TAICS

TAICS TS-0048 v1.0 : 2022

機上盒資安測試規範

Cybersecurity test specification for set-top boxes

2022/06/30

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

機上盒資安測試規範

Cybersecurity test specification for set-top boxes

出版日期: 2022/06/30

終審日期: 2022/03/29

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC 主席：神盾股份有限公司 張心玲 副總經理

TC 副主席：財團法人電信技術中心 林炫佑 副執行長

TC 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人電信技術中心 許博堯 副理、吳宗恩 工程師

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、中華電信股份有限公司、台灣是德科技股份有限公司、安華聯網科技股份有限公司、亞太電信股份有限公司、社團法人台灣數位電視協會、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、耀登科技股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國家通訊傳播委員會、台灣數位光訊科技股份有限公司、國立雲林科技大學

本規範由國家通訊傳播委員會支持研究制定

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業規範。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

數位經濟是國家發展之重要課題，其安全與可信賴的通傳網路則是重要之基礎，而機上盒屬於通傳網路用戶終端設備，也屬於通傳網路中的一環，除有線電視業者與多媒體隨選視訊服務(MOD)業者提供之機上盒，近年來亦有諸多以行動作業系統為基礎之 OTT(Over the Top, OTT)機上盒。用戶可使用內建或自行安裝影音視訊服務(如：Netflix、CatchPlay、HBO GO)，伴隨連網功能與應用日趨多元，包括影視服務、網購服務等，以致資安威脅相應而生。

以 CVE 漏洞為例，2020 年，由於機上盒可透過 Telnet 遠端服務於機器啟動時連帶開啟服務，攻擊者則可透過此服務連線進入機上盒系統存取系統儲存之敏感性資料；或機上盒使用未加密的方式通訊，導致攻擊者可惡意修改資訊，給予使用者錯誤訊息，甚至進行惡意詐騙或勒索威脅等惡意行為。又如 2021 年被發現機上盒存在訊息洩漏風險，該風險源於設備未對日誌進行身分驗證，攻擊者可利用該風險獲取使用者敏感性資料，甚至更進一步的攻擊。

基此，國家通訊傳播委員會(National Communications Commission, NCC)為確保機上盒之安全性，委託財團法人電信技術中心(Telecom Technology Center, TTC)參考國際標準、規範與指引，在台灣資通產業標準協會(Taiwan Association of Information and Communication Standards, TAICS)標準制定平臺，聚集產、官、學、研，依產業標準制定程序，進行機上盒資安標準之制定。後續除將建立產品認驗證制度，推動機上盒符合資安標準規範，以保障消費者的使用安全之外，同時協助產業提升資安能力及產品競爭力。

1. 適用範圍

本規範規定機上盒之資訊安全要求。機上盒是透過連接天線、衛星、同軸電纜、有線或無線網路，以接收並解調固定通信多媒體內容傳輸平臺、有線廣播電視系統及網際網路視聽服務平臺傳送之訊號，提供客戶端影視服務之終端設備。

適用範圍為機上盒本體，包含硬體、韌體、輸出入接口、傳輸協定、系統服務、出廠內建軟體、使用者在機上盒輸入的敏感性資料，及操作的訂閱繳費等金流活動。

不具備網路連線功能之機上盒設備、僅透過 APP 等軟體功能提供影視服務之行動裝置與個人電腦設備、影音內容保護及使用者額外安裝之 APP 與應用程式不在本標準規範之範圍。

適用範圍如圖 1 紅框所示。

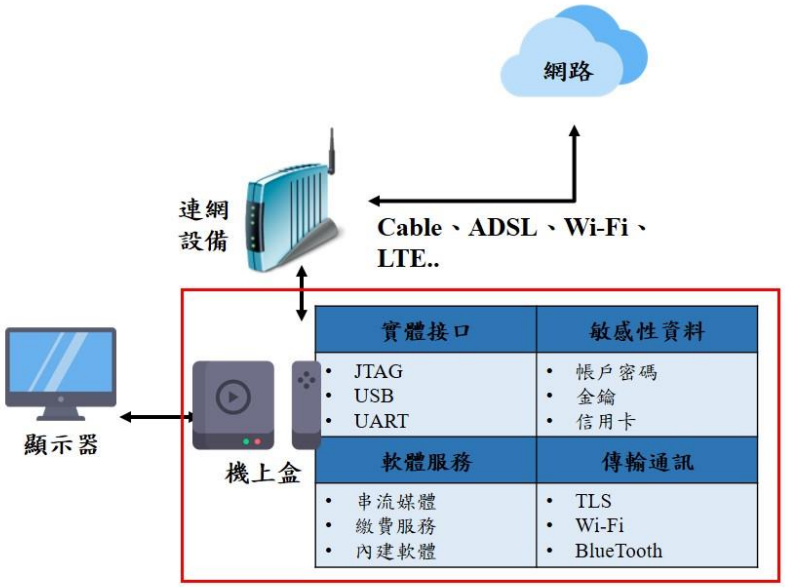

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(含補充增修)。未加註年份者，適用其最新版(含補充增修)。

[1] NIAP，Collaborative Protection Profile for Network Devices_V2.1：2019

[2] ITU-T，H.721 IPTV terminal devices: Basic model：2016

[3] CableLabs，Requirements CPE Security Common Security Requirements for IP-Based MSO-Provided CPE_V01：2013

[4] 國家通訊傳播委員會：資通安全指引 ISG012 - 具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視 機上盒資通安全檢測技術指引：2019

[5] 台灣資通產業標準協會：TAICS TS-0045 v1.0:2021 - 消費性物聯網產品資安標準：2021

[6] 台灣資通產業標準協會: TAICS TS-0029 v1.0:2020 -智慧型手機系統內建軟體資安標準：2020

[7] 台灣資通產業標準協會: TAICS TS-0047 v1.0 機上盒資安標準：2021

3. 用語及定義

TAICS TS-0047 v1.0「機上盒資安標準」所述，及下列用語及定義適用於本規範。

3.1 美國國家弱點資料庫（US National Vulnerabilities Database, NVD）

指美國國家標準暨技術研究院（US National Institute of Standards and Technology, NIST）提供的國家弱點資料庫，負責常見脆弱性與漏洞之資料的發布及更新。

3.2 常見弱點與漏洞(Common Vulnerabilities and Exposures, CVE)

指美國國土安全部贊助之弱點管理計畫，該計畫針對每一弱點項目賦予其全球認可唯一共同編號。

3.3 傳輸層安全性協定(Transport Layer Security, TLS)

指一種安全協定，為網際網路通訊提供安全及資料完整性保障。1999 年公布第一版 TLS 標準檔案。在瀏覽器、電子郵件、即時通訊、網路電話(Voice over Internet Protocol，VoIP)、網路傳真等應用程式中，廣泛支援這個協定。

3.4 完整性(Integrity)

指資料不會被未經授權改變或破壞的特性。

3.5 憑證(Certificate)

指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

3.6 受限制設備(Constrained Device)

為此類設備預期用途受限於實體而產生的限制，包括但不限於處理資料的能力、通訊的能力、資料儲存的能力或與使用者互動的能力。例如感測器，它可能是：

(a) 實體限制的設備，可能因電源、電池壽命、運算處理能力、實體的存取、功能有限、記憶體有限或網路頻寬有限，這些限制在設備運行時可能需要搭配另一設備來支援；或

(b) 可能是透過同一實體線路供電與資料傳輸，此設備的通訊協定與加密方式就受限於該線路配置。

4. 測試項目分級

本節依據 TAICS TS-0047 v1.0「機上盒資安標準」制定相對應之安全測試項目與測試方法，產品應先通過較低安全等級之測試，始可進行進階等級之測試。

實機測試標準等級總表，如表 1 所示，第一欄為安全構面，包括：(1)可用性、(2)身分識別、(3)隱私加密、(4)安全功能；第二欄為安全要求分項，係依各安全構面設計對應之安全要求；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求應先滿足較低安全等級要求。

表 1 實機測試標準等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 可用性	5.1.1 系統更新	5.1.1.1 5.1.1.2 5.1.1.3	-	-
	5.1.2 Wi-Fi 及藍牙模糊測試	-	5.1.2.1 5.1.2.2	-
	5.1.3 安全性回報	5.1.3.1	-	-
5.2 身分識別	5.2.1 工程模式	5.2.1.1		-
	5.2.2 繳費功能身分識別	-	-	5.2.2.1
5.3 隱私加密	5.3.1 登入保密功能	5.3.1.1	-	-
	5.3.2 最小化通訊埠	5.3.2.1	-	-
	5.3.3 資料傳輸	5.3.3.1 5.3.3.2	5.3.3.3	-
	5.3.4 敏感性資料存取	5.3.4.1 5.3.4.2	-	-
	5.3.5 資料紀錄刪除	5.3.5.1	-	-
	5.3.6 資料儲存保護	5.3.6.1	5.3.6.2 5.3.6.3 5.3.6.4	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.4 安全功能	5.4.1 作業系統常見漏洞	5.4.1.1	5.4.1.2	5.4.1.3
	5.4.2 實體埠安全	-	5.4.2.1	5.4.2.2
	5.4.3 敏感性資料儲存	-	-	5.4.3.1 5.4.3.2 5.4.3.3 5.4.3.4
	5.4.4 Wi-Fi 網路熱點	5.4.4.1	-	-
	5.4.5 內建軟體安全	-	5.4.5.1	5.4.5.2 5.4.5.3

5. 資安測試規範

檢視機上盒受測裝置設備、系統功能及傳輸通訊與廠商之書面送審資料相符且滿足安全測試需求，並確認其韌體版本於測試前更新為最新版本，以維持服務正常使用、新增功能或安全性。本章節定義之測試項目可依以下規範之測試佈局進行實機檢測。

圖 2 測試佈局一

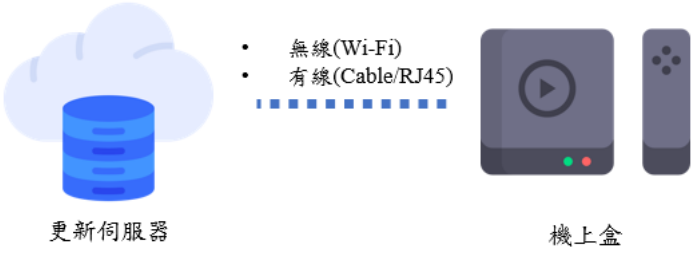

圖 3 測試佈局二

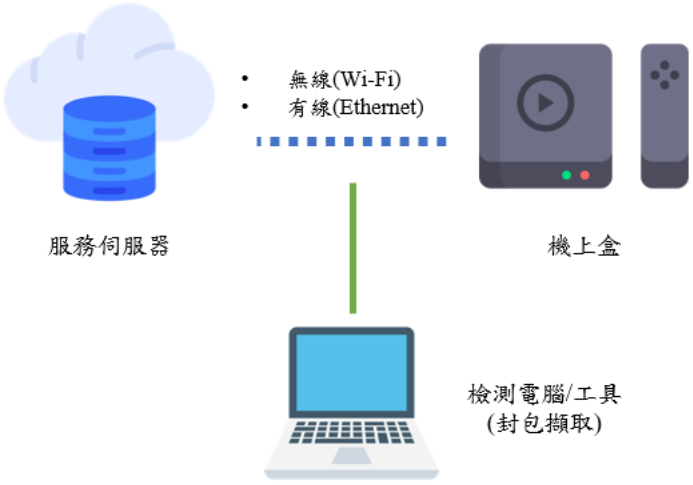

圖 4 測試佈局三

圖 5 測試佈局四

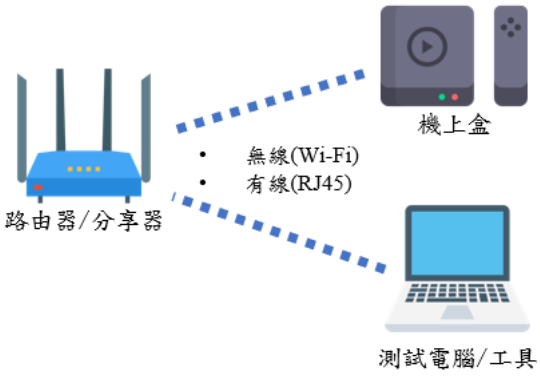

圖 6 測試佈局五

圖 7 測試佈局六

5.1 可用性

5.1.1 系統更新

5.1.1.1 機上盒應支援更新功能。

(a) 測試依據：

TAICS TS-0047 v.1.0「機上盒資安標準」第 5.1.1.1 節。

(b) 測試目的：

(c) 驗證機上盒是否具備更新功能。

(d) 測試條件：

(1) 請廠商協助更新(可能須至電視業者所在地進行)。

(e) 測試佈局：如圖 3。

(f) 測試方法：

(1) 請廠商先將機上盒版本降版後，執行更新升級至測試版本。

(2) 檢視是否完成系統更新，運行正常。

(g) 測試結果：

(1) 通過：可完成更新作業且服務運行正常。

(2) 不通過：無法完成更新或服務無法正常運行或屬於非受限制設備且無提供更新更能。

(3) 不適用：屬於受限制設備，請廠商於「附錄 A-廠商自我宣告表」說明。

5.1.1.2 機上盒進行系統更新後，用戶設定應與更新前相符。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.1.1.2 節。

(b) 測試目的：

驗證機上盒進行系統更新後，用戶設定(如：親子鎖、登入之帳戶或安裝之軟體)是否與更新前一致。

(c) 測試條件：

(1) 請廠商協助更新(可能須至電視業者所在地進行)。

(2) 具備更新功能。

(d) 測試佈局：如圖 3。

(e) 測試方法：

(1) 於機上盒上更改設定(如：更改親子鎖、登入帳戶、安裝軟體)。

(2) 請廠商先將機上盒版本降版後，執行更新升級至測試版本。

(3) 測試更新前變更之設定，檢視設定是否正常或還原。

(f) 測試結果：

(1) 通過：使用者設定可使用且未變回預設。

(2) 不通過：使用者設定無法使用或變回預設。

(3) 不適用：無更新功能。

5.1.1.3 機上盒更新服務應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.1.1.3 節。

(b) 測試目的：

驗證機上盒使用更新服務時是否使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(c) 測試條件：

(1) 請廠商協助更新(可能須至電視業者所在地進行)。

(2) 具備線上更新功能(採用 Wi-Fi、Ethernet 進行更新)。

(3) 請廠商於「附錄 A-廠商自我宣告表」提供更新伺服器 IP。

(d) 測試佈局：如圖 4。

(e) 測試方法：

(1) 請廠商先將機上盒版本降版後，執行更新升級至測試版本。

(2) 使用工具擷取更新封包。

(f) 測試結果：

(1) 通過：傳輸使用 TLS 1.2 同等或以上之安全通訊協定，並採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(2) 不通過：使用低於 TLS1.2 之加密編譯演算法，或未採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(3) 不適用：無更新功能或使用 Cable 進行更新。

5.1.2 Wi-Fi 及藍牙模糊測試

5.1.2.1 機上盒 Wi-Fi 傳輸應具有抗異常封包格式之保護機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.1.2.1 節。

(b) 測試目的：

驗證 Wi-Fi 傳輸接受測試樣本時，是否影響或中斷機上盒服務運行。

(c) 測試條件：

(1) 具備 Wi-Fi 熱點功能。

(2) 具備 Wi-Fi 接收功能。

(d) 測試佈局：如圖 5。

(e) 測試方法：

(1) 使用模糊測試工具對機上盒 Wi-Fi 熱點與 Wi-Fi 接收端進行測試。

(2) 針對具備之功能各傳輸 1,000,000 筆隨機樣本測試，或是連續傳輸樣本測試 8 小時。

(f) 測試結果：

(1) 通過：機上盒未中斷服務或重新啟動。

(2) 不通過：機上盒中斷服務或重新啟動。

(3) 不適用：未具備 Wi-Fi 熱點功能與 Wi-Fi 接收功能。

5.1.2.2 機上盒藍牙傳輸應具有抗異常封包格式之保護機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.1.2.2 節。

(b) 測試目的：

驗證藍牙傳輸接受測試樣本時，是否影響或中斷機上盒服務運行。

(c) 測試條件：

(1) 具備藍牙功能。

(d) 測試佈局：如圖 5。

(e) 測試方法：

(1) 使用模糊測試工具對機上盒藍牙功能進行測試。

(2) 傳輸 1,000,000 筆隨機樣本測試，或是連續傳輸樣本測試 8 小時。

(f) 測試結果：

(1) 通過：機上盒未中斷服務或重新啟動。

(2) 不通過：機上盒中斷服務或重新啟動。

(3) 不適用：未具備藍牙功能。

5.1.3 安全性回報

5.1.3.1 機上盒應具備安全性回報之機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.1.3.1 節。

(b) 測試目的：

驗證機上盒是否提供安全性回報之機制。

(c) 測試條件：無。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 檢查機上盒其官方網站或使用說明書是否提供問題回報機制(如：電話、E-mail 或線上客服等)。

(f) 測試結果：

(1) 通過：提供之問題回報機制並可實際聯絡成功。

(2) 不通過：無提供問題回報機制或無法聯絡成功。

(3) 不適用：無。

5.2 身分識別

5.2.1 工程模式

5.2.1.1 機上盒工程模式通行碼應為 8 字元(含)以上。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.2.1.1 節。

(b) 測試目的：

驗證機上盒提供的工程模式通行碼是否為 8 字元(含)以上。

(c) 測試條件：

(1) 提供工程模式。

(2) 使用通行碼方式進入工程模式。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」是否說明提供工程模式及進入方法。

(2) 檢視機上盒工程模式所需的通行碼是否為 8 字元(含)以上。

(f) 測試結果：

(1) 通過：工程模式通行碼具備 8 字元(含)以上。

(2) 不通過：工程模式通行碼不足 8 字元或無須通行碼即可進入工程模式。

(3) 不適用：使用非通行碼方式進入工程模式或未提供工程模式。

5.2.2 繳費功能身分辨識

5.2.2.1 機上盒服務與內建軟體繳費功能應使用多因子鑑別或強鑑別進行用戶身分辨識。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.2.2.1 節。

(b) 測試目的：

驗證使用機上盒服務或內建軟體使用繳費功能時，是否使用多因子或強鑑別來進行用戶身分辨識。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備繳費功能。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 運行機上盒內建服務與「附錄 B-內建軟體摘要表」提供之具備繳費功能內建軟體。

(2) 執行具備繳費功能之服務。

(3) 檢測是否支援多因子鑑別或強鑑別。

(f) 測試結果：

(1) 通過：身分驗證機制支援多因子鑑別(至少採用兩種因子以上)或強鑑別(包括但不限於硬體或軟體 Token、公開金鑰驗證、FIDO 聯盟之 UAF、U2F、FIDO2/WebAuthn 等驗證機制)。

(2) 不通過：無支援多因子鑑別或強鑑別。

(3) 不適用：未具備繳費功能。

5.3 隱私加密

5.3.1 登入保密功能

5.3.1.1 機上盒進行通行碼輸入時，應以特殊字元進行遮蔽。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.1.1 節。

(b) 測試目的：

驗證輸入通行碼時(如：親子鎖、工程模式、Wi-Fi 連接)，是否以特殊字元遮蔽輸入之通行碼。

(c) 測試條件：

(1) 具備親子鎖功能。

(2) 具備工程模式。

(3) 具備 Wi-Fi 接收功能。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 分別進入執行工程模式、鎖碼頻道、Wi-Fi 連接。

(2) 檢視輸入之通行碼。

(f) 測試結果：

(1) 通過：輸入之通行碼皆以特殊字元遮蔽。

(2) 不通過：輸入之通行碼以明文顯示。

(3) 不適用：未提供工程模式、親子鎖或 Wi-Fi 功能。

5.3.2 最小化通訊埠

5.3.2.1 機上盒系統與服務應關閉非必要使用的通訊埠及遠端存取服務。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.2.1 節。

(b) 測試目的：

驗證機上盒是否預設開啟不必要或未知的通訊埠及遠端存取服務。

(c) 測試條件：無。

(d) 測試佈局：如圖 6。

(e) 測試方法：

(1) 將機上盒還原為出廠狀態。

(2) 使用檢測工具對通訊埠進行掃描。

(f) 測試結果：

(1) 通過：掃描結果與「附錄 A-廠商自我宣告表」中宣告的預設開啟之通訊埠一致，且未開啟遠端存取服務。

(2) 不通過：發現開啟未知、不必要的通訊埠或遠端管理通訊埠。

(3) 不適用：無。

5.3.3 資料傳輸

5.3.3.1 機上盒 OTT 服務應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.3.1 節。

(b) 測試目的：

驗證機上盒使用 OTT 服務時是否使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(c) 測試條件：

(1) 請廠商協助(可能須至電視業者所在地進行)。

(2) 具備 OTT 服務(採用 Wi-Fi、Ethernet 進行傳輸)。

(d) 測試佈局：如圖 4。

(e) 測試方法：

(1) 在機上盒與 OTT 伺服器網路來源間進行封包側錄。

(f) 測試結果：

(1) 通過：傳輸使用 TLS 1.2 同等或以上之安全通訊協定，並採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(2) 不通過：使用低於 TLS1.2 之加密編譯演算法，或未採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(3) 不適用：未提供 OTT 服務或使用 Cable 傳輸。

5.3.3.2 機上盒繳費功能應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.3.2 節。

(b) 測試目的：

驗證機上盒使用線上繳費服務時是否使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(c) 測試條件：

(1) 內建繳費服務(非內建軟體)。

(2) 具備線上繳費功能(採用 Wi-Fi、Ethernet 進行傳輸)。

(3) 請廠商於「附錄 A-廠商自我宣告表」提供繳費服務之伺服器 IP。

(d) 測試佈局：如圖 4。

(e) 測試方法：

(1) 執行機上盒線上繳費功能。

(2) 在機上盒與網路來源間進行封包側錄。

(3) 檢視使用之安全通訊協定。

(f) 測試結果：

(1) 通過：傳輸使用 TLS 1.2 同等或以上之安全通訊協定，並採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(2) 不通過：使用低於 TLS1.2 之加密編譯演算法，或未採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(3) 不適用：未提供繳費服務或使用 Cable 傳輸。

5.3.3.3 機上盒內建軟體繳費功能應使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.3.3 節。

(b) 測試目的：

驗證內建軟體使用線上繳費服務時是否使用 TLS 1.2(含)以上之國際標準安全加密通道傳輸。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備線上繳費功能(採用 Wi-Fi、Ethernet 進行傳輸)。

(d) 測試佈局：如圖 4。

(e) 測試方法：

(1) 根據「附錄 B-內建軟體摘要表」提供之內建軟體與廠商提供對應繳費功能之 IP。

(2) 執行內建軟體線上繳費功能。

(3) 在機上盒與網路來源間進行封包側錄。

(4) 檢視使用之安全通訊協定。

(f) 測試結果：

(1) 通過：傳輸使用 TLS 1.2 同等或以上之安全通訊協定，並採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(2) 不通過：使用低於 TLS1.2 之加密編譯演算法，或未採用 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(3) 不適用：未提供繳費服務或使用 Cable 傳輸。

5.3.4 敏感性資料存取

5.3.4.1 機上盒服務與內建軟體存取敏感性資料時，應提供隱私權政策或使用聲明。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.4.1 節。

(b) 測試目的：

驗證使用機上盒服務與內建軟體需求敏感性資料時，是否提供隱私權政策或使用聲明。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 需求敏感性資料。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 執行機上盒服務與「附錄 B-內建軟體摘要表」提供之內建軟體。

(2) 檢視是否需求敏感性資料，且有無提供隱私權政策或使用聲明。

(f) 測試結果：

(1) 通過：提供隱私權政策或使用聲明。

(2) 不通過：未提供隱私權政策或使用聲明。

(3) 不適用：無須敏感性資料。

5.3.4.2 機上盒內建軟體開啟之權限，應與使用者同意開啟之權限一致。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.4.2 節。

(b) 測試目的：

驗證使用機上盒內建軟體開啟之權限，是否與使用者同意開啟之權限一致。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 執行「附錄 B-內建軟體摘要表」提供之內建軟體。

(2) 檢視是否需求使用者相關權限，且有無詢問使用者是否同意授權。

(3) 檢視應用程式開啟之權限，是否與詢問之權限一致。

(f) 測試結果：

(1) 通過：提供使用者授權機制，且與開啟之權限一致。

(2) 不通過：未經詢問即開啟未經授權之權限，或發現開啟未同意之權限。

(3) 不適用：無。

5.3.5 資料紀錄刪除

5.3.5.1 機上盒應具備可刪除使用者資料紀錄之機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.5.1 節。

(b) 測試目的：

驗證使用機上盒是否提供之刪除機制，可完全清除使用者資料紀錄。

(c) 測試條件：

(1) 具備記錄使用者資料(如帳戶、繳費資訊或訂購資訊等)。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 請廠商提供可刪除使用者資料紀錄之機制。

(2) 執行機上盒產生使用者資料紀錄(如帳戶登入、繳費或訂購等)。

(3) 執行廠商提供之刪除機制。

(4) 檢視產生之資料紀錄是否刪除。

(f) 測試結果：

(1) 通過：提供刪除機制且使用者資料紀錄已刪除。

(2) 不通過：未提供刪除機制或使用者資料紀錄未刪除。

(3) 不適用：不具備記錄使用者資訊功能(如帳戶、繳費資訊或訂購資訊等)。

5.3.6 資料儲存保護

5.3.6.1 機上盒提供使用者之紀錄或日誌，不應將敏感性資料以明文顯示。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.6.1 節。

(b) 測試目的：

驗證機上盒提供用戶之紀錄或日誌，是否將敏感性資料以明文顯示。

(c) 測試條件：

(1) 具備供使用者瀏覽之紀錄或日誌。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 啟動機上盒，檢視是否提供使用者瀏覽之紀錄或日誌。

(2) 檢視其內容是否明文顯示敏感性資料。

(f) 測試結果：

(1) 通過：未明文顯示敏感性資料。

(2) 不通過：明文顯示敏感性資料。

(3) 不適用：未提供使用者瀏覽之紀錄或日誌。

5.3.6.2 機上盒內建軟體應將帳號、通行碼或金鑰儲存於作業系統保護區內或以加密方式儲存。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.6.2 節。

(b) 測試目的：

驗證機上盒內建軟體是否將帳號、通行碼或金鑰儲存在作業系統保護區內或以加密方式儲存。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備帳號通行碼登入功能。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 運行「附錄 B-內建軟體摘要表」提供之內建軟體

(2) 執行具備輸入帳號、通行碼之內建軟體，同意儲存帳號與通行碼，並登入。

(3) 在非作業系統保護區內所存放之檔案進行讀取。

(4) 檢查是否將帳號、通行碼或金鑰以明文型態存放於非作業系統保護區內。

(f) 測試結果：

(1) 通過：以加密方式儲存或未發現儲存於非作業系統保護區。

(2) 不通過：以明文儲存於非作業系統保護區。

(3) 不適用：未具備帳號通行碼登入功能。

5.3.6.3 機上盒內建軟體不應將帳號、通行碼或金鑰以明文方式存在於執行檔中。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.6.3 節

(b) 測試目的：

驗證內建軟體之帳號、通行碼或金鑰，是否以明文方式儲存於執行檔中。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備帳號通行碼登入功能。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 請廠商提供「附錄 B-內建軟體摘要表」之內建軟體執行檔，或原始碼。

(2) 使用工具將內建軟體執行檔還原為原始碼。

(3) 檢視原始碼中是否以明文方式儲存帳號、通行碼或金鑰。

(f) 測試結果：

(1) 通過：未發現明文顯示之帳號、通行碼或金鑰。

(2) 不通過：發現明文顯示之帳號、通行碼或金鑰。

(3) 不適用：未具備帳號通行碼登入功能。

5.3.6.4 機上盒內建軟體不應在執行期間將敏感性資料明文儲存於系統日誌中。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.3.6.4 節。

(b) 測試目的：

驗證內建軟體在執行期間是否將敏感性資料明文儲存於系統日誌中。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備帳號通行碼登入功能。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 使用工具連接機上盒，開啟機上盒系統日誌。

(2) 根據「附錄 B-內建軟體摘要表」執行具備帳號通行碼登入功能之內建軟體，並完成登入。

(3) 檢視內建軟體是否在執行期間將敏感性資料明文儲存於系統日誌中。

(f) 測試結果：

(1) 通過：未發現明文顯示敏感性資料。

(2) 不通過：發現明文顯示敏感性資料。

(3) 不適用：未具備帳號通行碼登入功能。

5.4 安全功能

5.4.1 作業系統常見漏洞

5.4.1.1 機上盒作業系統不應存有 CVSS 評分 9.0(含)以上的已知漏洞。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.1.1 節。

(b) 測試目的：

驗證作業系統是否存有 CVSS 評分 9.0(含)以上的已知漏洞。

(c) 測試條件：無。

(d) 測試佈局：如圖 6。

(e) 測試方法：

(1) 將機上盒還原為出廠狀態。

(2) 更新弱點掃描工具漏洞資料庫。

(3) 使用弱點掃描工具對作業系統進行檢測。

(f) 測試結果：

(1) 通過：未發現 CVSS 評分為 9.0(含)以上的已知漏洞。

(2) 不通過：發現 CVSS 評分為 9.0(含)以上的已知漏洞。

(3) 不適用：無。

5.4.1.2 機上盒作業系統不應存有 CVSS 評分 7.0(含)以上的已知漏洞。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.1.2 節。

(b) 測試目的：

驗證作業系統是否存有 CVSS 評分 7.0(含)以上的已知漏洞。

(c) 測試條件：無。

(d) 測試佈局：如圖 6。

(e) 測試方法：

(1) 將機上盒還原為出廠狀態。

(2) 更新弱點掃描工具漏洞資料庫。

(3) 使用弱點掃描工具對作業系統進行檢測。

(f) 測試結果：

(1) 通過：未發現 CVSS 評分為 7.0(含)以上的已知漏洞。

(2) 不通過：發現 CVSS 評分為 7.0(含)以上的已知漏洞。

(3) 不適用：無。

5.4.1.3 機上盒作業系統不應存有 CVSS 評分 4.0(含)以上的已知漏洞。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.1.3 節。

(b) 測試目的：

驗證作業系統是否存 CVSS 評分 4.0(含)以上的已知漏洞。

(c) 測試條件：無。

(d) 測試佈局：如圖 6。

(e) 測試方法：

(1) 將機上盒還原為出廠狀態。

(2) 更新弱點掃描工具漏洞資料庫。

(3) 使用弱點掃描工具對作業系統進行檢測。

(f) 測試結果：

(1) 通過：未發現 CVSS 評分為 4.0(含)以上的已知漏洞。

(2) 不通過：發現 CVSS 評分為 4.0(含)以上的已知漏洞。

(3) 不適用：無。

5.4.2 實體埠安全

5.4.2.1 機上盒不得透過實體介面直接進入作業系統之除錯模式。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.2.1 節。

(b) 測試目的：

驗證機上盒是否可在未經授權下透過實體介面(如 UART、USB、JTAG)進入系統除錯模式。

(c) 測試條件：

(1) 機上盒具備實體介面。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 檢視「附錄 A-廠商自我宣告表」中是否使用實體介面進入除錯模式。

(2) 測試電腦連接機上盒之實體介面。

(3) 確認是否透過實體介面進入系統除錯模式。

(f) 測試結果：

(1) 通過：連接實體介面未有任何資訊回饋，或需進行身分驗證才可進入。

(2) 不通過：可直接進入系統除錯模式。

(3) 不適用：未具備實體介面可進入除錯模式。

5.4.2.2 機上盒應具備紀錄內部系統登入登出之日誌機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.2.2 節。

(b) 測試目的：無

(c) 測試條件：無。

(d) 測試佈局：無。

(e) 測試方法：

(1) 請廠商於「附錄 C-安全功能表」說明作為審查依據。

(f) 測試結果：

(1) 通過：「附錄 C-安全功能表」證實機上盒提供紀錄內部系統登入登出之日誌。

(2) 不通過：無法證實機上盒提供紀錄內部系統登入登出之日誌。

(3) 不適用：無。

5.4.3 安全資料儲存

5.4.3.1 機上盒持久性儲存器內之關鍵安全參數應具備保護機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.3.1 節。

(b) 測試目的：

驗證產品持久性儲存器之關鍵安全參數是否加密儲存或存放安全區域。

(c) 測試條件：

(1) 請廠商提供持久性儲存器中的關鍵安全參數之保存方式之書面資料作為審查依據。

(2) 依廠商聲明使用的安全儲存技術之書面資料作為審查依據，包括但不限於加密儲存、儲存於安全區域。

(d) 測試佈局：無。

(e) 測試方法：

(1) 請廠商於「附錄 C-安全功能表」說明作為審查依據。

(f) 測試結果：

(1) 通過：「附錄 C-安全功能表」證實產品之關鍵安全參數已加密儲存或存放於安全區域。

(2) 不通過：無法證實關鍵安全參數已加密儲存和存放於安全區域。

(3) 不適用：無。

5.4.3.2 機上盒產品唯一識別碼應具備防篡改之機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.3.2 節。

(b) 測試目的：

驗證產品之唯一識別碼是否以常數的形式儲存撰寫在原始碼中，或以雜湊演算法及簽章方式確保防止被篡改。

(c) 測試條件：

(1) 產品應支援產品識別碼唯一性。

(2) 產品應提供保護產品唯一識別碼遭篡改之安全設計書面資料作為審查依據。

(d) 測試佈局：無。

(e) 測試方法：

(1) 請廠商於「附錄 C-安全功能表」說明作為審查依據。

(f) 測試結果：

(1) 通過：「附錄 C-安全功能表」證實機上盒以安全晶片方式將產品唯一識別碼以常數的形式儲存撰寫在原始碼中或以雜湊演算法及簽章方式確保防止被篡改。

(2) 不通過：無法證實具備此安全設計。

(3) 不適用：產品不支援產品識別碼唯一性。

5.4.3.3 機上盒韌體檔內之關鍵安全參數應具備保護機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.3.3 節。

(b) 測試目的：

驗證產品之韌體程式碼是否存在未保護之關鍵安全參數。

(c) 測試條件：

(1) 廠商應提供產品之韌體檔案。

(2) 廠商應提供所使用之加密演算法書面資料作為審查依據。

(d) 測試佈局：無。

(e) 測試方法：

(1) 請廠商於「附錄 C-安全功能表」說明作為審查依據。

(2) 將廠商提供之韌體，使用具韌體拆解工具進行分析。

(3) 檢視韌體更新檔是否可被解析出檔案系統目錄。

(4) 確認是否有關鍵安全參數可被搜索。

(f) 測試結果：

(1) 通過：韌體無法解析出關鍵安全參數。

(2) 不通過：可搜索出關鍵安全參數。

(3) 不適用：無。

5.4.3.4 機上盒更新及關連服務間傳輸之關鍵安全參數應具備唯一性。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.3.4 節。

(b) 測試目的：

驗證產品於更新及與關連服務間傳輸所使用之關鍵安全參數是否具有唯一性。

(c) 測試條件：

(1) 廠商應聲明所使用之關鍵安全參數為何之書面資料作為審查依據。

(2) 廠商應提供具有唯一性關鍵安全參數生成機制之書面資料作為審查依據。

(d) 測試佈局：無。

(e) 測試方法：

(1) 請廠商於「附錄 C-安全功能表」說明作為審查依據。

(f) 測試結果：

(1) 通過：「附錄 C-安全功能表」證實產品用於更新及與關連服務間傳輸所使用的關鍵安全參數具唯一性。

(2) 不通過：無法證實關鍵安全參數具唯一性。

(3) 不適用：無。

5.4.4 Wi-Fi 網路熱點

5.4.4.1 機上盒開啟熱點時應提供 WPA2 以上加密通訊協定且應允許設定高複雜性之通行碼機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.4.1 節。

(b) 測試目的：

驗證機上盒開啟熱點是否提供 WPA2 以上加密通訊協定，且可讓使用者最少設定 8 碼，且包含特殊符號、大小寫英文或數字四種選三種字元組成之通行碼。

(c) 測試條件：

(1) 機上盒具備 Wi-Fi 熱點功能。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 開啟機上盒提供之熱點。

(2) 使用測試電腦連接熱點，並檢測其通訊協定。

(3) 測試是否接受 8 碼以上，包含特殊符號、大小寫英文或數字四種選三種字元組成通行碼之設定。

(f) 測試結果：

(1) 通過：使用 WPA2 以上加密通訊協定傳輸資料，且可接受設定 8 碼以上，包含特殊符號、大小寫英文或數字四種選三種字元組成之通行碼。

(2) 不通過：未使用 WPA2 以上加密通訊協定傳輸資料，或無法設定 8 碼以上，包含特殊符號、大小寫英文或數字四種選三種字元組成之通行碼。

(3) 不適用：未具備 Wi-Fi 熱點功能。

5.4.5 內建軟體安全

5.4.5.1 機上盒內建軟體之執行檔不應存有 CVSS 評分 7.0(含)以上的已知漏洞。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.5.1 節。

(b) 測試目的：

驗證機上盒內建軟體是是否存有 CVSS 評分 7.0(含)以上的已知漏洞。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 請廠商提供「附錄 B-內建軟體摘要表」之內建軟體執行檔。

(2) 更新弱點掃描工具漏洞資料庫。

(3) 掃描內建軟體。

(f) 測試結果：

(1) 通過：內建軟體未發現 CVSS 評分為 7.0 分(含)以上的已知漏洞。

(2) 不通過：內建軟體發現 CVSS 評分為 7.0 分(含)以上的以之漏洞。

(3) 不適用：無。

5.4.5.2 機上盒內建軟體可輸入之欄位應具備防護注入攻擊之機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.5.2 節。

(b) 測試目的：

驗證機上盒內建軟體提供之輸入欄位是否具備注入攻擊之防護機制。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(2) 具備可供使用者輸入資料之欄位。

(d) 測試佈局：如圖 2。

(e) 測試方法：

(1) 根據「附錄 B-內建軟體摘要表」之具備可供使用者輸入資料之欄位內建軟體。

(2) 執行內建軟體，並輸入 SQL 隱碼攻擊(SQL Injection Attack)、本地文件包含漏洞(Local File Inclusion)、JavaScript 注入攻擊(JavaScript Injection Attack)、格式化字串(Format String)與指令注入攻擊(Command Injection Attack)常見攻擊字串。

(f) 測試結果：

(1) 通過：未反饋任何資料，或未對輸入之字串有異常回應。

(2) 不通過：成功執行攻擊字串，造成軟體出錯，或是回饋非正常之資訊。

(3) 不適用：未具備可供使用者輸入資料之欄位。

5.4.5.3 機上盒內建軟體之執行檔應具備反編譯防護機制。

(a) 測試依據：

TAICS TS-0047 v1.0「機上盒資安標準」第 5.4.5.3 節。

(b) 測試目的：

驗證機上盒內建軟體之執行檔是否具備防止逆向工程機制，避免敏感性資料遭破解取得。

(c) 測試條件：

(1) 內建有圖示軟體、無圖示軟體(選測)。

(d) 測試佈局：如圖 7。

(e) 測試方法：

(1) 請廠商提供「附錄 B-內建軟體摘要表」之內建軟體執行檔。

(2) 使用反編譯工具將內建軟體執行檔進行逆向工程，檢查程式碼是否有加殼或混淆。

(f) 測試結果：

(1) 通過：反編譯工具未能執行成功或反編譯之程式碼為亂碼顯示。

(2) 不通過：可成功進行反編譯，且未出現亂碼。

(3) 不適用：無。

附錄 A
(參考)
廠商自我宣告

表 A.1 廠商自我宣告表

日期： 年 月 日

申請者(公司、商號名稱)		☐製造商 ☐系統業者 ☐代理商	○○○股份有限公司		申請者用印(大、小章)
統一編號					
營業所地址		☐☐☐-☐☐			
代表人姓名					
聯絡人	姓名及職稱		電子信箱		
	聯絡電話		傳真機		
製造商及地址		○○○股份有限公司 ☐☐☐-☐☐			
申請檢測安全等級		☐1 級 ☐2 級 ☐3 級			
名稱/廠牌/型號					
申請檢測之作業系統版本					
申請檢測之韌體版本					
設備識別	預設開啟之通訊埠	port 22 SSH 遠端控制用 port 80 Http 提供網頁			
	是否為受限制設備	☐ 否 ☐ 是，請說明原因			
	是否提供工程模式	☐ 否 ☐ 是，請說明進入方式(例如：密碼 1234，指令 Home 鍵+音量鍵)			
	是否支援更新功能	☐ 否 ☐ 是，請說明可使用的方式(例如：OTA、手動)			
	除錯模式進入方法(2 級)				
	更新伺服器 IP				
	內建繳費伺服器 IP				
	使用者紀錄刪除方法				
檢附文件(正本或影本)		☐1.廠商自我宣告表 ☐2.內建軟體摘要表 ☐3.內部系統登入登出日誌紀錄文件(申請 3 級者須檢附) ☐4.持久性儲存器關鍵安全參數之保存方式文件(申請 3 級者須檢附) ☐5.產品唯一識別碼遭篡改之安全設計文件(申請 3 級者須檢附) ☐6.韌體加密演算法文件(申請 3 級者須檢附) ☐7.關鍵安全參數文件(申請 3 級者須檢附)			
[註]檢測實驗室除留存本申請書正本及光碟片外，應將檢測申請書影本、機上盒樣品及其餘文件於出具檢測報告時一併發還申請者。					

附錄 B
(參考)
內建軟體摘要

表 B.1 內建軟體摘要表

測試軟體			
請填寫有圖示軟體與預檢測之無圖示軟體(選測)，欄位不夠請自行添加。			
1	軟體名稱		
	發行商/版本		
	軟體類型	☐有圖示軟體 ☐無圖示軟體	
	是否存取敏感性資料	☐否 ☐是，位置、帳戶、照片	
	是否具帳戶驗證登入機制	☐否 ☐是	
	是否具備金流交易(2 級)	☐否 ☐是(請填寫 IP)	IP：
2	軟體名稱		
	發行商/版本		
	軟體類型	☐有圖示軟體 ☐無圖示軟體	
	是否存取敏感性資料	☐否 ☐是，位置、帳戶、照片	
	是否具帳戶驗證登入機制	☐否 ☐是	
	是否具備金流交易(2 級)	☐否 ☐是(請填寫 IP)	IP：
3	軟體名稱		
	發行商/版本		
	軟體類型	☐有圖示軟體 ☐無圖示軟體	
	是否存取敏感性資料	☐否 ☐是，位置、帳戶、照片	
	是否具帳戶驗證登入機制	☐否 ☐是	
	是否具備金流交易(2 級)	☐否 ☐是(請填寫 IP)	IP：
4	軟體名稱		
	發行商/版本		
	軟體類型	☐有圖示軟體 ☐無圖示軟體	
	是否存取敏感性資料	☐否 ☐是，位置、帳戶、照片	
	是否具帳戶驗證登入機制	☐否 ☐是	
	是否具備金流交易(2 級)	☐否 ☐是(請填寫 IP)	IP：
5	軟體名稱		
	發行商/版本		
	軟體類型	☐有圖示軟體 ☐無圖示軟體	
	是否存取敏感性資料	☐否 ☐是，位置、帳戶、照片	
	是否具帳戶驗證登入機制	☐否 ☐是	
	是否具備金流交易(2 級)	☐否 ☐是(請填寫 IP)	IP：

附錄 C
(參考)
安全功能

表 C.1 安全功能表

安全功能		
1	5.4.2.2 內部系統登入登出日誌紀錄(3 級)	請給與儲存之路徑與紀錄內容之截圖。
2	5.4.3.1 持久性儲存器中關鍵安全參數之保存方式(3 級)	請說明與截圖證明(如:程式碼)。
3	5.4.3.2 關鍵安全參數加密儲存或存放於安全區域(3 級)	請說明防護方法與截圖證明(如:使用何種加密模組、存放位置路徑)
4	5.4.3.3 唯一識別碼安全設計(3 級)	請說明防護方式與截圖證明(如:程式碼)。
5	5.4.3.4 關鍵安全參數生成機制(3 級)	請說明產生方式與截圖證明(如:程式碼、亂數機制)。

參考資料

(1) SSLlabs，SSL and TLS Deployment Best Practices：2020。
(2) NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise：2013
(3) NIST SP 800-164 DRAFT, Guidelines on Hardware-Rooted Security in Mobile Devices：2012
(4) NIST SP 800-163, Vetting the Security of Mobile Applications：2015
(5) NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules：2021
(6) 個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
(7) Department of Homeland Security (DHS), Study on Mobile Device Security：2017
(8) OWASP，Mobile Security Project - Top Ten Mobile Risks：2016
(9) ETSI TS 103 645 V1.1.1 (2019-02), CYBER; Cyber Security for Consumer Internet of Things.
(10) NISTIR 8259 Draft (2nd) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline.
(11) NIST，National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing
(12) NIST，SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program
(13) NIST，SP 800-53 Rev.5，Security and Privacy Controls for Information Systems and Organizations：2020。
(14) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document
(15) NIST Special Publication 800-57: Recommendation for Key Management, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
(16) ENISA，Cybersecurity Certification: EUCC Candidate Scheme v1：2020。
(17) 政府組態基準(GCB)，TWGCB-01-004_Microsoft Windows 8.1 政府組態基準說明文件 v1.6：2020。

版本修改紀錄

版本	時間	摘要
v1.0	2022/06/30	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw