行動應用App基本資安檢測基準V3.1

WHY ???

妳你的行動裝置好玩嗎？好用嗎？

- 行動裝置的使用愈來愈多
- 行動裝置上的App愈來愈好用好玩
  (看看妳你的阿公阿嬤玩LINE就知道)
- 除了妳你認知的功能外，它們是否安分守己？不會偷偷的去做某些妳你未認知的事？

妳你的App可能很不安全

- 它們可能偷偷的將妳你的親密照片、機敏資料送給某一server
- 這技術，一個資工資管系大三大四學生就能做到
- 這不是科幻電影情節，這是現在進行式

背景說明

國人日益關心智慧型手機應用程式(App)資訊安全

– 台灣地區每天約有 4000 多部手機中毒遭駭

– 嚴重者可能造成民眾的財務損失

政府注意到這件事了：

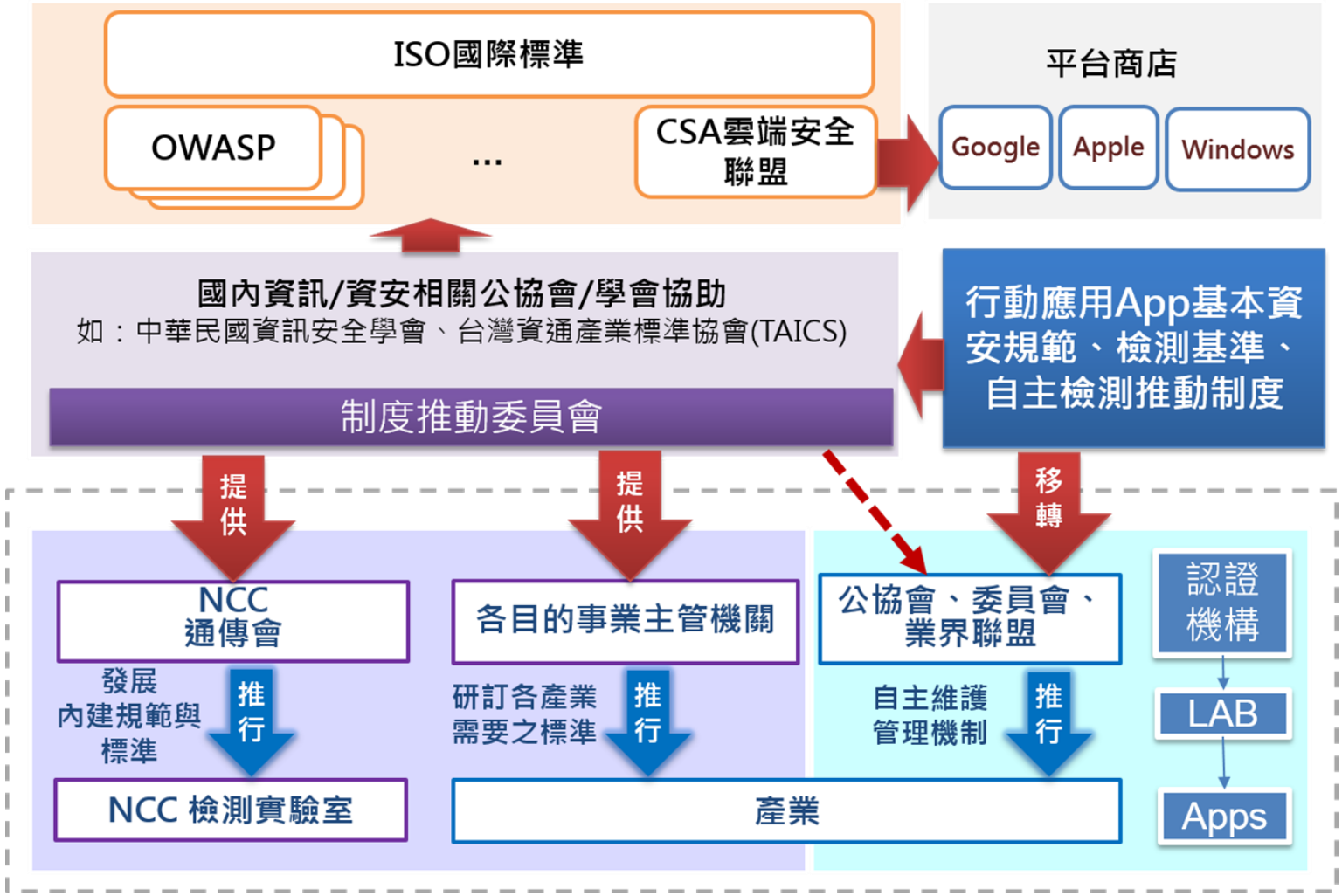
行政院國家資通安全會報於 103 年第 26 次委員會決議

手機應用軟體由經濟部工業局主責：

– 資安檢測標準制訂

– 鼓勵廠商自主驗證

推動架構


ISO國際標準
OWASP
...
CSA雲端安全聯盟
平台商店
Google
Apple
Windows
國內資訊/資安相關公協會/學會協助
如：中華民國資訊安全學會、台灣資通產業標準協會(TAICS)
制度推動委員會
行動應用App基本資安規範、檢測基準、自主檢測推動制度
提供
提供
移轉
NCC 通傳會
發展內建規範與標準
推行
NCC 檢測實驗室
各目的事業主管機關
研訂各產業需要之標準
推行
公協會、委員會、業界聯盟
自主維護管理機制
推行
產業
認證機構
LAB
Apps

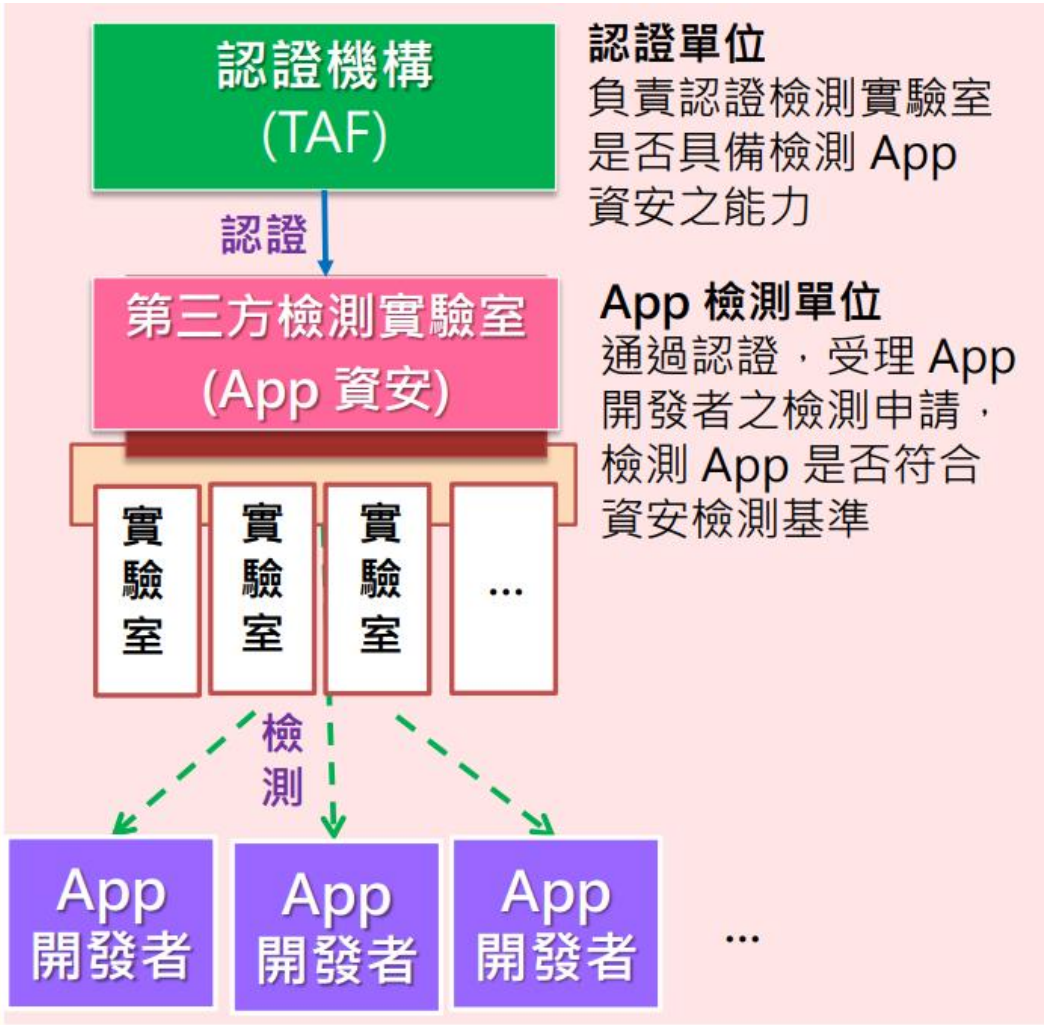
推動制度

主管機關

經濟部
工業局

運作檢測制度及標章管理

行動應用資安聯盟
(行動應用資安制度推動委員會)



認證單位
負責認證檢測實驗室是否具備檢測 App 資安之能力

App 檢測單位
通過認證，受理 App 開發者之檢測申請，檢測 App 是否符合資安檢測基準

TAF：財團法人全國認證基金會

APP 檢測實驗室認證

財團法人全國認證基金會(TAF)於 105 年 1 月正式公告受理檢測實驗室申請，截至 107年10月11日止，已有 11 家實驗室通過 TAF「行動應用 APP 基本資安檢測實驗室認證服務計畫」，成為 TAF 認可之「行動應用 App 基本資安檢測實驗室」，如下：

實驗室認證編號	機構名稱	實驗室名稱	TAF認可日期	聯絡人姓名	聯絡人電話
3016	鑒真數位有限公司	鑒真數位鑑識實驗室	2016/07/07	藍先生	(02)2517-2532#150
2918	勤業眾信聯合會計師事務所	資安科技暨鑑識分析中心	2016/07/07	陳先生	(02)2725-9988#7807
0263	中華電信股份有限公司電信研究院	測試中心	2016/08/02	羅小姐	(03)424-4540
3102	安華聯網科技股份有限公司	資安檢測實驗室	2017/01/24	劉先生	(02)8911-5035#371
3302	行動檢測服務股份有限公司	APP檢測實驗室	2017/02/23	林先生	(02)2226-6668
3325	財團法人台灣電子檢驗中心	資通訊檢測實驗室	2017/04/25	陳先生	(03)328-0026#559
3334	安碁資訊股份有限公司	數位鑑識中心實驗室	2017/07/21	鄭小姐	(02)2784-1000#6038
3336	安侯企業管理股份有限公司	數位科技安全實驗室	2017/11/23	林先生	(02)81016666#15320
1519	財團法人電信技術中心	資通安全檢測實驗室	2018/03/08	黃先生	(07)627-7067
3500	數聯資安股份有限公司	資通安全檢測實驗室	2018/07/24	鄭先生	(02)77008909
3496	關貿網路股份有限公司	關貿資安數位檢測中心	2018/10/11	蔡先生	(02)26551188#543

預期效益

- 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。

- 增進使用者對行動應用App之信賴度與使用意願：App開發者可參考相關規範，自主提升所開發之行動應用App安全品質以降低使用者對於App之安全性疑慮，創造App開發商與使用者雙贏局面。

- 提升我國行動應用App產品競爭力：藉由行動應用App基本資安自主檢測制度相關規範，加速App開發業者瞭解及參與App基本資安認證機制，以助於提升國內App產品的競爭力。

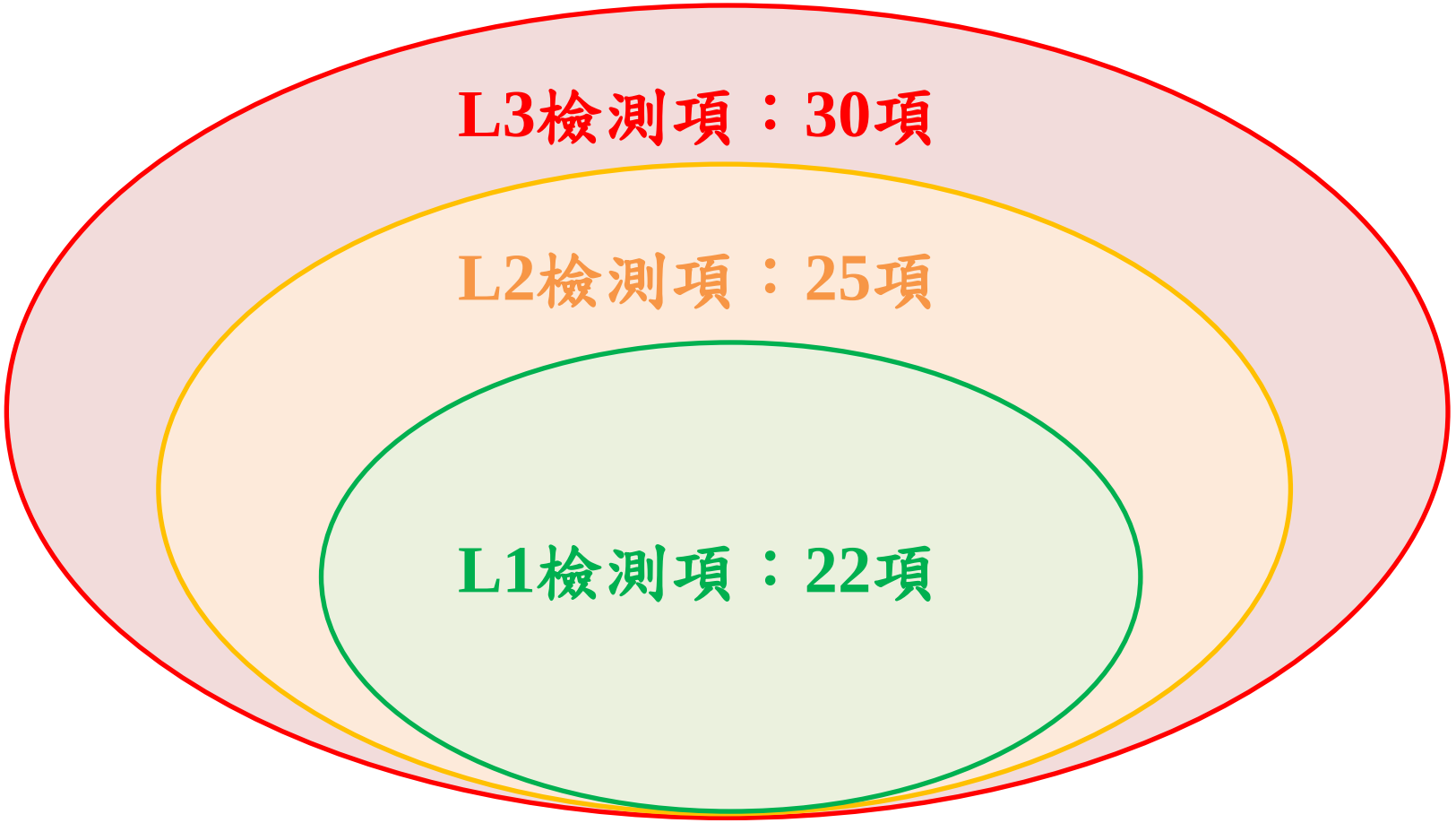
- 使我國行動應用App之資安開發環境更加完善：透過修訂相關規範與產官學研界等專業人士進行多場會議互相激盪，共同努力擘劃完善App資安發展環境，以塑造我國App資安品牌正面形象。

行動應用APP 基本資安檢測基準V3.1 修訂說明

重要變動

原內容	修訂後內容
甲類：無需使用者身分鑑別之行動應用程式。 乙類：需使用者身分鑑別之行動應用程式。 丙類: 含有交易行為之行動應用程式。	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。

行動應用App送測分類說明



用語與定義之注意事項

本規範之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。

Ex: Binary code → ~~二元碼、二進制碼~~
→ 二進位碼

行動應用App基本資安檢測基準版本沿革

日期	行動應用App基本資安檢測基準版本沿革	對應之行動應用App基本資安規範版本
民國104年8月	行動應用App基本資安檢測基準 V1.0	行動應用App基本資安規範 V1.0
民國105年2月	行動應用App基本資安檢測基準 V2.0	行動應用App基本資安規範 V1.0
民國106年3月	行動應用App基本資安檢測基準 V2.1	行動應用App基本資安規範 V1.1
民國107年5月	行動應用App基本資安檢測基準 V3.0	行動應用App基本資安規範 V1.2
民國108年9月	**行動應用App基本資安檢測基準 V3.1**	**行動應用App基本資安規範 V1.3**

檢測項目節錄（一）

檢測編號	4.1.1.1.2
檢測分類	L1、L2、L3 (原為乙級、丙級)
技術要求	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
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於可信任之應用程式商店，依實際需要說明欲存取之安全敏感性資料、行動裝置資源及宣告權限用途。 (刪除以下敘述: 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供欲存取之安全敏感性資料、行動裝置資源及宣告權限用途之說明。 如為「是」則符合檢測基準；「否」則不符合檢測基準)
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式不公開或尚未發布，則此項不須檢測
備註	須於「行動應用程式基本資料調查表」（附錄三、 行動應用App基本資安檢測資料調查表）自我宣告發布來源 應用程式商店之宣告以行動裝置之商店介面為主

檢測項目節錄（二）

檢測編號	4.1.1.3.1
檢測分類	L1、L2、L3 (原為乙級、丙級)
技術要求	行動應用程式開發者應提供回報安全性問題之管道
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內，提供聯絡網頁、留言板、電子郵件、電話或其他類型聯絡方式，並經測試可實際聯絡成功。 (刪除以下敘述: 若行動應用程式尚未發布或不公開發布，檢查調查表內是否有說明預計提供回報安全性問題之管道與聯絡方式。) 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準 不適用：行動應用程式不公開或尚未發布，則此項不須檢測
備註	應用程式商店之宣告以行動裝置之商店介面為主

檢測項目節錄（三）

檢測編號	4.1.2.3.1
檢測分類	L1、L2、L3 (原為乙級、丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內聲明。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2) 檢查行動應用程式是否於可信任之應用程式商店或行動應用程式內取得使用者同意。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準((刪除以下敘述: (3) 若行動應用程式尚未發布，檢查調查表內是否有說明預計於應用程式商店宣告之安全敏感性資料儲存聲明並取得使用者同意。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準)
檢測結果	(刪除以下敘述: 檢測規則： (一) 符合(1)、(2)之檢測基準 (二) 符合(3)之檢測基準 (三) 行動應用程式未儲存安全敏感性資料) 符合要求：符合所有檢測基準，或行動應用程式未儲存安全敏感性資料 不符合要求：任一檢測基準不符合 不適用：行動應用程式不公開或尚未發布，則此項不須檢測
備註	應用程式商店之宣告以行動裝置之商店介面為主

檢測項目節錄（四）

檢測編號	4.1.2.3.2
檢測分類	L1、L2、L3 (原為乙級、丙級)
技術要求	行動應用程式應提供使用者拒絕儲存安全敏感性資料之權利
檢測基準	(1) 檢查行動應用程式是否提供使用者拒絕儲存安全敏感性資料之選項。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2)檢查在使用者拒絕安全敏感性資料儲存的情況下，行動應用程式是否未儲存安全敏感性資料於行動裝置。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存安全敏感性資料 不符合要求：任一檢測基準不符合，或於檢測基準4.1.2.3.1之檢測結果因未聲明欲儲存之所有安全敏感性資料而不符合 不適用：行動應用程式不公開發布，則此項不須檢測
備註	於檢測基準4.1.2.3.1之檢測結果因未聲明欲儲存之所有安全敏感性資料，致使使用者無法對未聲明之安全敏感性資料行使拒絕權利

檢測項目節錄（五）

檢測編號	4.1.2.3.5
檢測分類	L3 (原為丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式是否未檢出將安全敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2) 檢查行動應用程式是否未檢出將安全敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (3) 檢查行動應用程式是否將安全敏感性資料儲存於冗餘檔案或日誌檔案且已用符合FIPS 140-2 Annex A 之安全之加密函式保護。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：檢測基準(1)、(2)皆符合或符合檢測基準(3) 不符合要求：檢測基準(1)或(2)不符合且檢測基準(3)不符合
備註	受作業系統保護之區域亦不可檢出

檢測項目節錄（六）

檢測編號	4.1.2.3.6
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式之非冗餘檔案及非日誌檔案內之安全敏感性資料是否採用金鑰有效長度為128位元（含）以上之先進加密標準（AES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2) 檢查行動應用程式之非冗餘檔案及非日誌檔案內之安全敏感性資料是否採用三重資料加密演算法（Triple DES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (3) 檢查行動應用程式所使用之加密函式之金鑰是否採用符合ANSI X9.17、FIPS 140-2、NIST SP 800-22及SP 800-90A (CAVP Testing: Random Number Generators) 至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合(1)或(2)任一檢測基準且符合(3)之檢測基準，或行動應用程式未儲存安全敏感性資料 不符合要求：檢測基準(1)、(2)皆不符合或檢測基準(3)不符合
備註	受作業系統保護之區域亦不可檢出

檢測項目節錄（七）

檢測編號	4.1.2.3.9
檢測分類	L3 (原為丙級)
技術要求	行動應用程式於非使用者主動擷取畫面時應主動警示使用者
檢測基準	檢查行動應用程式於非使用者主動擷取畫面時是否主動警示使用者。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	

檢測項目節錄（八）

檢測編號	4.1.2.4.1
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式是否採用TLS 1.1（含）以上版本加密協定傳輸安全敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2) 檢查行動應用程式是否採用金鑰有效長度為2048位元（含）以上之RSA加密演算法，或採用金鑰有效長度為224位元（含）以上之橢圓曲線加密演算法（Elliptic Curve Cryptography）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (3) 檢查行動應用程式是否採用金鑰有效長度為128位元（含）以上之進階加密標準（AES），或採用三重資料加密演算法（Triple DES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未傳輸安全敏感性資料 不符合要求：任一檢測基準不符合
備註	

檢測項目節錄（九）

檢測編號	4.1.3.1.1
檢測分類	L3 (原為丙級)
技術要求	行動應用程式應於使用交易資源時主動通知使用者
檢測基準	檢查行動應用程式內於交易時，是否主動通知使用者，且資訊至少包含交易資源名稱、金額及交易方式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	

檢測項目節錄（十）

檢測編號	4.1.3.2.2
檢測分類	L3(原為丙級)
技術要求	行動應用程式應記錄使用之交易資源與時間
檢測基準	檢查行動應用程式於交易後，是否提供查詢交易資源交易紀錄之管道，且交易資源交易紀錄至少包含交易資源名稱、交易時間及交易金額之記錄。如為「是」則符合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準(刪除以下敘述: 或行動應用程式無交易功能) 不符合要求：不符合檢測基準
備註	規範中所述之「交易資源與時間」於基準定義為「交易記錄」，即檢查行動應用程式是否提供交易記錄及記錄之內容

檢測項目節錄（十一）

檢測編號	4.1.4.2.2
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	行動應用程式應確認伺服器憑證之有效性
檢測基準	(1) 檢查行動應用程式使用之伺服器憑證是否仍於有效期間內、未被註銷（Revoke），且憑證之主體名稱與主體別名包含連線之伺服器網域名稱。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 (2) 檢查行動應用程式是否使用憑證綁定（Certificate Pinning）方式驗證，以確保連線之伺服器為行動應用程式開發者所指定。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或因行動應用程式不須傳輸安全敏感性資料因此未使用安全加密傳輸協定 不符合要求：任一檢測基準不符合
備註	

檢測項目節錄（十二）

檢測編號	4.1.4.2.3
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	行動應用程式應確認伺服器憑證為可信任之憑證機構、政府機關或企業所簽發
檢測基準	如行動應用程式使用安全加密傳輸協定，檢查行動應用程式是否驗證並確保伺服器憑證為行動作業系統內建可信任之憑證機構、政府機關、企業所簽發。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或因行動應用程式不須傳輸安全敏感性資料因此未使用安全加密傳輸協定 不符合要求：任一檢測基準不符合
備註	行動作業系統內建之可信任憑證機構：為行動作業系統廠商所安裝受信任之憑證簽發單位 若行動應用程式僅運用於封閉式內網連線，則企業自行簽發的憑證亦可視為可信任之憑證

檢測項目節錄（十三）

檢測編號	4.1.5.3.1
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式引用之函式庫是否不存在已知安全性漏洞。如為「是」則符合檢測基準；「否」則不符合檢測基準 (刪除以下敘述: (2) 檢查行動應用程式於安裝前，是否有於行動應用程式商店上之說明顯示警語建議使用者需安裝至最新作業系統版本。如為「是」則符合檢測基準；「否」則不符合檢測基準)
檢測結果	符合要求：符合檢測基準 不符合要求：不符合檢測基準
備註	不符合本項檢測基準之已知安全性漏洞，為具CVE編號且CVSS v3.0分數大於等於7(嚴重等級為High或Critical者)之漏洞。 須於「行動應用程式基本資料調查表」(附錄三、 行動應用App基本資安檢測資料調查表)自我宣告引用函式庫名稱及版本資訊

檢測項目節錄（十四）

檢測編號	4.2.2.1.2
檢測分類	L1、L2、L3 (原為甲級、乙級、丙級)
技術要求	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
檢測基準	(1) 檢查行動應用程式使用Webview呈現功能時，所連線之網域是否為安全網域且與開發商於資料調查表中宣稱實際所連線之網域一致。如為「是」則符合檢測基準；「否」則不符合檢測基準 (2) 檢查行動應用程式使用Webview呈現功能時，連線時是否進行憑證綁定。如為「是」則符合檢測基準；「否」則不符合檢測基準 (3) 檢查行動應用程式使用Webview呈現功能時，是否使用HTTPS連線。如為「是」則符合檢測基準；「否」則不符合檢測基準 (4) 檢查行動應用程式使用Webview呈現功能時，其伺服器弱點掃描須驗證Cross-Site Scripting 以及 Injection Flaws檢查是否全數通過。如為「是」則符合檢測基準；「否」則不符合檢測基準合檢測基準；「否」則不符合檢測基準
檢測結果	符合要求：符合檢測基準，或行動應用程式於Webview呈現功能時無連網，若連線並未傳輸敏感資料可不進行憑證綁定、HTTPS 連線 不符合要求：不符合任一檢測基準 不適用：行動應用程式無使用Webview呈現功能
備註	有關弱點掃描之詳細說明請參照「6. 補充說明 (一)」

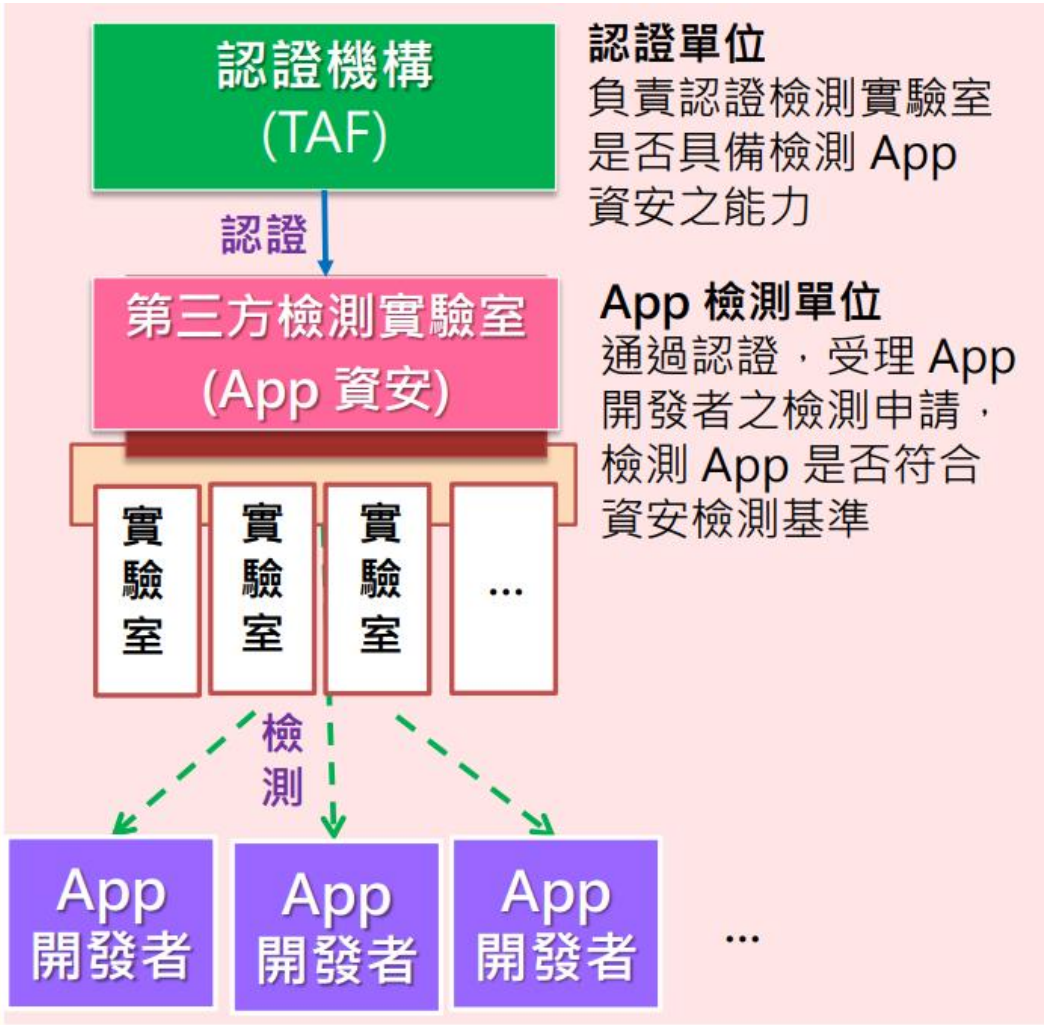
推動制度

主管機關

經濟部
工業局

運作檢測制度及標章管理

行動應用資安聯盟
(行動應用資安制度推動委員會)



認證單位
負責認證檢測實驗室是否具備檢測 App 資安之能力

App 檢測單位
通過認證，受理 App 開發者之檢測申請，檢測 App 是否符合資安檢測基準

TAF：財團法人全國認證基金會

檢測項問題與經驗分享

- Q：
  - L1、L2、L3三類，是由誰所訂定該送測App之類別？
- A：
  - App送測時，需由廠商自行於宣告表中勾選所屬類別，實驗室檢測前需驗證及判斷是否符合其所宣告之類別。

檢測項問題與經驗分享

- Q：
  - L1不需做使用者身分鑑別，L2需要做使用者身分鑑別，對於需要做身分鑑別之App是否有其規範？
- A：
  - 如App中包含個人隱私或安全敏感性資料，皆需要做身分鑑別。

檢測項問題與經驗分享

- Q：
  - 報案之App中需要使用者輸入手機號碼，若一旦做了身分鑑別，此功能於即時性上就會受到影響，此狀況下是否沒辦法跳過檢測？
- A：
  - App的開發架構上可以調整，可讓App有註冊登入功能，或者是上級主管單位規範可不做身分鑑別即可不用實作之（此處主管單位應為內政部）。

檢測項問題與經驗分享

- Q：
  - 有關主管機關同意免身分識別及授權是否能提供更詳細之說明？
- A：
  - 如報案之App儲存了使用者的手機號碼及報案紀錄，手機號碼屬於使用者之個人，於網路上無法得知，所以屬於個人資料，同理報案紀錄也是，故需做身分識別，若主管機關同意此兩項資料不需做識別，則遵循主管機關之規範。

檢測項問題與經驗分享

- Q：
  - 重新定義之交易資源，指對價值物品交換之前提，但很多醫療機構並非對價值資源的交換，如至醫療機構看病並付費，是否也包含於交易資源中？
- A：
  - 是，凡是與實體或虛擬之金流有關之交易，皆屬於交易資源。

檢測項問題與經驗分享

- Q：
  - 若App有更版，僅加上幾個功能及內容，是否還需要送測？
- A：
  - 因只要有所改版，其Hash值就會有所更動，但所發給證書上亦會註明該送測App之Hash值，故仍舊需要重新送測，如只有小改版欲盡快得到送測結果，可由廠商及實驗室之間互相協調。

檢測項問題與經驗分享

- Q：
  - 目前許多App結合FB進行登入，是否也屬於身分鑑別？
- A：
  - 目前許多App皆使用OAuth 2.0協定之應用，即算是身分鑑別。

THANK YOU