TAICS

TAICS TS-0030 v1.1 : 2021

智慧型手機系統內建軟體資安測試規範

Infocom security test specification for embedded software on smartphone systems

2021/01/28

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

智慧型手機系統內建軟體資安測試規範

Infocom security test specification for embedded software on smartphone systems

出版日期: 2021/01/28
終審日期: 2020/05/22

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 副主任

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 王慶豐 副主任、黃志安 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)：
中華民國資訊軟體協會、中華電信股份有限公司、台灣大哥大股份有限公司、台灣電信產業發展協會、台灣德國萊因技術監護顧問股份有限公司、吉康科技有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、宏達國際電子股份有限公司、亞太電信股份有限公司、香港商立德國際商品試驗有限公司桃園分公司、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、華碩電腦股份有限公司、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、台灣之星電信股份有限公司、國立雲林科技大學、國立臺灣科技大學、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

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

國家通訊傳播委員會(National Communications Commission, NCC)為確保消費者使用智慧型手機出廠之安全性，於 2017 年 3 月公告「智慧型手機系統內建軟體資通安全檢測技術規範」，由中華民國資訊安全學會擔任驗證機構；並於 2017 年 4 月啟動智慧型手機系統內建軟體(Embedded Software on Smartphone Systems, ESS)資安自主檢測及認證驗機制。然而手機功能日新月異，例如：eSIM 服務，衍生偽造 eSIM 設定檔與未經授權訪問行動網路；為此， 2019 年 7 月 NCC 委由財團法人電信技術中心(Telecom Technology Center, TTC)參考前述技術規範，在作業系統層中納入 eSIM 測項、應用程式層中納入常見弱點與漏洞(Common Vulnerabilities and Exposures, CVE)與敏感性資料儲存於系統日誌等測試項目，並於台灣資通產業標準協會辦理產業標準制定工作。

TAICS TS-0030 v1.0「智慧型手機系統內建軟體資安測試規範」(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-0029 v1.0「智慧型手機系統內建軟體資安標準」訂定，俾利手機製造商、軟體開發商及資安檢測實驗室等做為手機系統內建軟體檢測參考藍本。本測試規範中具體明列資安檢測之測試項目、測試條件、測試方法及測試標準等事項。

1. 適用範圍

本規範為依據 TAICS TS-0029 v1.0 「智慧型手機系統內建軟體資安標準」規定，所訂定之測試規範，適用範圍為手機製造商於出廠時安裝在手機上的軟體，包含系統內具圖示與無圖示軟體。使用者於初次開機後，自行下載之應用程式、附加服務或內容，例如：登入 Google Play 或 App Store 帳號後自行下載應用程式，自行上網下載之第三方應用程式，插入 SIM 卡自動安裝之電信服務或相關應用程式等，則不在本測試規範之範圍。適用範圍如圖 1 所示。

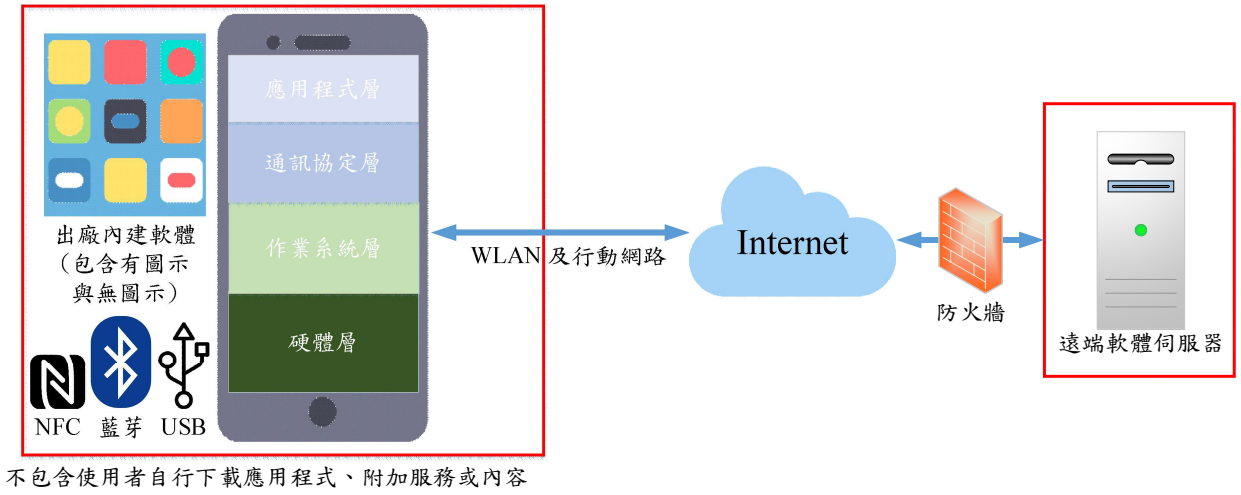

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

[1] 國家通訊傳播委員會，智慧型手機系統內建軟體資通安全檢測技術規範：2017

[2] European Union Agency for Network and Information Security (ENISA), Smartphone Secure Development Guidelines: 2017

[3] OWASP, Mobile Security Testing Guide (MSTG): 2018

[4] GSMA, SGP25-Embedded UICC for Consumer Devices Protection Profile Version 1.0 05-June-2018

[5] Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 2019

3. 用語及定義

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」所規定及下列用語及定義適用於本規範。

3.1 密碼套件 (Cipher suite)

指使用於安全通道(Secure sockets layer/ transport layer security, SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(Message authentication code, MAC)和金鑰交換演算法。

3.2 埠掃描 (Port scan)

指偵測應用程式開啟哪些網路埠或網路服務，探尋其漏洞之行為。亦稱為網路埠掃描、通訊埠掃描或連接埠掃描。

3.3 共同準則 (Common criteria, CC)

指國際資通安全產品評估及驗證之標準(ISO/IEC 15408)，依其定義之評估保證等級(Evaluation assurance level, EAL)判定產品之安全等級，EAL 共有 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7，提供申請者/贊助者、檢測實驗室與驗證機關(構)評估及驗證資通安全產品安全與功能性(1)。

3.4 安全標的 (Security target, ST)

指資通安全產品能符合保護剖繪(PP)或特定安全需求製作之規格文件。

3.5 安全功能 (TOE security functions, TSF)

指資通安全產品用於實現安全標的(ST)所要求安全功能需求 (Security functional requirement，SFR)之相關功能(1)。

3.6 安全功能需求 (Security functional requirement, SFR)

指共同準則第二部分(Common criteria part 2)所定義之安全相關需求條文，用以描述一資通安全產品之安全功能(TSF)所需滿足的各項要求。此要求條文會被引用於保護剖繪及安全標的中，用以具體陳述該產品功能於安全方面的需求(1)。

3.7 評估標的 (Target of evaluation, TOE)

指申請評估及驗證之資通安全產品及其相關使用手冊(1)。

3.8 保護剖繪 (Protection profile, PP)

指滿足資通安全產品評估標的(TOE)製作之安全基本需求文件。

3.9 安全功能介面 (TOE Security functions interface, TSFI)

指評估標的(TOE)用於實現安全功能需求(SFR)之對外溝通介面(1)。

3.10 安全領域 (Secure domain)

指一主動式個體(人或機器)被授權存取的資源集合，為安全架構的屬性之一(1)。

3.11 自我保護 (Self- protection)

指安全功能可以自動識別自身並加以保護，無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

3.12 防止繞道 (Non- bypassibility)

指防止避開待測物安全功能檢查之技巧(如：未經過身分鑑別，無法進入稽核功能介面)(2)。

3.13 資料型別 (Data type)

本規範依資料之敏感性與是否為使用者輸入等兩個因素分成第 1 型、第 2 型、第 3 型及第 4 型(如表 1)其中第 1 型及第 2 型為敏感性資料。

表 1 資料型別分類表

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
第 1 型	是	是	1.本標準第三節“用語及定義”之 3.1 個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置通行碼、帳號通行碼、金鑰、相片、生物特徵識別資料
第 2 型	是	否	IMEI、IMSI[註]、定位資訊。
第 3 型	否	否	MAC 位址、APP 列表、音樂播放資訊、手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、eSIM 設定檔。
第 4 型	無法判斷	無法判斷	資料加密、協定加密、無加密但內容未知。
[註] IMEI 碼及 IMSI 碼須與行動通信業者或手機廠商之銷售保固連結，該 IMEI 碼及 IMSI 碼才具備個資識別性，但使用人與登錄人可能不同，故歸類為第 2 型。			

3.14 常駐程式 (Resident program)

指留存於儲存裝置個別區域中之程式(2)。

3.15 安全通道 (Security tunnel)

為網際網路通訊端點與端點(End-to-End)間，兼顧資料隱密性及完整性所建立之通道，例：目前常見之實作通訊協定為安全接套層(Secure sockets layer, SSL)及傳送層安全性(Transport layer security, TLS)。

3.16 應用程式關閉 (Application destroy)

指應用程式停止並釋放所有剩餘資源(3)。

3.17 國際行動用戶識別碼 (International mobile subscriber identity, IMSI)

指結合所有 GSM 與 UMTS 網路行動裝置用戶的唯一識別碼。IMSI 由一串 10 進位數組成，最大長度為 15 位數，在行動電話裡面的 SIM 卡上所標示前 3 位數代表行

動裝置國碼(Mobile country code, MCC)；接續是行動裝置網路碼(Mobile network code, MNC)，它是 3 位數(北美標準式)或 2 位數(歐洲標準式)；其餘的位數代表行動訂閱辨識碼(Mobile subscription identification number, MSIN)，該數值由營運商自行分配，因此 IMSI 是由 MCC、MNC 及 MSIN 三種代表碼依次連接而成。

3.18 國際行動設備識別碼 (International mobile equipment identity，IMEI)

指行動網路中識別每一部獨立的行動通訊裝置，相當於該裝置之身分證。序列號共有 15 位數字，前 6 位(Type approval code, TAC)是型號核准號碼，代表手機類型；接著 2 位(Final assembly code, FAC)是最後裝配號，代表產地；後 6 位(Serial number, SNR)是序號，代表生產順序號；最後 1 位(SP)是檢驗碼，一般為 0。國際行動設備識別碼標示於機身背面與外包裝上，同時也存在手機記憶體中。

3.19 網際網路通訊協定位址 (Internet protocol address, IP Address)

指唯一識別網際網路上裝置的位址，簡稱為 IP 位址。

3.20 網域名稱 (Domain name, DN)

指用以與網際網路位址相對映，便於網際網路使用者記憶網路主機所在位址(即 IP 位址)之文字或數字組合。

3.21 憑證機構 (Certification authority, CA)

指簽發憑證之機關、法人，為使用者所信任之公正機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證、憑證機構註銷清冊及憑證廢止清冊。

3.22 模糊測試 (Fuzz testing)

指一種測試技術，其核心是將自動或半自動生成的亂數據輸入到應用程式或通訊協定中，並監視應程式異常，例如：程式崩潰(Program crash)、中斷(Assertion)等，以發現可能的程式錯誤。模糊測試常常用於檢測軟體或通訊協定安全漏洞。

3.23 SQL 隱碼攻擊 (SQL injection attack)

指利用資料庫的漏洞執行非預期之外部程式或指令，進而取得未經授權資料之攻擊(5)。

3.24 本地文件包含漏洞 (Local file inclusion, LFI)

指一種網路攻擊手法，因為程式撰寫者對於傳入的參數並未做合理的驗證，攻擊者可透過修改包含文件之參數路徑來存取伺服器上的敏感性資料。

3.25 JavaScript 注入攻擊 (JavaScript injection attack)

指一種網路攻擊手法，透過利用開發時留下的漏洞，注入惡意指令程式碼到應用程式，使用戶載入並執行後駭客可以竊取用戶敏感性資料。

3.26 格式化字串攻擊 (Format string attack)

指應用程式將輸入字串作為指令執行時，發生 Format String 漏洞。攻擊者可以執行指令，讀取正在執行的應用程式引起分段錯誤，進而導致新的行為，可能危及系統安全性或穩定性(6)。

3.27 指令注入攻擊(Command injection attack)

指透過應用程式在伺服器作業系統上執行任意指令。當應用程式將不安全的的數據(表格、Cookie、HTTP 標頭等)傳遞到系統執行時，可能會發生指令注入攻擊。在指令注入攻擊中，作業系統指令攻擊應用程式的特權執行。由於應用程式沒有足夠的輸入驗證，可能發生指令注入攻擊(7)。

4. 測試項目分級

本節依據 TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」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 2 所示，第一欄為安全構面，包括：應用程式層安全、通訊協定層安全、作業系統層安全、硬體層安全；第二欄為安全測試項目，係依第一欄安全構面設計對應之安全測試項目；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。

安全等級依敏感性資料相關保護、惡意攻擊與核心底層不被竄改或不正當擷取資訊，分為 1 級、2 級、3 級三個等級。不同等級安全測試，廠商申請應填寫附錄 A 之書面資料送審，並依實機測試標準等級 1 級與 2 級填寫附錄 B～E，3 級填寫附錄 B～G，並依各測試項目進行實機測試與核對廠商送審之書面資料。申請者於初次申請時，可任意指定欲檢測之級別。

表 2 實機測試標準等級總表

安全構面	安全測試項目	安全等級		
		1 級	2 級	3 級
5.1 應用程式層安全測試	5.1.1 程式資料使用授權測試	5.1.1.1	-	-
	5.1.2 程式資料儲存保護測試	5.1.2.1	5.1.2.2 5.1.2.3	-
	5.1.3 資料遺失保護測試	5.1.3.1	-	-
	5.1.4 程式身分辨識測試	5.1.4.1	-	5.1.4.2
	5.1.5 程式信任來源測試	5.1.5.1 5.1.5.2	-	-
	5.1.6 程式執行授權測試	5.1.6.1 5.1.6.2	5.1.6.3 5.1.6.4	-
	5.1.7 程式執行安全測試	5.1.7.1	5.1.7.2 5.1.7.3 5.1.7.4 5.1.7.5	5.1.7.6
5.2 通訊協定層安全測試	5.2.1 協定使用授權測試	5.2.1.1	-	-
	5.2.2 協定傳輸保護測試	5.2.2.1	5.2.2.2 5.2.2.3	-
	5.2.3 協定執行安全測試	-	5.2.3.1	-
5.3 作業系統層安全測試	5.3.1 系統操作授權測試	5.3.1.1 5.3.1.2	-	-
	5.3.2 系統身分辨識測試	5.3.2.1 5.3.2.2	5.3.2.3	5.3.2.4
	5.3.3 系統執行安全測試	5.3.3.1	5.3.3.2	5.3.3.3 5.3.3.4 5.3.3.5
	5.3.4 eSIM 傳輸保護測試	5.3.4.1	5.3.4.2	-
5.4 硬體層安全測試	5.4.1 實體安全測試	5.4.1.1	-	-
	5.4.2 金鑰管理保護測試	-	-	5.4.2.1 5.4.2.2 5.4.2.3
	5.4.3 演算法強度要求測試	-	-	5.4.3.1 5.4.3.2 5.4.3.3

5. 資安測試規範

檢視智慧型手機之應用程式層、通訊協定層、作業系統層與硬體層安全測試需求是否符合廠商送審之書面送審資料，內建軟體與韌體版本應於測試期間更新為最新版本，以維持內建軟體正常使用、新增功能或安全性，並依下列各測試項目進行實機測試。

5.1 應用程式層安全測試

5.1.1 程式資料使用授權測試

5.1.1.1 內建軟體於存取敏感性資料前，應取得使用者同意。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.1.1。

(b) 測試目的：

驗證內建軟體存取敏感性資料應取得使用者同意，防止敏感性資料在未經授權下使用。

(c) 檢測條件：

(1) 受測軟體具備存取敏感性資料的功能。

(2) 資料型別：第 1、2 型資料。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 檢查受測內建軟體之隱私權政策或使用聲明中，是否提供受測軟體存取敏感性資料之說明。

(2) 如未符合步驟(1)，則執行受測軟體，並存取使用者敏感性資料。

(3) 檢查受測軟體是否提供相對應的使用者同意機制。

(f) 判定標準：

(1) 步驟(1)中，隱私權政策或使用聲明中有提供受測軟體存取敏感性資料之說明。

(2) 或步驟(3)中，受測軟體提供相對應的使用者同意機制。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.2 程式資料儲存保護測試

5.1.2.1 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-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.2.1。

(b) 測試目的：

驗證手機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，防止帳號、通行碼或金鑰等資料洩漏。

(c) 檢測條件：

(1) 受測軟體具備帳號通行碼登入功能。

(2) 資料型別：第 1 型資料之帳號、通行碼與金鑰。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 2。

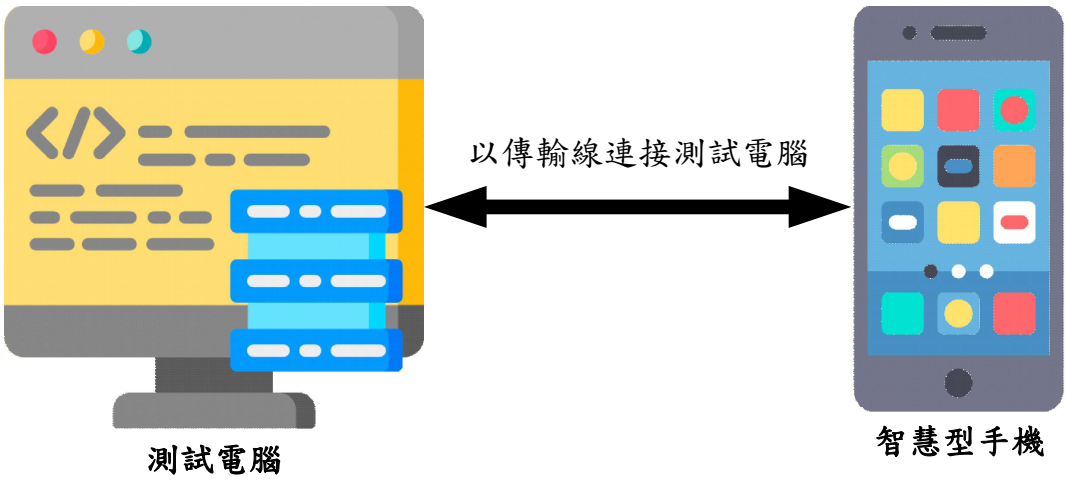

圖 2 測試示意圖

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 執行受測軟體輸入帳號、通行碼，同意儲存帳號與通行碼，並成功登入。

(3) 對受測軟體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。

(5) 比對「附錄 D 廠商自我宣告表-2」的敏感性資料儲存於非作業系統保護區欄位中廠商所宣告之加密方法，是否為 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)。

(f) 判定標準：

(1) 步驟(4)中，受測軟體將帳號、通行碼或金鑰以加密型態存放於非作業系統保護區。

(2) 步驟(5)中，比對廠商所宣告之加密方法符合。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.2.2 內建軟體於儲存敏感性資料時應提供資料加密功能

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.2.2。

(b) 測試目的：

驗證手機內建軟體應使用加密功能，防止攻擊者輕易取得敏感性資料。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限。

(2) 受測軟體具備儲存敏感性資料的功能。

(3) 資料型別：第 1 型資料(不包含相片與圖片)。

(4) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 執行受測軟體，並儲存敏感性資料。

(3) 以管理者權限檢查受測軟體是否以明文方式儲存敏感性資料。

(4) 比對「附錄 D 廠商自我宣告表-2」的敏感性資料儲存於非作業系統保護區欄位中廠商所宣告之加密方法，是否為 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)。

(f) 判定標準：

(1) 步驟(3)中，受測軟體未以明文方式儲存敏感性資料。

(2) 步驟(4)中，比對受測軟體使用廠商所宣告之加密方法儲存敏感性資料。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.2.3 內建軟體之帳號、通行碼或金鑰不應以明文方式存在於執行檔中

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.2.3。

(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，防止遭不正當的方式存取，攻擊者可能冒名登入或破解加密。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限、程式執行檔或原始碼。

(2) 受測軟體具備帳號通行碼登入功能。

(3) 資料型別：帳號及通行碼。

(4) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 使用測試電腦將受測軟體執行檔還原為原始碼。

(3) 檢查受測軟體執行檔原始碼中是否以明文方式儲存帳號、通行碼與金鑰。

(f) 判定標準：

(1) 步驟(3)中，執行檔中以加密方式儲存帳號、通行碼與金鑰。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.3 資料遺失保護測試

5.1.3.1 手機系統應提供資料保護與備份功能

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.3.1。

(b) 測試目的：

驗證手機系統是否提供使用者資料保護與備份功能，防止手機遺失時資料外洩與還原資料。

(c) 檢測條件：

(1) 受測系統具備遠端鎖定與刪除資料功能。

(2) 受測系統具備手機對手機、雲端備份、手機連接電腦資料備份功能。

(3) 資料型別：第 1、2、3 型資料。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 檢查受測系統是否提供資料備份功能。

(2) 檢查受測系統是否提供遠端鎖定與刪除資料功能。

(3) 設定並執行受測系統的遠端鎖定功能，檢查受測系統是否被遠端鎖定。

(4) 輸入測試資料後並儲存，執行受測系統的遠端刪除功能，檢查測試資料是否被刪除。

(5) 使用手機對手機、雲端備份、手機連接電腦資料備份功能其中一種進行測試。

(f) 判定標準：

(1) 步驟(3)中，受測系統已被遠端鎖定。

(2) 步驟(4)中，測試資料已被遠端刪除。

(3) 步驟(5)中，受測系統有提供資料備份功能且可實際備份成功。

(4) 若全部符合判定標準，則本檢測項目「符合」。

(5) 若任一不符合判定標準，則本檢測項目「不符合」。

5.1.4 程式身分辨識測試

5.1.4.1 內建軟體在初次存取使用者帳戶時，應告知使用者存取帳戶相關之敏感性資料

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.4.1。

(b) 測試目的：

驗證內建軟體第一次登入時是否綁定帳戶，並告知使用者存取相關敏感性資料，防止在不知情下洩漏。

(c) 檢測條件：

(1) 受測軟體具備連接使用者帳戶功能。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 執行受測軟體之使用者帳戶認證功能。

(3) 比對「附錄 D 廠商自我宣告表-2」廠商自我宣告表-2 欄位「是否具帳戶驗證登入機制」，受測內建軟體是否自動存取帳號。

(4) 檢查受測軟體是否提供使用者登入確認並告知使用者存取帳戶相關敏感性資料之機制。

(f) 判定標準：

(1) 步驟(3)中，受測內建軟體是否自動存取帳號。

(2) 步驟(4)中，受測軟體於存取使用者帳戶時，有提示使用者認證與敏感性資料授權之機制。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.4.2 內建軟體具備付費功能時，應使用多因子或強驗證進行用戶身分辨識。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.4.2。

(b) 測試目的：

驗證內建軟體具備付費功能時，使用多因子或強驗證來進行用戶身分辨識，防止在使用者不知情下造成財物損失。

(c) 檢測條件：

(1) 受測軟體具備付費功能。

(2) 受測軟體支援多因子驗證、硬體或軟體 Token、公開金鑰驗證、UAF、U2F、FIDO、FIDO2 與 WebAuthn 等驗證機制。

(3) 資料型別：無。

(4) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 執行受測軟體之付費功能。

(3) 比對「附錄 D 廠商自我宣告表-2」廠商自我宣告表-2 欄位「是否具帳戶具備付費功能」，受測內建軟體是否使用多因子或強驗證方法。

(4) 檢查受測軟體使用者付費時使用廠商自我宣告所宣稱之多因子或強驗證機制。

(f) 判定標準：

(1) 步驟(4)中，受測軟體於付費或存取使用者帳戶時，提供使用者多因子驗證之機制。

(2) 步驟(4)中，受測軟體使用強驗證於付費或存取使用者帳戶時，廠商提供書面證明，則本檢測項目「符合」。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.5 程式信任來源測試

5.1.5.1 內建軟體具備付費功能時，應使用有效期間之伺服器憑證。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.5.1。

(b) 測試目的：

驗證內建軟體是否使用為有效期限內，且為可信任憑證機構所簽發之伺服器憑證，確保付費交易之安全。

(c) 檢測條件：

(1) 受測軟體具備付費功能。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

參照圖 3。

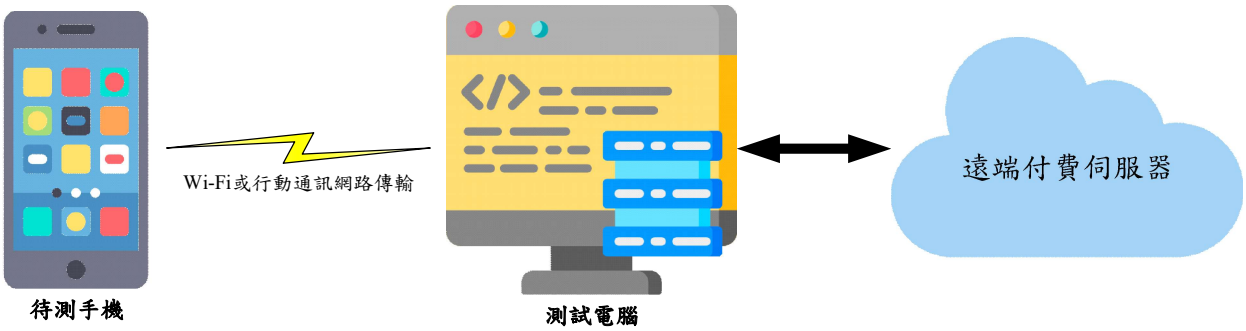

圖 3 測試示意圖

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 受測軟體透過網路傳輸資料至遠端付費伺服器。

(3) 檢查伺服器端提供給受測軟體之憑證資料是否過期，是否為可信任憑證機構所簽發之憑證。

(f) 判定標準：

(1) 步驟(3)中，伺服器端提供給受測軟體的憑證資料未過期，並驗證伺服器憑證為可信任憑證機構所簽發。

(2) 若是受測軟體與伺服器使用 TLS v1.3 以上或最新版本進行傳輸，以「附錄 D」之「資料連結伺服器之 IP/DN/公司名稱及伺服器類型」，提供之主機名稱，以情資蒐集方式驗證憑證，則本檢測項目「符合」。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.5.2 內建軟體應可識別其發行資訊。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.5.2。

(b) 測試目的：

驗證內建軟體具備發行資訊，確保使用者了解軟體來源。

(c) 檢測條件：

(1) 資料型別：無。

(2) 受測軟體屬性：出廠內建軟體。

(3) 申請者須填寫「附錄 C 廠商自我宣告表-1」。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認廠商已填寫「附錄 C 廠商自我宣告表-1」廠商。

(2) 檢查受測軟體與廠商填寫「附錄 C 廠商自我宣告表-1」之內容是否一致。

(f) 判定標準：

(1) 步驟(2)中，受測軟體或廠商填寫「附錄 C 廠商自我宣告表-1」提供受測軟體的發行商和版本資訊。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.6 程式執行授權測試

5.1.6.1 內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.6.1。

(b) 測試目的：

驗證內建軟體應於每次付費前，向使用者說明並取得同意後，才可執行付費，防止未經使用者同意下進行付費。

(c) 檢測條件：

(1) 受測軟體具備付費功能。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測軟體已符合檢測條件。

(2) 執行受測軟體，並開啟付費功能。

(3) 檢查受測系統或受測軟體是否經使用者同意才執行付費。

(f) 判定標準：

(1) 步驟(3)中，受測系統或受測軟體經使用者同意才執行付費。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.6.2 內建軟體預設之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.6.2。

(b) 測試目的：

驗證內建軟體預設之權限，是否與「附錄 D 廠商自我宣告表-2」權限說明相符，防止權限遭濫用。

(c) 檢測條件：

(1) 申請者須填寫「附錄 D 廠商自我宣告表-2」中之「功能說明」與「權限說明」欄位。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體、無圖示軟體選測。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 確認廠商已填寫「附錄 D 廠商自我宣告表-2」。

(2) 執行及操作受測軟體，並列舉受測軟體所使用的功能及存取權限。

(3) 比對步驟(2)列舉之內容是否與廠商宣告之內容相符。

(f) 判定標準：

(1) 步驟(2)中與步驟(3)列舉之內容與「附錄 D 廠商自我宣告表-2」宣告之內容相符。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.6.3 內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路埠」相符

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.6.3。

(b) 測試目的：

確認手機內建軟體所開啟之網路埠(Port)與「附錄 D 廠商自我宣告表-2」是否相符，防止攻擊者可能連線進入手機下指令或存取敏感性資料。

(c) 檢測條件：

(1) 受測軟體具備開啟網路連接埠進行網路連線功能。

(2) 申請者須填寫「附錄 D 廠商自我宣告表-2」中之「網路埠」欄位。

(3) 資料型別：無。

(4) 受測軟體屬性：出廠內建軟體、無圖示軟體選測。

(d) 測試佈局：

測試架構如圖 3。

(e) 測試方法：

(1) 開啟受測系統或內建軟體。

(2) 確認已符合檢測條件。

(3) 執行受測軟體並開始通訊，網路埠掃描取得受測軟體開啟之網路埠號。

(4) 檢查步驟(3)取得之網路埠號是否與「附錄 D 廠商自我宣告表-2」所宣告之「網路埠」相符。

(f) 判定標準：

(1) 步驟(4)中，取得之網路埠號與「附錄 D 廠商自我宣告表-2」所宣告之「網路埠」相符。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.6.4 內建軟體於使用者設定應用程式關閉時，應停止該內建軟體程序。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.6.4。

(b) 測試目的：

驗證手機內建軟體是否在關閉時，停止內建軟體程序。

(c) 檢測條件：

(1) 受測軟體不是常駐程式。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 取得所有執行中的應用程式清單。

(3) 執行並操作受測軟體。

(4) 關閉步驟(3)執行之受測軟體，並再次取得所有執行中的應用程式清單。

(f) 判定標準：

(1) 比對步驟(2)之清單與步驟(4)之清單相同，受測軟體不是常駐程式。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7 程式執行安全測試

5.1.7.1 內建軟體應提供回報安全性問題之管道

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.1。

(b) 測試目的：

驗證內建軟體是否提供使用者回報管道，確保可以傳達安全性問題。

(c) 檢測條件：

(1) 資料型別：無。

(2) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

檢查受測軟體、官方網站或使用說明書是否提供問題回報管道(如：電話、E-Mail、官網或線上客服等)。

(f) 判定標準：

(1) 步驟(1)中，受測軟體發現的問題可透過管道回報，並且可以實際聯絡成功。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7.2 內建軟體是否具備防護注入攻擊之設計。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.2。

(b) 測試目的：

驗證內建軟體是否具備 SQL 隱碼攻擊、本地文件包含漏洞、JavaScript 注入攻擊、格式化字串與指令注入攻擊的保護，確保內建軟體注入防護機制。

(c) 檢測條件：

(1) 受測軟體具備可供使用者輸入資料之欄位。

(2) 資料型別：第 1 型資料。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 執行受測軟體，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。

(3) 檢查步驟(2)之受測軟體是否執行字串。

(f) 判定標準：

(1) 步驟(3)中，受測軟體未執行攻擊字串。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7.3 內建軟體應具備可延伸標記語言外部實體攻擊處理能力。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.3。

(b) 測試目的：

驗證內建軟體是否具備可延伸標記語言外部實體攻擊的保護，防止檔案或資料內容可能遭到竄改。

(c) 檢測條件：

(1) 受測軟體可接收可延伸標記語言。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 4。

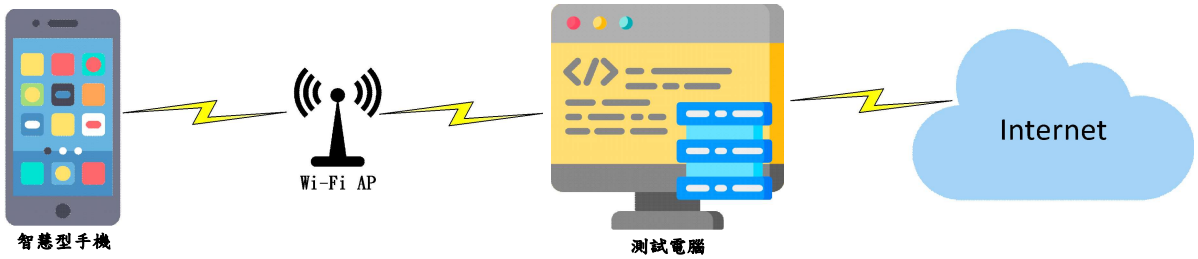

圖 4 測試示意圖

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 執行受測軟體之網路傳輸功能。

(3) 攔截遠端主機傳送至受測軟體之通訊封包。

(4) 將至少 10 組不同之可延伸標記語言外部實體攻擊字串逐一注入步驟(3)攔截之通訊封包，再傳送至受測軟體。

(5) 檢查受測軟體是否執行注入攻擊字串。

(f) 判定標準：

(1) 步驟(5)中，受測軟體未執行注入攻擊字串。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7.4 內建軟體第三方函式庫引用是否存在美國國家弱點資料庫公布及更新之常見弱點與漏洞資料，且漏洞評鑑系統 CVSS 嚴重性等級評比為高風險等級。

(g) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.4。

(h) 測試目的：

驗證手機內建軟體引用第三方函式庫是否存在已知 CVSS 嚴重性等級評比為高風險等級評比為高風險等級之漏洞，防止已知漏洞遭利用。

(i) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限、程式執行檔或原始碼。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體、無圖示軟體選測。

(j) 測試佈局：

無。

(k) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 更新測試設備漏洞偵測功能之 CVE 弱點資料庫，該資料庫應包含 NIST 發布之 CVE 漏洞，及採用 NIST 發布之弱點評估方式。

(3) 掃描內建軟體安裝檔第三方函式庫 CVE 漏洞。

(l) 判定標準：

(1) 步驟(3)中，內建軟體引用第三方函式庫不存在美國國家弱點資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞。

(2) 當檢測出之漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7.5 內建軟體是否在執行期間將敏感性資料儲存於系統日誌檔案中。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.5。

(b) 測試目的：

驗證內建軟體在執行期間是否將敏感性資料儲存於系統日誌檔案中，使用者拒絕存取敏感性資料後，不應存取敏感性資料，防止執行期間洩漏敏感性資料。

(c) 檢測條件：

(1) 資料型別：第 1、2 型資料。

(2) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

如圖 2。

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 將手機以傳輸線接上測試電腦，測試電腦應具備檢查手機應用程式系統日誌工具。

(3) 執行及操作受測軟體存取敏感性資料，並拒絕受測軟體存取敏感性資料，檢查應用程式是否仍可儲存敏感性資料。

(4) 執行及操作受測軟體，使用系統日誌工具檢查受測軟體是否在執行期間將敏感性資料儲存於日誌系統檔案中。

(f) 判定標準：

(1) 步驟(3)之受測軟體無法繼續操作或無存取使用者敏感性資料。

(2) 步驟(4)之日誌檔案，檢查是否有敏感性資料。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.1.7.6 內建軟體是否具備完整性確保判斷機制。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.1.7.6。

(b) 測試目的：

驗證手機內建軟體檢查手機是否被破解管理者權限或防止逆向工程機制，防止敏感性資料遭破解取得。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體、無圖示軟體選測。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測內建軟體已符合檢測條件。

(2) 利用具管理者權限之手機開啟受測內建軟體，檢查內建軟體是否判斷手機遭破解。

(3) 利用反編譯工具將受測軟體進行逆向工程，檢查程式碼是否有加殼或混淆。

(f) 判定標準：

(1) 步驟(2)、(3)中，檢查手機是否判斷管理者權限或防止逆向工程機制。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.2 通訊協定層安全測試

5.2.1 協定使用授權測試

5.2.1.1 手機系統應預設關閉近場通訊功能。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.2.1.1。

(b) 測試目的：

驗證手機是否預設開啟近場通訊(NFC)功能，防止手機以 NFC 下載惡意程式。

(c) 檢測條件：

(1) 受測手機具備近場通訊(NFC)功能。

(2) 資料型別：無。

(3) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測手機已符合檢測條件。

(2) 檢查手機在出廠設定是否預設開啟近場通訊(NFC)功能。

(f) 判定標準：

(1) 步驟(3)中，手機出廠設定近場通訊(NFC)功能預設關閉。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.2.2 協定傳輸保護測試

5.2.2.1 內建軟體透過無線傳輸技術功能傳輸敏感性資料時應使用加密傳輸。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.2.2.1。

(b) 測試目的：

驗證內建軟體使用無線傳輸敏感性資料時使用加密傳輸，防止攻擊者可輕易取得封包內之敏感性資料。

(c) 檢測條件：

(1) 軟體支援之無線傳輸技術：藍牙、WLAN 或行動通訊網路。

(2) 資料型別：第 1、2 型資料。

(3) 受測軟體屬性：出廠內建軟體、無圖示軟體選測。

(d) 測試佈局：

見圖 5。

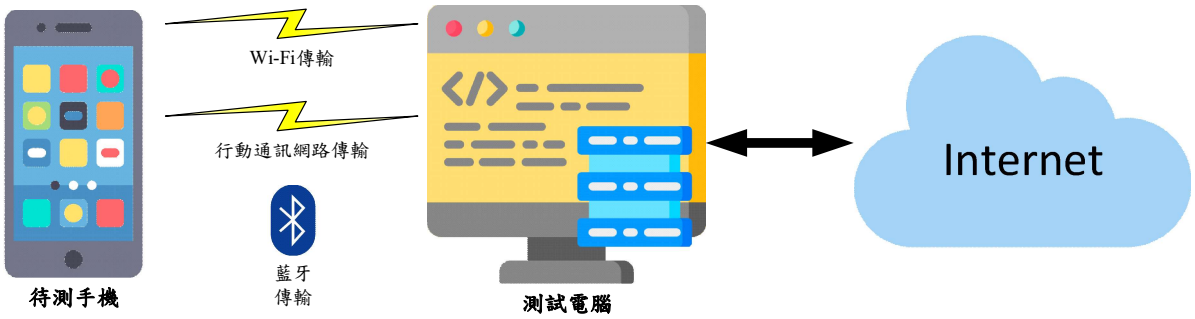

圖 5 測試示意圖

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 執行受測系統內建軟體，並依照內建軟體支援無線傳輸技術(藍牙、WLAN 及行動通訊網路)功能傳輸敏感性資料。

(3) 若受測系統內建軟體使用相同藍牙分享功能，僅進行一次測試即可。

(4) 以測試設備擷取受測系統內建軟體傳輸封包

(5) 檢查(3)是否以明文方式傳輸敏感性資料。

(f) 判定標準：

(1) 步驟(4)中，受測軟體未以明文方式傳輸敏感性資料。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.2.2.2 內建軟體應避免交談識別碼遭重送攻擊。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.2.2.2。

(b) 測試目的：

驗證內建軟體是否防護交談識別碼遭重送攻擊，防止攻擊者可能冒名登入或取得伺服器回傳敏感性資料。

(c) 檢測條件：

(1) 受測軟體透過網路傳輸資料時具備交談識別碼。

(2) 資料型別：無。

(3) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 4。

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 執行受測軟體之網路傳輸功能。

(3) 測試電腦應具備取得受測軟體與遠端主機間通訊封包之軟體，受測軟體進行登入，側錄受測軟體與遠端主機間之通訊封包，並擷取交談識別碼。

(4) 執行受測軟體登出功能。

(5) 將步驟(3)中之交談識別碼，透過測試電腦執行重送攻擊。

(f) 判定標準：

(1) 步驟(5)中，測試電腦使用交談識別碼執行重送攻擊，回傳內容不應包含敏感性資料。

(2) 若受測軟體進行憑證綁定，無法進行重送攻擊，則本檢測項目「符合」

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.2.2.3 內建軟體與付費功能伺服器間之加密傳輸，應使用安全之加密演算法。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.2.2.3。

(b) 測試目的：

驗證內建軟體使用付費功能應使用安全加密演算法，防止攻擊者可輕易取得付費資訊。

(c) 檢測條件：

內建軟體具備付費功能。

(d) 測試佈局：

見圖 4。

(e) 測試方法：

(1) 確認受測系統內建軟體已符合檢測條件。

(2) 執行受測軟體之網路傳輸功能。

(3) 檢查受測軟體所存取之伺服器，其使用之加密演算法是否為 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)或由申請者提供同等安全性之佐證資料。

(f) 判定標準：

(1) 步驟(3)中，受測軟體與伺服器端之通訊加密演算法為清單所列之加密演算法或申請者提供足以證明達同等安全性之佐證資料。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.2.3 協定執行安全測試

5.2.3.1 手機系統應具備通訊協定內容的錯誤處理能力。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.2.3.1。

(b) 測試目的：

驗證手機應具備通訊協定內容錯誤處理能力，防止未預期漏洞發生。

(c) 檢測條件：

(1) 受測無線傳輸技術：藍牙及 WLAN。

(2) 資料型別：無。

(3) 受測軟體屬性：無。

(d) 測試佈局：

見圖 6。

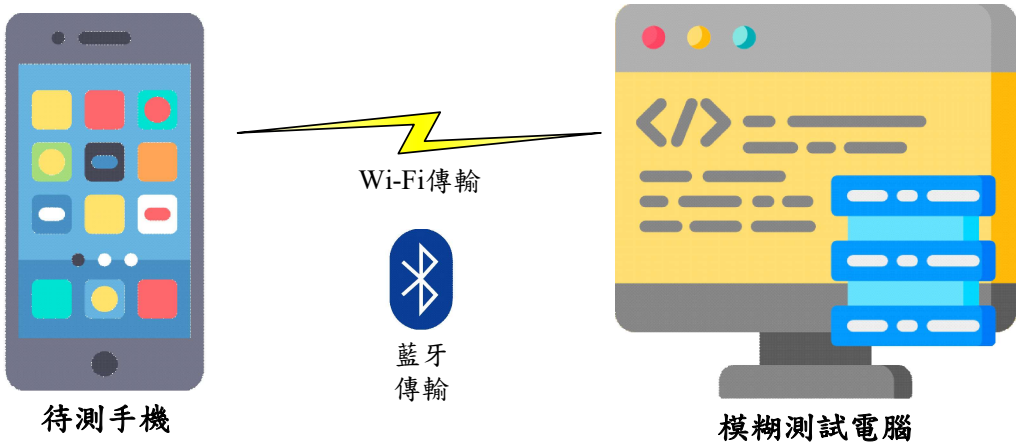

圖 6 測試示意圖

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 執行受測軟體之網路傳輸功能。

(3) 在受測的無線傳輸環境下，於通訊連線交涉(Negotiation)起，採用模糊測試方法，針對使用的通訊協定逐一發送不同錯誤封包達一萬次，或最少 8 小時的異常輸入測試。

(4) 檢查無線傳輸技術介面或受測系統是否仍正常運作。

(f) 判定標準：

(1) 步驟(3)中，受測系統均可正常進行通訊連線與資料傳輸，且正常運作。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3 作業系統層安全測試

5.3.1 系統操作授權測試

5.3.1.1 手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之IP/DN/公司主機名稱」相符。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.1.1。

(b) 測試目的：

驗證手機系統更新來源與廠商自我宣告表「附錄 D 廠商自我宣告表-2」是否相符資料連結伺服器之 IP/DN/公司主機名稱，防止從未知來源下載更新檔案。

(c) 檢測條件：

(1) 受測系統具備作業系統更新功能。

(2) 申請者須填寫「附錄 D 廠商自我宣告表-2」中之「資料連結伺服器之 IP/DN/公司主機名稱」欄位。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

見圖 4。

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 透過受測系統內建作業系統更新功能執行作業系統更新。

(3) 取得作業系統更新之連線目的地位址。

(4) 檢查步驟(4)中目的地位址是否與廠商填寫「附錄 D 廠商自我宣告表-2」之內容相符。

(f) 判定標準：

(1) 步驟(4)中，目的地位址與廠商填寫「附錄 D 廠商自我宣告表-2」之內容相符。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.1.2 手機系統於下載或安裝更新作業系統時應提供更新資訊，並告知使用者更新內容。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.1.2。

(b) 測試目的：

手機系統於下載或安裝更新作業系統時，確保使用者了解更新與修補內容。

(c) 檢測條件：

(1) 受測系統具備作業系統更新功能。

(2) 資料型別：無。

(3) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 檢查受測系統或官網是否提供作業系統更新資訊，並告知使用者更新內容，取得使用者之同意更新。

(f) 判定標準：

(1) 步驟(2)中，受測系統或官網有提供作業系統更新資訊，並告知使用者更新內容，取得使用者之同意更新。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.2 系統身分辨識測試

5.3.2.1 手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.2.1。

(b) 測試目的：

驗證手機系統應支援螢幕解鎖錯誤強制鎖定保護機制，防止個人資訊遭未經授權使用。

(c) 檢測條件：

(1) 資料型別：無。

(2) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 開啟受測系統之螢幕鎖定設定功能，並設定螢幕鎖定方式及解鎖資料。

(2) 鎖定受測系統(包含關閉螢幕及關閉受測系統)。

(3) 喚醒受測系統，並重複輸入數次錯誤的解鎖資料。

(4) 檢查是否可以步驟(3)是否顯示強制鎖定的訊息。

(f) 判定標準：

(1) 步驟(4)中，可以步驟(3)，受測系統有顯示強制鎖定的訊息。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.2.2 手機系統應提供使用者輸入高複雜度通行碼輸入值。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.2.2。

(b) 測試目的：

驗證手機系統通行碼強度鑑別機制，防止手機遭到暴力破解。

(c) 檢測條件：

(1) 資料型別：無。

(2) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 開啟受測系統輸入通行碼設定介面。

(2) 檢查受測系統提供之通行碼輸入值，是否包含英文大寫、英文小寫、數字及特殊符號。

(3) 檢查通行碼長度是否至少 6 碼以上。

(f) 判定標準：

(1) 步驟(2)中，受測系統提供之通行碼輸入值有包含英文大寫、英文小寫、數字及特殊符號。

(2) 步驟(3)中，通行碼至少 6 碼以上。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.3.2.3 手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.2.3。

(b) 測試目的：

驗證手機系統是否將螢幕鎖定解鎖資料以明文方式儲存於手機，防止遭未經授權的使用。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限。

(2) 螢幕鎖定功能：圖形、通行碼及生物特徵。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。

(3) 以管理者權限身分確認解鎖資料是否以明文方式儲存於手機上；若未能提供管理者權限者，得提供足以證明符合本測試項目之詳細說明、畫面及截圖等佐證資料，必要時檢測實驗室得要求申請者做功能示範。

(f) 判定標準：

(1) 步驟(4)中，未以明文方式將螢幕鎖定解鎖資料儲存於手機上。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.2.4 手機系統之金鑰、螢幕鎖定解鎖資料應存放於信任執行環境並加密。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.2.4。

(b) 測試目的：

驗證手機系統是否將金鑰、螢幕鎖定通行碼、指紋等生物特徵資料加密存放於信任執行環境(Trusted Execution Environment，TEE)，防止金鑰或螢幕鎖定解鎖資料等因不安全儲存而被不當應用。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限。
(2) 螢幕鎖定功能：圖形、通行碼、指紋、臉部等解鎖資料。
(3) 資料型別：無。
(4) 受測軟體屬性：無。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。
(2) 開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。
(3) 以管理者權限身分確認金鑰或螢幕解鎖資料是否並加密儲存於手機上信任執行環境(Trusted Execution Environment，TEE; 如 Apple 的 Secure Enclave 或 Android 的 KeyStore)；若未能提供管理者權限者，得提供足以證明符合本測試項目之詳細說明、畫面及截圖等佐證資料，必要時檢測實驗室得要求申請者做功能示範。

(f) 判定標準：

(1) 於步驟(3)或(2)中，受測系統將金鑰、螢幕鎖定解鎖資料應並加密存放於信任執行環境。
(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.3 系統執行安全測試

5.3.3.1 手機系統應提供回報安全性問題之管道。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.3.1。

(b) 測試目的：

驗證手機系統應提供安全性問題回報管道，確保可以傳達系統安全性問題。

(c) 檢測條件：

(1) 資料型別：無。

(2) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

檢查受測系統、官方網站或使用說明書是否提供問題回報管道，並且可以實際聯絡成功。

(f) 判定標準：

(1) 受測系統發現的問題可透過問題回報管道回報，並可實際聯絡成功。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.3.2 手機系統應具備記憶體配置保護機制。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.3.2。

(b) 測試目的：

驗證手機系統是否具備記憶體配置保護機制，防止程式與參考函式在記憶體中的位址被不當應用。

(c) 檢測條件：

(1) 申請者須填寫「附錄 E 安全功能規格表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

見圖 2。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測系統具備記憶體配置保護機制。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.3.3 手機系統應建立與通訊目標間受信任的傳輸通道。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.3.3。

(b) 測試目的：

驗證手機系統應建立受信任的傳輸通道，確保傳輸期間資料保護使用。

(c) 檢測條件：

(1) 申請者須填寫「附錄 E 安全功能規格表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

圖 5。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測系統之傳輸過程具備安全通道，安全通道應使用附錄 A 所列之通行碼套件。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.3.4 手機開機過程應提供通行碼功能測試與系統軟體完整性自我測試機制。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.3.4。

(b) 測試目的：

驗證手機開機過程應提供通行碼功能測試與系統軟體完整性測試，防止手機系統遭竄改或破解。

(c) 檢測條件：

(1) 申請者須填寫「附錄 E 安全功能規格表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測系統之開機過程具備自我安全功能測試。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.3.5 手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.3.5。

(b) 測試目的：

驗證手機系統應具備錯誤計數機制與抹除受保護之資訊，防止手機遭到暴力破解。

(c) 檢測條件：

(1) 申請者須填寫「附錄 E 安全功能規格表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測系統之認證失敗處理方式符合資料覆蓋方式，可安全抹除受保護之資料。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.3.4 eSIM 傳輸保護測試

5.3.4.1 手機系統 eSIM 透過遠端系統進行配置及管理，應使用 TLS v1.2(含)以上版本建立加密通道與使用安全之加密演算法進行加密傳輸 eSIM 設定檔。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.4.1。

(b) 測試目的：

驗證手機系統 eSIM 透過遠端系統進行配置及管理應使用加密傳輸，防止攻擊者替換 eSIM 設定檔。

(c) 檢測條件：

(1) 手機支援 eSIM 技術。

(2) 軟體支援之無線傳輸 eSIM 設定檔：WLAN 及行動通訊網路。

(3) 資料型別：第 1 型資料(eSIM 設定檔)。

(4) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

見圖 3。

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 執行手機 eSIM 行動服務，並以無線傳輸技術功能傳輸 eSIM 設定檔。

(3) 檢查受測系統是否以 TLS v1.2(含)以上版本進行加密傳輸 eSIM 設定檔。

(4) 檢查受測系統所存取之伺服器，其使用之加密演算法是否為國際公認的加密演算法。

(f) 判定標準：

(1) 步驟(3)中，受測系統以 TLS V1.2(含)以上版本進行加密傳輸 eSIM 設定檔。

(2) 步驟(4)中，受測系統與伺服器端之通訊加密演算法為國際公認的加密演算法(參考 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10))。

(3) 若符合判定標準，則本檢測項目「符合」。

(4) 若不符合判定標準，則本檢測項目「不符合」。

5.3.4.2 手機系統儲存 eSIM 設定檔時應提供加密功能，以避免遭不正當方式取得 eSIM 設定檔所儲存之敏感性資料。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.3.4.2。

(b) 測試目的：

驗證手機系統應具備 eSIM 設定檔保護機制，防止攻擊者取得設定檔中敏感性資料。

(c) 檢測條件：

(1) 手機支援 eSIM 技術。

(2) 應用程式支援 eSIM 設定檔管理。

(3) 資料型別：第 1 型資料(eSIM 設定檔)。

(4) 受測軟體屬性：出廠內建軟體。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 確認受測系統已符合檢測條件。

(2) 執行手機 eSIM 行動服務，並以無線傳輸技術功能傳輸 eSIM 設定檔，並取得電信服務。

(3) 檢查手機內儲存 eSIM 設定檔是否以明文方式儲存敏感性資料。

(f) 判定標準：

(1) 於步驟(3)中，手機內儲存 eSIM 設定檔未以明文方式儲存敏感性資料。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4 硬體層安全測試

5.4.1 實體安全測試

5.4.1.1 手機系統連接實體介面傳輸資料前，應取得使用者同意。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.1.1。

(b) 測試目的：

驗證手機系統連接實體介面應取得使用者同意，防止手機遭植入惡意程式。

(c) 檢測條件：

(1) 手機支援 USB、HDMI 或其他實體線連結傳輸資料。

(2) 資料型別：無。

(3) 受測軟體屬性：無。

(d) 測試佈局：

見圖 7。

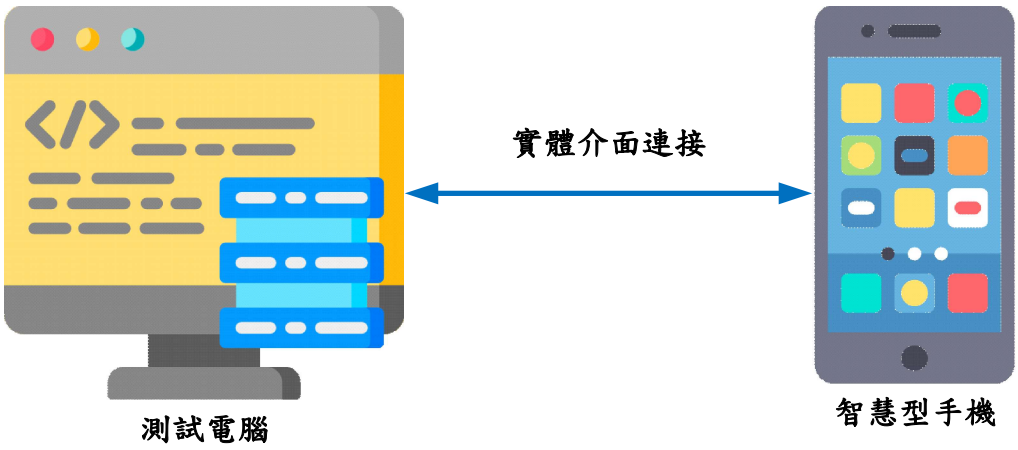

圖 7 測試示意圖

(e) 測試方法：

(1) 將手機以 USB、HDMI 或其他實體線連結測試電腦。

(2) 檢查手機是否取得使用者同意存取檔案。

(f) 判定標準：

(1) 於步驟(2)中，將手機以 USB、HDMI 或其他實體線連結測試電腦，手機詢問使用者是否同意電腦存取檔案。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.2 金鑰管理保護測試

5.4.2.1 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合國際標準組織所公布具安全性之金鑰使用及管理標準。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.2.1。

(b) 測試目的：

手機之金鑰管理應符合國際標準組織所公布具安全性之金鑰使用及管理標準，防止攻擊者可能輕易破解。

(c) 檢測條件：

(1) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測硬體之金鑰儲存保護機密性與完整性之要求，擇一符合所列金鑰使用及管理標準。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.2.2 儲存於手機之金鑰，都應對其機密性與完整性提供額外保護。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.2.2。

(b) 測試目的：

驗證儲存於手機之金鑰應提供機密性與完整性提供額外保護，防止遭到攻擊者利用或修改檔案。

(c) 檢測條件：

(1) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(2) 必要時請廠商進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測硬體之金鑰儲存保護機密性與完整性之要求。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.2.3 金鑰不得以明文方式存放於記憶體。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.2.3。

(b) 測試目的：

驗證手機系統金鑰不應以明文方式存放於記憶體，防止以明文型態對外傳輸。

(c) 檢測條件：

(1) 申請者須提供智慧型手機管理者權限。

(2) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(3) 必要時請申請者進行功能示範。

(4) 資料型別：無。

(5) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(2)中，受測硬體之金鑰傳輸保護符合不匯出或傳輸之要求。金鑰若需以加密方式匯出或傳輸，加密之強度須為原演算法金鑰強度等級(含)以上。加密強度參考 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)所列之資料。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.3 演算法強度要求測試

5.4.3.1 手機實作之加密、解密及簽章演算法，應符合國際標準組織所公布具安全性之金鑰演算法標準。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.3.1。

(b) 測試目的：

驗證手機系統實作之加密、解密及簽章演算法應符合金鑰演算法標準，防止攻擊者輕易破解。

(c) 檢測條件：

(1) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 相關標準參考 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)。

(3) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(3)中，受測硬體之演算法符合技術要求，擇一符合所列之金鑰演算法標準。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.3.2 手機實作之演算法，應依據各模式要求，產生啟始向量，並應符合國際標準組織所發布之啟始向量要求。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.3.2。

(b) 測試目的：

驗證手機系統實作之演算法應依據各模式要求產生啟始向量，防止攻擊者輕易破解。

(c) 檢測條件：

(1) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 相關標準參考 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)。

(3) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(3)中，受測硬體之啟始向量符合技術要求，擇一符合所列之初始化向量標準。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

5.4.3.3 金鑰使用之隨機數，應符合國際標準組織所公布具安全性之隨機位元產生規範要求。

(a) 測試依據：

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」之 5.4.3.3。

(b) 測試目的：

驗證手機系統金鑰使用之隨機數，應符合國際標準組織所公布具安全性之隨機位元產生規範要求，防止攻擊者輕易破解亂數。

(c) 檢測條件：

(1) 申請者須填寫「附錄 F 設計安全性表」與「附錄 G 安全架構表」作為審查依據。

(2) 必要時請申請者進行功能示範。

(3) 資料型別：無。

(4) 受測軟體屬性：無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 依書面資料審查是否具備此功能。

(2) 相關標準所參考 FIPS 140-2 Annex A 或最新版本核准之加密編譯演算法(10)。

(3) 當無充分資料顯示具備此功能時，則請申請者做功能示範。

(f) 判定標準：

(1) 於步驟(1)或(3)中，受測硬體之隨機數符合技術要求，擇一符合所列之隨機位元產生規範。

(2) 若符合判定標準，則本檢測項目「符合」。

(3) 若不符合判定標準，則本檢測項目「不符合」。

附錄 A
(規定)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
  - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
  - - TLS_AES_128_GCM_SHA256
  - - TLS_AES_256_GCM_SHA384
  - - TLS_CHACHA20_POLY1305_SHA256
  - - TLS_AES_128_CCM_SHA256
  - - TLS_AES_128_CCM_8_SHA256

附錄 B(規定)
智慧型手機系統內建軟體資安檢測申請書

申請日期： 年 月 日

<table>
<tr><td>申請者
(公司、商號名稱)</td><td colspan="2">☐製造商 ☐電信業者
☐我國代理商</td><td colspan="2">○○○股份有限公司</td><td rowspan="5">申請者用印
(大、小章)</td></tr>
<tr><td>統一編號</td><td colspan="4"></td></tr>
<tr><td>營業所地址</td><td colspan="4">☐☐☐-☐☐</td></tr>
<tr><td>代表人姓名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">聯絡人</td><td>姓名及職稱</td><td></td><td>電子信箱</td><td></td></tr>
<tr><td>聯絡電話</td><td></td><td>傳真機</td><td></td></tr>
<tr><td>製造商及地址</td><td colspan="5">○○○股份有限公司
☐☐☐-☐☐</td></tr>
<tr><td colspan="2">智慧型手機之廠牌/型號/名稱</td><td colspan="4">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="2">智慧型手機申請檢測之作業系統版本</td><td colspan="4">○○○手機申請檢測之作</td></tr>
<tr><td colspan="2">申請檢測安全等級</td><td colspan="4">☐1 級 ☐2 級 ☐2 級(含選擇檢測項目) ☐3 級 ☐3 級(含選擇檢測項目)</td></tr>
<tr><td rowspan="5">智慧型手機具備功能資訊</td><td>定位功能</td><td colspan="4">☐ 美國全球定位系統 GPS ☐ 歐盟伽利略 Galileo
☐ 俄羅斯格洛納斯 GLONASS ☐ 其他，_____
☐ 中國北斗衛星導航(☐可雙向傳輸)</td></tr>
<tr><td>無線傳輸技術</td><td colspan="4">☐ 藍牙 ☐行動通訊網路 (☐2G ☐3G ☐4G)
☐ WLAN ☐其他，_____
☐ NFC (☐ Peer-to-Peer Mode ☐ Read/Write Mode)</td></tr>
<tr><td>生物辨識</td><td colspan="4">☐ 無 ☐ 有，指紋辨識、…</td></tr>
<tr><td>外接記憶體</td><td colspan="4">☐ 無 ☐ 有，microSD card、…</td></tr>
<tr><td rowspan="3">檢附智慧型手機樣品數量</td><td>1 級</td><td colspan="4">☐ 受測樣品 2 支</td></tr>
<tr><td>2 級</td><td colspan="4">☐ 受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td>3 級</td><td colspan="4">☐ 受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td colspan="2">檢附文件
(正本或影本)</td><td colspan="4">☐1.中文或英文之使用手冊或說明書
☐2.中文或英文之規格資料
☐3.公司登記證明文件或商業登記證明文件；申請者為外國製造商者，應檢附該製造商之設立相關證明文件
☐4.廠商自我宣告表、內建軟體摘要表
☐5.安全功能規格表、設計安全性表及安全架構表(申請高級者須檢附)
☐6.光碟片乙份(含檢測申請書及第 1 項至第 5 項內容)
☐7.通過相關標準認證之證明文件</td></tr>
<tr><td colspan="6">[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、智慧型手機樣品及其餘文件於出具檢測報告時一併發還申請者。</td></tr>
<tr><td rowspan="4">檢測實驗室(由實驗室填寫)</td><td colspan="4">檢測實驗室名稱：</td><td rowspan="4">檢測實驗室用印</td></tr>
<tr><td colspan="4">出具檢測報告乙份：
1.檢測報告編號：_____
2.安全等級：☐1 級 ☐2 級 ☐3 級</td></tr>
<tr><td>受理日期</td><td></td><td>完成日期</td><td></td></tr>
<tr><td>聯絡人</td><td></td><td>聯絡電話</td><td></td></tr>
</table>

附錄 C
(規定)
廠商自我宣告表-1

受測軟體基本資訊					作業系統層	
項次	受測軟體名稱	發行商及版本	受測套件名稱	受測軟體名稱	是否支援嵌入式 SIM 卡(ESIM)	是否支援雲端備份
1	電話	company 1.2.2	com. android. phone	☐出廠內建軟體 ☐無圖示軟體	☐否 ☐是 eSIM 的 package name 與 eSIM 存取路徑：___	☐否 ☐是

附錄 D(規定)
廠商自我宣告表-2

項次	1		
受測軟體基本資訊	受測軟體名稱	是否存取敏感性資料	□否 □第 1 型 □第 2 型
		是否具帳戶驗證登入機制	□否 □是 帳號/通行碼類型：____ □是否自動存取帳號 使用綁定帳號 APP 範圍____
		是否支援無線傳輸技術	□否 □Wifi □GPS(定位服務)□ 藍牙 □行動網路 □NFC □紅外線
		功能說明	□常駐軟體 □非常駐軟體 說明： 可從通訊錄中撥打電話。
		權限說明	READ_CONTACTS：用於訊息分享功能 ACCOUNT_MANAGER：用於新增帳號到社群 CAMERA：用於圖片紀錄功能 INTERNET：用於連線主機，取得最新公告
		資料連結伺服器之 IP/DN/公司名稱及伺服器類型	apPchat. example.net：一般主機 111.112. 113.114：付費功能主機
		是否開啟網路埠	□否 □是，埠號：____
		是否將敏感性資料儲存於非作業系統保護區	□否 □是，加密方法：____
		是否具帳戶具備付費功能	□否 □是 多因子認證方法：____

[註] 伺服器類型包含一般主機及付費功能主機。

附錄 E
(規定)
安全功能規格表

安全功能介面名稱 TSFI	目的 Purpose	安全功能介面可實現之安全功能需求 SFR	操作方式 Method of Use	參數 Parameter	執行動作 Actions	錯誤訊息 Error Message
列出所有安全功能介面。	說明各安全功能介面之安全功能目的。	說明各安全功能介面如何實現附檢測項目之第三級所列之安全功能需求。	說明如何使用各安全功能介面。	說明各安全功能介面所有參數及其意義。	說明各安全功能介面如何運作及其執行細節。	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。
範例：TSFI_CLI	*範例：提供命令列模式操作介面*	*範例：SFR_安全管理：提供安全管理功能*	*範例：以 ssh 連接待測物，即提供命令列模式操作介面*	*範例：ID & password*	*範例：可下達管理命令操作待測物*	*範例：連接失敗認證失敗*

附錄 F
(規定)
設計安全性表

子系統名稱 Subsystem	目的 Purpose	子系統隸屬之安全功能介面 TSFI	子系統行為說明 Behavior Description
列出各安全功能介面之子系統。	說明各子系統之安全功能目的。	說明各子系統隸屬於附件 3 所列之安全功能介面。	說明各子系統行為如下： (1) 如何實現安全功能介面的功能。 (2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。
範例： *Subsystem_ssh*	*範例：* *提供 ssh 服務*	*範例：* *TSFI_CLI*	*範例：* *(1) 提供 TSFI_CLI 命令列模式操作介面* *(2) 與其他子系統之互動：* *(A) Subsystem_auth: 傳遞認證資訊給 Subsystem_auth，並由回覆訊息確認認證是否成功* *(B) Subsystem_terminal: ...*

附錄 G
(規定)
安全架構表

項目	說明	
1.安全領域 Security Domain	**安全領域名稱**	**安全領域說明**
	列出各安全功能介面對應之安全領域 *範例：* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：* *透過 TSFI_GUI 來執行管理功能石，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*
2.初始程序 Secure Initialization	**相關元件**	**初始程序說明**
	操作待測物的相關元件/環境 *範例：* *待測物網路連接程序*	提供安全啟動待測物之相關元件啟始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/ 0(ethernet0 / 0 接口)連接一個 RJ- 45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/ 1(ethernet0 / 1 接口)連接一個 RJ- 45 電纜到交換機或路由器中的 DMZ 安全區。*

項目	說明		
	自我保護功能	**與外部設備之關係**	**自我保護機制說明**
3.自我保護 Self-Protection	列出各安全功能介面對應之自我保護機制 *範例：* *TSFI_WEB:* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密*	說明安全功能及其介面與外部設備之資料交換動作 *範例：* *遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	需說明安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *1. 應輸入通行碼才能進入介面。* *2. 資料傳輸機制：TLS/SSL。* *3. 特殊執行方式：指紋辨識。* *4. 特殊設備需求：指紋辨識器。*

項目	說明	
4.防止繞道 Non-Bypassibility	**防止繞道功能**	**防止繞道機制說明**
	列出各安全功能對應之防止繞道機制 *範例：* *TSF_Authentication 身分驗證功能*	1. 列舉可能繞道之手法 2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：* *可能直接以維護介面不經身分認證操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。*

參考資料

(1) Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, 2017.
(2) CNS9359-7 資訊技術－詞彙－第 7 部：電腦程式設計,CNS 2011.
(3) 管理 Activity 生命週期 https://developer.android.com/guide/components/activities?hl=zh-tw#Lifecycle
(4) Department of Homeland Security (DHS), Study on Mobile Device Security：2017
(5) OWASP SQL Injection 說明 https://owasp.org/www-community/attacks/SQL_Injection
(6) OWASP Format String Attack 說明 https://owasp.org/www-community/attacks/Format_string_attack
(7) OWASP Command Injection 說明 https://owasp.org/www-community/attacks/Command_Injection
(8) 台灣資通產業標準協會 TAICS TS-0015-1v1.0-影像監控系統資安標準測試規範-第一部_一般要求：2018
(9) OWASP, Mobile Security Project – Top Ten Mobile Risks：2016

版本修改紀錄

版本	時間	摘要
v1.0	2020/07/10	出版
v1.1	2021/01/28	出版

勘誤表

項目	頁碼	修訂前	修訂後
1	p.9	表 1 資料型別分類表中，第一型項目的“範例”欄位： (空白)	表 1 資料型別分類表”中，第一型項目的“範例”欄位： 1.本標準第三節”用語及定義”之 3.10 個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置通行碼、帳號通行碼、金鑰、相片、生物特徵識別資料。
2	p.60	附錄 B(規定) “智慧型手機系統內建軟體資安檢測申請書”中，“申請檢測安全等級”欄位的內容： ☐初級 ☐中級 ☐中級(含選擇檢測項目) ☐高級 ☐高級(含選擇檢測項目)	附錄 B(規定) “智慧型手機系統內建軟體資安檢測申請書”中，“申請檢測安全等級”欄位的內容： ☐1 級 ☐2 級 ☐2 級(含選擇檢測項目) ☐3 級 ☐3 級(含選擇檢測項目)
3	p.60	附錄 B(規定) “智慧型手機系統內建軟體資安檢測申請書”中，“檢測實驗室(由實驗室填寫)”欄位的內容： ☐1 級 ☐2 級 ☐2 級	附錄 B(規定) “智慧型手機系統內建軟體資安檢測申請書”中，“檢測實驗室(由實驗室填寫)”欄位的內容： ☐1 級 ☐2 級 ☐3 級

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