App 檢測項目一致性決議事項彙編表

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
T0001	檢測基準	針對 App 應用程式商店中，App 開發商提供於開發人員的聯絡資訊及留言板，是否可算是提供回報安全性問題的管道？	App 應用程式商店中，App 開發商提供於開發人員的聯絡資訊及留言板，屬於「4.1.1.3.1.行動應用程式開發者應提供回報安全性問題之管道」中的連絡網頁，**若經測試可實際連絡成功，即可視為該 App 提供回報安全性問題的管道。**	4.1.1.3.1.	106/2/13
T0002	檢測基準	行動應用程式應針對使用者輸入之特殊字元，該欄位本身就會輸入特殊符號且無法限制字串長度？	針對欄位本身可輸入特殊字元，屬於「4.1.5.4.1.行動應用程式應針對使用者輸入之字串，進行安全檢查」的「(1)檢查行動應用程式是否針對預期使用者輸入之字串驗證型別。」若原本預期的輸入就可包含特殊字元，4.1.5.4.1(1)即符合檢測基準；另外無法限制字串長度的情況，目前不論是在資料庫的儲存或是表單的輸入，都應該有其上限。	4.1.5.4.1.	106/2/13
T0003	規範	若行動應用 App 內無實際金錢交易，而是透過其他網站儲存的點數購買東西是否算是第三類的 App？	在行動應用 App 中若非金流交易，就不算在第三類，以購買點數為例，金流發生在購買點數的時候，故以點數交換東西不算第三類。	內文	106/2/13
T0004	檢測基準	購買付費資源時，是否需要每次都要重新輸入密碼？或是允許在一定時間(如：15 分鐘內)內可不需輸入？	根據「4.1.3.2.1.行動應用程式應於使用付費資源前進行使用者認證」，應於付費時進行認證，於備註中對於「付費時」的	4.1.3.2.1. 4.1.3.2.2.	106/2/13

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
			定義為「檢查行動應用程式於付費前是否進行使用者認證」，故以基準的符規性來說，只要在付費前有使用者認證的程序即符合規範。建議廠商若要提供使用者一段時間內不需輸入，App 需提供使用者選擇是否該時間內不需輸入密碼，已符合未來基準修改方向。		
T0005	檢測基準	關於 App 檢測認定通過的版本，為行動應用程式商店上所顯示的版本為認定標準，還是 apk/ipa 算出來的 Hash 值作版本認定，此兩個基準以何者為正確？ 1.若以 Google play 商店或 App Store 上所顯示的版本為認定標準，廠商可以更改程式內容但 App 版本不變。 2.若以 apk/ipa 算出來的 Hash 值作版本認定版本，廠商在更改程式碼任一字元後，Hash 值所算出來的值就會不同，會認定為不同版本的 App。	由於檢測結果不符合基準事項之修正涉及複測議題，以檢測報告可信為前提下，修正後之 App 仍應重測，但考量實務之可行性，於複測時可採送測廠商切結方式處理，即送測廠商於複測時檢附具公司大小章之聲明書，內容聲明修正部分與修正後 App 版本，實驗室得就修正部分進行複測，待複測部分確認符合檢測基準要求後，實驗室針對修正後 App 版本發給合格證書。 送測廠商後續於 App 商店上架時，App 商店內及 App 程式內可查詢之版本資訊，應與合格證書記載之版本相同。關於 App 複測費用議題，建議實驗室可依合理性，預先研擬相關配套計費方式，或是於收件前與送測廠商協商雙方認可之合理費用。	內文	106/3/3

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
T0006	檢測基準	加密後的敏感性資料，應於多久的時間後清除才符合現行的 App 基本資安規範？	目前規範並未對於此要求，於 App 應用情境下，加密後的敏感性資料可設計於合理固定時間內自動或手動清除，惟此合理固定之時間應告知使用者，且應考量當加密後之敏感性資料不再需要使用時須進行刪除之設計。	4.1.2.	106/3/3
T0007	檢測基準	在遊戲購買商品裡面呼叫 Google 或 iOS，是算中級還是高級？	In-app Billing 與 In-App Purchase 的交易為行動作業系統內建之付費機制，故屬高級。	4.1.3.	106/3/7
T0008	檢測基準	根據規範 4.1.4.2.4.的說明，如不符合檢測編號 4.1.4.2.2.或 4.1.4.2.3.之技術要求,檢查行動應用程式是否未與伺服器進行連線與傳輸敏感性資料。 ● 是否有傳送機敏資料的連線才需實作憑證綁定機制，如果未傳輸機敏資料原本 4.1.4.2.2.與 4.1.4.2.3.的 FAIL 會變成 PASS。 若未傳輸機敏資料，只有 4.1.4.2.4.是 PASS，4.1.4.2.2.與 4.1.4.2.3.仍為 FAIL	若未傳輸敏感性資料，為符合檢測項目 4.1.4.2.4.之要求；若有使用了 TLS 加密協定，不論是否傳輸敏感性資料，即應符合 4.1.4.2.2.與 4.1.4.2.3.。	4.1.4.2.2. 4.1.4.2.3. 4.1.4.2.4.	106/3/7
T0009	檢測基準	有關「4.1.3.2.1.行動程式應於使用付費資源前進行使用者認證」測項，App 開發商詢問其 App 在使用所有功能前，已要求使用者登入帳號，在此前提下是否已符合此條測項規範，或須強制於付費	在使用 App 付費功能前，**任何時機點進行身分認證**，已符合「4.1.3.2.1 行動程式應於使用付費資源前進行使用者認證」之要求，**但為強化交易安全之嚴謹性，實驗室可建議廠商於進行付費行為的前**	4.1.3.2.1.	106/3/16

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		時再次做使用者的身分認證？	**一步驟，再次進行使用者身分確認。**		
T0010	制度	請問實驗室要發出合格證明證書，需要檢測項目全部符合，若檢測項目有不適用的情形，是否可以發布合格證明？	**需要檢測項目全部符合，實驗室才可核發合格證明。** 若檢測項目有不適用，如 App 還未上線，沒有實際交易行為可供實驗室進行檢測，應請廠商提供切結書或聲明書(廠商需蓋大小章)，說明 App 是採用 Google 的 In-app Billing 做為付費管道，檢測報告結果標示為符合，發布合格證明。實驗室需在 App 上線後再進行追蹤檢測，如檢測結果不符合，可撤銷其合格證明。	第三部分	106/4/7
T0011	檢測基準	針對金管會要求各銀行業者送行動網銀 App 進行檢測時，未進行開戶，導致部份須權限之功能無法得到測試。	未進行開戶的部分，由於是金管會要求送測，應請送測廠商提供測試所需之相關資訊，如帳號密碼等，以進行測試。	內文	106/4/7
T0012	檢測基準	「4.1.2.3.7.敏感性資料應避免出現於行動應用程式之程式碼 (arcgis username password)」測到廠商使用地圖元件時出現敏感性資料，但此地圖元件為第三方 Library 驗證機制？	開發商使用第三方 Library 應該盡到確保第三方 Library 沒有安全疑慮的義務，應請廠商向第三方 Library 廠商提出此問題，並請第三方 Library 廠商修改，或是請廠商改用其他 Library，若是廠商使用的第三方 Library 有問題，則廠商的 App 無法符合檢測基準。	4.1.3.	106/4/7
T0013	制度	關於金融業部分所提及行動應用 APP 之檢測項目，能否至測試環境進行檢測作業?	檢測實驗室須請送測單位提供測試帳號，至實際環境下進行檢測作業，通過後方可發放檢測合格證書。	第一部份	106/4/17

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		● 許多金流交易(如銀行常見的電子錢包交易、行動支付、證券下單等行動應用 APP)，其交易帳號需要使用真實身分才能登入檢測，惟實務上無法全面使用正式環境進行測試(可能受限無端末設備、無法進行開戶作業或客戶怕會擾亂其金融秩序等考量)，部份情況需至客戶端的上版/測試環境才能進行，故想請問能否同意金融業的檢測項目，可於銀行的正式測試/上版環境裡進行檢測作業？	若送測單位無法提供測試帳號或有其他需求，可進行檢測並出具測試報告，並須述明於非實際環境下所進行檢測，且不可發放檢測合格證書。		
T0014	制度	有時在客戶的測試環境內，受檢測 APP 因開發時程或版本管控等原因，致使該 APP 是處在已上線 APP 版號之前(非目前正式上架版號，但客戶使用之程式碼主體不變，僅做些微調整與修改，如連線 IP 等)，請問 秘書組能否接受客戶提出背書之證明文件(如聲明並確保與架上版本的行動應用 APP 程式碼相同)?	1. 可由送測單位說明原委，並簽署聲明文件及切結書(如聲明並確保與架上版本的行動應用 App 程式碼相同)，且要送原檢測實驗室檢測。如前述聲明文件，有造假情事或不符事實，須由送測單位承擔法律責任並賠償之責。 檢測實驗室依據送測單位之改版 App 聲明文件內容，可依前次送測差異部分進行檢測，且於檢測報告內需註明本次檢測項目，及引用前次 App 版本已通過之檢測項目，及檢附前次通過 App 版本測	第一部份	106/4/24

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
			試報告為佐證附件。		
T0015	檢測基準	在 App 檢測基準中，4.1.2.1.2.、4.1.2.3.2.、4.1.2.5.2.及 4.1.3.1.2.等檢測基準皆要求行動應用程式需提供使用者拒絕之權利，請問是否需明確於行動應用程式畫面出現"拒絕"選項才視為符合，若是就以下二種情況其判定應為符合或不符合? 1.行動應用程式在敏感性資料聲明選項要求使用者打勾才視為使用者同意，未打勾者視為不同意，是否符合"拒絕"之定義 2.Google Play 本身在付費時未明確提供"拒絕"選項 (Apple 的有)，但使用者可以透過點選作業系統本身的返回鍵回到上一頁，是否符合"拒絕"之定義？ ● 建議作法可能問題或影響： 以 Google Play 機制為例，開發廠商無法調整 Google Play 顯示的畫面內容，若是需要明確有"拒絕"選項，可能會導致 Android 遊戲無法通過；或者是遊戲廠商需另外再產生同意/拒絕的選項給使用者點選後，再帶出 Google Play。	1. 實驗室應該以使用者角度出發進行判斷，該測試標的是否有允許使用者表達拒絕的權利(若是提供拒絕選項，但是使用者拒絕後仍然進行該操作也是違反使用者拒絕的權利)，故不強制限定拒絕之形式，未來基準修訂會如「提供使用者拒絕.....之『功能』」的方向進行修改而非「提供使用者拒絕.....之『選項』」，避免造成誤會。 2. 本基準所述拒絕之權利，指使用者可於進入付費畫面後，可經由具有返回功能之按鈕或點擊付費視窗以外之區域回到付費前頁面，而非需要關閉應用程式後重新開啟，其他拒絕的判斷依據同第 1 點。	4.1.2.	106/4/24

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		● 調整意見說明(或論述理由)： 建議跟提供使用者拒絕權利相關之檢測基準，不需明確有"拒絕"選項，行動應用程式可以透過其他方式取消付費流程，回到付費前的畫面(狀況 2)或者是讓使用者可以有選擇的權利(狀況 1)，即可符合"拒絕"的精神；其他方式包括：行動應用程式畫面內的返回按鈕、作業系統本身之返回鍵(Android)，但不包括作業系統本身的 Home 鍵(回到桌面關閉應用程式重新開啟進入行動應用程式)			
T0016	制度	針對因受測App改版次數頻繁造成成本增加，同意送測單位在App改版幅度不大者，針對部分修改處進行檢測作業。	1. 可由送測單位提供App改版內容與前次送測差異，並簽署聲明文件及切結書，且要送原檢測實驗室檢測。如前述聲明文件，有造假情事或不符事實，須由送測單位承擔法律責任並賠償之責。 2. 檢測實驗室依據送測單位之改版 App 聲明文件內容，可依前次送測差異部分進行檢測，且於檢測報告內需註明本次檢測項目，及引用前次 App 版本已通過之檢測項目，及檢附前次通過 App 版本測試報告為佐證附件。	第一部分	106/4/21

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
T0017	規範	針對若受測App為已經加殼軟體處理過	1. 檢測實驗室須依據App檢測基準所規範檢測項目逐項進行檢測，且App開發商應提供未加殼前App軟體進行測試，檢測通過後將出具未加殼前App軟體檢測合格證明，建議App開發商可於App資安檢測通過後再進行加殼服務，並須取得經加殼服務後，App軟體前後一致證明。 2. App開發商如使用App加殼服務，向聯盟申請MAS標章時，須同時提供未加殼前檢測合格證明，及加殼服務後App軟體前後一致證明。 3. 檢測實驗室須依據App檢測基準所規範檢測項目逐項進行檢測，不可因是否有加殼或其他特定App因素，而減少任何應檢測項目。 2. 檢測實驗室若有其他技術因素導致無法檢出是否符合檢測基準要求，僅可出具檢測報告，不可出具檢測合格證明。		106/5/11
T0018	制度	針對「行政院資安處」規定之16項App資安檢測項目，檢測實驗室是否可進行	針對「行政院資安處」規定之 16 項 App 資安檢測項目，檢測實驗室可進行檢測	第一部分	106/5/4

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		檢測。	並出具測試報告。但因未完整涵蓋 App 基本資安檢測基準中，所定義初級、中級、高級檢測項目，故不可出具「行動應用 App 基本資安檢測合格證明」。且於檢測報告中，註明為依據「行政院資安處」16 項 App 資安檢測規定檢測。		
T0019	檢測基準	針對進行App資安檢測時，無法繞過憑證綁定限制，使得部分測試項目執行無法繞過事宜，決議作法如下：	1. 如App軟體傳輸與後台傳輸資料，若無傳輸敏感性資料，無須綁定憑證。 2. 如App軟體已憑證綁定且無法於測試時繞過憑證綁定，依據目前檢測基準V2.1規格，因無法有效檢測所傳輸資料，於檢測報告中標示為未檢出（符合檢測基準）；此部分僅依由App開發商於送測時宣告	4.1.4	106/5/11
T0020	檢測基準	檢測對稱式金鑰之長度是否符合規定。如 App 沒有對稱式加密之需要(不須儲存敏感性資料，亦不需要從伺服器端下載敏感性資料)。則是否該檢測項目只需要填未檢出(符合基準)。	如有敏感性資料傳輸，則勢必有對稱式加密，理應會有驗出。	4.1.2.4.1	106/8/15
T0021	檢測	4.1.2.3.4.應避免將敏感性資料儲存於暫	網頁快取部分不可驗出。	4.1.2.3.4	106/5/11

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
	基準	存檔或紀錄檔中」，若為網頁快取相關資料，是否可排除？		4.1.2.3.5	
T0022	檢測基準	4.1.2.3.5 規定，所有儲存於手機之敏感性資料，應以 AES 或 Triple DES 加密。然 4.1.2.3.7 中規定，程式碼中不得檢出對稱式加密之金鑰。此兩項規定似乎無法同時達到。	對稱式加密之金鑰可以打散，或者依照一些特性產生，不一定要連網獲得。	4.1.2.3.5 4.1.2.3.7	106/08/15
T0023	檢測基準	4.1.2.3.4 未針對冗餘檔案進行定義，會混淆實驗室檢測進行判斷	冗餘檔案定義為：移出時不影響 App 運作之檔案。 2.暫存檔與 log 檔案一定不可驗出敏感性資料。	4.1.2.3.4	106/12/25
T0024	檢測基準	行動應用程式應針對使用者輸入之字串安全檢查，可分為 Client 端檢測或 Server 端檢查，檢測標準應以哪一端之檢測結果為主?	應以Client 的檢測結果為主。如 Server 端有問題，則請實驗室建議 App 開發商修正，此部分先不修正規定。	4.1.5.4.1 4.1.5.4.2	106/12/25
T0025	檢測基準	4.1.2.3.1 行動應用程式應於儲存敏感性資料前，取得使用者同意，若 App 開發者有進行加密處理，而未能辨識之時，是否認定為符合?	如果 App 廠商已有宣告，那麼就算是有儲存。若廠商無宣告，但實驗室判斷為有檢出，則為有儲存。	4.1.2.3.1	106/12/25
T0026	檢測基準	4.1.5.3.1 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。	若 App 開發商已於宣告書中提供所引用函式庫名稱及版本資訊，則可以 App 開	4.1.5.3.1	106/12/25

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		是否可參考 App 開發商所提之宣告書?是否仍須檢視程式碼內容?	發商所宣告之內容為主。		
T0027	檢測基準	App 所連向之後端伺服器的相關設定若有變動，可能會導致檢測結果與先前不同，此時該如何處置?	建議實驗室與檢測時，留下檢測紀錄，避免未來有爭議。	4.1.2.1.1 4.1.2.3.1 4.1.5.4	106/12/25
T0028	檢測基準	關於檢測編號 4.1.2.4.1 行動應用程式敏感性資料傳輸問題，於實際檢測作業上，發現存在一部分行動應用程式會使用特殊 Port 進行連線,且其傳輸敏感性資料亦有進行安全等級之加密(從實際檢測的角度上確實未檢出傳輸敏感性資料)。但目前上述情形因該行動應用程式未使用安全加密傳輸協定(TLS),故在規範下會被判定為不符合。	要求能夠提供獨立第三方來驗證其安全加密傳輸協定，如通過 CC 或 FIPS-140-2。	4.1.2.4.1	106/12/25
T0029	規範	行動應用程式欲存取之敏感性資料是否必須逐項明確列出?或可以用概括式描述	個人資料定義範圍太廣，盡量逐項明確表列為原則。	內文	107/4/3
T0030	檢測基準	(1)行動應用程式“取得使用者同意”是否一定要有明確的使用者動作表示，例如：按下同意或拒絕按鍵；或僅為聲明內容之意思表示即可(例如：”安裝本程式即表示同意隱私權政策”)?	1. 可以以彈跳式視窗取得使用者同意。但彈跳式視窗的方式是加分作用，建議還是以聲明書為主。開發商需告知與說明，所要的敏感性資料及權限之用途。除告知使用者外，亦確認開發商明確知道該敏感性資料及權限為開發商所	4.1.2.1.1 4.1.2.1.2 4.1.2.3.1 4.1.2.3.2 4.1.2.5.1 4.1.2.5.2 4.1.3.1.1 4.1.3.1.2	107/4/3

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		(2).承(1)，若須有明確的使用者動作表示同意或拒絕，則行動應用程式是否必須確保使用者先看過聲明，才能執行該動作? (3).若行動應用程式於蒐集、儲存、分享前，以彈出式對話視窗，是否可視為行動應用程式內之聲明，並取得使用者同意或拒絕?	預期。 2. 個人及敏感性資料的蒐集、儲存、分享等聲明標準目前是以本國為主。若要將歐盟的標準納入，此問題牽涉到法律問題，將交由法律專家確認。		
T0031	檢測基準	建議於 4.1.4.2.4 基準要求(2) 納入以下考量：於檢測編號 4.1.4.2.2 與 4.1.4.2.3 為符合，但可能因憑證綁定未檢出傳輸敏感性資料。	雖有憑證綁定之限制，但仍應儘可能嘗試測試檢出傳輸敏感性資料。	4.1.4	107/4/3
T0032	檢測基準	在尚未檢測通過前，未了避免頻繁更新造成使用者的體驗變差，所以暫不將 APP 上架至正式環境，於檢測編號 4.1.4.2.3 內的備註中，有一條有關憑證簽發單位的說明，請問遠傳電信簽發之企業憑證，是否可符合「3.企業：企業自行成立之憑證簽發單位」的條件。此憑證為正式環境的憑證，且目前已是公發且受信任的憑證單位簽發。	因使用非CA 上的憑證會產生中間人攻擊法。發證書的Hash 值與將上架App Hash 將會不一致，以至於上架之App 與通過驗證之App 不同。仍依據標準執行檢測。	4.1.4.2.3	107/4/3
T0033	規範	安全敏感性資料以及個人資料內包含「但不限於」字眼，無法以白名單式明	若有對於資料定義有疑問可向聯盟提出，由聯盟決議後舉列白名單。	內文	107/4/3

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		確列舉定義，容易有模糊地帶，安全敏感性資料及個人資料之明確，提請討論。			
T0034	規範	通常希望行動裝置提供身分認證機制，是擔心攻擊者若拿到原用戶的行動裝置，可能在未授權的情況下，從行動裝置取得原用戶的個人資料。但於安全敏感性資料定義之即時通訊訊息、筆記、備忘錄、通訊錄、地理位置、行事曆、通話紀錄及簡訊.....等，若用行動裝置原生軟體也能取得原用戶的資料。於實務上似乎沒有提供身分鑑別的意義，有時甚至影響到使用者體驗，如此是否有必要做身分鑑別機制，提請討論。	除了即時的地理位置外，地理位置歷史紀錄及其它資料皆有必要做身分鑑別機制。	內文	107/4/3
T0035	規範	未有安全敏感性資料的蒐集及儲存符合條件之定義，提請討論。	有存取便屬於蒐集，儲存於本地空間內即屬儲存。	內文	107/8/28
T0036	檢測基準	於檢測基準4.1.1.1.2、4.1.1.3.1、4.1.2.1.1、4.1.2.3.1、4.1.2.5.2，行動應用程式不公開及尚未發布似乎未有一致性，其差異性及試用時機提請詳細說明。另於「行動應用程式內」發	因4.1.1 之檢測基準標題為「行動應用程式發布安全」，所以若未公開或未發佈，必須為「不適用」，其他項可選擇「不適用」或「符合」。	4.1.2.1.1 4.1.2.1.2 4.1.2.3.1 4.1.2.5.1 4.1.2.5.2 4.1.5.4.1	107/8/28

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		佈聲明，是否可判為符合，提請討論。		4.1.5.4.2	
T0037	檢測基準	明確定義此項發生的時機，是使用者主動截取畫面或是APP 本身或其他執行中的APP 截取畫面。若是使用者主動截取畫面，此動作是在受測APP"外部"的行為，是否需要主動警示， 提請討論。	若偵測到其他執行中之程式擷取畫面，則需警示	4.1.2.3.9	107/8/28
T0038	檢測基準	檢測基準4.1.4.2.3 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。依目前定義，則若為送測單位內部的企業CA 自行簽發的憑證或 GCA 的憑證，因不屬於行動作業系統廠商所安裝受信任之憑證簽發單位，應如何判定，提請討論	檢測基準中明指憑證簽發機構須為簽發憑證之機關、法人，若尚有疑問可由聯盟列舉白名單。	4.1.4.2.3	107/8/28
T0039	規範	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。 這邊之前有個疑問是對於股票下單的	如股票下單等有風險的敏感操作行為，需要為使用者留下紀錄，以保障消費者權益。	內文	107/8/28

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		界定，因為下單這動作不一定會造成交易。股票下單是 否屬於交易，提請討論。			
T0040	檢測基準	第二次之後的交易不須再身分鑑別，首次、第二次的明確定義，提請討論	若為同一連線內不須再做身分鑑別，若 Session 改變，便須再做身分鑑別。	4.1.4.2.2 4.1.4.2.3 4.1.4.2.4	107/8/28
T0041	檢測基準	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。根據先前的一致性會議此項僅要求於用戶端驗證(伺服器端不強制)，但理論上會將安全檢查做於伺服器端更加安全。	用戶端也是會有SQL Injection 的問題，所以還是須要求用戶端驗證，長度驗證的問題再另行研議。	4.1.5.4.2	107/8/28
T0042	檢測基準	行動應用程式本身需要接收網頁post的值，但因webview 須作憑證綁定以及https，便無法擷取post的資料，相關做法提請討論。	Webview 使用https 傳輸資料，也是OWASP MASVS 6.6 的要求，可請開發商以其他方式實作。	4.2.2.1.2	107/8/28
T0043	檢測基準	Webview 之檢測，伺服器弱點掃描指的是 "系統弱點掃描"還是"網站弱點掃描"，且必須全數通過於實務上很難做到。各實驗室必須提供伺服器端之弱點掃描資訊，其中弱點掃描對應 之檢測項目中所謂的對應項目定義不清。	Webview 所連到的頁面須做弱點掃描，須驗證Cross-Site Scripting 以及 Injection Flaws。	4.2.2.1.2	107/8/28
T0044	檢測	Webview 若無傳輸安全敏感性資料，	一般熟知之公共安全網域可由聯盟舉列	4.2.2.1.2	107/8/28

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
	基準	認為沒有做到憑證綁定或https 之必要。且安全網域，如檢測基準描述應支援OAuth 2.0，是否可以此作為webview之檢測結果。而未支援OAuth 2.0 的一般熟知之公共安全網域是否就不符合安全網域的定義，提請討論	白名單，以此判定其安全性。		
T0045	檢測基準	Intent Injection 改為IPC Injection，但iOS 目前似乎不太容易做到實質意義的IPC，能否以iOS 並無IPC 議題作為檢測結果，提請討論。	以靜態檢測看其是否有使用IPC 相關的function。	4.1.5.4.2	107/8/28
T0046	檢測基準	檢測項目4.1.5.3.1(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。 1. 行動應用程式於行動應用程式商店上的敘述，若牽涉到非行動應用程式本身、或有妨礙到使用者行為自主權時，很有可能不符合iOS App Store 的平台規範，進而造成應用程式遭下架處置，此風險亦存在於Android Google play 平台。 2. 此基準無「不公開發布」時的不適用條件，若App 為「不公開發布」該如	請聯盟明定iOS(8.0)/Android(5.0)最低安裝版本，將來可列在要點或細則內。	4.1.5.3.1	107/8/28

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		何於行動應用商店上說明？ 3. 在檢測時只有這個項目不通過，但 Apple Store 只能上新程式時才能修改描述，程式沒有更改，描述也無法更改。 以上問題提請討論。			
T0047	檢測基準	1. 行動應用程式使用 Webview 呈現功能時，若連線並未傳輸敏感資料(如：廣告或新聞頁面)，是否可不進行憑證綁定、HTTPS 連線與伺服器弱點檢測。 2. 若行動應用程式使用 Webview 連到外部網站(如：Yahoo 或某某訂票網、某某金流結帳頁面)，如何做弱點掃描？若掃出弱點又如何令其修改？ 3. 若連線之伺服器本身已做過滲透測試，是否可以出具滲透測試報告證明，以符合檢測標準。 4. 弱點掃描之安全等級通過基準為何？ 以上問題提請討論。	1. 若連線並未傳輸敏感資料可不進行憑證綁定、HTTPS 連線。 2. 滲所有第一層之連結均需附弱點掃描報告。 3. 滲透測試報告不可等同於弱點掃描結果。	4.2.2.1.2	107/8/28
T0048	檢測基準	不公開發布App 若採VPN 方式連線，雖採HTTPS 但憑證為企業內部自簽，4.1.2.4.1 和憑證相關測項	內部使用的App 走這種Citrix 或類VPN 環境，企業可於調查表中宣告自簽憑	4.1.2.4.1 4.1.4.2.2 4.1.4.2.3	107/8/28

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		4.1.4.2.2、4.1.4.2.3、4.1.4.2.4 應如何判定？	證，並由檢測實驗室比對。	4.1.4.2.4	
T0049	檢測基準	App 於檢測時發現會在共享區域（/sdcard/SPen/Images/）之下儲存案件影像，包括個人電子簽名在內，自手機匯出後可直接檢視內容，但App 開發商表示由於權限之故，無法對儲存在前述路徑下的檔案進行加密等處理，如何判定通過與否，提請討論。	App 不應將電子簽名等敏感性資料放置無法控制之共享區內。	4.1.2.3.9	107/8/28
T0050	檢測基準	此測項4.1.2.3.9 檢測目的如下： 1. 不禁止使用者使用任何方式自行截圖 2. 使用者非自行截圖時，有警示 3. 不會在非使用者的操作下被截圖 4. 但根據開發廠商回饋，要讓非使用者操作下的情況下無法截圖，也會讓使用者自己也無法截圖。有鑑於「使用者可以截圖」是常見的使用需求，就開發商的立場，許多使用者，特別是年齡較高的族群，較常需要螢幕截圖功能輔助其使用，而為了通過規範達到不會在非使用者的操作下被截圖的目的，會讓開發商無法提供使用者自行截圖的商業	1. 實作部分可參考華南銀行，產生圖片附檔儲存。 2. 截圖限制可只限於包含敏感性資料之畫面。	4.1.2.3.9	107/12/26

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		邏輯，影響部分使用者的使用權利跟意願。			
T0051	規範	1. 銀行業者認為，因約定帳戶需臨櫃申請，又金管會電子銀行安控基準屬低風險交易，故不需要提供身分鑑別。則是否依據基準交易前是否需提供身分鑑別機制呢? 2. 如證券下單、搶標、搶票等應用，若要符合基準於交易前進行身分驗證會導致競爭上的劣勢，於實務上有不適之處，若要申請合格證明或標章，目前是否有配套措施可行? 以上問題提請討論。	1. 若約定帳戶於金管會電子銀行安控基準屬低風險交易，可不須提供身份鑑別。 2. 檢測基準明定，於第一次登入需進行身分鑑別，於同個連線內之交易行為，無需再做身分鑑別。	內文	107/12/26
T0052	檢測基準	1. App 提供使用者Google、Facebook 或 Advertising ID (裝置的ID)。App 會自動選擇先以使用者裝置的 ADID 建立並連結 User ID，使用者也可以主動選擇 Google 或Facebook 帳號連結 User ID。App 取得裝置ID 作為身份認證，但是此動作使用者在操作時並不會知道（沒有畫面顯示），是否也算是身份認證的一種？ 2. App 中個人相關敏感性資料，單純	1. App 會自動選擇先以使用者裝置的 ADID 建立並連結 User ID，不算是身份認證。 2. 單純提供資料，無交易行為並且無儲存於App 中便不需再做身份認證。 3. App 上傳個人相關敏感性資料甚至身分證正反面，無儲存於App 中，屬於註冊的過程。	4.1.4	107/12/26

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		使用在中獎後傳送姓名及獎品寄送地點，並無儲存於App 中是否還是需要做身份認證？ 3. App 可以上傳個人相關敏感性資料甚至身分證正反面，無儲存於App 中，是否還是需要做身份認證？驗證碼是否可以做為身份認證？ 以上提請討論。			
T0053	制度	憑證的有效期，可能因行政作業處理時常有差距，判定標準提請討論。	以實驗室檢測日期為審查依據。		107/12/26
T0054	規章	App內的交易機制為採用 Google Play, App Store或其他可信任之第三方支付軟體，或是App內僅提供收款功能，是否依然歸類於丙類，提請討論。	皆仍屬於丙類	內文	107/12/26
T0055	檢測基準	是否能讓使用者自主決定是否需要畫面擷圖警示。	須明確告知使用者其不安全性，提醒使用者須保護敏感資料。	4.1.2.3.9	107/12/26
T0056	檢測基準	實驗室與多家廠商合作，所以會嵌入很多活動頁的webview(如廣告頁面)，這些WebView更換頻繁，但仍需要交付弱點掃描報告，並須進行憑證綁定機制，導致檢測困難。此外，弱掃報告屬公司資訊資產，且若外流可能造成公司承擔	由檢測實驗室與開發商協議正向表列網域，實驗室僅需擔保表列網域之安全並與檢測報告書上詳細列出與客戶協議的內容以及檢測結果。	4.2.2.1.2	107/12/26

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		資安風險，屬機密資料，理當不應提供給其他任何單位檢視；僅為了通過App資安檢測標章，而交付公司多台伺服器弱掃報告不符合比例原則，難以控管風險。WebView弱點掃描實施做法，提請討論。			
T0057	檢測基準	行動應用App未發佈，便無法於行動應用程式商店上說明。	未發佈之App可透過其他管道加註警語。於下次檢測基準中將未發佈App之檢測基準加入，並將最新作業系統版本改成最低要求版本。	4.1.5.3.1	107/12/26
T0058	檢測基準	安全亂數產生函式的檢測實作難以達成。	安全亂數產生函式的基準訂定的原意是希望開發者可以依照這些標準產生，目前各實驗室以內建的安全亂數產生函式，作為檢測方式。	4.1.2.3.6	108/4/1
T0059	制度	專家回覆的時程並不如預期，導致進度延宕。	目前已經建立相關機制，往後會盡量在5-10工作天內回覆各實驗室。		108/4/1
T0060	檢測基準	webview一般大眾所知安全網域白名單判定基準為何，提請討論。	目前並無相關機制，僅由實驗室提出，並同時提出需列入的原因。	4.2.2.1.2	108/4/1
T0061	檢測基準	App常有第一次以帳號密碼登入，往後則可用指紋登入的方式，此方式是否可	第一次以帳號密碼登入，往後可以用指紋登入。	4.1.4	108/4/1

編號	類型	議題	決議作法	對應檢測項目編號	決議日期
		以作為身份鑑別。			
T0062	制度	檢測報告說明及截圖補充。	1. 為保留完整佐證資料，並確保檢測報告完整性以及各檢測項目之獨立性，所有檢測項目皆須擷圖以及清楚標示，同時附上完整說明，也利於加速審查時程。 2. 若檢測項目之結果為未檢出，或難以舉證檢測結果時，則須提供檢測過程之擷圖(至少一種檢測方法之擷圖)，以佐證該檢測項目確實有經過檢測。且擷圖內容須具可識別性。		108/4/1