行動應用 App 基本資安規範

V1.5

行動應用資安聯盟
中華民國 113 年 9 月

行動應用 App 基本資安規範版本沿革

日期	行動應用 App 基本資安規範版本沿革
民國 104 年 4 月	行動應用 App 基本資安規範 V1.0
民國 105 年 10 月	行動應用 App 基本資安規範 V1.1
民國 107 年 8 月	行動應用 App 基本資安規範 V1.2
民國 108 年 9 月	行動應用 App 基本資安規範 V1.3
民國 111 年 1 月	行動應用 App 基本資安規範 V1.4
民國 113 年 9 月	行動應用 App 基本資安規範 V1.5

目　次

1. 前言 **1**

2. 適用範圍 **2**

3. 用語及定義 **3**

3.1. 行動應用程式（Mobile Application） 3

3.2. 行動應用程式商店（Application Store） 3

3.3. 個人資料（Personal Data） 3

3.4. 敏感性資料（Sensitive Data） 3

3.5. 密碼（Password） 3

3.6. 交易資源（Transaction Resource） 3

3.7. 交易記錄（Transaction Record） 3

3.8. 預授權交易（Pre-authorization Transaction） 4

3.9. 交談識別碼（Session Identification, Session ID） 4

3.10. JWT（JSON Web Token） 4

3.11. 生物特徵身分鑑別（Biometric Authentication） 4

3.12. 一次性密碼（One Time Password, OTP） 4

3.13. 伺服器憑證（Server Certificate） 4

3.14. 憑證機構（Certification Authority） 4

3.15. 惡意程式碼（Malicious Code） 4

3.16. 網路釣魚（Phishing） 5

3.17. 殭屍網路（Botnet） 5

3.18. 間諜軟體（Spyware） 5

3.19. 下載器（Downloader）.....5
3.20. 資訊安全漏洞（Vulnerability）.....5
3.21. 螢幕覆蓋攻擊（Screen Overlay Attack）.....5
3.22. 函式庫（Library）.....5
3.23. 注入攻擊（Code Injection）.....5
3.24. 行動作業系統（Mobile Operating System）.....5
3.25. 行動裝置資源（Mobile Resource）.....6
3.26. 行動應用程式內部更新（In-Application Update）.....6
3.27. 模擬器（Emulator）.....6
3.28. USB 偵錯模式（USB Debugging Mode）.....6
3.29. 偵錯模式（Debug Mode）.....6
3.30. 常見弱點與漏洞（Common Vulnerabilities and Exposures）.....6
3.31. 常見弱點列舉（Common Weakness Enumeration）.....6
3.32. 已知安全性漏洞（Known Vulnerabilities）.....6
3.33. 身分鑑別（Authentication）.....6
3.34. Chacha20 加密演算法.....7
3.35. 進階加密演算法（Advanced Encryption Standard）.....7
3.36. 三重資料加密演算法（Triple Data Encryption Standard）.....7
3.37. 橢圓曲線加密演算法（Elliptic Curve Cryptography）.....7
3.38. 憑證綁定（Certificate Pinning）.....7
3.39. 雜湊（Hash）.....7
3.40. 混淆（Obfuscation）.....7

3.41. 加殼（Packing）.....8
3.42. 使用敏感性資料（Using Sensitive Data）.....8
3.43. 日誌檔案 （Log File）.....8
3.44. 系統日誌（System Logs）.....8
3.45. 裝置識別符 （Device Identifier）.....8
3.46. 冗餘檔案 (Cache Files or Temporary Files).....8
3.47. 設定檔（Configuration File）.....8
3.48. 處理間通信（Inter-Process Communication）.....9
3.49. 編碼（Encode）.....9
3.50. 解碼（Decode）.....9
3.51. 酬載（Payload）.....9
3.52. 蒐集敏感性資料（Collecting Sensitive Data）.....9
3.53. 儲存敏感性資料（Storing Sensitive Data）.....9
3.54. 通用漏洞評分系統（Common Vulnerability Scoring System）.....9
3.55. 安全亂數產生函式 (Secure Random Number Generator).....9
3.56. 安全網域 (Secure Domain).....9
3.57. 安全加密函式 (Secure Encryption Function).....9
3.58. 系統憑證儲存設施 (System Credentials Storage Facilities).....10
3.59. App 切換模式 (App Switching Mode）.....10
4. 技術要求.....11
4.1. 行動應用程式資訊安全技術要求事項 11
4.1.1. 行動應用程式發布安全..... 11

4.1.2. 敏感性資料保護 11
4.1.3. 交易資源控管安全 13
4.1.4. 行動應用程式使用者身分鑑別、授權與連線管理安全 14
4.1.5. 行動應用程式碼安全 14
4.2. 伺服器端資訊安全技術要求事項 15
4.2.1. 伺服器端安全管理 16
4.2.2. 伺服器端安全檢測 16
5. 行動應用程式分類 17
6. 參考資料 18
Open Web Application Security Project (OWASP) 18
美國 18
歐洲 18
日本 19
國際標準 19
國內法律 19
附錄一、技術要求事項與各國規範對照表 20
附錄二、技術要求事項參考檢核表 23

1. 前言

行動裝置帶來的便利已使之成為國人生活中不可或缺的設備，各類行動應用程式（Mobile Application, App）應運而生，惟部分行動應用 App 開發者缺乏資安意識，恐造成使用者資料外洩或財務損失之風險。經濟部工業局(民國 111 年數位發展部數位產業署承接)依據民國 103 年 6 月 24 日行政院國家資通安全會報第 26 次委員會議決議，積極研議「行動應用 App 基本資安規範」（以下稱本規範）。

爰此，經濟部工業局(民國 111 年數位發展部數位產業署承接)委由財團法人資訊工業策進會邀集國內資安領域專家成立工作小組，參酌國際相關資安規範與準則，進行本規範編修工作。於規範編修各階段，透過辦理專家座談會及公開研討會等會議，徵詢產官學研先進之建議，聽取各界意見，作為編修重要方向，以完成本規範之訂定，供業界開發行動應用 App 自主遵循參考。本規範於民國 107 年 8 月修訂至 V1.2，於民國 108 年 9 月更新修訂為「行動應用 App 基本資安規範 V1.3」，民國111 年 1 月由台北市電腦公會為執行單位，更新修訂「行動應用 App 基本資安規範 V1.4」，並於民國 113 年 7 月由台北市電腦公會為執行單位，更新修訂「行動應用 App 基本資安規範 V1.5」（以下稱本規範），以規範行動應用程式之安全性。

本規範係屬非強制性規定，主要目的在於提升我國行動應用 App 基本安全防護能力，從設計初始階段即導入基本資安概念，透過規範之重點要項，提醒行動應用 App 開發者強化資訊安全意識，並逐步完善自身 App 安全防護能力。

本規範分別從「行動應用程式發布安全」、「敏感性資料保護」、「交易資源控管安全」、「行動應用程式使用者身分鑑別、授權與連線管理安全」、「行動應用程式碼安全」、「伺服器端安全管理」及「伺服器端安全檢測」等七個層面提出資訊安全技術要求，行動應用 App 開發者可參考規範，自主提升所開發之行動應用 App 安全品質，增進使用者之信賴度與使用意願，創造行動應用 App開發者與使用者雙贏局面。

2. 適用範圍

本規範主要針對行動應用程式於行動裝置端之安全提出基本資訊安全要求，並包含伺服器端之資訊安全需求。

本規範適用於非特定領域[1]之行動應用程式，與行動應用程式之共通性功能[2]。特定領域之行動應用程式，其領域功能所需之資訊安全規範，建議應由各目的事業主管機關訂定之。

本規範為提供行動應用程式相關業者之基本資訊安全準則，屬自願性準則，各業者可參酌遵循。

[1] 特定領域：指歸類於某一專門領域，由特定主管機關及法律加以規範、管制，例如金融、醫療、稅務等。

[2] 共通性功能：指行動應用程式運作所需、具有共同性、相類似之基礎功能，例如資料儲存、傳輸保護機制或使用者身分鑑別機制等。

3. 用語及定義

本章節中文技術用語譯名主要採用教育部之國家教育研究院雙語詞彙、學術名詞暨辭書資訊網之翻譯用語：

3.1. 行動應用程式（Mobile Application）

指一種設計給智慧型手機、平板電腦使用之應用程式，本文中亦簡稱「行動應用 App」。

3.2. 行動應用程式商店（Application Store）

指提供行動裝置使用者對行動應用程式進行瀏覽、下載、購買之平台或網站。

3.3. 個人資料（Personal Data）

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括但不限於自然人之姓名、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。

3.4. 敏感性資料（Sensitive Data）

指依使用者行為或行動應用程式之運作，於行動裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，其中對個人隱私資料之存取便屬於蒐集、儲存於本地空間內即屬儲存，而該資訊之洩漏有對使用者造成損害之虞，除包括 3.3 內定義之個人資料之外，並包括但不限於密碼、金鑰、視訊、照片、通話、錄音檔、即時通訊訊息、通話記錄、簡訊、備忘錄、通訊錄、筆記、地理位置、行事曆及裝置識別符等有關個人隱私之資料。

3.5. 密碼（Password）

指一組能讓使用者使用系統或用以識別使用者身分之字元串。

3.6. 交易資源（Transaction Resource）

指透過行動應用程式內所提供涉及交易行為之項目，包括但不限於實體貨幣、虛擬貨幣(包含點數或序號)、票券(包含股票)等有價值項目。

3.7. 交易記錄（Transaction Record）

指透過行動應用程式進行交易時，與達成交易有關之資料，包含交易對象、交易商品名稱、交易時間、交易金額、支付方式（例如：信用卡、電子支付）及交易狀態（例如：交易完成、交易中、交易取消）。

3.8. 預授權交易（Pre-authorization Transaction）

指使用者事先對應用程式開放特定交易類型的授權，使得在後續符合授權範圍與條件的情況下，交易得自動執行，而無須再次取得使用者同意。此授權須明確界定可執行的交易範疇（如例行性付款、固定金額扣款），且使用者可隨時查看、取消或變更該預授權設定。

3.9. 交談識別碼（Session Identification, Session ID）

指在建立連線時，指派給該連線之識別碼，並做為連線期間之唯一識別碼；當連線結束時，該識別碼可釋出並重新指派給新連線。

3.10. JWT（JSON Web Token）

指一種開放標準（RFC 7519），透過 HMAC、RSA、ECDSA 等演算法進行簽章，經常用於對使用者進行身分驗證，使用者透過 JWT 向資源伺服器請求資源，若該 JWT 為有效，則使用者能獲得相對應的資源。

3.11. 生物特徵身分鑑別（Biometric Authentication）

指使用者透過其身體的生物特徵進行身分認證。生物特徵可以包括指紋、虹膜、臉部、聲紋等。

3.12. 一次性密碼（One Time Password, OTP）

指行動應用裝置或其他數位裝置上只能使用一次的密碼，有效期為單次登錄使用。

3.13. 伺服器憑證（Server Certificate）

指載有簽章驗證資料，提供行動應用程式鑑別伺服器身分及資料傳輸加密使用。

3.14. 憑證機構（Certification Authority）

指簽發憑證之機關、法人。

3.15. 惡意程式碼（Malicious Code）

指在未經使用者同意之情況下，侵害使用者權益，包括但不限於任何具有惡意特徵或行為之程式碼。

3.16. 網路釣魚（Phishing）

此種類型之惡意程式主要是將使用者導入釣魚網站，並且誘導使用者輸入相關資訊，以竊取個人資料。

3.17. 殭屍網路（Botnet）

此種惡意程式可以在行動裝置後台運作，和殭屍控制主機（Botmaster）聯繫並執行命令，使用者不易察覺。

3.18. 間諜軟體（Spyware）

此種應用程式會監控和記錄使用者的設備資訊或行為資訊，例如簡訊、電子郵件、電話記錄、聯絡人、地理位置等訊息，並分享給遠端的伺服器。

3.19. 下載器（Downloader）

此種應用程式自身並非惡意程式，但會隱身於 App 中，負責下載其他的惡意程式到使用者行動裝置中。

3.20. 資訊安全漏洞（Vulnerability）

指行動應用程式安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性、可用性面臨威脅。

3.21. 螢幕覆蓋攻擊（Screen Overlay Attack）

指攻擊者的應用程式會在行動應用程式上繪製一個視窗，誤導使用者將自己點擊的入侵視窗當作正常視窗。

3.22. 函式庫（Library）

指將一些繁複或者牽涉到硬體層面之程式包裝成函式（Function）或物件（Object）收集在一起，編譯成二進位碼（Binary code）提供程式設計者使用。

3.23. 注入攻擊（Code Injection）

指因行動應用程式設計缺陷而執行使用者所輸入之惡意指令，包括但不限於命令注入（Command Injection）及資料隱碼攻擊（SQL Injection）。

3.24. 行動作業系統（Mobile Operating System）

指在行動裝置上運作的作業系統。

3.25. 行動裝置資源（Mobile Resource）

指行動裝置提供之功能或服務，包括但不限於相機、相片、麥克風、無線網路、感應器及地理位置。

3.26. 行動應用程式內部更新（In-Application Update）

指不更動發布於行動應用程式商店之主要版本，透過自訂的方法更新行動應用程式內容與功能。

3.27. 模擬器（Emulator）

指在電腦或是其他非行動裝置之設備上，模擬行動裝置之執行環境，用於在非行動裝置上執行行動應用程式。

3.28. USB 偵錯模式（USB Debugging Mode）

指在 Android 行動裝置可啟用的一個功能，可讓 Android 行動裝置與運行 Android SDK 的電腦進行通訊，目的為方便行動應用 App 開發者透過 USB 連線到 Android 行動裝置，並對行動應用程式進行偵錯或測試。

3.29. 偵錯模式（Debug Mode）

指一種在行動應用程式的開發模式，提供額外的偵錯功能，方便行動應用 App 開發者對該行動應用程式進行偵錯。

3.30. 常見弱點與漏洞（Common Vulnerabilities and Exposures）

簡稱「CVE」，由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.31. 常見弱點列舉（Common Weakness Enumeration）

簡稱「CWE」，由美國國土安全部網路與基礎設施安全局所贊助，由非營利的研發機構 MITRE 負責管理的弱點列表。這些弱點列表提供評估軟體安全的共通語言，羅列各種軟體弱點、識別方法、緩解與預防工作的知識。

3.32. 已知安全性漏洞（Known Vulnerabilities）

指具 CVE 編號之漏洞。

3.33. 身分鑑別（Authentication）

指對個體所宣稱之身分提供證明。

3.34. Chacha20 加密演算法

指一種串流加密算法，由丹麥計算機科學家 Daniel J. Bernstein 於 2008 年開發，使用一個 128 位的密鑰和一個 64 位的初始向量（IV）作為輸入，並生成一個 256 位的密鑰流（Keystream）。然後，將密鑰流與明文數據進行 XOR 運算。

3.35. 進階加密演算法（Advanced Encryption Standard）

指美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於 2001 年發佈於 AES（Advanced Encryption Standard）加密演算法，文件編號為 FIPS PUB 197 標準，並在 2002 年正式實施此標準。AES 可以支援 128 位元資料區塊（Data Block），並支援 128、192 與 256 位元金鑰長度（Key Size），提高安全性，AES 的加解密包含十個以上的回合數（Round Number），每個回合包含四個主要基本單元。

3.36. 三重資料加密演算法（Triple Data Encryption Standard）

指一種乘積加密法，使用三重資料加密標準（Triple Data Encryption Standard），處理 64 位元的資料區塊。

3.37. 橢圓曲線加密演算法（Elliptic Curve Cryptography）

指一種建立公開金鑰加密的演算法，基於橢圓曲線所生成之加法群或數學結構。橢圓曲線在密碼學中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分別獨立提出的。

3.38. 憑證綁定（Certificate Pinning）

指將伺服器憑證預先存放於應用程式內，用於連線時確認是否與伺服器憑證相符。

3.39. 雜湊（Hash）

指由一串資料中經過演算法計算出來的資料指紋，經常用來識別檔案與資料是否有被竄改，以保證檔案與資料確實是由原創者所提供。

3.40. 混淆（Obfuscation）

指將行動應用程式原始碼，在不影響功能執行的情況下，轉換為難以閱讀之形式。

3.41. 加殼（Packing）

指將行動應用程式原始碼進行加密，並在行動應用程式執行期間進行解密的技術，目的是防止攻擊者利用逆向工程技術獲得行動應用程式的原始碼。

3.42. 使用敏感性資料（Using Sensitive Data）

指包含應用程式本身及提供給第三方進行之應用。

3.43. 日誌檔案 （Log File）

僅供於進行除錯使用之應用程序日誌、安全日誌、除錯日誌或自定義日誌檔。

3.44. 系統日誌（System Logs）

指作業系統記錄各種事件、錯誤、警告等的日誌文件，用於行動應用 App 開發者除錯應用程式、分析系統崩潰問題、以及系統維護。

3.45. 裝置識別符 （Device Identifier）

指硬體或軟體之唯一識別資訊，包括國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、行動設備識別碼（Mobile Equipment Identifier, MEID）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）、積體電路卡識別碼（Integrated Circuit Card Identifier, ICCID）、媒體存取控制位址（Media Access Control Address, MAC Address）、安卓系統識別碼（Android Identifier, Android ID）、安卓系統廣告識別碼（Android Advertising ID, AID）、iOS IFAID（Identifier for Advertisers Identifier, IFAID）及 Windows Phone Device ID。

3.46. 冗餘檔案 (Cache Files or Temporary Files)

指行動應用程式安裝、運行後，產生之與應用程式功能性無關的檔案，通常於應用程式結束時刪除。該檔案存在與否，不影響行動應用程式再次執行時的功能與表現，如暫存檔或快取。此外，如刪除某檔案造成自動登入功能失效，則該檔案應屬於設定檔而非冗餘檔案。

3.47. 設定檔（Configuration File）

指行動應用程式儲存相關設定的檔案，刪除時會影響行動應用程式再次執行時功能的表現。

3.48. 處理間通信（Inter-Process Communication）

簡稱「IPC」，是不同的程序之間的通訊機制，允許不同的程序之間進行資訊交換，以實現共享資源的目的。

3.49. 編碼（Encode）

指將數據轉換為代碼或字符的動作，且該代碼或字符可以譯（解）碼成原來數據。

3.50. 解碼（Decode）

指將編碼後的代碼或字符轉譯成原來數據的動作。

3.51. 酬載（Payload）

指封包、訊息或程式碼內容中的有效資料或指令。

3.52. 蒐集敏感性資料（Collecting Sensitive Data）

指行動應用程式取得行動裝置內建或使用者輸入之敏感性資料。

3.53. 儲存敏感性資料（Storing Sensitive Data）

指行動應用程式將敏感性資料以檔案形式寫入行動裝置或其附屬儲存媒介。

3.54. 通用漏洞評分系統（Common Vulnerability Scoring System）

簡稱「CVSS」，使用IT漏洞的特點與影響進行評分，由美國國家基礎建設諮詢委員會負責研究（National Infrastructure Advisory Council, NIAC），現轉由資安事件應變小組論壇（Forum of Incident Response and Security Teams, FIRST）發展，目前以第3版為主。

3.55. 安全亂數產生函式 (Secure Random Number Generator)

符合或引用 ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項標準之亂數產生函式。

3.56. 安全網域 (Secure Domain)

一般熟知之公共安全網域包括 Facebook、Google 或 Twitter。

3.57. 安全加密函式 (Secure Encryption Function)

符合 FIPS 140-3 SP800-140C 所列舉之加密函式，並且禁止使用三重資料加

密演算法。

3.58. 系統憑證儲存設施(System Credentials Storage Facilities)

指行動作業系統提供行動應用App 開發者及行動裝置使用者用於儲存用戶憑證或密碼金鑰之服務，例如：Keystore (Android)、Keychain (iOS) 或其它類似機制。

3.59. App 切換模式（App Switching Mode）

指一個行動設備（如智慧手機或平板電腦）的執行模式，其中使用者可以同時預覽多個應用程式。iOS 中稱為 App 切換器（App Switcher），Android 則為「切換畫面與應用程式」功能。

4. 技術要求

4.1. 行動應用程式資訊安全技術要求事項

本節針對不同面向之行動應用程式安全訂定技術要求，其中包括五大面向：「行動應用程式發布安全」、「敏感性資料保護」、「交易資源控管安全」、「行動應用程式使用者身分鑑別、授權與連線管理安全」及「行動應用程式碼安全」。

4.1.1. 行動應用程式發布安全

本面向主要適用於發布行動應用程式之相關資訊安全技術要求，包括發布、更新與問題回報等。

4.1.1.1. 行動應用程式發布

行動應用程式應於可信任來源之行動應用程式商店發布。

行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。

行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體。

4.1.1.2. 行動應用程式更新

行動應用程式應於可信任來源之行動應用程式商店發布更新。

行動應用程式應提供更新機制。

行動應用程式應於安全性更新時主動公告。

4.1.1.3. 行動應用程式安全性問題回報

行動應用 App 開發者應提供回報安全性問題之管道。

行動應用 App 開發者應於適當期間內回覆問題並改善。

4.1.2. 敏感性資料保護

本面向主要適用於敏感性資料與個人資料保護之相關資訊安全技術要求，包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等。

4.1.2.1. 敏感性資料蒐集

行動應用程式應於蒐集敏感性資料前，取得使用者同意。

行動應用程式應提供使用者拒絕蒐集敏感性資料之權利。

4.1.2.2. 敏感性資料利用

行動應用程式應於使用敏感性資料前，取得使用者同意。

行動應用程式應提供使用者拒絕使用敏感性資料之權利。

行動應用程式如採用密碼認證，應主動提醒使用者設定較複雜之密碼。

行動應用程式應提醒使用者定期更改密碼。

4.1.2.3. 敏感性資料儲存

行動應用程式應於儲存敏感性資料前，取得使用者同意。

行動應用程式應提供使用者拒絕儲存敏感性資料之權利。

行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途。

行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中。

行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中。

敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。

敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。

敏感性資料應避免出現於行動應用程式之程式碼。

行動應用程式於非使用者主動進行的畫面擷取時應主動警示使用者。

行動應用程式應將個人可識別資訊、使用者憑證及加密金鑰等敏感性資料儲存於系統憑證儲存設施。

行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉。

行動應用程式應避免在 IPC 機制中洩漏敏感性資料。

行動應用程式中的使用者介面應避免洩漏敏感性資料。

行動裝置作業系統的備份資料中不應存有行動應用程式的敏感性資料。

行動應用程式應避免重複使用相同的對稱式加密金鑰。

行動應用程式應避免將敏感性資料輸出於系統日誌。

4.1.2.4. 資料傳輸安全

行動應用程式透過網路傳輸資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。

4.1.2.5. 敏感性資料分享

行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意。

行動應用程式應提供使用者拒絕分享敏感性資料之權利。

行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取。

4.1.2.6. 敏感性資料刪除

行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能。

4.1.3. 交易資源控管安全

本面向主要適用於交易資源控管之相關資訊安全技術要求，包括交易資源之使用與控管等。

4.1.3.1. 交易資源使用

行動應用程式應於使用交易資源時主動通知使用者。

行動應用程式應提供使用者拒絕使用交易資源之權利。

行動應用程式應於交易收款時主動通知使用者。

4.1.3.2. 交易資源控管

行動應用程式應於使用交易資源時進行使用者身分鑑別。

行動應用程式應提供使用交易資源之交易紀錄。

行動應用程式應提供預授權交易之記錄。

4.1.4. 行動應用程式使用者身分鑑別、授權與連線管理安全

本面向主要適用於行動應用程式身分鑑別、授權與連線管理之相關資訊安全技術要求，包括使用者身分鑑別與授權及連線管理機制等。

4.1.4.1. 使用者身分鑑別與授權

行動應用程式應有適當之身分鑑別機制，確認使用者身分。

行動應用程式應依使用者身分授權。

4.1.4.2. 連線管理機制

行動應用程式應避免使用具有規則性之交談識別碼。

行動應用程式應確認伺服器憑證之有效性。

行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發。

行動應用程式封包流向應與所宣告的內容一致。

4.1.5. 行動應用程式碼安全

本面向主要適用於行動應用程式開發之相關資訊安全技術要求，包括防範惡意程式碼與避免資訊安全漏洞、行動應用程式完整性、函式庫引用安全與使用者輸入驗證等，本面向參照 OWASP MASVS V7 之要求。

4.1.5.1. 防範惡意程式碼與避免資訊安全漏洞

行動應用程式應避免含有惡意程式碼。

行動應用程式應避免資訊安全漏洞。

行動應用程式應針對螢幕覆蓋攻擊進行防護。

4.1.5.2. 行動應用程式完整性

行動應用程式應使用適當且有效之完整性驗證機制，以確保其完整性。

4.1.5.3. 函式庫引用安全

行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全。

4.1.5.4. 使用者輸入驗證

行動應用程式應針對使用者於輸入階段之字串，進行安全檢查。

行動應用程式應提供相關注入攻擊防護機制。

4.1.5.5. 防止動態分析及竄改

行動應用程式須偵測行動作業系統保護層是否有被破解(如:Root、Jailbreak)或保護不當之情形，如有，應主動通知使用者或關閉應用程式。

行動應用程式應可主動偵測在沙盒中所有檔案以及資料是否有遭到竄改。

行動應用程式應偵測行動裝置中是否有使用動態分析工具或框架。

行動應用程式應偵測在記憶體中的程式碼以及資料是否遭到竄改。

屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。

行動應用程式應有程式碼混淆機制。

行動應用程式須偵測當前的執行環境是否為模擬器。

行動應用程式須偵測行動裝置是否開啟 USB 偵錯功能。

行動應用程式應將偵錯模式(Debug Mode)設為關閉。

4.2. 伺服器端資訊安全技術要求事項

本規範旨在針對行動應用程式安全提出基本資訊安全要求，如行動應用程式涉及伺服器端之資訊安全需求，建議應由業者自我宣告或切結其伺服器端資訊安全防護與管理措施，或對於其伺服器端服務之資訊安全防護

與管理，出具第三方檢測通過證明。

4.2.1. 伺服器端安全管理

伺服器端安全建議應以提供之應用與服務為出發點，進行應用與服務整體之威脅模型分析，找出對服務造成的安全性風險，以實施必要與有效的後續管控措施。

4.2.2. 伺服器端安全檢測

行動應用程式所搭配之行動應用平台伺服器端，由於其提供之存取介面為行動應用程式，而非使用者直接存取之介面，行動應用 App 開發者易忽略伺服器端安全的防護措施。行動應用平台伺服器端本質為網站及 Web Service 伺服器，若無適當的安全設計與開發，同樣會存在傳統網頁應用程式所具有的弱點。因此，在伺服器端的安全檢測，建議行動應用 App 開發者可斟酌採用滲透測試方式進行檢測。

4.2.2.1. Webview 安全檢測

行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換。

行動應用程式於 Webview 呈現功能時，所連線之網域應執行安全檢測。

5. 行動應用程式分類

不同應用類別之行動應用程式對於安全性有不同之要求，本章節針對不同類型行動應用程式之資訊安全要求事項進行區分，分為三類以及一類加測類別，分別為：

L1：無須使用者身分鑑別之行動應用程式。

L2：須使用者身分鑑別之行動應用程式。

L3：含有交易行為之行動應用程式。

F：屬於安全性需求較高之行動應用程式，為加測項目。

針對每一行動應用程式分類，定義應符合資訊安全技術要求事項之最小集合，即行動應用程式應符合其所屬分類中之所有資訊安全技術要求事項，非屬上述分類之特殊情況，於檢測標準另行說明。除了針對行動應用程式功能分類之外，另有 F 類檢測項為高安全性 App 之進階加測項目，主要檢測內容為逆向工程分析、竄改攻擊等。

6. 參考資料

Open Web Application Security Project (OWASP)

[1] OWASP Mobile App Security Checklist v1.7.0

https://mas.owasp.org/checklists/

[2] OWASP Mobile Application Security Testing Guide (MASTG) v1.7.0
https://mas.owasp.org/MASTG/

[3] OWASP Mobile Application Security Verification Standard (MASVS) v2.0
https://mas.owasp.org/MASVS/

[4] Mobile Application Security Testing Initiative, Cloud Security Alliance (CSA)
https://www.csaapac.org/mast.html, 2016

美國

[5] Vetting the Security of Mobile Applications, NIST Special Publication 800-163,
https://csrc.nist.gov/pubs/sp/800/163/r1/final, 2019

[6] Cryptographic Algorithm Validation Program (CAVP),
http://csrc.nist.gov/groups/STM/cavp/, NIST

[7] Cryptographic Module Validation Program (CMVP),
http://csrc.nist.gov/groups/STM/cmvp/, NIST

[8] Government Mobile and Wireless Security Baseline, Federal CIO Council,
https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf, 2013

歐洲

[9] Smartphone Secure Development Guidelines,
https://www.enisa.europa.eu/publications/smartphone-secure-development-

guidelines-2016, ENISA, 2017

日本

[10] Security Guideline for using Smartphones and Tablets - Advantages for work style innovation - [Version 1], https://www.jssec.org/dl/guidelines2012Enew_v1.0.pdf, JSSEC, 2011

國際標準

[11] ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection — Information security management systems — Requirements)

[12] ISO/IEC 20000: 2019 (Information technology - Service management)

[13] ISO/IEC 19790:2012 (Information technology - Security techniques - Security requirements for cryptographic modules)

[14] ISO/IEC 15408: 2022 (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security)

[15] ISO/IEC 14598:2001 (Software engineering — Product evaluation)

[16] ISO/IEC TR 9126-4:2004 (Software engineering - Product quality)

國內法律

[17] 個人資料保護法（民國 104 年 12 月 30 日）

[18] 個人資料保護法施行細則（民國 105 年 3 月 2 日）

附錄一、技術要求事項與各國規範對照表

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]
4.1.1.1.行動應用程式發布	MASVS-PLATFORM	Executive Summary	9. Secure software distribution
4.1.1.2.行動應用程式更新	MASVS-PLATFORM	Executive Summary	9. Secure software distribution
4.1.1.3.行動應用程式安全性問題回報	N/A	Executive Summary	9. Secure software distribution
4.1.2.1.敏感性資料蒐集	MASVS-STORAGE	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data
4.1.2.2.敏感性資料利用	MASVS-STORAGE	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data
4.1.2.3.敏感性資料儲存	MASVS-STORAGE	4. Mobile App Evaluation - Protect Sensitive Data	1. Identify and protect sensitive data on the mobile device
4.1.2.4.資料傳輸安全	MASVS-NETWORK	4. Mobile App Evaluation - Protect	4. Ensure sensitive data protection in transit

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]
		Sensitive Data	
4.1.2.5.敏感性資料分享	MASVS-STORAGE	4. Mobile App Evaluation - Preserve Privacy	1. Identify and protect sensitive data on the mobile device
4.1.2.6.敏感性資料刪除	MASVS-STORAGE	N/A	1. Identify and protect sensitive data on the mobile device
4.1.3.1.交易資源使用	MASVS-AUTH	N/A	8. Protect paid resources
4.1.3.2.交易資源控管	MASVS-AUTH	N/A	8. Protect paid resources
4.1.4.1.使用者身分鑑別與授權	MASVS-AUTH	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	3. Handle authentication and authorization factors securely on the device correctly
4.1.4.2.連線管理機制	MASVS-NETWORK	4. Mobile App Evaluation – Network Events	2. User authentication, authorization and session management
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	MASVS-CODE	4. Mobile App Evaluation: Malicious Functionality Malware Detection	6. Secure data integration with third party code 10. Handle runtime code interpretation

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]
		Communication with Known Disreputable Sites Libraries Loaded	
4.1.5.2.行動應用程式完整性	MASVS-CODE	4. Mobile App Evaluation – Classes Loaded	N/A
4.1.5.3.函式庫引用安全	MASVS-CODE	4. Mobile App Evaluation: Native Methods Libraries Loaded	6. Secure data integration with third party code
4.1.5.4.使用者輸入驗證	MASVS-CODE	4. Mobile App Evaluation – Input Validation	10. Handle runtime code interpretation
4.1.5.5.防止動態分析及竄改	MASVS-RESILIENCE	N/A	11. Check device and application integrity
4.2.2.1. Webview 安全檢測	N/A	N/A	N/A

[註 1] Vetting the Security of Mobile Applications, NIST Special Publication 800-163, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf, 2019

[註 2] Smartphone Secure Development Guidelines, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, ENISA, 2017

附錄二、技術要求事項參考檢核表

項次	序號	技術要求
4.1.1.1.行動應用程式發布	1	行動應用程式應於可信任來源之行動應用程式商店發布。
	2	行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。
	3	行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動裝置上安裝防護軟體。
4.1.1.2.行動應用程式更新	4	行動應用程式應於可信任來源之行動應用程式商店發布更新。
	5	行動應用程式應提供更新機制。
	6	行動應用程式應於安全性更新時主動公告。
4.1.1.3.行動應用程式安全性問題回報	7	行動應用App 開發者應提供回報安全性問題之管道。
	8	行動應用 App 開發者應於適當期間內回覆問題並改善。
4.1.2.1.敏感性資料蒐集	9	行動應用程式應於蒐集敏感性資料前，取得使用者同意。

	10	行動應用程式應提供使用者拒絕蒐集敏感性資料之權利。
4.1.2.2.敏感性資料利用	11	行動應用程式應於使用敏感性資料前，取得使用者同意。
	12	行動應用程式應提供使用者拒絕使用敏感性資料之權利。
	13	行動應用程式如採用密碼認證，應主動提醒使用者設定較複雜之密碼。
	14	行動應用程式應提醒使用者定期更改密碼。
4.1.2.3.敏感性資料儲存	15	行動應用程式應於儲存敏感性資料前，取得使用者同意。
	16	行動應用程式應提供使用者拒絕儲存敏感性資料之權利。
	17	行動應用程式儲存之敏感性資料，應僅用於其使用聲明之用途。
	18	行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中。
	19	行動應用程式應避免將敏感性資料儲存於冗餘檔案

		或日誌檔案中。
	20	敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。
	21	敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。
	22	敏感性資料應避免出現於行動應用程式之程式碼。
	23	行動應用程式於非使用者主動進行的畫面擷取時應主動警示使用者。
	24	行動應用程式應將個人可識別資訊、使用者憑證及加密金鑰等敏感性資料儲存於系統憑證儲存設施。
	25	行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉。
	26	行動應用程式應避免在IPC 機制中洩漏敏感性資料。
	27	行動應用程式中的使用者介面應避免洩漏敏感性資料。
	28	行動裝置作業系統的備份資料中不應存有行動應用程式的敏感性資料。

	29	行動應用程式應避免重複使用相同的對稱式加密金鑰。
	30	行動應用程式應避免將敏感性資料儲存或輸出於系統日誌。
4.1.2.4.資料傳輸安全	31	行動應用程式透過網路傳輸資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。
4.1.2.5.敏感性資料分享	32	行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意。
	33	行動應用程式應提供使用者拒絕分享敏感性資料之權利。
	34	行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取。
4.1.2.6.敏感性資料刪除	35	行動應用程式如涉及儲存使用者敏感性資料，應提供使用者刪除之功能。
4.1.3.1.交易資源使用	36	行動應用程式應於使用交易資源時主動通知使用者。
	37	行動應用程式應提供使用者拒絕使用交易資源之權利。
	38	行動應用程式應於交易收款時主動通知使用者。

4.1.3.2.交易資源控管	39	行動應用程式應於使用交易資源時進行使用者身分鑑別。
	40	行動應用程式應記錄使用之交易資源與時間。
	41	行動應用程式應提供預授權交易之記錄。
4.1.4.1.使用者身分鑑別與授權	42	行動應用程式應有適當之身分鑑別機制，確認使用者身分。
	43	行動應用程式應依使用者身分授權。
4.1.4.2.連線管理機制	44	行動應用程式應避免使用具有規則性之交談識別碼。
	45	行動應用程式應確認伺服器憑證之有效性。
	46	行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發。
	47	行動應用程式封包流向應與所宣告的內容一致。
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	48	行動應用程式應避免含有惡意程式碼。
	49	行動應用程式應避免資訊安全漏洞。
	50	行動應用程式應針對螢幕覆蓋攻擊進行防護。
4.1.5.2.行動應用程式完整性	51	行動應用程式應使用適當且有效之完整性驗證機制，

		以確保其完整性。
4.1.5.3.函式庫引用安全	52	行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌 4.1.1.行動應用程式發布安全。
4.1.5.4.使用者輸入驗證	53	行動應用程式應針對使用者於輸入階段之字串，進行安全檢查。
	54	行動應用程式應提供相關注入攻擊防護機制。
4.1.5.5.防止動態分析及竄改	55	行動應用程式須偵測行動作業系統保護層是否有被破解(如:Root、Jailbreak)或保護不當之情形，如有，應主動通知使用者或關閉應用程式。
	56	行動應用程式應可主動偵測在沙盒中所有檔案以及資料是否有遭到竄改。
	57	行動應用程式應偵測行動裝置中是否有使用動態分析工具或框架。
	58	行動應用程式應偵測在記憶體中的程式碼以及資料是否遭到竄改。
	59	屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜

		態分析不易取出重要的程式碼或資料。
	60	行動應用程式應有程式碼混淆機制。
	61	行動應用程式須偵測當前的執行環境是否為模擬器。
	62	行動應用程式須偵測行動裝置是否開啟 USB 偵錯功能。
	63	行動應用程式應將偵錯模式(Debug Mode)設為關閉。
4.2.2.1. Webview 安全檢測	64	行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換。
	65	行動應用程式於 Webview 呈現功能時，所連線之網域應執行安全檢測。