannot easily be changed by the user?

☐ Yes ☐ No

(25) Is it a cryptographic activation token designed or modified to enable, by means of "cryptographic activation":

(a) For converting, an item not specified in Category 5 – Part 2 "Information Security" into an item stated in (32) or (33) or into "software" having the characteristics of, or performing or simulating the functions of (26), (27) and (28)?

☐ Yes ☐ No

(b) For enabling, additional functionality stated in (32) or (33) of an item already specified in Category 5 – Part 2 "Information Security"?

☐ Yes ☐ No

(26) Is it designed or modified to use or perform "quantum cryptography"?

("Quantum cryptography" means a family of techniques for the establishment of shared key for "cryptography" by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory or quantum electrodynamics).

"Quantum cryptography" is also known as Quantum Key Distribution (QKD).)

☐ Yes ☐ No

(27) Is it designed or modified to use cryptographic techniques to generate channelising codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having either a bandwidth exceeding 500 MHz or a "fractional bandwidth" of 20% or more?

("Fractional bandwidth" means the "instantaneous bandwidth" divided by the centre frequency, expressed as a percentage.

"Instantaneous bandwidth" means the bandwidth over which output power remains constant within 3 dB without adjustment of other operating parameters.)

☐ Yes ☐ No

(28) Is it designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, other than those stated in (26) including the hopping code for "frequency hopping" systems?

("Spread spectrum" means the technique whereby energy in a relatively narrow-band communication channel is spread over a much wider energy spectrum.

"Frequency hopping" means a form of "spread spectrum" in which the transmission frequency of a single communication channel is made to change by a random or pseudo-random sequence of discrete steps.)

☐ Yes ☐ No

(29) Is it a communications cable system designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion?

(Communications cable system only includes physical layer security where the physical layer includes Layer 1 of the Reference Model of Open Systems Interconnection (OSI) (Ref. ISO/IEC 7498-1).)

☐ Yes ☐ No

(30) Is it specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards?

☐ Yes ☐ No

(31) Is it designed or modified to perform 'cryptanalytic functions'?

(This includes systems or equipment, designed or modified to perform 'cryptanalytic functions' by means of reverse engineering.

'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.)

☐ Yes ☐ No

SECTION D TECHNICAL QUESTIONS

If your answers to any of the following is 'Yes', please provide the relevant details and supporting information.

Does the item contain the following cryptographic functions?

(32) A "symmetric algorithm" employing a key length in excess of 56 bits, not including parity bits?

("Symmetric algorithm" means a cryptographic algorithm using an identical key for both encryption and decryption.)

☐ Yes ☐ No

If 'Yes', please state the following:

(a) Full name:

(b) Key length: bits

(c) Is it used for any of the following?

(i) "Authentication"

☐ Yes ☐ No

(ii) Digital signature

☐ Yes ☐ No

(iii) Data integrity

☐ Yes ☐ No

(iv) Non-repudiation

☐ Yes ☐ No

(v) Digital rights management, including the execution of copy-protected software

☐ Yes ☐ No

(vi) Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management

☐ Yes ☐ No

(vii) Key management in support of any of the cryptographic functions in (32) (c) (i) to (vi)

☐ Yes ☐ No

(d) Is it used for encryption or decryption other than the cryptographic functions in (32) (c)?

☐ Yes ☐ No

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

☐ Files ☐ Text ☐ Communication

☐ Others, please specify:

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

("Asymmetric algorithm" means a cryptographic algorithm using different, mathematically-related keys for encryption and decryption.

An algorithm described by 33 (c), (d) and (e) below may be referred to as being post-quantum, quantum-safe or quantum-resistant.)

(a) Factorisation of integers in excess of 512 bits (e.g. RSA)

☐ Yes ☐ No

(b) Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g. Diffie-Hellman over Z/pZ)

☐ Yes ☐ No

(c) Shortest vector or closest vector problems associated with lattices (e.g. NewHope, Frodo, NTRUEncrypt, Kyber, Titanium)

☐ Yes ☐ No

(d) Finding isogenies between Supersingular elliptic curves (e.g. Supersingular Isogeny Key Encapsulation)

☐ Yes ☐ No

(e) Decoding random codes (e.g. McEliece, Niederreiter)

☐ Yes ☐ No

(f) Other public key primitives in excess of 112 bits (e.g. Diffie-Hellman over an elliptic curve)

☐ Yes ☐ No

If 'Yes' to any of the above, please state the following:

(i) Describe briefly the primitives used:

(ii) Full name:

(iii) Key length: bits

(iv) Is it used for any of the following?

(a) "Authentication"

☐ Yes ☐ No

(b) Digital signature

☐ Yes ☐ No

(c) Data integrity

☐ Yes ☐ No

(d) Non-repudiation

☐ Yes ☐ No

(e) Digital rights management, including the execution of copy-protected software

☐ Yes ☐ No

(f) Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management

☐ Yes ☐ No

(g) Key management in support of any of the cryptographic functions in (33) (a) (iv) (a) to (f)

☐ Yes ☐ No

(v) Is it used for encryption or decryption other than the cryptographic functions in (33) (a) (iv)?

☐ Yes ☐ No

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

☐ Files ☐ Text ☐ Communication

☐ Others, please specify:

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