



**TAICS**

TAICS TS-0032 v1.0: 2020

# 智慧音箱資安測試規範

Cybersecurity test specification for smart speakers

2020/09/18

社團法人台灣資通產業標準協會  
Taiwan Association of Information and Communication Standards



# 智慧音箱資安測試規範

## Cybersecurity test specification for smart speakers

出版日期: 2020/09/18

終審日期: 2020/07/24

此文件之著作權歸台灣資通產業標準協會所有，  
非經本協會之同意，禁止任何形式的商業使用、重製或散佈。

Copyright© 2020 Taiwan Association of Information  
and Communication Standards. All Rights Reserved.

## 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。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 博士

TC5 秘書：財團法人資訊工業策進會 秦燕君

技術編輯：財團法人電信技術中心 吳勁儔 工程師、許博堯 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)：

中華電信股份有限公司、台灣德國萊因技術監護顧問股份有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、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、國立交通大學、國家儀器股份有限公司、華碩電腦股份有限公司、勤業眾信聯合會計師事務所、遠傳電信股份有限公司。

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、台灣小米通訊有限公司、台灣獵豹移動股份有限公司、美商蘋果亞洲股份有限公司、英華達股份有限公司、國立台灣科技大學、國立雲林科技大學、經濟部標準檢驗局。

本規範由國家通訊傳播委員會支持研究制定。

## 目錄

誌謝.....	1
目錄.....	2
前言.....	3
引言.....	4
1. 適用範圍.....	5
2. 引用標準.....	6
3. 用語及定義.....	7
4. 測試項目分級.....	8
5. 資安測試規範.....	10
5.1 實體安全.....	10
5.2 系統安全.....	12
5.3 通訊安全.....	23
5.4 身分鑑別與授權機制安全.....	30
5.5 隱私保護.....	37
5.6 行動應用程式安全.....	45
附錄 A (參考) 設備商自我宣告表.....	47
附錄 B (參考) 設備商隱私聲明表.....	48
參考資料.....	49
版本修改紀錄.....	50

## 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

近年來網路相關應用呈現爆炸性發展，各種五花八門的連網硬體與軟體服務一一出現，智慧音箱便是其中一款硬體結合軟體服務的物聯網設備。不同於以往傳統的藍牙喇叭，智慧音箱具備人工智慧語音處理功能，能夠通過喚醒詞、語音輸入、語音辨識、語意理解、語音合成等技術與用戶互動，並獲取來自網路的內容播放；但由於具備網路連接功能，相關的安全性問題也隨之而來：病毒攻擊、個人隱私資料洩漏、硬體及韌體漏洞相繼成為智慧音箱的安全隱患。此外，智慧音箱透過 WiFi、藍牙、ZigBee 等無線通訊技術與其他智慧家電串聯，若缺乏足夠的網路安全機制，將容易遭受蓄意者入侵並嚴重影響用戶隱私安全與服務使用安全。

TAICS TS-0032 「智慧音箱資安測試規範」(以下簡稱本測試規範)，依據台灣資通產業標準協會所制定之 TAICS TS-0031 「智慧音箱資安標準」訂定，俾利智慧音箱設備商、製造商、服務業者及資安檢測實驗室等作為相關產品、服務檢測技術的參考藍本。本測試規範中具體明列資安檢測之測試目的、測試環境、測試步驟、測試基準及測試結果等事項。

## 1. 適用範圍

本規範為依據 TAICS TS-0031 v1.0 「智慧音箱資安標準」規定，所訂定之測試規範，適用範圍為適用於智慧音箱本體、產品應用程式、音箱對外之通訊傳輸網路(如圖 1)。

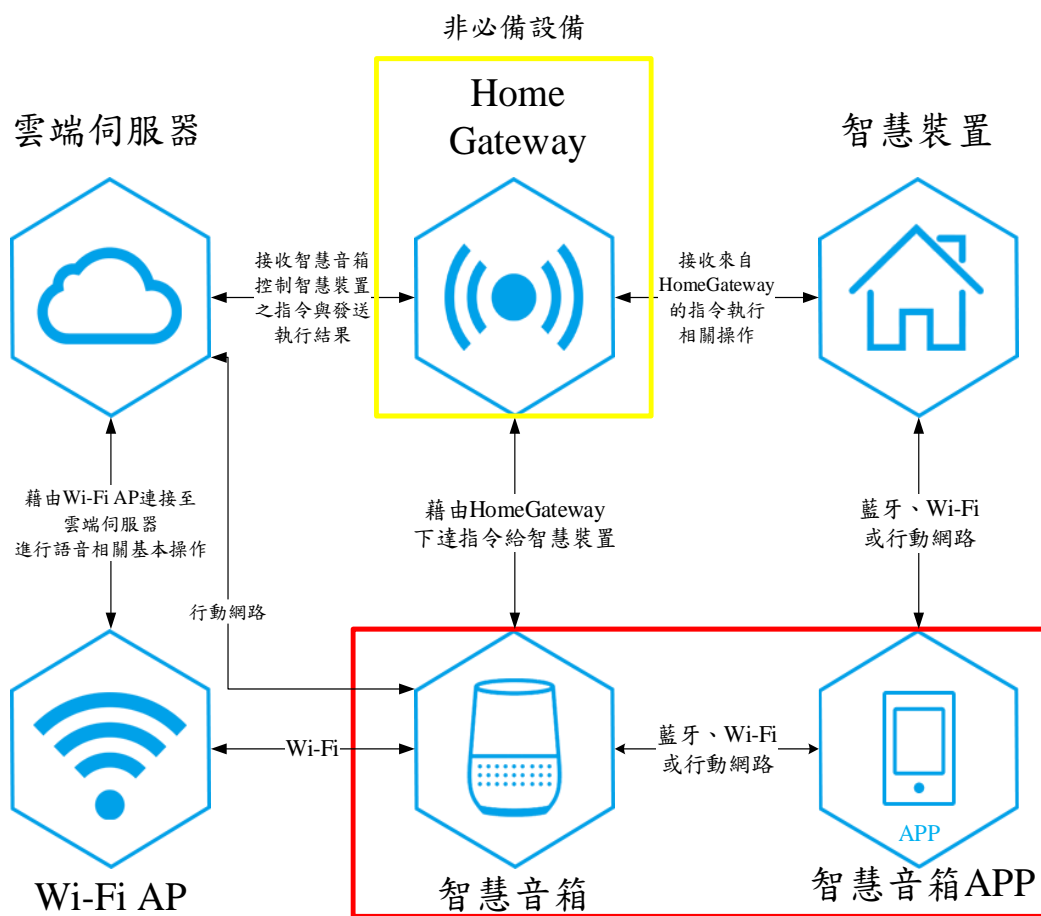


圖 1 適用範圍示意圖

## 2. 引用標準

以下引用標準係本規範必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

- [1] NIST FIPS 140-2 Security Requirements for Cryptographic Module, Annex A: Approved Security Functions , 2019/06
- [2] ETSI TS 103 645 CYBER; Cyber Security for Consumer Internet of ThingsV1.1.1. 2019/02
- [3] ISO/IEC 27030 Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT), 2018/01
- [4] ISO/IEC 15408-1: 2014 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 2014/01
- [5] IEC 62443-4-2:2019 Security for industrial automation and control systems –Part 4-2: Technical security requirements for IACS components, 2019/02
- [6] IEEE Standard Association, P2413.1 Standard for a Reference Architecture for Smart City (RASC), 2018/06
- [7] NIST, Guide to Bluetooth Security, SP 800-121 Revision 2, 2017/05
- [8] FIRST.org, Common Vulnerability Scoring System v2.0, 2007/06
- [9] FIRST.org, Common Vulnerability Scoring System v3.0, 2015/06
- [10] FIRST.org, Common Vulnerability Scoring System v3.1, 2019/11
- [11] OECD Privacy Guidelines, 2013/03
- [12] 行動應用資安聯盟，行動應用 App 基本資安檢測基準 V3.1, 2019/09



### 3. 用語及定義

TAICS TS-0031 v1.0 「智慧音箱資安標準」所規定之用語及定義適用於本規範。

#### 3.1 開放式 Wi-Fi(Open Wi-Fi)

係指沒有經過通行碼身分認證的 Wi-Fi 熱點。

#### 3.2 信任區域(TrustZone)

係指一種消費電子裝置的硬體架構，旨在為消費電子產品構建一個安全框架來抵禦各種可能的攻擊，以保護敏感性資料。

#### 3.3 可信任平台模組(Trusted Platform Module, TPM)

係指一項安全密碼處理器的國際標準，旨在整合裝置中的加密金鑰。

#### 3.4 可信任執行環境(Trusted Execution Environment, TEE)

係指中央處理器的安全區域，該區域可保證內部載入的程式碼與資料能受到機密性與完整性的保護。

## 4. 測試項目分級

本節依據 TAICS TS-0031 v1.0 「智慧音箱資安標準」制定相對應之安全測試項目與測試方法。

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：實體安全、系統安全、通訊安全、身分鑑別與授權機制安全、隱私保護、行動應用程式安全；第二欄為安全要求分項之安全測試項目，係依第一欄各安全構面設計對應之各安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級等三個等級，產品須先通過較低安全等級之測試。設備商需提供之書面審查與協助清單如表 2 所示。

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
實體安全	5.1.1 實體埠之安全管控	-	5.1.1.1	-
系統安全	5.2.1 韌體更新功能	5.2.1.1	-	-
	5.2.2 韌體更新檔之完整性及合法性	-	5.2.2.1	-
	5.2.3 韌體檔案加密	-	5.2.3.1	-
	5.2.4 作業系統與網路服務安全	5.2.4.1	-	-
	5.2.5 敏感性資料之儲存加密	-	5.2.5.1	5.2.5.2
	5.2.6 通訊協定安全	-	5.2.6.1 5.2.6.2	-
通訊安全	5.3.1 HTTP 傳輸安全	5.3.1.1	-	-
	5.3.2 最小化網路服務連接埠	5.3.2.1	-	-
	5.3.3 憑證認證應具 MITM 防護	5.3.3.1	-	-
	5.3.4 敏感性資料之 Wi-Fi 傳輸安全	-	5.3.4.1	-
	5.3.5 藍牙傳輸安全	-	5.3.5.1	-
身分鑑別與授權機制安全	5.4.1 預設通行碼安全	5.4.1.1	-	-
	5.4.2 網頁管理頁面之身分鑑別機制	5.4.2.1 5.4.2.2	-	-
	5.4.3 敏感性功能之身分鑑別機制	-	5.4.3.1	5.4.3.2
隱私保護	5.5.1 隱私政策條款與機制	5.5.1.1 ~ 5.5.1.12	-	5.5.1.13

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
行動應用程式安全	5.6.1 行動應用 App 基本資安認證		5.6.1.1	5.6.1.2

表 2 設備商書面審查與協助清單總表

測試項目	設備商須提供資料
5.1.1.1 產品提供使用者透過實體埠存取系統功能，須具備身分鑑別機制	進入作業系統除錯模式之方法 (附錄 A 設備商自我宣告表)
5.2.2.1 產品需具備自我驗證韌體完整性及合法性之功能，且需具備可追蹤韌體更新紀錄之管理功能	韌體檔案數位簽章之方法 (附錄 A 設備商自我宣告表) 韌體檔案更新日誌
5.2.3.1 韌體內之設定檔或資料庫檔案，是否存在未加密之敏感性資料或可識別之隱私資料	韌體燒錄工具
5.2.5.1 產品所儲存之敏感性資料不得明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A 核准之加密演算法	敏感性資料儲存加密方式 (附錄 A 設備商自我宣告表)
5.2.5.2 敏感性資料須存放於產品的安全區域 (Secure Zone)，從正常作業環境中隔離	安全晶片相關證明文件
5.3.2.1 5.3.2.1 產品出廠所開啟之網路通訊埠，應為設備商提供必要服務之所需，並載明於產品文件中，以防止產品因網路介面設定不當而被侵入	預設開啟之網路通訊埠 (附錄 A 設備商自我宣告表)
5.5.1.1 符合國家個人資料保護法及經濟合作暨發展組織 (Organization for Economic Co-operation and Development, OECD) 公布之限制蒐集原則，即蒐集個人資料時，確認有合法、公正、通知當事人並獲得使用者同意	資料蒐集與處理者、蒐集資料、蒐集方式、蒐集的目的、資料保留時間與使用期限 (附錄 B 設備商隱私聲明表)
5.5.1.10 智慧音箱應有實體麥克風關閉功能，且於麥克風關閉狀態時，不得有任何收音及上傳之行為 5.5.1.11 智慧音箱在服務偵測狀態，未偵測到喚醒詞前，不得有任何資料上傳行為	音箱於關閉收音功能或於開啟收音功能但未偵測到喚醒詞前須連線之 IP 資訊 (附錄 B 設備商隱私聲明表)
5.5.1.12 智慧音箱應聲明在偵測到喚醒詞，進入服務狀態後，收集語音資料時間長度與資料上傳機制	智慧音箱收音時長或機制說明 (附錄 B 設備商隱私聲明表)

## 5. 資安測試規範

### 5.1 實體安全

檢視智慧音箱之實體安全測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

#### 5.1.1 實體埠之安全管控

5.1.1.1 產品提供使用者透過實體埠存取系統功能，須具備身分鑑別機制

(a) 測試目的：測試透過受測物實體介面存取作業系統之除錯模式時，是否具備通行碼鑑別機制。

(b) 測試環境

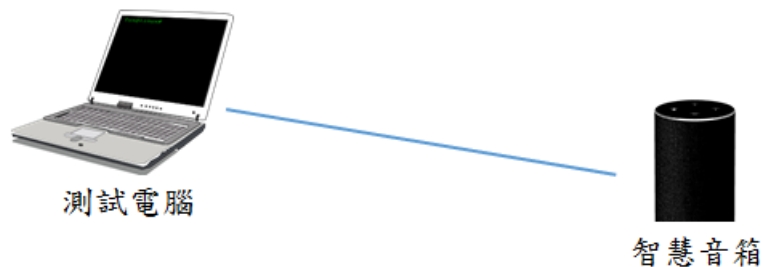


圖 2 實體埠之安全管控測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱。

(2) 測試設備及受測物連接方式如圖 2。

(c) 測試步驟

(1) 根據設備商設備商自我宣告表(附錄 A)所提供進入作業系統除錯模式之方法。

(2) 以測試電腦連接受測物之 USB/UART/JTAG 介面。

(3) 確認是否透過 USB/UART/JTAG 埠存取作業系統之除錯模式。

(4) 必須經過通行碼鑑別以存取作業系統之除錯模式時，檢視通行碼鑑別是否符合 5.4.2.2 通行碼鑑別機制須具備複雜度及強度測試的要求。

(5) 如果身分驗證方式非為通行碼機制，則檢驗其身分驗證功能是否正常，是否需驗證身分才可進入除錯模式。

(d) 測試基準

(1) 無法透過 USB/UART/JTAG 介面存取作業系統之除錯模式。

(2) 存取除錯模式若須經過身分驗證，且通行碼鑑別符合 5.4.2.2 通行碼鑑別機制須具備複雜度及強度測試的要求。

(3) 具備其餘身分驗證方式者，身分驗證功能正常，需驗證身分才可進入除錯模式。

(e) 測試結果

(1) 通過：符合測試基準(1)~(3)其中一項。

(2) 不通過：測試基準(1)~(3)三項皆不符合。

(3) 不適用：無。

## 5.2 系統安全

檢視智慧音箱之系統安全測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

### 5.2.1 韌體更新功能

#### 5.2.1.1 產品須具備韌體更新功能

(a) 測試目的：測試受測物是否具備韌體更新之功能。

(b) 測試環境

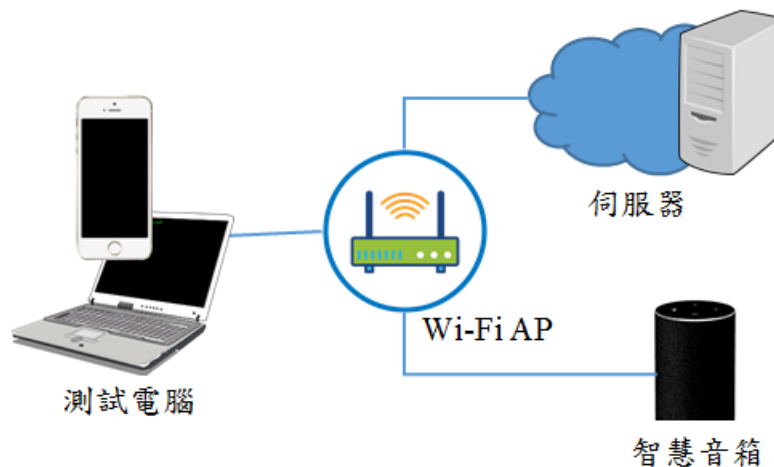


圖 3 韌體更新功能測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 3。

(c) 測試步驟

(1) 根據設備商使用說明文件中所提供之韌體安全性更新方法，請設備商觸發更新。

(2) 檢視受測物是否能進行更新。

(d) 測試基準

(1) 受測物韌體具備更新功能且能更新成功。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

## 5.2.2 韌體更新檔之完整性及合法性

5.2.2.1 產品需具備自我驗證韌體完整性及合法性之功能，且需具備可追蹤韌體更新紀錄之管理功能

(a) 測試目的：測試受測物韌體是否具備查驗韌體更新檔案真確之能力，並且具有韌體版本更新紀錄日誌。

(b) 測試環境

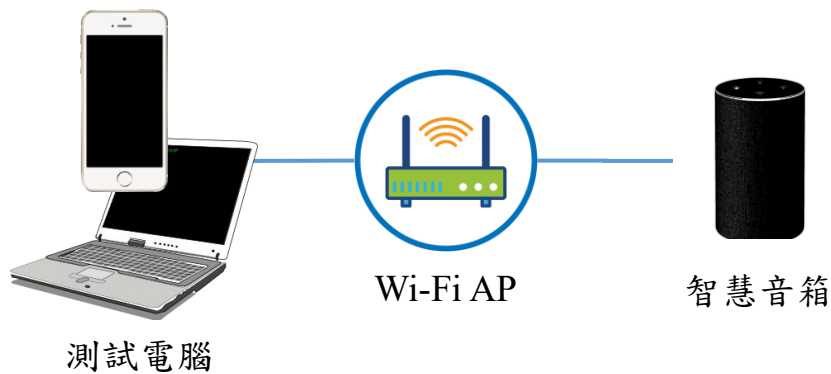


圖 4 韌體更新檔之完整性及合法性測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 4。

(c) 測試步驟



- (1) 受測物之韌體更新機制為手動更新，修改更新用韌體之內容並上傳至受測物。
- (2) 根據設備商所提供韌體檔案數位簽章之方法，對韌體更新檔重新簽章並上傳至受測物。
- (3) 執行受測物手動更新，並檢視更新是否成功。
- (4) 檢視設備商所提供韌體檔案更新日誌，確認是否正確紀錄韌體更新內容(更新日誌內容至少需包含版本號、更新日期以及更新內容)。

(d) 測試基準

- (1) 置換或修改韌體檔案後，更新受測物韌體失敗。
- (2) 設備商具備韌體檔案更新日誌。

(e) 測試結果

- (1) 通過：符合測試基準(1)、(2)。
- (2) 不通過：不符合測試基準(1)或(2)。
- (3) 不適用：設備商無提供手動更新。

## 5.2.3 韌體檔案加密

5.2.3.1 韌體內之設定檔或資料庫檔案，不得包含未加密之敏感性資料或可識別之隱私資料

- (a) 測試目的：測試受測物韌體的敏感性資料是否會洩露。
- (b) 測試環境





圖 5 韌體檔案加密測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱、韌體燒錄或傾印工具。
- (2) 請設備商提供燒錄工具。

(備註：若設備商有提供燒錄工具，即不會破壞裝置進行測試)

- (3) 測試設備及受測物連接方式如圖 5。

#### (c) 測試步驟

- (1) 啟動設備並進行正常操作。
- (2) 檢視受測物硬體有無明顯之 Flash 晶片接腳或 MCU 之韌體燒錄接腳。
- (3) 傾印(dump)韌體檔案(如果無法 Dump 韌體，則以設備商提供之韌體進行以下測試)。
- (4) 使用具韌體拆解功能之工具(如：binwalk 等)，對受測物 Dump 之韌體及設備商提供之韌體分別進行拆解。
- (5) 使用檢索工具或系統指令如 strings, grep, find 等，針對敏感性資料之關鍵字詞(如：password、pwd、private key、config、conf....等)進行作業系統或 MCU 韌體掃描，確認是否有未加密之敏感性資料。
- (6) 檢視韌體內之設定檔或資料庫檔案，是否存在未加密之敏感性資料或可識別之隱私資料。

#### (d) 測試基準

(1) 受測物硬體無明顯之 Flash 晶片接腳及 MCU 燒錄接腳，或韌體無法傾印 (dump)。

(2) 韌體內之敏感性資料，加密機制採用 FIPS 140-2 Annex A 核准之安全功能。

(e) 測試結果

(1) 通過：符合測試基準(1)或(2)。

(2) 不通過：測試基準(1)與(2)皆不符合。

(3) 不適用：無。

## 5.2.4 作業系統與網路服務安全

5.2.4.1 產品之作業系統與網路服務，不得有美國國家弱點資料庫所公布及更新的常見弱點與漏洞資料，且 CVSS 評分為 9.0 以上。

(a) 測試目的：測試受測物作業系統與網路服務是否含有已知 CVSS v3.0 或 CVSS v3.1 評分為 9.0 分以上之漏洞。

(b) 測試環境

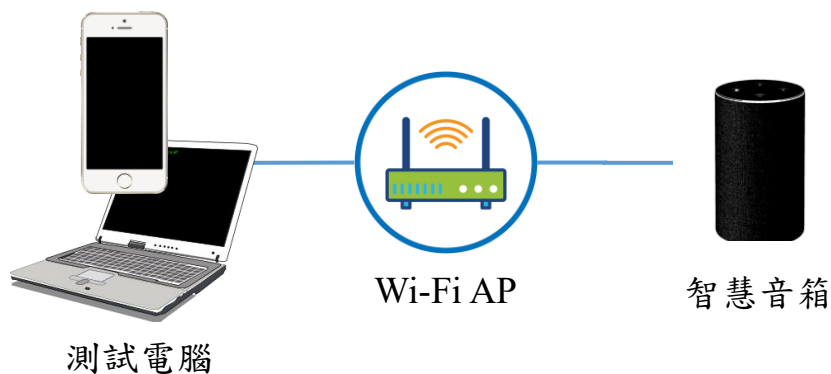


圖 6 作業系統與網路服務安全測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 6。

(c) 測試步驟

- (1) 測試電腦連接受測物，以管理者權限登入作業系統。
- (2) 使用弱點掃描工具掃描智慧音箱作業系統與網路服務。
- (3) 檢視掃描結果，確認作業系統與網路服務是否存在安全漏洞。

(d) 測試基準

- (1) 受測物之作業系統與網路服務不存在 CVSS v3.0 或 CVSS v3.1 評分為 9.0 以上之共同資安弱點與漏洞。當檢測出之資安漏洞不具有 CVSS v3.0 或 CVSS v3.1 評分時，以 CVSS v2 評分為依據。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：無。

## 5.2.5 敏感性資料之儲存加密

5.2.5.1 產品所儲存之敏感性資料不得明文儲存，而保護資料的加密方式須採用 FIPS 140-2 Annex A 核准之加密演算法

(a) 測試目的：測試受測物韌體是否具備保護敏感性資料的能力。

(b) 測試環境

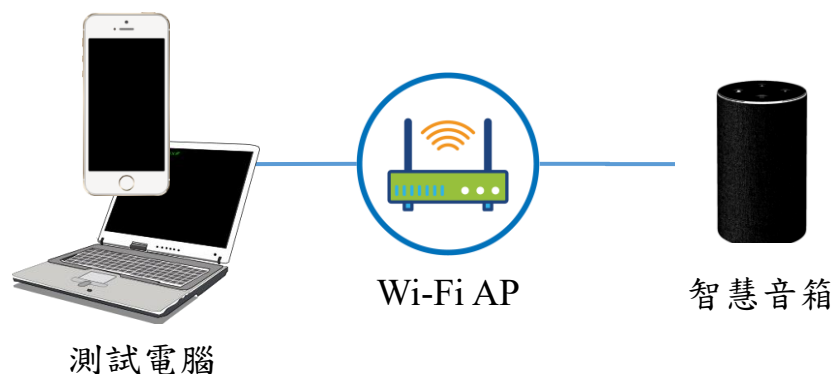


圖 7 敏感性資料之儲存加密測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 7。

(c) 測試步驟

(1) 請設備商提供登入受測物作業系統層之方法。

(2) 登入受測物系統之作業系統層。

(3) 使用檢索工具或系統指令(如：strings, grep, find...等)，針對敏感性資料之關鍵字詞(如：password, pwd, private key, config, conf...等)進行作業系統掃描，確認是否有未加密之敏感性資料。

(4) 檢視作業系統內之設定檔或資料庫檔案，是否存在未加密之敏感性資料或可識別之隱私資料。

(5) 檢視設備商提供之敏感性資料儲存加密演算法文件的資料，且加密演算法是否為 FIPS 140-2 Annex A 核准之加密演算法。

(d) 測試基準

(1) 受測物不存在存取作業系統之介面。

(2) 受測物作業系統內之敏感性資料，加密機制採用 FIPS 140-2 Annex A 核准之安全功能。

(e) 測試結果

(1) 通過：符合測試基準(1)或(2)。

(2) 不通過：不符合測試基準(1)與(2)。

(3) 不適用：無。

5.2.5.2 敏感性資料須存放於產品的安全區域(Secure Zone)，從正常作業環境中隔離

(a) 測試目的：測試受測物敏感性資料之存放與正常作業系統隔離。

(b) 測試環境



圖 8 安全晶片之儲存保護聲明測試環境示意圖

- (1) 測試設備：智慧音箱。
- (2) 測試設備及受測物連接方式如圖 8。

(c) 測試步驟

- (1) 檢視設備商提供之書面審查安全晶片(如：TrustZone、TPM、TEE、不可移除式 SIM 卡等)之使用證明文件。
- (2) 檢視智慧音箱是否具備此晶片。

(d) 測試基準

- (1) 設備商有提供安全晶片之使用證明文件及受測物確實具備安全晶片。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：無。

## 5.2.6 通訊協定安全

5.2.6.1 產品之 Wi-Fi 通訊協定，不得有錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生異常而服務中斷的情形

- (a) 測試目的：測試受測物 Wi-Fi 相關之通訊協定是否存在未知之資安漏洞。

(b) 測試環境

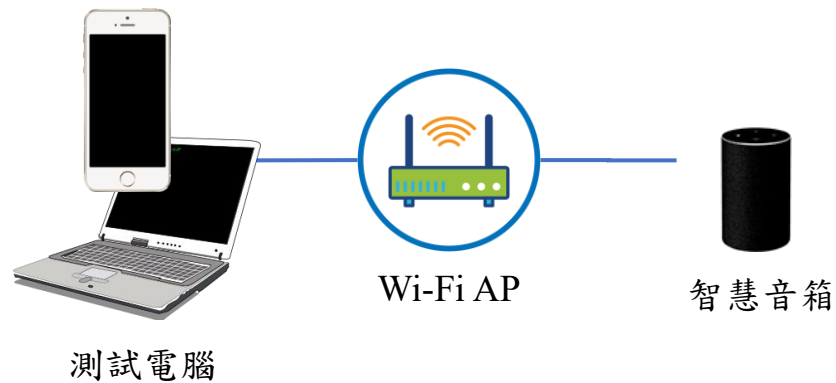


圖 9 Wi-Fi 功能防堵異常內容測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 9。

(c) 測試步驟

(1) 將測試電腦連接產品。

(2) 啟動具模糊測試功能之工具執行對 IEEE 802.11x 通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試。

(3) 檢查產品是否仍正常運作。

(d) 測試基準

(1) 受測物經過異常輸入測試後系統仍正常運作。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：受測物無 Wi-Fi 功能。

5.2.6.2 產品之藍牙通訊協定，不得有錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生異常而服務中斷的情形

(a) 測試目的：測試受測物藍牙相關之通訊協定是否存在未知之資安漏洞。

(b) 測試環境



圖 10 藍牙功能防堵異常內容測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱。

(2) 測試設備及受測物連接方式如圖 10。

(c) 測試步驟

(1) 將測試電腦連接產品。

(2) 啟動具模糊測試功能之工具執行對藍牙通訊協定所有欄位至少 10 萬筆唯一且獨立之測試項，或者最少 8 小時的異常輸入測試。

(3) 檢查產品是否仍正常運作。

(d) 測試基準

(1) 受測物經過異常輸入測試後系統仍正常運作。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：受測物無藍牙功能。





## 5.3 通訊安全

檢視智慧音箱之通訊安全測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

### 5.3.1 HTTP 傳輸安全

5.3.1.1 網路傳輸預設須通過安全通道之驗證，且安全通道版本需使用 TLS 1.2 同等或以上之安全通訊協定，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)

(a) 測試目的：測試受測物敏感性資料之安全通道，是否支援強加密演算法。

(b) 測試環境

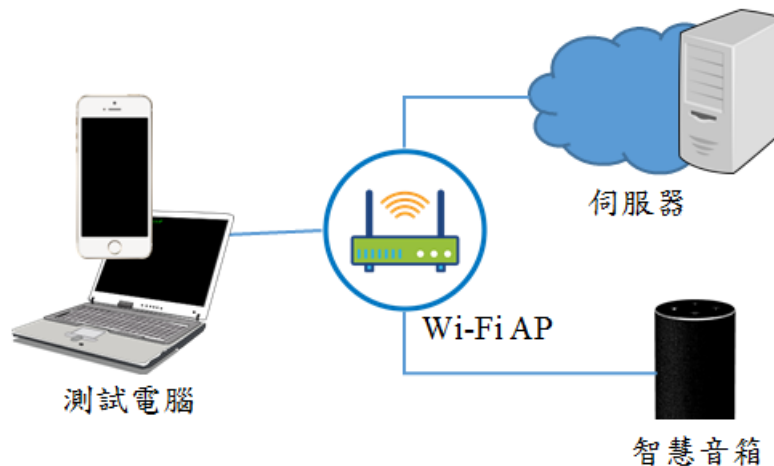


圖 11 HTTP 傳輸安全測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 11。

(c) 測試步驟

(1) 將測試電腦連接受測物之管理介面。

(2) 使用安全通道掃描工具，確認系統所使用之安全通道版本。

- (3) 使用封包側錄工具，擷取受測物使用之通訊封包，確認其於傳輸過程中使用之安全通道設定。
- (4) 對智慧音箱與雲端伺服器間的通訊鏈路使用安全通道掃描工具，確認系統所使用之安全通道版本。
- (5) 將受測物連接雲端伺服器。
- (6) 使用封包側錄工具，擷取受測物使用之通訊封包，確認其於傳輸過程中使用之安全通道設定。

(d) 測試基準

- (1) 測試電腦與受測物之間使用 TLS 1.2 同等或以上之安全通訊協定。
- (2) 雲端伺服器與受測物之間使用 TLS 1.2 同等或以上之安全通訊協定。

(e) 測試結果

- (1) 通過：符合測試基準(1)與(2)。
- (2) 不通過：不符合測試基準(1)或(2)其中一項。
- (3) 不適用：無。

## 5.3.2 最小化網路服務連接埠

5.3.2.1 產品出廠所開啟之網路通訊埠，應為設備商提供必要服務之所需，並載明於產品文件中，以防止產品因網路介面設定不當而被侵入

- (a) 測試目的：測試受測物是否存在預期以外之網路埠。
- (b) 測試環境

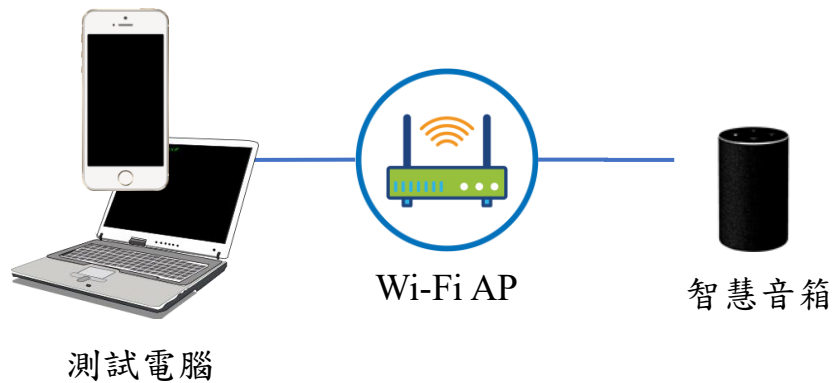


圖 12 最小化網路服務連接埠測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 12。

#### (c) 測試步驟

(1) 檢視設備商自我宣告表(附錄 A)提供受測物使用之通訊服務與宣告之通訊埠資料。

(2) 以測試電腦連接受測物。

(3) 使用通訊埠掃描軟體進行埠掃描。

(4) 確認是否存在未宣告之通訊埠。

#### (d) 測試基準

(1) 受測物所開啟之通訊埠與設備商自我宣告表一致。

#### (e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

### 5.3.3 憑證認證應具 MITM 防護

5.3.3.1 產品憑證應具備有效鑑別性，在遭受竄改或置換憑證時，能有效阻擋連線

- (a) 測試目的：測試受測物是否能鑑別安全通道所使用憑證之合法性。
- (b) 測試環境

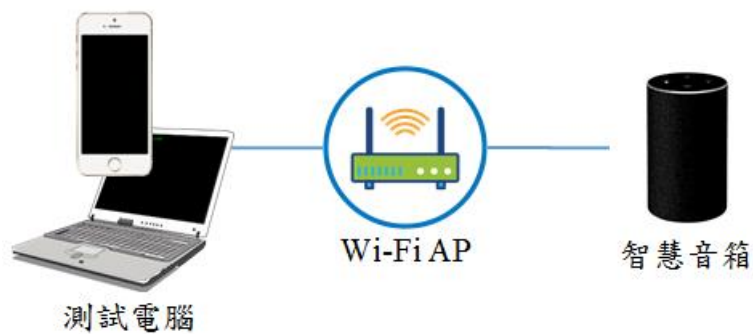


圖 13 憑證認證應具 MITM 防護測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。
- (2) 測試設備及受測物連接方式如圖 13。
- (c) 測試步驟
  - (1) 將測試電腦與受測物連接，登入網頁管理介面。
  - (2) 當受測物發送憑證予測試電腦時攔截其憑證，並置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
  - (3) 發送已竄改之憑證予受測物並監聽封包，檢視受測物是否接受此憑證。
- (d) 測試基準
  - (1) 遭竄改之憑證不被受測物接受。
- (e) 測試結果
  - (1) 通過：符合測試基準(1)。
  - (2) 不通過：不符合測試基準(1)。

(3) 不適用：智慧音箱不具備網頁管理介面。

### 5.3.4 敏感性資料之 Wi-Fi 傳輸安全

#### 5.3.4.1 無線網路傳輸的安全機制預設須採用 WPA2(含)以上之加密機制

(a) 測試目的：測試受測物是否存在不安全的 Wi-Fi 通道保護設定。

(b) 測試環境

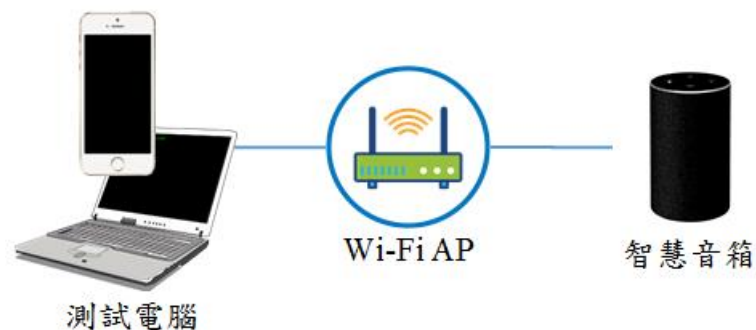


圖 14 敏感性資料之 Wi-Fi 傳輸安全測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 14。

(c) 測試步驟

(1) 將測試手機連線至裝置 Wi-Fi AP，啟動裝置配對模式。

(2) 使用 Wi-Fi 掃描工具(如：Wi-Fi Scanner 等)，確認裝置所使用之 Wi-Fi 通道設定。

(3) 如果通道設定為 Open Wi-Fi，使用封包側錄工具(如：Wireshark 等)，確認系統所使用之通道。

(d) 測試基準

(1) 使用 WPA2 同等或以上之 Wi-Fi 安全通道。

- (2) 若通道設定為 Open Wi-Fi，確認傳輸使用 TLS 1.2 同等或以上之安全通訊協定。

(e) 測試結果

- (1) 通過：符合測試基準測試基準(1)或(2)其中一項。
- (2) 不通過：測試基準測試基準(1)與(2)皆不符合。
- (3) 不適用：受測物沒有支援 Wi-Fi。

### 5.3.5 藍牙傳輸安全

#### 5.3.5.1 藍牙傳輸須採用 AES128 以上之加密演算法

- (a) 測試目的：測試受測物藍牙是否使用安全的藍牙加密傳輸。
- (b) 測試環境



圖 15 藍牙傳輸安全測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱。
- (2) 測試設備及受測物連接方式如圖 15。
- (c) 測試步驟
- (1) 使用藍牙傳輸側錄工具，擷取受測物之藍牙封包，確認裝置所使用之藍牙傳輸是否加密。
- (2) 藍牙傳輸是否採用 AES128 以上之加密演算法。

(d) 測試基準

- (1) 藍牙傳輸採用 AES128 以上之加密演算法。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：受測物沒有支援藍牙。

## 5.4 身分鑑別與授權機制安全

檢視智慧音箱之身分鑑別與授權機制安全測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

### 5.4.1 預設通行碼安全

5.4.1.1 設備商所生產之同一款裝置，若以通行碼作為身分鑑別與授權機制，其預設通行碼不可相同；或者首次成功取得產品存取之授權，須強制更改預設通行碼

(a) 測試目的：測試受測物是否有相同的預設通行碼。

(b) 測試環境

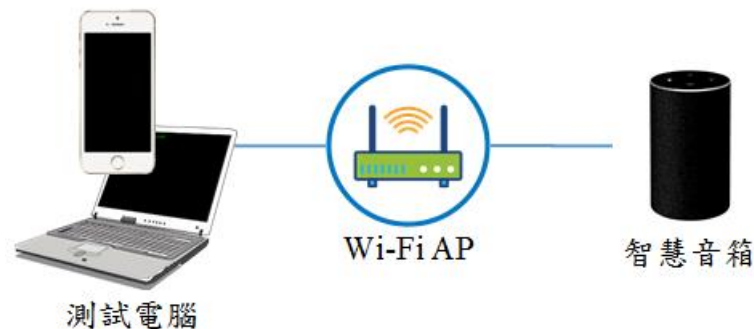


圖 16 身分鑑別與授權機制安全測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 16。

(c) 測試步驟

(1) 將測試設備恢復出廠預設設定。

(2) 觀察設備是否具有預設出廠通行碼(或配對通行碼)。

(3) 觀察預設通行碼是否不同或初次登入時通行碼無須經過修改。

(d) 測試基準



(1) 預設通行碼不同或初次使用通行碼需經過修改才可使用。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：無。

## 5.4.2 網頁管理頁面之身分鑑別機制

### 5.4.2.1 網頁管理介面需具備身分鑑別機制並具備抵抗重送攻擊的能力

- (a) 測試目的：測試受測物是否具備抵抗重送攻擊的能力。
- (b) 測試環境

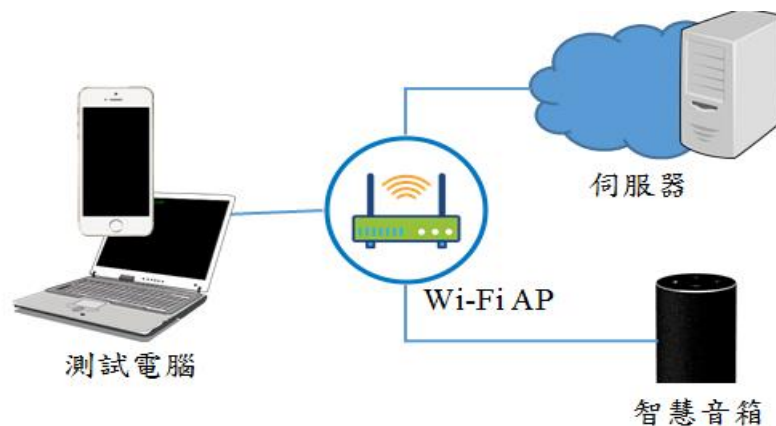


圖 17 網頁管理頁面之身分鑑別機制測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。
  - (2) 測試設備及受測物連接方式如圖 17。
- (c) 測試步驟
- (1) 連接測試電腦與受測物，同時側錄封包。
  - (2) 執行相關操作，檢視封包側錄結果是否要求身分鑑別。



- (3) 檢視身分鑑別因子(如：session id, token 等)產生之設計方法，確認身分鑑別因子是否不可預測(不可於網頁原始碼內明碼顯示)。
- (4) 當受測物要求身分鑑別，將側錄的身分鑑別封包，修改身分鑑別之內容，重新發送至受測物。
- (5) 檢視鑑別結果是否成功。
- (6) 執行受測物登出並再次登入，檢視身分鑑別功能是否正常執行。

#### (d) 測試基準

- (1) 網頁管理介面具備身分鑑別。
- (2) 身分鑑別機制具備抵抗重送攻擊的能力。
- (3) 身分鑑別因子(如：session id, token 等)不可於網頁原始碼內明碼顯示。
- (4) 登出後確實須再次登入，方可存取受測物。

#### (e) 測試結果

- (1) 通過：(1)~(4)四項皆符合。
- (2) 不通過：測試基準(1)~(4)其中一項不符合。
- (3) 不適用：受測物不具備網頁管理頁面。

5.4.2.2 若以通行碼作為網頁管理頁面之身分鑑別機制，通行碼強度需符合政府組態基準原則(2)，包括最小通行碼長度原則(CCE-33789-9)、複雜性需求原則(CCE-33777-4)及強制執行通行碼歷程記錄原則(CCE-35219-5)。

(a) 測試目的：測試受測物是否具備可靠之身分鑑別機制。

(b) 測試環境

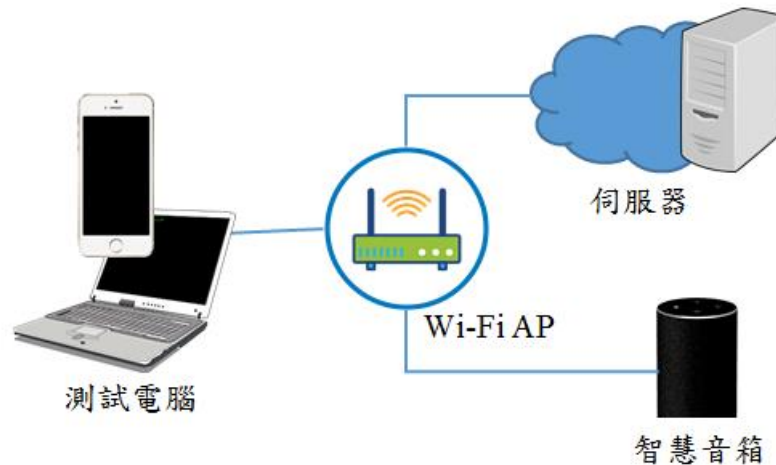


圖 18 通行碼鑑別機制須具備複雜度及強度測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 18。

(c) 測試步驟

(1) 將測試電腦或行動裝置連接受測物，根據受測物使用說明，開啟相應之網頁管理介面連接工具。

(2) 依據最小通行碼長度原則(CCE-33789-9)，輸入小於 8 個字元長度之通行碼，檢查通行碼是否能成功建立或變更。

(3) 依據複雜性需求原則(CCE-33777-4)，輸入僅同時含下述四者字元中任意兩種，1.英文大寫字元(A 到 Z)；2.英文小寫字元 (a 到 z)；3.十進位數字 (0 到 9)；4.非英文字母字元 (例如：!、\$、#、%)，檢查通行碼是否能成功建立或變更。

(d) 測試基準

(1) 通行碼複雜度符合測試步驟(2)與不符合測試步驟(3)。

(2) 通行碼複雜度不符合測試步驟(2)或符合測試步驟(3)。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：符合測試基準(2)。
- (3) 不適用：無。

### 5.4.3 敏感性功能之身分鑑別機制

#### 5.4.3.1 觸發智慧音箱之金流交易功能(如：語音購物等)時，需經過身分鑑別機制

(a) 測試目的：測試受測物執行金流交易功能時，是否具備可靠之身分鑑別機制。

(b) 測試環境

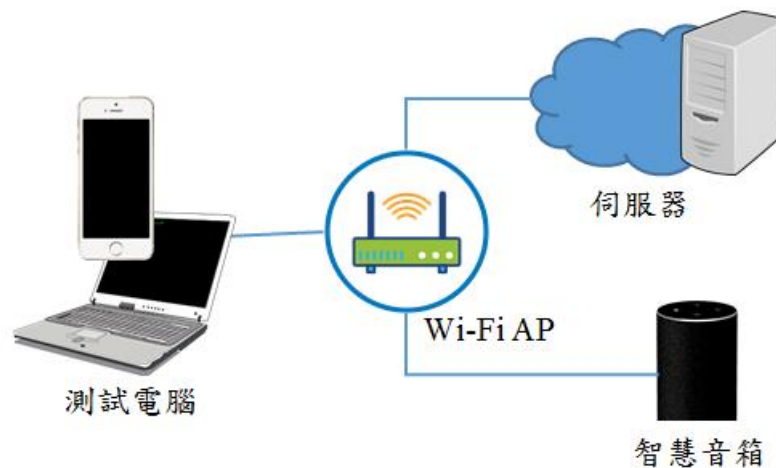


圖 19 金流交易功能之身分鑑別機制測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。
- (2) 測試設備及受測物連接方式如圖 19。

(c) 測試步驟

- (1) 根據受測物之使用說明文件，觸發智慧音箱之金流交易功能(如：語音購物等)。
- (2) 檢視受測物是否需經身分鑑別機制後才能執行金流交易功能。

(d) 測試基準

(1) 智慧音箱之金流交易功能需經過身分鑑別機制才可使用。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：受測物不具備金流交易功能。

5.4.3.2 觸發智慧音箱之人身安全功能(如：家用安防設備等)時，需經過多因子鑑別機制鑑別

(a) 測試目的：測試受測物執行人身安全功能時，是否具備兩種以上可靠之身分鑑別機制。

(b) 測試環境

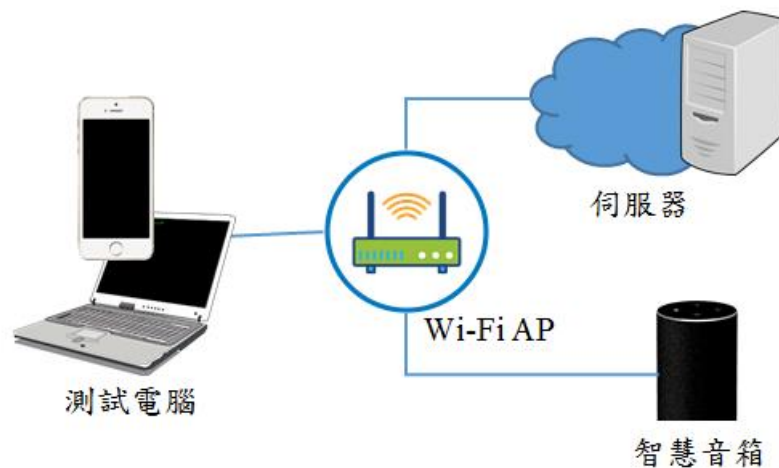


圖 20 人身安全功能之多因子鑑別測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 20。

(c) 測試步驟

(1) 將測試電腦連接受測物。



- (2) 根據受測物之使用說明，觸發智慧音箱之人身安全功能(如：家用安防設備等)以執行身分鑑別。
- (3) 執行多因子身分鑑別操作，檢查是否每次的身分鑑別都採用不同種類之鑑別因子。
- (4) 檢查鑑別過程中是否採用簡訊服務(Short Message Service, SMS)獲取通行碼。
- (5) 檢查鑑別過程中，使用行動裝置作為所持之物(something you have)之鑑別因子時，檢視是否僅可在 1 台行動裝置上獲取鑑別因子。

#### (d) 測試基準

- (1) 受測物之人身安全功能的身分鑑別，透過多因子身分鑑別。
- (2) 每一階段身分鑑別皆採用不同因素的鑑別因子。
- (3) 當使用鑑別因子時，未採用簡訊服務獲取通行碼。
- (4) 當行動裝置作為所持之物之鑑別因子時，僅可在 1 台行動裝置上獲取鑑別因子。

#### (e) 測試結果

- (1) 通過：符合測試基準(1)~(4)四項。
- (2) 不通過：測試基準(1)~(4)其中一項不符合。
- (3) 不適用：受測物不具備人身安全功能。

## 5.5 隱私保護

檢視智慧音箱之隱私保護測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

### 5.5.1 隱私保護條款與機制

5.5.1.1 符合國家個人資料保護法及經濟合作暨發展組織 (Organization for Economic Co-operation and Development, OECD)公布之限制蒐集原則[11]，於蒐集個人資料時，確認有合法、公正、通知當事人並獲得使用者同意

(a) 測試目的：測試受測物隱私保護聲明是否符合要求。

(b) 測試環境

無。

(c) 測試步驟

(1) 檢視受測物是否符合 OECD 公布之原則，即需於設備商隱私聲明表(附錄 B)中載明並提供以下資訊：

(i) 資料蒐集與處理者(例如:XXX 股份有限公司)。

(ii) 蒐集了什麼資料(例如:IP 位置、使用者位置)。

(iii) 蒐集的方式(例如:使用者使用語音查詢時，自動蒐集)。

(iv) 蒐集的目的(例如:提供個人化推薦內容與廣告)。

(v) 資料保留時間與使用期限(例如:保留時間：蒐集日起 12 個月)。

(vi) 須提供使用者完整刪除使用紀錄與資料之功能。

(vii) 須提供使用者更新使用者資料之功能。

(viii) 個人資料除得當事人同意或法律另有規定者外，不得為蒐集目的外之揭露或利用。

- (ix) 蒐集個人資料時，確認有合法、公正、通知當事人並獲得使用者同意(使用程式前會有隱私聲明宣告視窗，且不可預設選項為同意，聲明內容不可太多專有名詞，艱澀難懂，需有繁體中文。)

(d) 測試基準

- (1) 測試步驟(1)九項結果皆符合。
- (2) 測試步驟(1)九項結果其中一項以上(含)不符合。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：符合測試基準(2)。
- (3) 不適用：無。

測試項目 5.5.1.1 之測試環境、測試步驟、測試基準、測試結果皆適用於測試項目 5.5.1.2~5.5.1.8。



5.5.1.2 符合國家個人資料保護法及 OECD 公布之目的明確原則，於聲明書內容，個人資料之蒐集目的，最遲應於蒐集時提醒

5.5.1.3 符合國家個人資料保護法及 OECD 公布之利用限制原則，於聲明書內容，個人資料除得當事人同意或法律另有規定者外，不得為蒐集目的外之揭露或利用

5.5.1.4 符合國家個人資料保護法及 OECD 公布之安全措施原則，於聲明書內容，個人資料應予以合理的安全措施加以保護，以防止個人資料被竊取、竄改、毀損、滅失或洩漏等危險

5.5.1.5 符合國家個人資料保護法及 OECD 公布之公開原則，於確認有提供聲明書，並有關個人資料之蒐集、處理、或利用及政策之制定，對社會大眾為公開

5.5.1.6 符合國家個人資料保護法及 OECD 公布之個人參與原則，於聲明書內容，使用者關於自己的資料得享有得於合理期間內管理有關於自己的資料，可要求資料控制者對於資料加以刪除、修改、完整及補充

5.5.1.7 符合國家個人資料保護法及 OECD 公布之責任原則，於聲明書內聲明負責提供使用者之個人資料管理之責任

5.5.1.8 符合國家個人資料保護法及 OECD 公布之資料品質原則，於聲明書內容，需由使用者確認個人資料之正確、完整及保持全新狀態

5.5.1.9 智慧音箱應有不同提示顯示設備處於服務偵測狀態或服務狀態

(a) 測試目的：測試受測物是否具備服務狀態提示功能。

(b) 測試環境

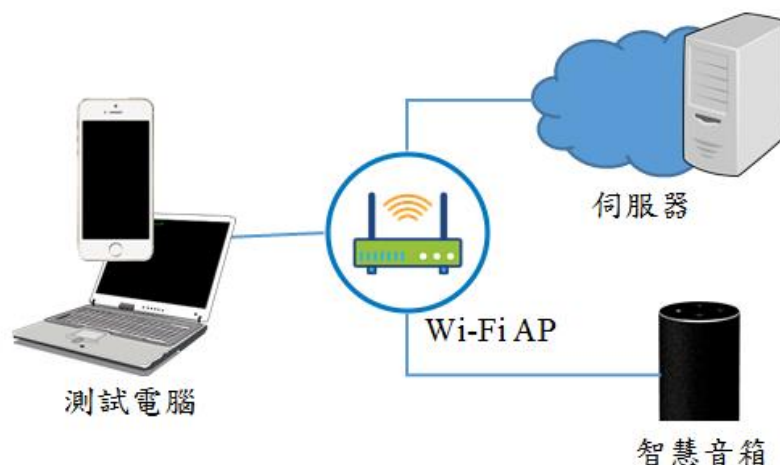


圖 21 隱私保護測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 21。

(c) 測試步驟

(1) 開啟智慧音箱麥克風功能，檢視是否有相對應之提示功能。

(2) 關閉智慧音箱麥克風功能，檢視是否有相對應之提示功能。

(d) 測試基準

(1) 開啟與關閉智慧音箱麥克風功能時，皆具有相對應之提示功能。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

5.5.1.10 智慧音箱應有實體麥克風關閉功能，且於麥克風關閉狀態時，不得有任何收音及上傳之行為

(a) 測試目的：測試受測物是否具有實體麥克風開關，且麥克風關閉時是否仍有收音或上傳資料之行為。

(b) 測試環境

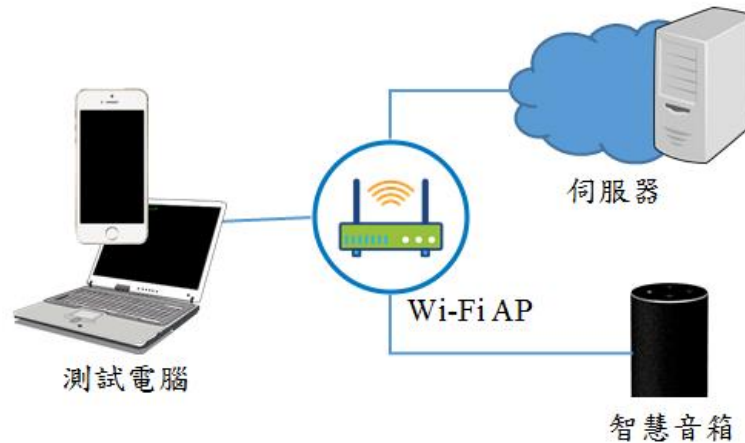


圖 22 隱私保護測試環境示意圖

- (1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。
- (2) 測試設備及受測物連接方式如圖 22。

#### (c) 測試步驟

- (1) 關閉智慧音箱之麥克風開關，即停止收音功能。
- (2) 使用網路封包測錄工具連續抓取智慧音箱之封包適當時數(建議 8 小時以上)。
- (3) 若音箱有其餘須對外之封包，必須提供相連伺服器之 IP 位置資訊，並於說明書或設備商隱私聲明表中作相關聲明(例：該音箱於開啟麥克風時會有網路連接用於檢查更新、校時功能等)。
- (4) 檢視測錄之封包是否包含任何對外之封包。

#### (d) 測試基準

- (1) 測試步驟(4)之封包未含設備商所聲明以外之封包。

#### (e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

5.5.1.11 智慧音箱在服務偵測狀態，未偵測到喚醒詞前，不得有任何資料上傳行為

(a) 測試目的：測試受測物未偵測到喚醒詞前，是否仍有上傳資料之行為。

(b) 測試環境

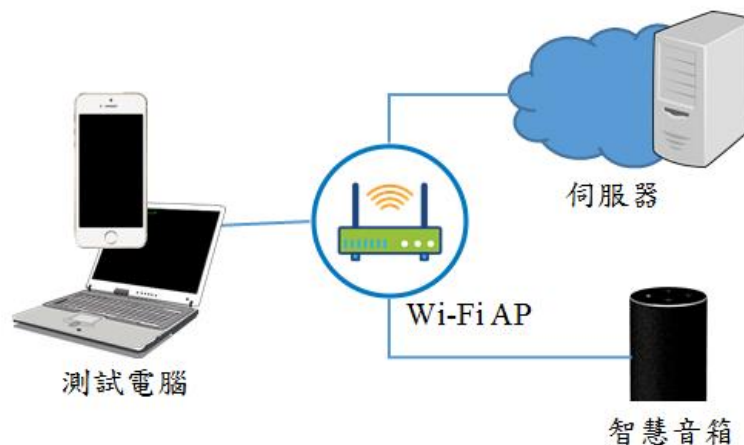


圖 23 隱私保護測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 23。

(c) 測試步驟

(1) 開啟智慧音箱之麥克風開關，即開始收音功能。

(2) 使用網路封包測錄工具連續抓取智慧音箱之封包適當時數(建議 8 小時以上)。

(3) 若音箱有其餘須對外之封包，必須提供相連伺服器之 IP 位置資訊，並於說明書或設備商隱私聲明表中作相關聲明(例：該音箱於開啟麥克風時會有網路連接用於檢查更新、校時功能等)。

(4) 檢視測錄之封包是否包含非設備商所聲明之封包。

(d) 測試基準

(1) 測試步驟(4)之封包未含設備商所聲明以外之封包。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：無。

5.5.1.12 智慧音箱應聲明在偵測到喚醒詞，進入服務狀態後，收集語音資料時間長度與資料上傳機制

(a) 測試目的：檢視設備商是否提供聲明收集語音資料時間長度與資料上傳機制。

(b) 測試環境

無。

(c) 測試步驟

- (1) 檢視受測物是否於設備商隱私聲明表(附錄B)中載明，並提供智慧音箱收音時長或機制。

(d) 測試基準

- (1) 設備商於設備商隱私聲明表(附錄B)中載明，並提供智慧音箱收音時長或機制。

(e) 測試結果

- (1) 通過：符合測試基準(1)。
- (2) 不通過：不符合測試基準(1)。
- (3) 不適用：無。

5.5.1.13 智慧音箱對外傳輸資料時，應有適當提醒告知之機制

(a) 測試目的：檢視受測物對外傳輸資料時，是否具有適當提醒告知之機制。

(b) 測試環境

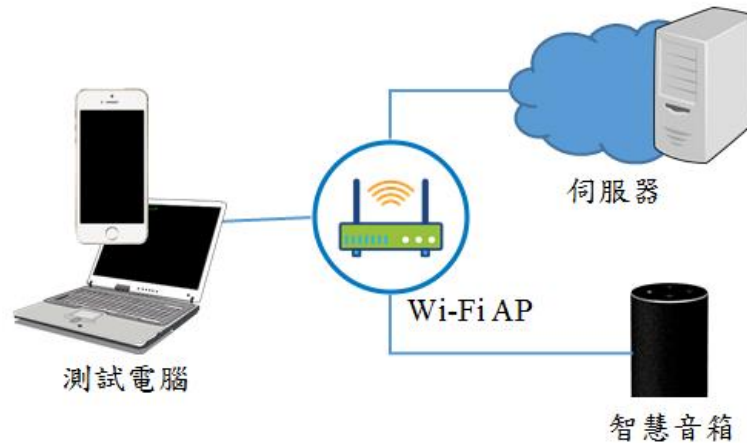


圖 24 隱私保護測試環境示意圖

(1) 測試設備：測試電腦、智慧音箱、Wi-Fi AP。

(2) 測試設備及受測物連接方式如圖 24。

(c) 測試步驟

(1) 開啟智慧音箱之麥克風開關，即開始收音功能。

(2) 使用喚醒詞觸發智慧音箱相關功能產生對外網路之封包。

(3) 檢視智慧音箱是否具有資料上傳行為之相對應提示功能(例如：燈號)。

(d) 測試基準

(1) 智慧音箱具有傳輸對外封包時之提示功能。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

## 5.6 行動應用程式安全

檢視智慧音箱之行動應用程式安全測試需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

### 5.6.1 行動應用 App 基本資安認證

5.6.1.1 智慧音箱搭配之手機 APP 須通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1[12] L2 之認證。

(a) 測試目的：檢視受測物手機 APP，是否具備基本資安要求。

(b) 測試環境

無

(c) 測試步驟

(1) 檢視設備商提供書面資料，判斷是否符合行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L2 之認證文件。

(d) 測試基準

(1) 受測物通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L2，並提供相關證明文件。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。

5.6.1.2 智慧音箱搭配之手機 APP 需通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L3 之認證。

(a) 測試目的：檢視受測物手機 APP，是否具備基本資安要求。

(b) 測試環境

無

(c) 測試步驟

(1) 檢視設備商提供書面資料，判斷是否符合行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L3 之認證文件。

(d) 測試基準

(1) 受測物通過行動應用資安聯盟所推出之行動應用 App 基本資安檢測基準 V3.1 L3，並提供相關證明文件。

(e) 測試結果

(1) 通過：符合測試基準(1)。

(2) 不通過：不符合測試基準(1)。

(3) 不適用：無。



**附錄 A**  
**(參考)**  
**設備商自我宣告表**

設備商自我宣告表		填寫日期：
		填寫人：
設備名稱		
廠牌		
型號		
申請者 (公司、商號名稱)	<input type="checkbox"/> 設備商 <input type="checkbox"/> 進口商 <input type="checkbox"/> 經銷商	
設備商		
韌體版本 (含雜湊資訊)		
進入作業系統除錯 模式之方法		
韌體檔案數位 簽章方法		
敏感性資料儲存 加密方式		
預設開啟之 網路通訊埠		

## 附錄 B (參考) 設備商隱私聲明表


隱 私 聲 明 表	填寫日期：
填寫人：	
資料蒐集與處理者 (例如:XXX股份有限公司)	
蒐集資料 (例如:IP 位置、使用者位置)	
蒐集方式 (例如:使用者使用語音查詢時，自動蒐集)。	
蒐集的目的 (例如:提供個人化推薦內容與廣告)	
資料保留時間與使用期限 (例如:保留時間：蒐集日起12個月)	
音箱於關閉收音功能或於開啟收音功能  但未偵測到喚醒詞前須連線之IP資訊	
智慧音箱收音時長或機制說明	

## 參考資料

- (1) SB-327 Information privacy: connected devices. 2018
- (2) 政府組態基準 GCB\_帳戶原則與精細密碼原則設定說明(V1.0), 2017/01

## 版本修改紀錄

版本	時間	摘要
v1.0	2020/09/22	出版



# 台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

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](mailto:secretariat@taics.org.tw)

[www.taics.org.tw](http://www.taics.org.tw)