行動應用 App 基本資安規範

V1.4

經濟部工業局

中華民國 108 年 11 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 108 年 11 月	行動應用 App 基本資安規範 V1.4

目　次

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）遂應運而生，惟部分程式開發者缺乏資安意識，於 App 設計、開發、應用等階段未考慮相關安全性議題，恐造成使用者資料外洩或財務損失之風險。經濟部工業局依據民國 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，並目前於民國 109 年 11 月更新修訂至 V1.4。

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 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」、「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及授權與連線管理安全」、「行動應用程式碼安全」及「伺服器端安全檢測」等六個層面提出資訊安全技術要求，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 App 開發商與使用者雙贏局面。

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，其領域功能所須之資訊安全規範，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經濟部標準檢驗局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、平板電腦和其他行動裝置使用之應用程式。

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、國際行動設備識別碼（International Mobile Equipment Identity, IMEI）、國際行動用戶識別碼（International Mobile Subscriber Identity, IMSI）及其他得以直接或間接方式識別該個人之資料。

3.4. 安全敏感性資料（Secure 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，其中對個人隱私之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 上定義之個人資料之外，並包含但不限定通行碼、金鑰、視訊、照片、通話、錄音檔、即時通訊訊息、通話紀錄、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. 通行碼（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，包括本機儲存資料加密檔案密碼、自身帳號及密碼、遠端網路服務帳號及密碼。

3.6. 交易資源（Transaction Resource）

指透過行動應用程式內所提供購買功能，並可直接或間接取得之額外功能、內容或訂閱項目，凡有牽涉金流者，不論是虛擬或實體貨幣（包含點數或序號）等有價值物品皆視為交易資源。如售票系統 App 內購買票券得到一組 QRcode 可做為票卷的憑證；如網路書店 App 內購買電子書得到電子書的內容可供閱讀；如訂閱或訂購 App 內的交易服務項目，於交易後提供新的功能、移除使用限制功能或移除廣告功能等；或繳費網 App 提供繳費功能、銀行類型 App 提供轉帳或 App 提供購買實體或虛擬商品之功能。股票下單等有風險的敏感操作行為亦須要為使用者留下紀錄，以保障消費者權益。

3.7. 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。

3.8. 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。

3.9. 憑證機構（Certificate Authority）

指簽發憑證之機關、法人。

3.10. 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。

3.11. 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。

3.12. 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。

3.13. 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）、資料隱碼攻擊（SQL Injection）。

3.14. 行動作業系統（Mobile Operating System）

指在行動裝置上運作的作業系統。

3.15. 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。

3.16. 行動應用程式內部更新（In-App 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。

3.17. 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。

3.18. 脆弱加密演算法（Weak Cryptographic Algorithm）

指具 CVE 編號之加密演算法。

3.19. 已知安全性漏洞（Known Vulnerabilities）

指具 CVE 編號之漏洞。

3.20. 身分鑑別（Authentication）

指對個體所宣稱之身分提供保證。

3.21. 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。

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

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

3.23. 橢圓曲線密碼學（Elliptic Curve Cryptography）

指一種建立公開金鑰加密的演算法，其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。

3.24. 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。

3.25. 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。

3.26. 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。

3.27. 使用安全敏感性資料 （Using Secure Sensitive Data）

指包含應用程式本身及提供給第三方進行之應用。

3.28. 日誌檔案 （Log File）

僅供於進行除錯使用之系統日誌、應用程序日誌、安全日誌、除錯日誌或

自定義日誌檔。

3.29. 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）、Windows Phone Device ID。

3.30. 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。

3.31. 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。

3.32. 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。

3.33. 解碼（Decode）

指將編碼後的代碼或字符轉譯成原來數據的動作。

3.34. 酬載（Payload）

指封包、訊息或程式碼內容中的有效資料或指令。

3.35. 蒐集安全敏感性資料（Collecting Secure Sensitive Data）

指行動應用程式取得行動裝置內建或使用者輸入之安全敏感性資料。

3.36. 儲存安全敏感性資料（Storing Secure Sensitive Data）

指行動應用程式將安全敏感性資料以檔案形式寫入行動裝置或其附屬儲存媒介。

3.37. 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。

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

符合或引用 ANSI X9.17、FIPS 140-2、NIST SP 800-22 以及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項標準之亂數產生函式。

3.39. 安全網域 (Secure Domain)

範圍包括開發商、客戶所屬網域或一般熟知之公共安全網域，一般熟知之公共安全網域包括 Facebook、Google 或 Twitter 等支援 OAuth 2.0 協定之應用。

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

符合 FIPS 140-2 Annex A 之加密函式。

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」、「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及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安全敏感性資料、行動裝置資源及宣告之權限用途。

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，並於有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

行動應用程式開發者應提供回報安全性問題之管道。

行動應用程式開發者應於適當期間內回覆問題並改善。

4.1.2. 安全敏感性資料保護

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

4.1.2.1. 安全敏感性資料蒐集

行動應用程式應於蒐集安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

4.1.2.2. 安全敏感性資料利用

行動應用程式應於使用安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。

行動應用程式應提醒使用者定期更改通行碼。

4.1.2.3. 安全敏感性資料儲存

行動應用程式應於儲存安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

行動應用程式儲存之安全敏感性資料，應僅用於其使用聲明之用途。

行動應用程式儲存之安全敏感性資料，應避免將安全敏感性資料儲存於冗餘檔案或日誌檔案中。

安全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。

安全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。

安全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。

4.1.2.4. 安全敏感性資料傳輸

行動應用程式透過網路傳輸安全敏感性資料，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. 安全敏感性資料分享

行動裝置內之不同行動應用程式間，應於分享安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。

行動應用程式分享安全敏感性資料時，應避免未授權之行動應用程式存

取。

4.1.2.6. 安全敏感性資料刪除

行動應用程式如涉及儲存使用者安全敏感性資料，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，並提供使用者拒絕之權利。

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。

行動應用程式應於使用交易資源後記錄使用之交易資源與時間。

4.1.4. 行動應用程式使用者身分鑑別及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及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，並依使用者身分授權。

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。

行動應用程式連線使用之伺服器憑證應為可信任之憑證機構所簽發。

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。

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。

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，進行安全檢查並提供相關注入攻擊防護機制。

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，建議開發商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，所連線之網域應為安全網域。

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，共分為三類，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。

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。

6. 參考資料

Open Web Application Security Project (OWASP)

[1] Mobile App Security Checklist 1.1

https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide, 2017

Cloud Security Alliance (CSA)

[2] Mobile Application Security Testing Initiative, https://www.csaapac.org/mast.html, 2016

美國

[3] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

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

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

[6] 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

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

大陸

[8] 移動智慧終端安全能力技術要求, YD/T 2407-2013, 2013

[9] 移動智慧移終端安全能力測試方法, YD/T 2408-2013, 2013

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 27001:2013 (Information security management)

[12] ISO/IEC 20000:2011 (Information technology - Service management)

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

[14] ISO/IEC 15408:2009 (Information technology - Security techniques - Evaluation criteria for IT security)

[15] ISO/IEC 14598:2001 (Information technology - Software 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]	大陸 YD/T 2407-2013 [註 3]
4.1.1.1.行動應用程式發布	N/A	Executive Summary	9. Secure software distribution	5.5.2 應用軟件安全認證機制要求
4.1.1.2.行動應用程式更新	N/A	Executive Summary	9. Secure software distribution	5.5.4 預置應用軟件安全要求
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	5.5.4 預置應用軟件安全要求
4.1.2.1.安全敏感性資料蒐集	N/A	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data	5.5.4 預置應用軟件安全要求
4.1.2.2.安全敏感性資料利用	V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data	5.5.4 預置應用軟件安全要求 5.6.2 文件類用戶數據的授權訪問

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
4.1.2.3.安全敏感性資料儲存	V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys	4. Mobile App Evaluation - Protect Sensitive Data	1. Identify and protect sensitive data on the mobile device	5.6.3 用戶數據的加密存儲
4.1.2.4.安全敏感性資料傳輸	V2.6: Verify that no sensitive data is exposed via IPC mechanisms	4. Mobile App Evaluation - Protect Sensitive Data	4. Ensure sensitive data protection in transit	5.5.4 預置應用軟件安全要求 5.6.2 文件類用戶數據的授權訪問
4.1.2.5.安全敏感性資料分享	V2.3: Verify that no sensitive data is shared with third parties unless it is a necessary part of the architecture	4. Mobile App Evaluation - Preserve Privacy	1. Identify and protect sensitive data on the mobile device	5.6.2 文件類用戶數據的授權訪問
4.1.2.6.安全敏感性資料刪除	V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys	N/A	1. Identify and protect sensitive data on the mobile device	5.6.4 用戶數據的徹底刪除

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
4.1.3.1.交易資源使用	V4.9: Verify that step-up authentication is required to enable actions that deal with sensitive data or transactions	N/A	8. Protect paid resources	5.5.4 預置應用軟件安全要求
4.1.3.2.交易資源控管	V4.9: Verify that step-up authentication is required to enable actions that deal with sensitive data or transactions	N/A	8. Protect paid resources	5.5.4 預置應用軟件安全要求
4.1.4.1.使用者身分鑑別與授權	V4.1 : Verify that if the app provides users with access to a remote service, an acceptable form of authentication such as username/password authentication is performed at the remote endpoint	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	3. Handle authentication and authorization factors securely on the device correctly	5.6.2 文件類用戶數據的授權訪問
4.1.4.2.連線管理機制	V5.4: Verify that the	4. Mobile App	2. User authentication,	5.5.4 預置應用軟件安

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
	app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA	Evaluation – Network Events	authorization and session management	全要求
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	V1.7: Verify that a threat model for the mobile app and the associated remote services, which identifies potential threats and countermeasures, has been produced	4. Mobile App Evaluation: Malicious Functionality Malware Detection Communication with Known Disreputable Sites Libraries Loaded	6. Secure data integration with third party code 10. Handle runtime code interpretation	5.5.4 預置應用軟件安全要求
4.1.5.2.行動應用程式完整性	V7.2: Verify that the app has been built in release mode, with	4. Mobile App Evaluation – Classes Loaded	N/A	5.5.4 預置應用軟件安全要求

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
	settings appropriate for a release build (e.g. non-debuggable)			
4.1.5.3.函式庫引用安全	V1.2: Verify all third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities	4. Mobile App Evaluation: Native Methods Libraries Loaded	6. Secure data integration with third party code	5.5.4 預置應用軟件安全要求
4.1.5.4.使用者輸入驗證	V6.2: Verify that all inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources	4. Mobile App Evaluation – Input Validation	10. Handle runtime code interpretation	5.5.4 預置應用軟件安全要求
4.2.2.1. Webview 安全	N/A	N/A	N/A	N/A

技術要求事項	OWASP 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
檢測				

[註 1] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

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

[註 3] 移動智慧終端安全能力技術要求, YD/T 2407-2013, 2013

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安全敏感性資料、行動裝置資源及宣告之權限用途。
4.1.1.2.行動應用程式更新	3	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。
	4	行動應用程式應提供更新機制，並於有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	5	行動應用程式開發者應提供回報安全性問題之管道。
	6	行動應用程式開發者應於適當之期間內回覆問題並改善。
4.1.2.1.安全敏感性資料蒐集	7	行動應用程式應於蒐集安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
4.1.2.2.安全敏感性資料利用	8	行動應用程式應於使用安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
	9	行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。
	10	行動應用程式應提醒使用者定期更改通行碼。
4.1.2.3.安全敏感性資料儲存	11	行動應用程式應於儲存安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
	12	行動應用程式儲存之安全敏感性資料，應僅用於其使用聲明之用途。
	13	行動應用程式應避免在關閉及登出後將安全敏感性資料儲存於冗餘檔案或日誌檔案中

項次	序號	技術要求
	14	行動應用程式應避免將安全敏感性資料儲存於冗餘檔案或日誌檔案中
	15	安全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。
	16	安全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。
	17	安全敏感性資料應避免出現於行動應用程式之程式碼。
	18	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。
4.1.2.4.安全敏感性資料傳輸	19	行動應用程式透過網路傳輸安全敏感性資料，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.安全敏感性資料分享	20	行動裝置內之不同行動應用程式間，應於分享安全敏感性資料前，取得使用者同意，並提供使用者拒絕之權利。
	21	行動應用程式分享安全敏感性資料時，應避免未授權之行動應用程式存取。
4.1.2.6.安全敏感性資料刪除	22	行動應用程式如涉及儲存使用者安全敏感性資料，應提供使用者刪除之功能。
4.1.3.1.交易資源使用	23	行動應用程式應於使用交易資源時主動通知使用者，並提供使用者拒絕之權利。
4.1.3.2.交易資源控管	24	行動應用程式應於使用交易資源時進行使用者身分鑑別。
	25	行動應用程式應於使用交易資源後記錄使用之交易資源與時間。
4.1.4.1.使用者身分鑑別與授權	26	行動應用程式應有適當之身分鑑別機制，確認使用者身分，並依使用

項次	序號	技術要求
		者身分授權。
4.1.4.2.連線管理機制	27	行動應用程式應避免使用具有規則性之交談識別碼。
	28	行動應用程式應確認伺服器憑證之有效性。
	29	行動應用程式連線使用之伺服器憑證應為可信任之憑證機構所簽發。
4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	30	行動應用程式應避免含有惡意程式碼。
	31	行動應用程式應避免資訊安全漏洞。
4.1.5.2.行動應用程式完整性	32	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	33	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	34	行動應用程式應針對使用者於輸入階段之字串，進行安全檢查並提供相關注入攻擊防護機制。
4.2.2.1. Webview 安全檢測	35	行動應用程式應使用 Webview 與遠端伺服器進行網頁資源交換
	36	行動應用程式於 Webview 呈現功能時，所連線之網域應為安全網域