TAICS

TAICS TS-0029 v1.0 : 2020

智慧型手機系統內建軟體資安標準

Infocom security standard of embedded software on smartphone systems

2020/07/10

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標準

Infocom security standard of embedded software on smartphone systems

出版日期: 2020/07/10
終審日期: 2020/06/08

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

本標準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：財團法人資訊工業策進會 毛敬豪 所長

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

TC 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

此標準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、財團法人台灣電子檢驗中心、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。

本標準由國家通訊傳播委員會支持研究制定。

目錄

前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準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。

本標準之部分內容，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

智慧型手機軟、硬體技術一日千里，便利民眾日常生活的應用服務愈趨多元化；然而，其便利性也潛藏不同資安風險。自 2014 年起手機資安事件日益頻繁，如 2014 年國際知名資安公司分析某款中國手機，發現未經使用者同意傳送個資至中國伺服器；又如 2018 年外國資安團隊於 DEFCON 26 會議上發表 25 款 Android 手機，其出廠的韌體或預設程式含有安全漏洞，讓駭客取得裝置最高權限，進而執行任意程式、取得數據與程式系統日誌、移除使用者資料、讀取或變更裝置組態等。其中，由於手機系統內建軟體無法被刪除、停用，且防毒軟體並不會標記為有害軟體，並能以無圖示方式保持隱藏，往往讓人忽略其潛藏的資安風險。

國家通訊傳播委員會(National Communications Commission, NCC)為確保消費者智慧型手機出廠之安全性，於 2017 年 3 月公告「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 設定檔與未經授權存取行動網路；為此 NCC 於 2019 年 7 月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)、防護注入攻擊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標準制定平台進行產業標準制定。

TAICS TS-0029 v1.0「智慧型手機系統內建軟體資安標準」(以下簡稱本標準)基於「智慧型手機系統內建軟體資通安全檢測技術規範」[1] ，並參照國際智慧型手機相關資安標準、規範或指引，包括 Smartphone Secure Development Guidelines[2] 、Mobile Security Testing Guide[3] 與 GSMA SGP.25 [4] 等，區分(1)應用程式層、(2)通訊協定層、(3)作業系統層及(4)硬體層四項安全構面，以規範智慧型手機應採取的共通方法，俾利手機製造商、軟體開發商及檢測實驗室等做為手機系統內建軟體檢測參考藍本。

1. 適用範圍

本標準規定智慧型手機系統內建軟體之資訊安全要求，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，則不在本標準之範圍。適用範圍如圖 1 所示。

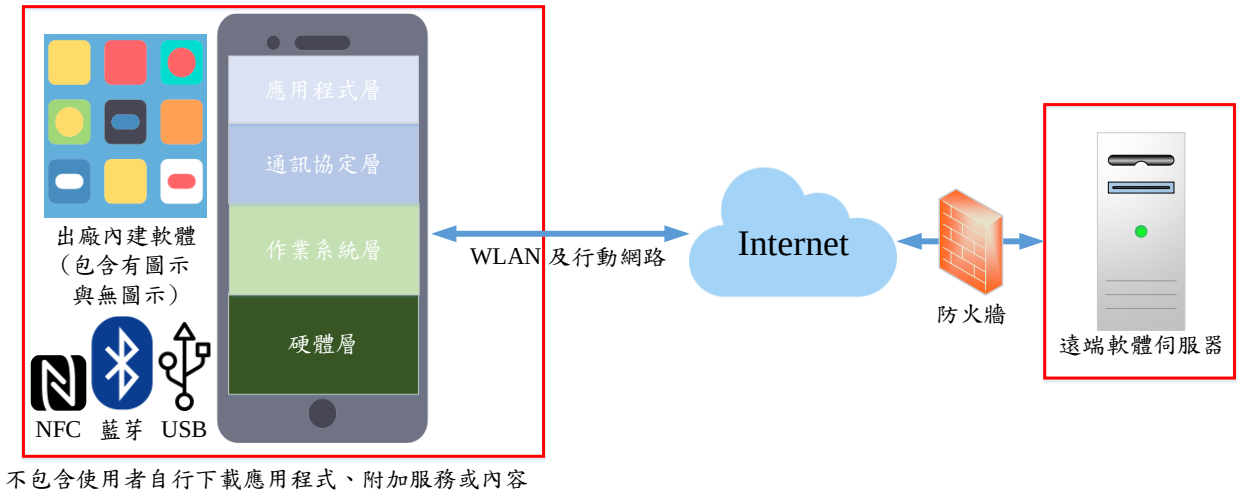

圖 1 適用範圍示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。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] 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: 2018

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

3. 用語及定義

下列用語及定義適用於本標準。

3.1 加密(Encryption)

指明文資訊透過數學演算法進行改變，使原來的資料不可讀而達到保密的目的。

3.2 嵌入式 SIM 卡(Embedded SIM, eSIM)

指基於嵌入式通用積體電路卡(Embedded UICC, eUICC)，UICC 嵌入設備中不容易移除或更換，並且可以安全地更改 eSIM 設定檔(Profile)(7)。

3.3 通用積體電路卡(Universal Integrated Circuit Card，UICC)

指符合 ETSI 智慧卡平台專案編寫和維護的規範的智慧卡(8)。

3.4 eSIM 設定檔(Profile)

指採用嵌入式通用積體電路卡(Embedded UICC, eUICC)中的解決方案，透過 OTA(Over-the-air)遠端下載電信門號設定檔。

3.5 通訊埠(Port)

通訊埠，又稱為網路埠或者連接埠，內建軟體因服務需求開啟，作為連網裝置與外部來源之間傳送/接收通訊資料。

3.6 交談識別碼(Session Identification, Session ID)

指在建立連接時，指派給每個使用者連接的唯一工作階段識別碼。當連接結束時，即釋出該識別碼，讓伺服器重新指派給新的使用者連接。

3.7 近場通訊(Near Field Communication, NFC)

指一種近距離(通常小於 10 公分)的無線通訊技術，主要運作頻率是 13.56 MHz，資料傳輸速度每秒最高可達 424 Kbps。NFC 包含三種模式，分別為點對點模式(Peer-to-Peer Mode)、讀寫模式(Read/Write Mode)及卡片模擬模式(Card Emulation Mode)，其中卡片模擬模式可模擬多種實體卡片功能，如信用卡、悠遊卡等，當近場通訊技術使用卡片模擬模式時，可在無電力供應情況下使用。

3.8 可延伸標記語言外部實體攻擊(XML External Entity Attack)

指一種網路攻擊手法，XML 格式的檔案常用來作為應用程式的輸入和輸出，當應用程式以XML格式作為執行作業的輸入時，攻擊者可能透過變更XML格式的結構或資料，以此來竄改重要檔案或資料之內容，達到入侵目的(10)。

3.9 重送攻擊(Replay Attack)

指一種網路攻擊手法，透過惡意重複或拖延正常的資料傳輸而實施。

3.10 個人資料(Personal Data)

指包含自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料(11)。

3.11 敏感性資料(Sensitive Data)

指洩漏時可能對使用者造成損害之資料，包括但不限於個人資料、通行碼、金鑰或地理位置等。此等資料依使用者行為或行動應用程式之運作，於裝置及其附屬儲存媒體建立、儲存或傳輸。

3.12 通行碼(Password)

指一組字元串，能使系統辨識用戶身分，並進一步控管用戶存取系統之權限。

3.13 使用者協議(User Agreement)

指系統透過訊息提示方式提供使用者選擇「同意」或「不同意」的機制。由使用者主動操作之行為和系統透過使用者同意機制取得使用者同意之情況。

3.14 資訊安全弱點(Security Vulnerability)

指裝置安全之缺陷，使得系統、應用程式或資料機密性、完整性及可用性面臨威脅。

3.15 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。

3.16 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。

3.17 漏洞評鑑系統(Common Vulnerability Scoring System, CVSS)

指一套漏洞評鑑系統的判定標準，包括威脅所造成損害的嚴重性、資安脆弱性的可利用程度與攻擊者不當運用該脆弱性的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險(2)。

3.18 無線傳輸技術(Wireless Transmission Technology)

指透過無線通訊標準的連接，讓智慧型手機透過網路或點對點等連線方式來傳輸資料，手機使用的無線傳輸技術如藍牙、WLAN、NFC、行動通訊網路、定位服務、紅外線及無線充電等。

3.19 無線區域網路(Wireless Local Area Network, WLAN)

指透過無線電波、雷射光或紅外線作為傳輸資料的媒介與網路連線，其功能與有線區域網路相同。

3.20 無圖示軟體(Iconless Software)

指智慧型手機出廠時已預設安裝之應用程式，使用者無法透過圖示啟動，且該軟體會啟動通訊功能。

3.21 內建軟體(Embedded Software)

指手機製造商於出廠時安裝在手機上的軟體，包含系統內之圖示與無圖示軟體。

3.22 作業系統保護區(Operating System Protection Area)

指使用者透過外部裝置連接手機，在管理者權限下可存取之空間，包含手機本身儲存空間和出廠時提供的外接記憶卡。

3.23 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。RFC 5246(1)，在瀏覽器、電子郵件、即時通訊、VoIP、網路傳真等應用程式中，廣泛支援這個協定。

3.24 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(12)。

3.25 啟始向量(Initialization Vector, IV)

指資料序列在加密過程的啟始點之值，可經由所導入之加密變化來增加安全性，且可同步加密設備。

3.26 金鑰(Key)

指為了驗證、鑑別、加密或解密的目的，而和演算法結合使用的參數。

3.27 金鑰管理(Key Management)

指遵循安全政策來管理並使用建立金鑰資料之產生、註冊、驗證(Certification)、解除註冊(Deregistration)、分配、安裝、儲存、歸檔(Archive)、廢止(Revocation)、推衍(Derivation)及破壞(Destruction)(12)。

3.28 機密性(Confidentiality)

指資訊不提供或不揭露予未獲授權之個人、實體或過程的性質(11)。

3.29 完整性(Integrity)

指資料不會被未經授權改變或破壞的特性(11)。

3.30 時變參數(Time Variant Parameter)

指個體用以查證訊息非重演所使用之資料項目，例如：隨機數、序號或時戳(13)。

3.31 隨機數(Random Number)

指無法預測其值之時變參數(Time Variant Parameter)(13)。

3.32 安全等級(Security Level)

指因應產品面臨不同程度之資安威脅，針對產品所需的安全功能要求提供不同強度之分級。

3.33 信任執行環境(Trusted Execution Environment, TEE)

指信任一個安全的操作系統(OS)，透過硬體、軟體與作業系統隔離，可提供受信任的執行環境(TEE)。TEE 隔離可保護用戶敏感性資料避免遭受惡意應用程式或潛在漏洞影響(15)。

3.34 多因子驗證(Multi-Factor Authentication)

指使用者在登入過程中經提示而提供其他形式的識別程序，以增強應用程式與服務的安全性。

3.35 強驗證(Strong Authentication)

指使用者在登入過程中，要求使用者針對登入詢問輸入獨一無二的單次回應，或輸入由驗證伺服器提供的特殊代碼。例如：硬體或軟體 Token、公開金鑰驗證(PKI)、UAF、U2F、FIDO2 與 WebAuthn 等驗證機制。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。本標準安全等級 1、2、3 分別對應至「智慧型手機系統內建軟體資通安全檢測技術規範」[1] 安全等級初、中、高，同時擴增原技術規範之各安全等級之安全要求。

4.1 安全等級概述

安全等級總表，如表 1 所示，第一欄為安全構面，包括：(1) 應用程式層安全要求、(2)通訊協定層安全要求、(3)作業系統層安全要求、(4)硬體層安全要求；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。本安全等級總表各欄的關連性，須依循下節 6.1 至 6.4 之技術規範內容。

表 1 安全等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 應用程式層安全要求	5.1.1 程式資料使用授權	5.1.1.1	-	-
	5.1.2 程式資料儲存保護	5.1.2.1	5.1.2.2 5.1.2.3	-
	5.1.3 資料遺失保護	5.1.3.1	-	-
	5.1.4 程式身分辨識	5.1.4.1	-	5.1.4.2
	5.1.5 程式信任來源	5.1.5.1 5.1.5.2	-	-
	5.1.6 程式執行授權	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	5.1.7.1	5.1.7.2 5.1.7.3 5.1.7.4 5.1.7.5	5.1.7.6
	5.2.1 協定使用授權	5.2.1.1	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.2 通訊協定層安全要求	5.2.2 協定傳輸保護	5.2.2.1	5.2.2.2 5.2.2.3	-
	5.2.3 協定執行安全	-	5.2.3.1	-
5.3 作業系統層安全要求	5.3.1 系統操作授權	5.3.1.1 5.3.1.2	-	-
	5.3.2 系統身分辨識	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	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	5.3.4.1	5.3.4.2	-
5.4 硬體層安全要求	5.4.1 實體安全	5.4.1.1	-	-
	5.4.2 金鑰管理保護	-	-	5.4.2.1 5.4.2.2 5.4.2.3
	5.4.3 演算法強度要求		-	5.4.3.1 5.4.3.2 5.4.3.3

4.1.1 安全構面

(a) 應用程式層(APPs)安全要求：包含資料儲存或使用等相關安全，並應確保使用者個人資料免遭系統內建軟體未經授權之蒐集、分享、使用、刪除、竄改及儲存，內建軟體信任來源、執行授權等相關安全，並應防止系統內建軟體未經授權存取系統資源。

(b) 通訊協定層(Protocol)安全要求：包含無線傳輸技術及通訊協定等相關安全，並應確保使用者對資料之傳輸、周邊設備之連接的可控管性。

(c) 作業系統層(Operating System)安全要求：包含作業系統相關服務與身分辨識等相關安全，並應確保作業系統對系統資源之保護、提醒，同時讓使用者於知情的狀況下進行更新。

(d) 硬體層(Hardware)安全要求：包含金鑰與演算法模組等安全，並應確保金鑰管理、存放之保護，及演算法之安全強度符合國際規範，同時讓使用者於知情的狀況下進行更新。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個以上之安全要求。

4.1.3 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。其對應之列即其所應符合的安全要求分項，安全等級越高代表安全性越佳，如表 2 安全等級之要求及說明。

表 2 安全等級之要求及說明

安全等級	說明
第 1 級	為智慧型手機基本隱私保護之最低要求，針對內建軟體資料的保護儲存方式、通訊傳輸時設定的加密機制、手機系統功能與內建軟體權限檢查，讓使用者在安全的環境下防止資料洩漏。
第 2 級	除須符合第 1 級之所有安全要求外，並增加資料進階保護之安全要求，防止內建軟體私下傳送資料，或內建軟體被惡意攻擊導致無法使用或資料外洩。
第 3 級	為確保智慧型手機之核心底層不被竄改或不正當地擷取資訊，除須符合第 1 級與第 2 級之所有安全要求外，並增加手機設計相關安全文件審查之安全要求、檢測信任執行環境、應用程式具備手機完整性判斷機制與付費功能多因子或強驗證。

5. 標準規範

本節詳盡載明智慧型手機應用程式、通訊協定、作業系統與硬體為滿足系統內建軟體安全功能應採取的共通方法，所有智慧型手機應符合本節中所有安全要求。

5.1 應用程式層安全要求

5.1.1 程式資料使用授權

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。

5.1.2 程式資料儲存保護

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。

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。

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。

5.1.3 資料遺失保護

5.1.3.1 手機系統應提供資料保護與備份功能。

5.1.4 程式身分辨識

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。

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。

5.1.5 程式信任來源

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。

5.1.5.2 內建軟體應可識別其發行資訊。

5.1.6 程式執行授權

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。

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

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「通訊埠」相符。

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。

5.1.7 程式執行安全

5.1.7.1 內建軟體應提供回報安全性問題之管道。

5.1.7.2 內建軟體是否具備防護注入攻擊之設計。

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。

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。

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。

5.1.7.6 內建軟體是否具備完整性確保判斷機制。

5.2 通訊協定層安全要求

5.2.1 協定使用授權

5.2.1.1 手機系統應預設關閉近場通訊功能。

5.2.2 協定傳輸保護

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。

5.2.2.2 內建軟體應避免交談識別碼遭重送攻擊。

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。

5.2.3 協定執行安全

5.2.3.1 手機系統應具備通訊協定內容的錯誤處理能力。

5.3 作業系統層安全要求

5.3.1 系統操作授權

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。

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。

5.3.2 系統身分辨識

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。

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。

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。

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。

5.3.3 系統執行安全

5.3.3.1 手機系統應提供回報安全性問題之管道。

5.3.3.2 手機系統應具備記憶體配置保護機制。

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。

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。

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。

5.3.4 eSIM 傳輸保護

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)版本以上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。

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。

5.4 硬體層安全要求

5.4.1 實體安全

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。

5.4.2 金鑰管理保護

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。

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。

5.4.2.3 金鑰不得以明文方式存放於記憶體。

5.4.3 演算法強度要求

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。

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。

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。

附錄 A
(參考)
標準規範要求事項與各標準規範對照表

表 A.1 標準規範要求事項與各標準規範對照表

資安脆弱性	本標準要求事項	參考或對應標準規範
資料明文傳輸	5.2.2.1	● **NIST SP 800-163** ➢ 未加密通訊：當應用程式之間進行內部通訊，則將可能讓應用程式收集額外資訊，並注入惡意資訊。而當使用在對外通訊時 (Data network, Wi-Fi, Bluetooth, NFC, etc.) 則可能招致中間人攻擊之威脅。 ● **OWASP Mobile Top 10 Risk (2016)** ➢ M3：應用程式可應用 SSL / TLS 傳輸機敏資訊，網路會談層或其他敏感數據傳輸到後端 API 或Web 服務通道之加密保護。
資料明文儲存、不安全儲存位置	5.1.2.1	● **OWASP Mobile Top 10 Risk (2016)** ➢ M2:應避免使用 NSUserDefaults 的儲存敏感資訊，例如: 避免使用 NSManagedObject 所有資料將儲存在未加密的資料庫文件中。 ➢ M2:機密資訊的儲存或暫存有必要考慮使用一個標準的加密函式庫，如 CommonCrypto。但對於特殊敏感的資訊應用，則可考慮使用白箱加密，以避免數位簽名在通用加密函式庫中被找到而造成洩漏。 ➢ M2:Android 可用“setStorageEncryption”以強制加密本地端文件的儲存。而對於 SD 卡儲存某些安全函式可以透過javax.crypto 中的函式庫實現。 ● **NIST SP 800-164** ➢ 受保護的儲存裝置：保護儲存在設備上資料的機密性和完整性，並當使用中的資料發生未授權的應用程式試圖存取被保護的項目時，應撤銷其存取權限。

不安全文件權限、讀取敏感性資料	5.1.6.2 5.1.6.3 5.1.6.4	● **CVE-2019-15395** ➢ The Asus ZenFone 3s Max Android device with a build fingerprint of asus/IN_X00G/ASUS_X00G_1:7.0/NRD90M/IN_X00G-14.02.1807.33-20180706:user/release-keys contains a pre-installed app with a package name of com.asus.loguploaderproxy app (versionCode=1570000015, versionName=7.0.0.3_161222) that allows other pre-installed apps to perform command execution via an accessible app component. This capability can be accessed by any pre-installed app on the device which can obtain signatureOrSystem permissions that are required by other other pre-installed apps that exported their capabilities to other pre-installed app. ● **NIST SP 800-163** ➢ 啟用已獲得使用者授權功能：應用程式必須描述所有工作、按鈕，選項和其他介面連接所必需的作業並得到使用者確認。 ➢ 避免啟用未授權功能：權限可能透過隱式授予，使應用程式能在未經使用者同意的前提下，擅自使用相關功能。 ➢ 限制權限：應用程式應該只有最小的必要權限，且應避免與使用者授權聲明不一致。需要被加以考量應用程式所獲取權限的如下： ◆ File input/output (I/O) and removable storage ◆ Privileged commands ◆ APIs ● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **12. Protect the application from client side injections** Restrict what apps can cause an application component (e.g., Android Activity) to start or are able to interact with it (e.g., Android Service and Content Provider). This can be accomplished using strict permissions.
第三方程式庫漏洞	5.1.7.4	● **TAICS_TS0015-1_v1.0-影像監控系統資安標準測試規範-第一部_一般要求** ➢ 5.2.1.1 測試作業系統是否存在 CVSS v3 評分為 9.0 分以上之常見資安共同脆弱性及曝露
機密資料被寫入系統日誌	5.1.7.5	● **Department of Homeland Security (DHS), Study on**

		Mobile Device Security：2017 ➢ **Sensitive Information Written to System Log.** Applications for Android and iOS have been found that write sensitive information into plaintext log files that may be read by attackers. The instances that prompted inclusion in the Common Vulnerabilities and Exposures (CVE) database (CVE-2012-2630 and CVE-2014-0647) revealed Twitter credentials and Starbucks usernames, passwords, and e-mail account information. This threat has largely been mitigated in recent versions of Android and iOS that have stricter access controls to the system log.
USB 安裝惡意程式	5.4.1.1	● **Department of Homeland Security (DHS), Study on Mobile Device Security：2017** ➢ Physical-based attack vectors against mobile devices exist. Mobile devices use USB (or a similar communication channel such as Apple's Lightning) primarily for power charging, but the same interface enables data communication to and from a mobile device. If a mobile device is plugged in to a compromised or malicious PC or charging station the PC or charging station could potentially abuse the communication channel to attempt to exploit vulnerabilities on the mobile device or to steal sensitive data. Billy Lau et al. of Georgia Tech demonstrated a proof-ofconcept of this kind of attack against iOS devices in 2013125 and in March 2016 Palo Alto Networks reported on a family of malware they named "AceDeceiver" that attacks iOS devices from compromised Windows PCs.
設備備份	5.1.3.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **1. Identify and protect sensitive data on the mobile device** Exclude sensitive application files from device backups and cloud synchronization services. If this option is not available in the in use platform (e.g., Android), exclude the whole application from device backups. ● **OWASP Mobile Top 10 Risk (2016)** ➢ M6：理想情況下，行動裝置應用程式應使用能夠讓用戶自行撤銷已安裝特定於裝置之憑證，以確保可避免裝置被盜或遺失時，遭到未經授權的存取。 ● **Department of Homeland Security (DHS), Study on Mobile Device Security：2017**

		➢ **IV.5.2 Defenses** The most important action to defend against physical threats is to ensure that mobile devices always have a screen lock PIN or password. If there is not a screen lock, it is easy for an attacker to access the data or functionality of a lost or stolen mobile device. Enrolling devices into an EMM system provides an enterprise the ability to enforce use of a screen lock.
NFC	5.2.1.1	● **CVE-2019-2114** ➢ In the default privileges of NFC, there is a possible local bypass of user interaction requirements on package installation due to a default permission. This could lead to local escalation of privilege by installing an application with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-123700348
eSIM	5.3.4.1 5.3.4.2	● **GSMA SGP.25 Embedded UICC for Consumer Devices Protection Profile Version 1.0 05-June-2018** ➢ **1.3.2 High-level view of threats** eUICC cloning An off-card Actor may also try to use a legitimate Profile on an unauthorized eUICC, or on a simulator. The Protection Profile prevents cloning by guaranteeing the identity of the eUICC to an off-card Actor before a Profile can be downloaded, or during the usage of the eUICC. The objects used to prove the eUICC identity are controlled by the ECASD security domain. ➢ **1.3.2 High-level view of threats** Unauthorized access to the mobile network An Actor may try to leverage upon flaws of the network authentication algorithms to gain access to network authentication keys, in order to later authenticate in place of a legitimate Profile. ➢ **LPAd impersonation** Within the eUICC, the interfaces to connect to an LPAd are always present, even if the off-eUICC LPAd itself is not present. The attacker can exploit those interfaces to impersonate the LPAd (Man-in-the-middle, masquerade).
程式使用辨識	5.1.4.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ Mobile devices are often shared temporarily, lost or

		stolen. Mobile applications can be undermined by an insecure authentication or authorization control. Unauthorized individuals may obtain access to sensitive data or sensitive systems by circumventing authentication (logins) or by reusing valid tokens or cookies.
隨意讀取手機資料	5.1.1.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **3. Handle authentication and authorization factors securely on the device** User account credentials, if stolen, not only provide unauthorized access to the mobile backend service but potentially to other services and accounts owned by the user. Mobile applications need to designed to protect user credentials to protect the users as well as the application's backend infrastructure.
敏感性資料明文儲存於執行檔	5.1.2.3	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **5. Secure the backend services and the platform server and APIs** Carry out a specific check of your code for sensitive data unintentionally transferred between the mobile device and web-server back-ends and other external interfaces - (e.g., is location or other information transferred within file metadata).
不安全交易	5.1.5.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **8. Protect paid resources** Smartphone applications give programmatic access to paid resources on mobile phones such as phone calls, SMS, phone calls and SMS to premium numbers, roaming data, NFC payments, and third party payment systems. Applications that integrate those services must take particular care to prevent abuse. ➢ **4. Ensure sensitive data is protected in transit** Design the user interface in a way that warns the user if the peer certificate does not match the expected certificate and provide the ability to abort any further interaction.
不明應用程式	5.1.5.2	● **Department of Homeland Security (DHS), Study on Mobile Device Security：2017** ➢ **IV.2.1 Mobile Operating System** The application package management capabilities of mobile operating systems provide control over what applications can be installed on mobile devices. The

		mobile operating system ensures that applications and their updates are only installed from authorized sources (unless the device is configured otherwise).
交易授權	5.1.4.2 5.1.5.1 5.1.6.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **8. Protect paid resources** Authentication should not be used as a replacement of authorization security controls. Authorization verifies the permissions of a user and presupposes strong authentication. SMS and MMS should not be used to send sensitive data (e.g., two-factor authentication tokens) to or from mobile end-points as SMS and MMS can be intercepted. Check for anomalous usage patterns in paid-for resources usage and trigger re-authentication (e.g., when significant change in location, user-language changes, significant higher paid-for service usage). Follow the OS/device vendor guidelines for implementing In-App payment: ● Implement validation of payment receipts on the backend server not on the device. ● Pay specific attention when integrating payment acceptance from a third party wallet (wallet not integrated into the mobile OS).
應用程式背景執行	5.1.6.4	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **2. Implement user authentication, authorization and session management correctly** Clear any maintained sensitive data and attempt to also terminate any server side session after application state change (e.g., termination, backgrounding). Consider a user request for application termination as a request to logout.
應用程式安全問題回報	5.1.7.1	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **9. Secure software distribution** Provide feedback channels for users to report security problems with apps such as a security@ email address.
注入式攻擊	5.1.7.2 5.1.7.3	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **12. Protect the application from client side injections** Mobile apps present increased opportunities for client side injections, since they constantly interact with sensors, other installed apps and third party services. Existing mobile application flaws can be exploited in a similar way to vulnerabilities in traditional software

		applications. Attackers may force the application to use specially crafted data that will modify the application logic flow and lead to access control bypass or information disclosure attacks. ● **The Mobile Security Testing Guide (MSTG)** ➢ **SQL Injection** SQL injection attack involves integrating SQL commands into input data, mimicking the syntax of a predefined SQL command. A successful SQL injection attack allows the attacker to read or write to the database and possibly execute administrative commands, depending on the permissions granted by the server. ➢ **XML Injection** In a XML injection attack, the attacker injects XML metacharacters to structurally alter XML content. This can be used to either compromise the logic of an XML-based application or service, as well as possibly allow an attacker to exploit the operation of the XML parser processing the content.
假冒使用者	5.2.2.2	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **2. Implement user authentication, authorization and session management correctly** Ensure that the session management is handled securely7 after the initial authentication, using appropriate secure protocols.
不安全加密	5.2.2.3	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **4. Ensure sensitive data is protected in transit** Use strong and standardized encryption algorithms (e.g., AES) and appropriate key lengths (check recommendations for the algorithm you use e.g. for the TLS configuration). Remove support for weak ciphers.
惡意修改通訊協定傳輸格式	5.2.3.1	● **The Mobile Security Testing Guide (MSTG)** ➢ **Dynamic Analysis** Memory corruption bugs are best discovered via input fuzzing: an automated black-box software testing technique in which malformed data is continually sent to an app to survey for potential vulnerability conditions. During this process, the application is monitored for malfunctions and crashes. Should a crash occur, the hope (at least for security testers) is that the conditions creating the crash reveal an exploitable security flaw.
版本漏洞	5.3.1.1 5.3.1.2	● **NIST SP 800-124 r1** ➢ **4.3 Implementation** Security of the Implementation. The mobile device

		implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. Organizations with high security needs may choose to perform extensive vulnerability assessments against the mobile device solution components. At a minimum, all components should be updated with the latest available patches and configured following sound security practices. The organization should also take basic measures to prevent the user from circumventing the device's security features. Also, jailbroken or rooted mobile devices should be automatically detected to prohibit their use, for cases in which detection is feasible. ● **Department of Homeland Security (DHS), Study on Mobile Device Security：2017** ➢ **IV.2.1 Mobile Operating System** Exploitation of mobile operating system vulnerabilities can provide an attacker the ability to bypass the important security protections provided by the operating system, including the application isolation and package management capabilities, resulting in impacts including attacker access to sensitive enterprise data. Just as with any software, vulnerabilities are constantly discovered in mobile operating systems. Typically, on notification of a vulnerability, mobile operating system vendors fix the issue and the fix (often referred to as a patch) is also included in a software update.
被讀取記憶體	5.3.3.2	● **ENISA Smartphone Secure Development Guidelines 2016** ➢ **1. Identify and protect sensitive data on the mobile device** There is currently no standard secure deletion procedure for flash memory (unless wiping the entire medium/card). Therefore, data encryption and secure key management are especially important. ● **The Mobile Security Testing Guide (MSTG)** ➢ **Memory Corruption Bugs** Memory corruption bugs are a popular mainstay with hackers. This class of bug results from a programming error that causes the program to access an unintended memory location. Under the right conditions, attackers can capitalize on this behavior to hijack the execution flow of the vulnerable program and execute arbitrary code.
資訊被截取修改	5.3.3.3	● **NIST FIPS PUB 140-2** ➢ **4.2 Cryptographic Module Ports and Interfaces** the physical port(s) used for the input and output of

		plaintext cryptographic key components, authentication data, and CSPs shall be physically separated from all other ports of the cryptographic module. the logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path. plaintext cryptographic key components, authentication data, and other CSPs shall be directly entered into the cryptographic module (e.g., via a trusted path or directly attached cable). (See Section 4.7.4).
系統被修改	5.3.3.4	● **NIST FIPS PUB 140-2** ➢ **Self-Tests** Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.

附錄 B
(參考)
風險來源分析與資安需求

本標準以 2017 年 NCC 公告之「智慧型手機系統內建軟體資通安全檢測技術規範」為基礎，參考近年來智慧型手機資安威脅與攻擊案例來分析風險來源，在應用程式層、通訊協定層、作業系統層與硬體層等構面提出防護對策，例如：2018 年 DEFCON 會議，外國資安團隊發布的手機內建軟體漏洞，並增加「智慧型手機系統內建軟體資通安全檢測技術規範」無法防護的手機漏洞項目。由威脅目標與攻擊技術制定安全等級與標準規範，風險來源分析與資安需求分析表，如表 B.1 所示。

表 B.1 風險來源分析與資安需求分析表

威脅描述	威脅目標	攻擊技術	防護對策	安全構面
不安全儲存位置	敏感性資料	資料爬蟲	存放於作業系統保護區	應用程式
	參考來源： DEFCON 2018: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices[1]			
第三方函式庫漏洞	系統軟體	利用已知漏洞	已知漏洞修補	應用程式
	參考來源： A Pattern for Remote Code Execution using Arbitrary File Writes and MultiDex Applications[2]			
機密資料被寫入系統日誌	敏感性資料、系統事件日誌	資料爬蟲	檢查執行期間系統日誌	應用程式
	參考來源：			

[1] https://www.kryptowire.com/android-firmware-defcon-2018/

[2] https://www.nowsecure.com/blog/2015/06/15/a-pattern-for-remote-code-execution-using-arbitrary-file-writes-and-multidex-applications/

	Modem Log and Logcat Log Vulnerability allows any app to access text messages and call data and logcat logs – Can be activated by any app on the device – Transparent to the user (no notifications, toast messages, etc.) Writes to a base directory of /sdcard/sd_logs[3]			
隨意讀取手機資料	敏感性資料	未經授權讀取資料	敏感性資料使用前取得使用者同意	應用程式
	參考來源： DEFCON 2018: Vulnerable Out of the Box - An Evaluation of Android Carrier Devices[4]			
注入式攻擊	資料庫、取得使用者之權限	SQL Injection、XML Injection、Command Injection 或其他 Injection 攻擊	提供注入攻擊防護	應用程式
	參考來源： 某 KTV 架構問題導致任意點歌、訊息發送、SQL Injection 等多個漏洞[5]			
不安全加密	敏感性資料	解密工具	使用安全合格的加密演算法	應用程式
	參考來源： CWE-327: Use of a Broken or Risky Cryptographic Algorithm[6]			
惡意修改	裝置可用性	修改通訊協定	模糊測試	通訊協定

[3] https://www.slideshare.net/cisoplatform7/vulnerable-out-of-the-box-an-evaluation-of-android-carrier-devices

[4] https://www.kryptowire.com/android-firmware-defcon-2018/

[5] https://zeroday.hitcon.org/vulnerability/ZD-2016-00074

[6] https://cwe.mitre.org/data/definitions/327.html

通訊協定傳輸格式		傳輸格式		
	參考來源： Smartphone Secure Development Guidelines[7]			
傳輸資訊截取修改	通訊資料	中間人	提供信任傳輸通道	通訊協定
	參考來源： 手機應用程式開發上被忽略的 SSL 處理[8]			
NFC	敏感性資料、盜取信用卡資料	安裝惡意軟體	NFC 預設關閉	作業系統
	參考來源： 駭客利用 Android 的 NFC 漏洞，就能在手機上植入惡意程式[9]			
eSIM 安全	eSIM 與 eSIM 配置文件	中間人攻擊	提供配置文件無線傳輸與儲存保護	作業系統
	參考來源： GSMA: Embedded UICC for Consumer Devices Protection Profile[10]			
USB 安裝惡意程式	敏感性資料	AceDeceiver	實體介面連接通知	硬體
	參考來源： 手機充電被「遠端操控」[11]			

[7] https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

[8] https://devco.re/blog/2014/08/15/ssl-mishandling-on-mobile-app-development/

[9] https://www.ithome.com.tw/news/133995

[10] https://www.gsma.com/newsroom/resources/sgp-25-embedded-uicc-for-consumer-devices-protection-profile/

[11] https://news.ltn.com.tw/news/world/breakingnews/2572997

參考資料

(1) RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2
(2) First, Common Vulnerability Scoring System v3.0 Specification, https://www.first.org/cvss/specification-document
(3) NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise：2013
(4) NIST SP 800-164 DRAFT, Guidelines on Hardware-Rooted Security in Mobile Devices：2012
(5) NIST SP 800-163, Vetting the Security of Mobile Applications：2015
(6) NIST FIPS PUB 140-2, Security Requirements For Cryptographic Modules：2001
(7) GSMA, Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.2：2017
(8) ETSI, Smart Cards; Vocabulary for Smart Card Platform specifications V5.0.0：2019
(9) 法務部, 個人資料保護法, Dec., 2015
(10) OWASP XXE 說明 https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
(11) 個人資料保護法 https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
(12) CNS 13587 銀行業金鑰管理(批發用)Banking-Key Management(wholesale)
(13) CNS 14381-1 X6033-1 資訊技術－安全技術－金鑰管理－第 1 部：框架
(14) Department of Homeland Security (DHS), Study on Mobile Device Security：2017
(15) 信任執行環境 https://source.android.com/security/trusty/index.html
(16) 台灣資通產業標準協會 TAICS TS-0015-1 v1.0-影像監控系統資安標準測試規範-第一部_一般要求：2018
(17) 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

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