

第 2 部—“資訊安全”

註釋：

1. 類別 5 第 2 部界定“資訊安全”裝備、“軟件”、系統、特定應用“電子組件”、模組、集成電路、部件或功能的狀況，而不論其是否為其他裝備的部件或“電子組件”。(2010 年第 45 號法律公告)

2. 類別 5 第 2 部不適用於被用戶攜帶作私人用途的產品。(2010 年第 45 號法律公告)

3. 密碼學註釋：

項目 5A002 及 5D002 不適用於符合以下所有各項說明的物品：
(2010 年第 45 號法律公告)

(a) 普遍地在沒有限制下在零售點以下述任何方式從存貨中向公眾售賣：

- (1) 門市交易；
- (2) 郵購交易；
- (3) 電子交易；或
- (4) 電話訂購交易；

(b) 其密碼功能不容易遭用戶更改；

(c) 該物品的設計可供用戶在並無供應商進一步充分支援下自行安裝；及 (2001 年第 132 號法律公告；2008 年第 254 號法律公告)

(d) 已刪除；(2001 年第 132 號法律公告)

(e) 如需要時，物品詳情可應要求而供出口國有關主管當局查閱或提供予出口國有關主管當局，以確定上文(a)至(c)段所描述的條件獲符合。(2001 年第 132 號法律公告；2010 年第 45 號法律公告)

4. 類別 5 第 2 部不適用於納入或使用“密碼學”並符合以下各項說明的物品：

(a) 首要功能或功能組合並非以下任何一項：

- (1) “資訊安全”；
- (2) 電腦，包括其作業系統、零件及部件；
- (3) 傳送、接收或貯存資料(支援娛樂、大眾商業廣播、數碼權管理及醫療紀錄管理除外)；
- (4) 網絡連結(包括操作、行政、管理及供應)；

(b) 密碼功能只限於支援其首要功能或功能組合；

(c) 如需要時，物品詳情可應要求而供出口國有關主管當局查閱或提供予出口國有關主管當局，以確定上文(a)及(b)段所描述的條件獲符合。

(2010 年第 45 號法律公告)

技術註釋：

在類別 5 第 2 部內，奇偶檢驗位並不包括在密碼匙長度內。

5A2 系統、裝備及部件

5A002 以下的“資訊安全”系統、其裝備及部件：

(a) 以下的“資訊安全”系統、裝備、特定應用“電子組件”、模組及集成電路，以及它們的為“資訊安全”而特別設計的部件：

注意：

至於包含或利用解密技術的全球衛星導航系統 (GNSS)接收裝備，參閱項目 7A005。(2010 年第 45 號法律公告)

(1) 設計或改裝以使用利用數位技術的“密碼學”，除執行認證或數位式簽名外，具有下列任何一項的任何密碼功能：

技術註釋：

1. 認證及數位式簽名功能包括其關鍵字管理功能。
2. 在檔案或文字並無受加密保護的情況下，認證的範圍包括所有存取的控制，但直接涉及為防止未授權盜用而對密碼、個人身份號碼(PINs)或類似資料予以保護者則除外。
3. “密碼學”不包括“固定式”資料壓縮或編碼技術。

註釋：

項目 5A002(a)(1)包括為在採用實施數位技術的同時以模擬原則運用“密碼學”而設計或改裝的裝備。

(a) 使用密碼匙長度超過 56 位元的“對稱演算法”；或

(b) “非對稱演算法”，其算法的保密性以下列任何一項為基準：

- (1) 超過 512 位元因子公解法的整數(例：RSA)；
- (2) 在具大於 512 位元的乘法群的有限域中將離散對數

計算機化(例如：迪菲—赫爾曼技術(Diffie-Hellman)在於 Z/pZ)；或

(3) 項目 5A002(a)(1)(b)(2)所述者以外超過 112 位元的乘法群中的離散對數(例如：迪菲—赫爾曼技術 (Diffie-Hellman)在於橢圓曲線)；

- (2) 設計或改裝成執行破解密碼的功能；
- (3) 已刪除；
- (4) 特別設計或改裝以減低超出健康、安全或電磁干預標準所需的帶有資訊的訊號的折衷發送；
- (5) 設計或改裝成使用密碼技術，以產生用於不受項目 5A002(a)(6)管制的“展頻”系統的延展碼(包括用於“跳頻”系統的跳躍碼)；(2001 年第 132 號法律公告；2006 年第 95 號法律公告)
- (6) 設計或改裝成使用密碼技術，以產生頻道碼、擾碼或網絡辨識碼，供用於使用超寬頻調變技術的系統，並且具有下列任何一項特性：
 - (a) 頻寬超過 500 兆赫；或
 - (b) “分頻寬” 20%或以上；(2006 年第 95 號法律公告)
- (7) 根據通用條件(CC)或等同準則被評為保證水平超過 EAL-6 級(評估保證水平)的非編碼的資訊及通訊科技(ICT)保安系統及裝置；(2009 年第 226 號法律公告)
- (8) 經設計或改裝的通訊纜線系統以使用機械、電機或電子方法偵測暗中入侵者；(2004 年第 65 號法律公告)
- (9) 設計或改裝以使用“量子密碼技術”；

技術註釋：
“量子密碼技術”亦稱為量子鑰匙分發(QKD)。 (2006 年第 95 號法律公告)

註釋：
項目 5A002 不包括以下任何一項：(2008 年第 254 號法律公告)

(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電子可讀個人證件(例如代幣、電子護照)：

(a) 密碼功能只限於在藉類別 5 第 2 部註釋 4 或本註釋 (d)、(e)、(f)、(g)及(i)段而豁除於項目 5A002 之外的裝備或系統中使用，而該功能的程式不可被重新編排作任何其他用途；

(b) 具有以下所有特性：

(1) 經特別設計用於保障貯存於卡內的‘個人資料’以及只限用於該用途；

(2) 已經或只可以將其個人化以作公眾或商業交易或個人識別；

(3) 密碼功能並非使用者可取得；

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，例如所貯存的金額及進行認證所需的資料。

(2) 為本註釋(a)(1)段指明的物品而特別設計或改裝並只限用於該物品的‘讀卡器/寫卡器’；

技術註釋：

‘讀卡器/寫卡器’包括透過網絡連繫智能卡或電子可讀文件的裝備。(2010 年第 45 號法律公告)

(b) 已刪除；(2010 年第 45 號法律公告)

(c) 已刪除；(2010 年第 45 號法律公告)

(d) 經特別設計的密碼裝備並只限使用於銀行或貨幣流通方面；

技術註釋：

項目 5A002 註釋(d)的“貨幣流通”包括費用的代收及結算或信貸功能。

(e) 不能直接傳送加密數據至其他無線電話或設備(無線電接入網絡設備除外)，亦不能經無線電接入網絡設備(例如無線電網絡控制器或基地電台控制器)轉移加密數據的民用(例如配合民用商業蜂巢式無線電通訊系統一起使用)手提或流動式無線電話；(2008 年第 254 號法律公告)

(f) 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無線操作的最大有效範圍(即終點與家居據點之間的一無中繼距離)少於 400 米的無線電話裝備；(2008 年第 254 號法律公告)

(g) 手提或流動式無線電話和類似的民用客戶無線裝置，而該等電話或裝置只採用已公布或商用的密碼標準(可能不公布的反盜版功能除外)，並符合密碼學註釋(類別 5 第 2 部註釋 3)(b)至(e)段的條文，且已調整其功能作特定的民間工業用途，而不影響原本未作調整的裝置所應具有的密碼功能；(2008 年第 254 號法律公告；2009 年第 226 號法律公告)

(h) 已刪除；(2010 年第 45 號法律公告)

(i) 只採用已公布或商用的密碼標準的無線“個人區域網絡”的裝備，且按照製造商的說明，密碼功能的標稱操作範圍只限於不超過 30 米。(2009 年第 226 號法律公告)

5B2 測試、檢驗及生產裝備

5B002 以下的“資訊安全”測試、檢驗及“生產”裝備：

(a) 為“發展”或“生產”項目 5A002 或 5B002(b)指明的裝備而特別設計的裝備；

(b) 為評估及驗證項目 5A002 指明的裝備或項目

5D002(a)或 5D002(c)指明的“軟件”的“資訊安全”功能而特別設計的測量裝備；
(2009 年第 226 號法律公告)

5C2 物料

無；

5D2 軟件

5D002 (a) 為“發展”、“生產”或“使用”項目 5A002 指明的裝備或項目 5D002(c)指明的“軟件”而特別設計或改裝的“軟件”；

(b) 為支援項目 5E002 指明的“技術”而特別設計或改裝的“軟件”；

(c) 以下的特定“軟件”：

(1) 具有項目 5A002 指明的裝備的特性，或可執行或模擬該裝備的功能的“軟件”；

(2) 核證項目 5D002(c)(1)指明的“軟件”的“軟件”；

註釋：(2008 年第 254 號法律公告)

項目 5D002 不管制：

(a) 項目 5A002 的註釋所指不受管制的裝備的“使用”所需的“軟件”；

(b) 提供項目 5A002 的註釋所指的不受管制的裝備的任何功能的“軟件”。

(2009 年第 226 號法律公告)

5E2 技術

5E002 (a) 按照一般技術註釋，供“發展”、“生產”或“使用”項目 5A002 或 5B002 指明的裝備或項目 5D002(a) 或 5D002(c)指明的“軟件”的“技術”；

(1999 年第 183 號法律公告；2009 年第 226 號法律公告)