行動應用 App 基本資安規範V1.5 修改對照

孫宏民教授

資訊安全實驗室

國立清華大學資訊工程系

Outline

- 行動應用 App 基本資安規範V1.5修改前後對照

封面 修改部分

行動應用資安聯盟 中華民國 113 年 7 月	行動應用資安聯盟 中華民國 113 年 9 月

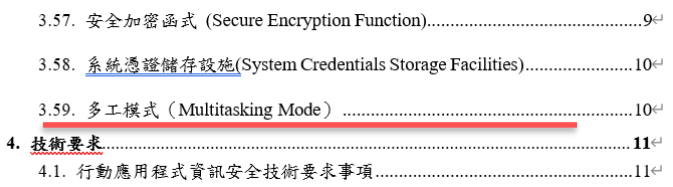
- 行動應用 App 基本資安規範V1.5 編修時間改為113年9月

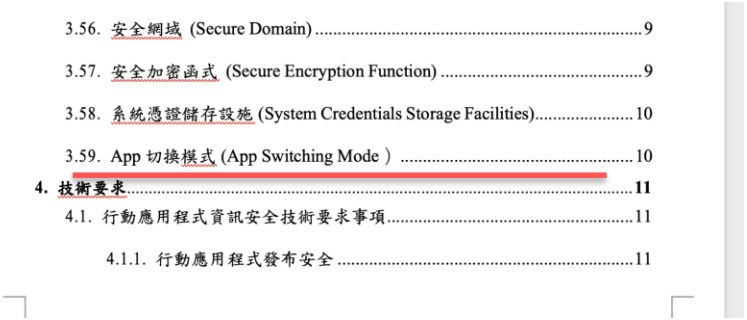
封面 修改部分

民國 113 年 7 月↵	行動應用 App 基本資安規範 V1.5↵
民國 113 年 9 月↵	行動應用 App 基本資安規範 V1.5↵

- 行動應用 App 基本資安規範V1.5 編修時間改為113年9月

修改目錄





- “多工模式”修改為”App 切換模式”

1. 前言 修改部分

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，惟部分程式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）。↵

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）。↵

- “程式開發者”修改為”行動應用App開發者”

1. 前言 修改部分

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

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

- 新增”（民國111年數位發展部數位產業署承接）”

3. 用語及定義 修改部分

▪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. 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：↵

- “經濟部標準檢驗局”修改為”教育部”

3.3 個人資料

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、帳戶餘額、社會活動。↵

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。↵

修改定義（刪除帳戶餘額）

3.4 敏感性資料

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~~通行碼~~密碼、金鑰、視訊、照片、通話、錄音檔、即時通訊訊息、通話~~紀錄~~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。

修改定義

3.5 密碼

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。↵

3.5. 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。

通行碼改成密碼、今後所有使用到通行碼之詞彙皆改為密碼

3.6 交易資源

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 可做為票券的憑證；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為使用者留下紀錄，以保障消費者權益。

修改定義

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。

新增 3.7 交易記錄，3.8 預授權交易

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。

新增定義

新增 3.10 JWT, 3.11 生物特徵身份鑑別, 3.12 一次性密碼

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。

新增定義

新增 3.16 網路釣魚，3.17 殭屍網路，3.18 間諜軟體，3.19 下載器

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。

新增定義

新增 3.21 螢幕覆蓋攻擊

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。↵

新增定義

新增 3.27 模擬器，3.28 USB 偵錯模式，3.29 偵錯模式

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，目的為方便開發人員透過 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，方便開發者對該行動應用程式進行偵錯。

新增定義

新增 3.31 常見弱點列舉

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。↵

新增定義

新增 3.33 身分鑑別

3.19. 身分鑑別（Authentication）

指對個體所宣稱之身分提供保證。

3.33. 身分鑑別（Authentication）↵

指對個體所宣稱之身分提供證明。↵

修改定義

新增 3.34 ChaCha20加密演算法

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。↵

新增定義

3.36 三重資料加密演算法

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

指一種乘積~~密碼法~~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。

修改定義

3.37 橢圓曲線加密演算法

3.22. 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，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。↵

3.37. 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。↵

修改定義標題

新增 3.41 加殼

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。

新增定義

新增 3.44. 系統日誌（System Logs）

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，用於開發者除錯應用程式、分析系統崩潰問題、以及系統維護。

新增定義

新增 3.45 裝置識別符

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。

3.45. 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, AAID）、iOS IDFA（Identifier for Advertisers, IDFA）及 Windows Phone Device ID。

修正縮寫

新增 3.48 處理間通信

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。

新增定義

3.55 安全亂數產生函式

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

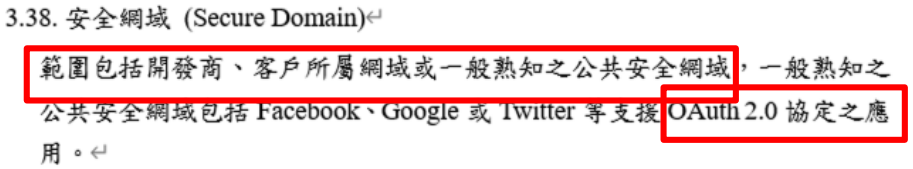
符合或引用 ANSI X9.17、FIPS 140-2、NIST SP 800-22 以及 SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項標準之亂數產生函式。↵

3.55. 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。↵

修改定義

3.56 安全網域


3.38. 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。↵


3.56. 安全網域 (Secure Domain)
一般熟知之公共安全網域包括Facebook、Google或Twitter。

刪除開發商、客戶所屬網域及OAuth2.0之敘述

3.57 安全加密函式

3.39. 安全加密函式 (Secure Encryption Function)↵

符合 FIPS 140-2 Annex A 之加密函式。↵

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。↵

修改定義

修改 3.59. App 切換模式（App Switching Mode）

3.59. 多工模式（Multitasking 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。

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。

修改定義名稱、定義

4.1.1.3. 行動應用程式安全性問題回報

4.1.1.3. 行動應用程式安全性問題回報

行動~~應用程式~~應用 App 開發者應提供回報安全性問題之管道。

行動~~應用程式~~應用 App 開發者應於適當期間內回覆問題並改善。

修改檢測項

4.1.2.2. 敏感性資料利用

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~~通行碼~~密碼認證，應主動提醒使用者設定較複雜之~~通行碼~~密碼。

行動應用程式應提醒使用者定期更改~~通行碼~~密碼。

修改檢測項

4.1.2.3.10. 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。

行動應用程式應適當使用系統憑證儲存設施儲存敏感性資料。

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。

4. 敏感性資料傳輸

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。

修改檢測項

4.1.2.3. 敏感性資料儲存

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~~適當使用~~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~~儲存敏感性資料~~。

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。

新增檢測項

4.1.2.4. 資料傳輸安全

4.1.2.4. 敏感性資料傳輸

針對「敏感性資料傳輸」之檢測項目，L1、L2、L3 行動應用程式於「4.1.2.4.1. 行動應用程式透過網路傳輸敏感性資料，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。」檢測結果須為「符合」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。

4.1.2.4.1. 行動應用程式透過網路傳輸敏感性資料，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

4.1.2.4 資料傳輸安全

針對「資料傳輸安全」之檢測項目，L1、L2、L3 行動應用程式於「4.1.2.4.1. 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。」檢測結果須為「符合」，始符合本資訊安全技術要求事項；否則未符合本資訊安全技術要求事項。根據 Mobile Application Security Testing Guide（MASTG）V1.7.0，禁止明文傳輸任何資料。

4.1.2.4.1. 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

修改標題，因OWASP規定所有傳輸皆須加密

4.1.3.1. 交易資源使用

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。

新增檢測項

4.1.3.2. 交易資源控管

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。

行動應用程式應記錄提供使用交易資源之交易資源與時間記錄。

行動應用程式應提供預授權交易之記錄。

修改及新增檢測項

4.1.4.2. 連線管理機制

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。

新增檢測項

4.1.5.1. 防範惡意程式碼與避免資訊安全漏洞

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。

新增檢測項

4.1.5.5. 防止動態分析及竄改

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 偵錯模式。

行動應用程式應將偵錯模式(Debug mode)設為關閉。

新增檢測項

4.2.2.1. Webview安全檢測

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。

修改檢測項名稱

6. 參考資料 修改部分

[5] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2019↵

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

- 更新 NIST 參考 URL

6. 參考資料 修改部分

歐洲

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

大陸

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

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

日本

[12] 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

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

- 刪除 大陸 參考資料

附錄一、技術要求事項與各國規範對照表

附錄一、技術要求事項與各國規範對照表

P 對應項目	美國 NIST [註 1]	歐洲 ENISA [註 2]	大陸 YD/T 2407-2013 [註 3]
chitecture, and threat ing	Executive Summary	9. Secure software distribution	5.5.2 應用軟件安全認證機制要求
chitecture, and threat ing	Executive Summary	9. Secure software distribution	5.5.4 預置應用軟件安全要求
	Executive Summary	9. Secure software distribution	5.5.4 預置應用軟件安全要求
chitecture, and threat ing	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
ta Storage and	4. Mobile App	1. Identify and protect	5.5.4 預置應用軟件安

附錄一、技術要求事項與各國規範對照表

[	OWASP對應項目	美國NIST [註1]	歐洲ENISA [註2]
用程式	MASVS-PLATFORM	Executive Summary	9. Secure software distribution
用程式	MASVS-PLATFORM	Executive Summary	9. Secure software distribution
用程式報	N/A	Executive Summary	9. Secure software distribution
資料蒐	MASVS-STORAGE	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data
資料利	MASVS-STORAGE	4. Mobile App	1. Identify and protect

- 更新OWASP對應項目
- 刪除大陸YD/T 2407-2013

附錄二、技術要求事項參考檢核表

新增檢測項

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
38. 行動應用程式應於交易收款時主動通知使用者
41. 行動應用程式應提供預授權交易之記錄
47. 行動應用程式封包流向應與所宣告的內容一致
50. 行動應用程式應針對螢幕覆蓋攻擊進行防護
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偵錯模式
63. 行動應用程式應將偵錯模式(Debug mode)設為關閉