可輸入資料 Fillable Form　列印 Print　重設 Reset

香港九龍城協調道 3 號
工業貿易大樓
工業貿易署
戰略貿易管制科
工業貿易署署長
（經辦單位：分類組）
傳真號碼: +852 3525 1526

工業貿易署
密碼學問卷-加密產品分類
CSC037 (2025/05)

(請在適當空位內加上✓號)

第一部份　　產品資料

a) 品牌擁有人名稱：_____

b) 品牌：_____

c) 型號／零件號碼：

_____

(備註：如本表格中包含多於一個型號／零件號碼，請於另頁列出所有相關型號／零件號碼。)

d) 產品描述：_____

e) 種類：☐ 集成電路/ ☐ 模組 / ☐電子組件/ ☐ 裝備 /
☐系統 / ☐軟件 / ☐ 其他 _____

f) 出口國（地）的管制狀態： ☐受管制 / ☐不受管制
出口管制資料（如有）：

_____
(例如：美國加密產品的出口管制分類編號 (ECCN) 和貨品分類自動追踪系統 (CCATS))

g) 原產地：_____（註：貨物的「原產地」未必等同製造或出口國/地，例如，一般而言，如果貨物由源自美國的技術或軟件製成，則不管其製造國/地，該貨物均可被視為美國原產。）

h) 其他補充資料：

第二部份　　有關第一部份所述的產品資料 (請回答所有問題，並在適當格內加上 ✓號)

		是	否
Q.1	請說明所述的產品是否設計或改裝利用數位技術的密碼學來執行密碼功能。 如答案為「否」，請前往第三部份。	☐	☐
Q.2	(1) 請說明所述產品是否完全符合附件 1（第 6 頁）註釋 3（a）中所規定的物品。	☐	☐
	(2) 請說明該產品是否符合有多類別個人及行業對有關物品有潛在興趣。	☐	☐
	(3) 請說明該產品是否符合在購買前可獲取有關物品的價錢和主要功能資料。	☐	☐
Q.3	請說明所述產品是否完全符合附件 1（第 6 頁）註釋 3（b）中所規定之現有物品的硬部件或可執行軟件。 如答案為「是」，請列出現有物品的例子：包括牌子、型號和產品描述。 _____	☐	☐
Q.4	請說明所述產品是否經設計或改裝以使用設有‘說明的保安演算法’的‘資料機密性密碼學’的物品：		
	(1) 以‘資訊安全’為首要功能的物品；	☐	☐
	(2) 不在 Q.4 項目 (1) 管制中的數碼通訊或網絡連結系統、裝備或部件；	☐	☐
	(3) 不在 Q.4 項目 (1)或項目(2) 管制中的電腦、其他以資料儲存或處理為首要功能的物品及該等物品的部件；	☐	☐
	(4) 不在 Q.4 項目 (1)、項目 (2)及項目 (3)指明的物品，而其設有‘說明的保安演算法’的‘資料機密性密碼學’功能符合以下所有說明：		
	(i) 支援該物品的非首要功能；	☐	☐
	(ii) 由經裝嵌的裝備或‘軟件’執行，而該裝備或‘軟件’作為獨立物品時，屬類別 5 第 2 部份指明者；	☐	☐
	如在 Q.1 的回答為「是」，而在 Q.4 項目 (4)(ii) 的回答同樣為「是」，請提供能執行加密功能的獨立物品之詳細資料（例如：品牌，型號及產品操作細節） _____		

Q.5	請說明所述產品是否符合附件 2（第 7-8 頁）註釋 5A002 中提及的物品／裝備。 如答案為「是」，請說明在註釋 5A002 中相關段落的字母（例如：h） _____	☐	☐
Q.6	請說明所述產品的密碼功能用於 (1) 加密或解密數據文件（包括圖像，語音或文本等） (2) 其他，請說明：_____	 ☐ ☐	 ☐ ☐
Q.7	如 Q.6 的答案為「是」，請說明其保安演算法： (1) 「對稱演算法」 全名：_____； 密碼匙長度： _____ 位元； (2) 「非對稱演算法」 (i) 因子公解法的整數 (例如：RSA) ； 全名：_____； 密碼匙長度： _____ 位元； (ii) 乘法群的有限域中，離散對數之計算機化（例如：在於 Z/pZ 上之迪菲─赫爾曼技術（Diffie-Hellman））； 全名：_____； 密碼匙長度： _____ 位元； (iii) 在上述(2)(ii)提及者以外乘法群中的離散對數（例如：在於橢圓曲線上之迪菲─赫爾曼技術（Diffie-Hellman））； 全名：_____； 密碼匙長度： _____ 位元； (iv) 與格相關的最短向量或最近向量問題（例如: NewHope, Frodo, NTRUEncrypt，Kyber, Titanium）; 全名：_____； 密碼匙長度： _____ 位元； (v) 在超奇異橢圓曲線之間找尋同源（例如: 超奇異質性密鑰封裝 (Supersingular Isogeny Key Encapsulation)）; 全名：_____； 密碼匙長度： _____ 位元； (vi) 解碼隨機碼 (例如: McEliece, Niederreiter). 全名：_____； 密碼匙長度： _____ 位元；	☐ ☐	☐ ☐
Q.8	請說明所述產品密碼技術，用於下列任何密碼功能： (請選擇所有適用項目) (1) 核證 (2) 數碼簽署 (3) 資料完整性 (4) 不可否認性 (5) 數碼權管理，包括執行原件受保護的軟件	 ☐ ☐ ☐ ☐ ☐	 ☐ ☐ ☐ ☐ ☐

	(6) 支持娛樂、大眾商業廣播或醫療紀錄管理的加密或解密 (7) 只執行已公布密碼標準或商業密碼標準的無線個人區域網絡功能 (8) 特定為銀行用途或金錢交易(包括收集及結算費用或信貸功能)而設計(並只限於上述用途)的密碼操作 (9) 支援並只限於上方項目(1)至(8) 所述的功能及能力的金鑰管理 (10) 未被啟動或未被啟用的密碼功能或能力，而該等功能或能力只能以安全的啟動密碼方式啟動或啟用	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
Q.9	如 Q.8 的答案為「是」，請說明其保安演算法： (1) 「對稱演算法」 全名：_____； 密碼匙長度：_____ 位元； (2) 「非對稱演算法」 (i) 因子公解法的整數 (例如：RSA)； 全名：_____； 密碼匙長度：_____ 位元； (ii) 乘法群的有限域中，離散對數之計算機化（例如：在於 Z/pZ 上之迪菲─赫爾曼技術（Diffie-Hellman））； 全名：_____； 密碼匙長度：_____ 位元； (iii) 在上述(2)(ii)提及者以外乘法群中的離散對數（例如：在於橢圓曲線上之迪菲─赫爾曼技術（Diffie-Hellman））； 全名：_____； 密碼匙長度：_____ 位元； (iv) 與格相關的最短向量或最近向量問題（例如: NewHope, Frodo, NTRUEncrypt，Kyber, Titanium）; 全名：_____； 密碼匙長度：_____ 位元； (v) 在超奇異橢圓曲線之間找尋同源（例如: 超奇異質性密鑰封裝 (Supersingular Isogeny Key Encapsulation)）; 全名：_____； 密碼匙長度：_____ 位元； (vi) 解碼隨機碼 (例如: McEliece, Niederreiter). 全名：_____； 密碼匙長度：_____ 位元；	☐ ☐	☐ ☐

註釋：

品牌擁有人或須應要求提供相關詳情和證明資料，例如信件，以確認符合相關標準。

第三部份 第一部份產品的其他信息

		Yes	No
Q.10	源自美國的產品是否受美國出口管理條例 US EAR 740.17(b)(2)或 740.17(b)(3)(iii)管制？ 如答案為「是」，請提供由美國政府工業及安全局 (Bureau of Industry and Security) 發出的貨品分類自動追踪系統 (Commodity Classification Automated Tracking System (CCATS)) 的相關副本。	☐	☐

Q.11	(適用於通用集成電路) 請提供在整個周圍溫度內操作的額定溫度範圍：由攝氏_____至攝氏____度。 請說明有關集成電路是否為民用汽車或火車應用而設計的。	 ☐ ☐

第四部份　　聲明

本人聲明，本人是第一部份所述產品的**品牌擁有人**，據本人所知及所信，上述資料均屬真實無訛。

簽署人姓名： _____

簽署人在公司的職位： _____

(請以正楷填寫)

公司名稱： _____
(*註：公司名稱應與品牌擁有人名稱一致*)

簽署及公司印章： _____

公司電話： _____

公司電郵地址： _____

公司網頁： _____

日期： _____

重要說明：　本署會對此表格內的資料嚴格保密。不過，本署或會將該等資料向政府其他部門，或向在香港或其他地方的第三者披露。此等情況包括：本署認為需要披露該等資料，以便考慮有關的申請；為了維護本港貿易的利益；根據法律授權或規定；獲有關申請人／資料當事人明確同意披露該等資料。

工業貿易署署長有權要求申請人遞交額外資料及其他證明文件以支持有關的分類申請。問卷如未填妥，或未附有所需的文件，將延遲處理／不獲受理。

至於有關本署處理個人資料方面的詳情，請參閱本署就有關事項所發的說明。該等說明可於香港九龍城協調道 3 號工業貿易大樓 16 字樓戰略貿易管制科索取。

附件 1

第 60G 章 –《進出口(戰略物品)規例》類目 5 –「電訊及資訊安全」第 2 部 –「資訊安全」

<u>註釋 3</u>　<u>密碼學註釋：</u>

項目 5A002, 5D002(a)(1), 5D002(b)及 5D002(c)(1)不適用於以下物品：

(a) 符合以下所有描述的物品：

(1) 在零售點，以下列任何方式將存貨普遍而無限制地售予公眾：

(a) 門市交易；

(b) 郵購交易；

(c) 電子交易；

(d) 電話訂購交易；

(2) 密碼功能不能被用户輕易更改；

(3) 該物品的設計可供用户在無需供應商進一步大量支援下自行安裝；

(4) 在需要時，可應要求讓出口國有關主管當局查閱該物品的詳情並將該等詳情提供予該主管當局，以確定該物品符合上文(a)(1)、(2)及(3)段的描述；

(b) 為本註釋(a)段所描述的現有物品而設計、符合下列所有描述的硬部件或‘可執行軟件’：

(1) ‘資訊安全’並非該部件或‘可執行軟件’的首要功能或功能組合；

(2) 該部件或‘可執行軟件’沒有改變該等現有物品的任何密碼功能，亦沒有為該等現有物品加入新密碼功能；

(3) 該部件或‘可執行軟件’的特性設定是固定的，而非按顧客的指示而設計或改裝；

(4) 在出口國有關主管當局決定有需要時，可應要求讓該主管當局查閱該部件或‘可執行軟件’和有關最終物品的詳情並提供該等詳情予該主管當局，以確定該部件或‘可執行軟件’符合(b)(1)、(2)及(3)段的描述。

<u>技術註釋：</u>

就註釋 3 而言，‘可執行軟件’指出自被註釋 3 豁除於項目 5A002 之外的現有硬部件的、屬可執行形式的 ‘軟件’。

<u>註釋：</u>

‘可執行軟件’不包括在最終物品運行的 ‘軟件’的完整二進制影像。

附件 2

註釋

項目 5A002(a) 不管制以下任何一項物品或該等物品的特別設計 ‘資訊安全’部件：

(a) 以下的智能卡及智能卡‘讀卡器／寫卡器’：

(1) 符合以下任何一項說明的智能卡或可作電子閱讀的個人證件(例如代幣、電子護照)：

(a) 符合以下所有說明的設有‘說明的保安演算法’的‘資料機密性密碼學’：

(1) 限使用於項目5A002(a)所不適用(除密碼學註釋(類別5第2部註釋3)以外原因)的裝備或系統；

(2) 該功能的程式不能被重新編排作任何其他用途；

(b) 符合以下所有描述：

(1) 經特別設計並只限保障內存‘個人資料’之用；

(2) 已被個人化或只能個人化以作公眾或商業交易或個人識別用途；

(3) 設有‘說明的保安演算法’的‘資料機密性密碼學’並非使用者可取得；

技術註釋：

‘個人資料’ 包括關於某人或某實體的任何特定資料，例如所儲存的金額及進行認證所需的資料。

(2) ‘讀卡器／寫卡器’

技術註釋：

‘讀卡器／寫卡器’包括透過網絡跟智能卡或可作電子閱讀的文件連繫的裝備。

(b) *(廢除)*

注意：

至於原在本註釋(b)提及的物品，參閱項目5A002(a)技術註釋1第(h)段。

(c) 除了衞星電話以外，設計供民用並符合任何以下說明的手提或流動式無線電話：

(1) 不能直接傳送加密數據至其他無線電話或設備(無線電接入網絡裝備除外);

(2) 不能經無線電接入網絡裝備(例如無線電網絡控制器(RNC)或基地電台控制器(BSC))轉移加密數據；

(d) 不具備終點至終點加密能力，且製造商指明其沒有功率放大的無線操作的最大有效範圍(即終點與家居據點之間的唯一無中繼距程)少於 400 米的無線電話裝備；

(e) 設計供民用的手提或流動式無線電話和類似的客户無線裝置，而該等電話或裝置已調整其功能作特定的民間工業用途，且符合以下所有描述：

(1) 未調整的裝置，符合密碼學註釋(類別5第2部註釋3)的條文；

(2) 未經調整的裝置的設有‘說明的保安演算法’的‘資料機密性密碼學’不受有關調整影響，並只實施已公布密碼標準或商業密碼標準；

(f) *(廢除)*

注意：

至於原在本註釋(f)所描述的物品，參閱項目5A002(a)技術註釋1第(g)段。

(g) 設計供民用，並符合密碼學註釋(類別 5 第 2 部註釋 3)(a)(2)至(4)段的條文的流動通訊無線電接入網絡裝備，而該裝備具有的射頻輸出功率限於 0.1 瓦(20 dBm)或以下，以及支援32名或以下同步使用者；

(h) 路由器、轉換器、閘道器或中繼器，而設有‘說明的保安演算法’的‘資料機密性密碼學’只限實施已公布或商用密碼標準的 ‘操作、管理或維修’任務；

(i) 一般用途電腦裝備或伺服器，但以設有‘說明的保安演算法’的‘資料機密性密碼學’符合以下所有描述為限：

(1) 只實施已公布或商用密碼標準；

(2) 屬以下任何一項：

(a) 與符合類別 5 第 2 部註釋 3 的條文的中央處理器一體化；

(b) 與不適用於並非項目5D002的作業系統一體化；

(c) 限於 ‘操作、管理或維修’ 該裝備；

(j) 為‘連接的民間工業用途’而特別設計的，兼符合以下所有描述的物品：

(1) 屬以下任何一項：

(a) 符合以下任何描述、具網絡功能的端點裝置：

(1) 設有‘說明的保安演算法’的‘資料機密性密碼學’ 是限於獲取‘非任意資料’或 ‘操作、管理或維修’任務；

(2) 該裝置限於特定的 ‘連接的民間工業用途’；

(b) 符合以下所有描述的網絡連結裝備：

(1) 特別設計供與本註釋(j)(1)(a)段指明的裝置通訊；

(2) 設有‘說明的保安演算法’的‘資料機密性密碼學’是限於支援本註釋(j)(1)(a)段指明的裝置的‘連接的民間工業用途’，或本網絡連結裝備或本註釋(j)段指明的其他物品的‘操作、管理或維修’任務；

(2) 設有‘說明的保安演算法’的‘資料機密性密碼學’只實施已公布或商用密碼標準，而密碼功能不能被用户輕易更改。

技術註釋：

1. ‘連接的民間工業用途’ 是連接至網絡的消費者或民間工業用途，而該用途並不包括‘資訊安全’、數碼通訊、一般網絡連結或電腦用途。
2. ‘非任意資料’ 指直接關乎系統穩定性、性能或物理測量(如溫度、壓力、流速、質量、容量、電壓、物理位置等)的感測器或度量資料，而該等‘非任意資料’不能被有關裝置的用户更改。