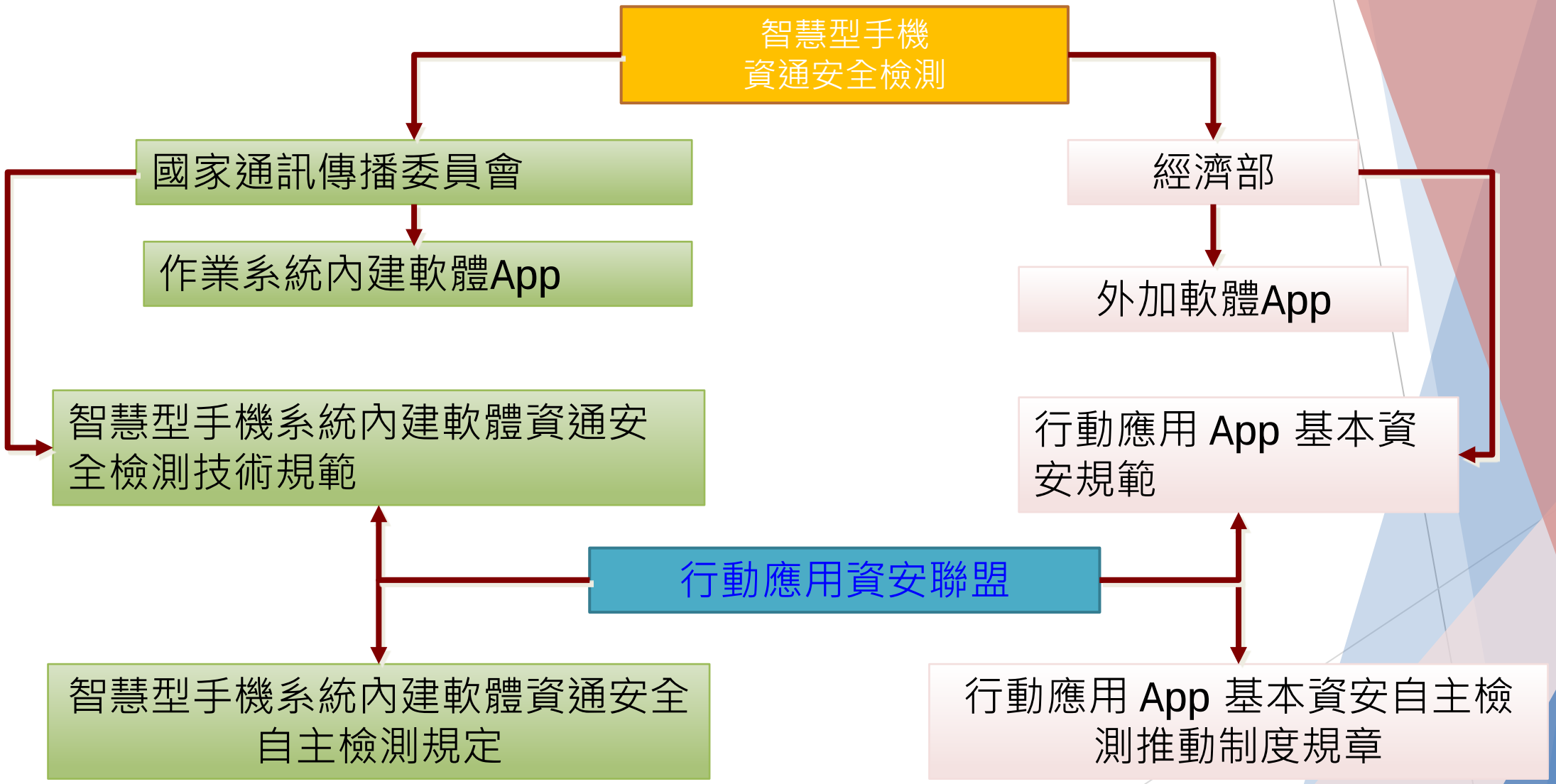
智慧型手機系統內建軟體資通安全檢測試辦實驗室說明會

中華民國資訊安全學會
郭文中 秘書長

智慧型手機系統內建軟體資通安全檢測推動說明

智慧型手機安全檢測 範疇說明



推動依據

國家通訊傳播委員會

智慧型手機系統內建軟體資通安全檢測技術規範

中華民國資訊安全學會

智慧型手機系統內建軟體資通安全自主檢測規定

推動目標

- 建立明確之業界自主規範，鼓勵業界遵循及積極辦理檢測，共同保護消費者隱私。
- 落實「智慧型手機系統內建軟體資通安全檢測技術規範」，強化智慧型手機內建軟體基本資安防護。
- 推廣「智慧型手機系統內建軟體資通安全等級標章」（Embedded Software Security，簡稱E.S.S.標章），使消費者易於識別通過資安檢測之智慧型手機，以保障消費者權益。

推動單位　中華民國資訊安全學會

行動應用資安聯盟

	會長	台灣科技大學	李漢銘	教授
規範增修組	副會長	中國科技大學	陳振楠	教授
國際合作組	副會長	中華民國資訊軟體協會	邱月香	理事長
交流推廣組	副會長	台北市電腦商業同業公會	張永美	副總幹事

行動應用資安聯盟

行動應用資安聯盟

http://www.mas.org.tw/

相關文件與資料下載

檢測說明

測試框架與流程、適用範圍、安全等級

國際標準/規範行動裝置層級定義

檢測規範層別	OWASP TOP 10 Mobile Risks	NIST SP 800-164	ITU-T	DoD-DISA	NSA-IAD
1.資料層	Information/ Data	Information/ Data	用戶數據	Information/ Data	Information/ Data
2.應用程式層	APPs	APPs	應用層	APPs	APPs
3.通訊協定層	Library/ Dependencies /Driver	OS	外圍接口	N/A	N/A
4.作業系統層	OS	Firmware	操作系統	OS	OS
5.硬體層	Hardware	Hardware	硬件	N/A	N/A

測試框架與流程


申請者
檢測申請書
廠商自我宣告表
安全功能規格表
設計安全性表
安全架構表
實驗室
書面檢視
測試項目
硬體層
作業系統層
通訊協定層
應用程式層
資料層
實機測試
申請者
實驗室
溝通/提供資料
測試報告

適用範圍

- 本規範適用於:
  - 智慧型手機系統內建軟體，以確保其符合資訊安全要求

與其它規範差異

國際規範

工業局行動應用APP基本資安規範

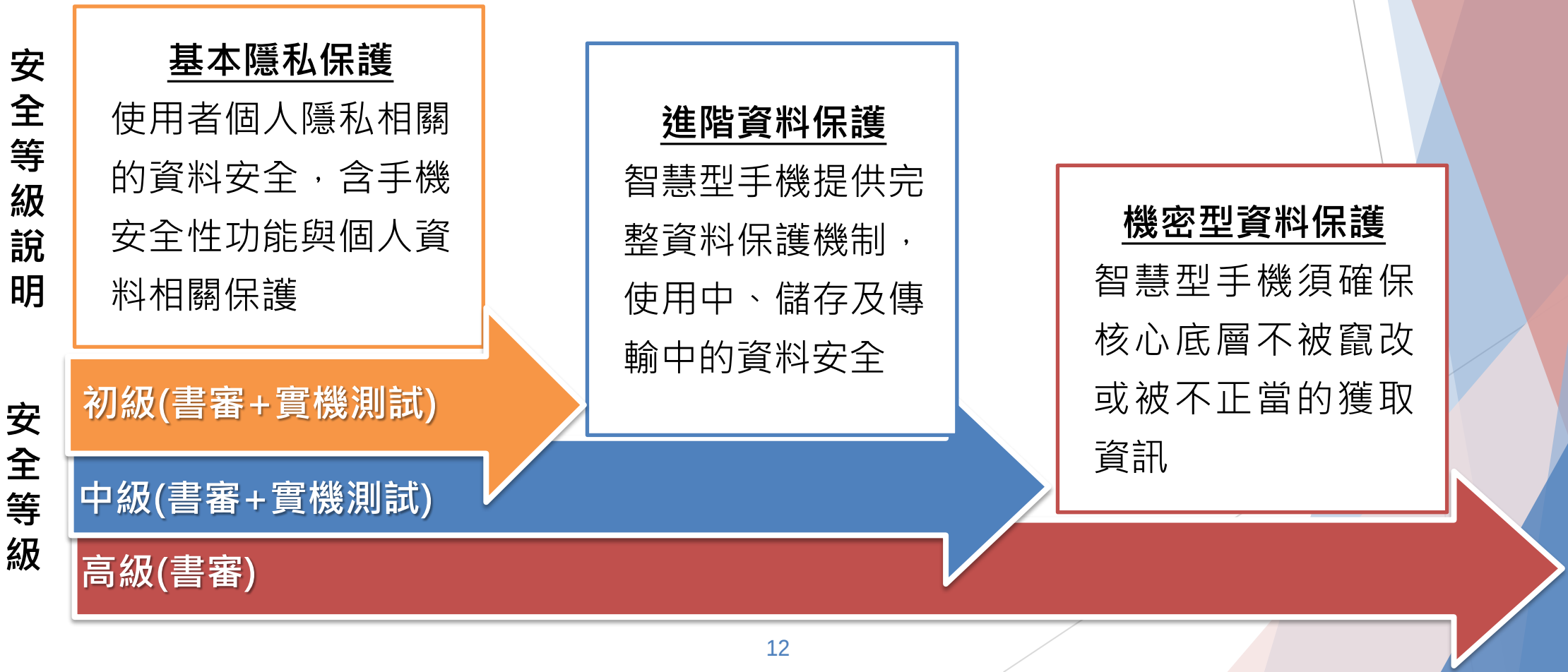
本規範

本規範特色

1. 可涵蓋整支智慧型手機安全之技術規範
2. 適用於不同平台的智慧型手機
3. 依據資安強度建立安全分級制度

安全等級

- 初級為智慧型手機安全最基本要求，所有送測之智慧型手機應符合初級的檢測標準，中、高級採自願性
- 等級越高表示通過之安全要求項目越多



檢測要求

內建軟體屬性、資料型別、書面檢視資料

檢測要求-內建軟體屬性

出廠 預載軟體	智慧型手機出廠時預設搭載安裝之應用程式，且使用者可透過圖示啟動
銷售商 加載軟體	智慧型手機銷售時預設搭載或首次連結網路後自動安裝之應用軟體，且使用者可透過圖示啟動。
無圖示軟體	於上述兩種情況所安裝之應用軟體，使用者無法透過圖示啟動，且該軟體會啟動通訊功能。

檢測要求-資料型別

- 依據資料敏感性與否以及是否為使用者輸入兩個因素，將資料分為第1~4型

型別	判斷標準		範例
	是否屬於敏感性資料	是否為使用者輸入	
第1型	是	是	帳號密碼、聯絡方式(包括但不限於通訊錄如：姓名、地址、電話、電子郵件帳號、電子郵件內容等之相關資訊)、簡訊內容、通話錄音、裝置密碼
第2型	是	否	IMEI、IMSI、定位資訊
第3型	否	否	APP列表、音樂播放資訊、手機作業系統手機型號、手機韌體版本、MCC、MNC、行動通信業者、網路傳送方式、設定檔
第4型	N/A	N/A	資料加密、協定加密、無加密但內容未知

檢測要求-書面檢視資料

初級(B)	中級(M)	高級(H)
1.檢測申請書 2.廠商自我宣告表	1.檢測申請書 2.廠商自我宣告表	前述中級所需文件項目、安全功能規格表、設計安全性表及安全架構表

書面檢視處理原則

符合下列情況之一者即由檢測實驗室通知送測單位於期限內補齊，未補齊則將文件與送測設備退還至送測單位：

1. 檢測申請書未填寫完整
2. 廠商自我宣告表未填寫完整
3. 安全功能規格表、設計安全性表、安全架構表未填寫完整 (申請安全等級高之送測單位)
4. 送測設備之名稱、型號、版本或數量等不符
5. 送測設備功能不符合要求

書面檢視資料(1/3)

- 申請單位應依送測文件描述，提供相關符合性說明文件，以協助檢測實驗室與測試人員瞭解待測物運作方式與相關功能，藉以提升檢測效率，並確保宣稱的內容與實際產品相同

檢附文件項目(必要文件)	說明
廠商自我宣告表	描述具體功能內容，以確認產品是否符合文件宣稱之用途
中文或英文之使用手冊或說明書乙份	提供智慧型手機之使用手冊，以增加測試人員檢測效率
光碟片乙份	包含送測設備之廠商自我宣告表與檢附文件之電子檔供檢測實驗室備查

書面檢視資料(2/3)廠商自我宣告表

- 申請單位應於送測前應詳細填寫廠商自我宣告表，以利後續檢測人員檢測效率提升

受測軟體基本資訊					資料層		通訊協定
項次	受測軟體名稱	發行商及版本	受測套件名稱	受測軟體屬性	是否存取敏感性資料	是否支援無線傳輸技術	是否具備帳號密碼輸入
1	電話		com.android.phone	☐出廠預載軟體 ☐銷售商加載軟體 ☐無圖示軟體	☐否 ☐第1型 ☐第2型	☐否 ☐WiFi ☐GPS(定位服務) ☐藍牙 ☐行動網路 ☐NFC(Peer-to-Peer模式) ☐NFC(Read/Write模式) ☐紅外線 ☐其他_____	☐是， 埠號：____ ☐否

書面檢視資料(3/3)-安全等級高級之需求文件

- 送測單位如欲申請安全等級高者為確保產品的安全與功能性得以實現，須檢附：
  - 安全功能規格表
  - 設計安全性表
  - 安全架構表
- 檢測實驗室則依據文件檢視安全功能介面是否可確實實現安全功能需求

檢測項目

各檢測項目之安全需求與編碼原則

檢測項目(1/2)

- 依據智慧型手機之層別(資料層、應用程式層、通訊協定層、作業系統層及硬體層)可將檢測項目依相關類型向下展開
- 各層別之安全需求

層別	檢測項目	安全需求
資料層	D.1資料使用授權	手機系統內建軟體對敏感性資料進行存取前，應取得使用者同意。
	D.2資料儲存保護	手機系統內建軟體應將敏感性資料儲存於作業系統保護區域，並提供資料加密功能，以避免敏感性資料遭不正當方式存取。
	D.3資料遺失保護	手機系統應提供資料保護與備份功能，以避免資料外洩和防止資料損失。
應用程式層	A.1程式身分辨識	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。
	A.2程式信任來源	手機系統內建軟體應確認付費功能機制與資料來源的安全。
	A.3程式執行授權	手機系統內建軟體所執行的行為，應取得使用者同意，並與其宣告之內容相符。
	A.4程式執行安全	手機系統內建軟體應具備惡意字串輸入時的處理能力。

檢測項目(2/2)

層別	檢測項目	安全需求
通訊協定層	P.1協定使用授權	手機與外部設備進行連接時，應給予使用者相對應的提示，並提供開啟及關閉無線傳輸技術之功能。
	P.2協定傳輸保護	手機系統內建軟體與伺服器間之資料加密傳輸，應使用安全之加密演算法，並避免可能的傳輸攻擊。
	P.3協定執行安全	手機系統應具備通訊協定內容的錯誤處理能力。
作業系統層	O.1系統操作授權	手機系統所執行的行為，應取得使用者同意，必要時並提供風險提示。
	O.2系統身分辨識	手機系統應提供安全的身分辨識及保護機制。
	O.3系統執行安全	手機系統應具備程式執行期的記憶體保護機制，並提供安全回報之管道
硬體層	H.1金鑰管理保護	手機之金鑰管理，應符合金鑰使用及管理標準。
	H.2演算法強度要求	手機實作之加密、解密及簽章演算法，應符合金鑰演算法標準與初始化向量要求。

檢測細項-編碼原則

- 每一檢測項目與檢測細項具所屬編號
- 格式：層別代碼.檢測項目編號.檢測細項編號.安全等級
  - 各層別代碼依序為D(資料層)、A(應用程式層)、P(通訊協定層)、O(作業系統層)、H(硬體層)
  - 各安全等級之代碼依序為初級(B)、中級(M)及高級(H)
- 如資料層第一個檢測項目所屬編號為D.1，檢測細項因為是初級故為D.1.1.B，依此類推
- 選測項目之檢測細項則標示(+)可由送測單位自由選擇是否檢測

必測項目

檢測編號、檢測範例

必測項目-檢測細項(1/6)

檢測項目	檢測編號	檢測細項
D.1資料使用授權	D.1.1.B	手機系統內建軟體於存取敏感性資料前，應取得使用者同意。
D.2資料儲存保護	D.2.1.B	手機系統內建軟體應將帳號之密碼儲存於作業系統保護區內或以加密方式儲存。
D.3資料遺失保護	D.3.1.B	手機系統應提供使用者遠端鎖定功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端啟動鎖定。
	D.3.2.B	手機系統應提供使用者遠端刪除資料功能及相關安全設定，以確保手機在遺失或遭竊的情況下，可讓使用者在遠端刪除資料。
	D.3.3.B	手機系統應提供資料備份功能。

必測項目-檢測細項(2/6)

檢測項目	檢測編號	檢測細項
A.1程式身分辨識	A.1.1.B	手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以確保內建軟體具備該帳戶使用權限。
A.2程式信任來源	A.2.1.B	手機系統內建軟體具備付費功能時，應使用有效期間之伺服器憑證，以確保付費交易之安全。
	A.2.2.B	手機系統內建軟體應可識別其發行資訊，以確保使用者瞭解其來源。
A.3程式執行授權	A.3.1.B	手機系統內建軟體在未調整付費功能使用設定情況下，應於每次付費前，提示並取得使用者同意後才可執行。
	A.3.2.B	手機系統內建軟體所需之權限須與「廠商自我宣告表」所宣告之「功能說明」與「權限說明」相符。
	A.3.3.M	手機系統內建軟體所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「通訊埠」相符。
A.4 程 式 執行安全	A.4.1.B	手機系統內建軟體應提供回報安全性問題之管道。
	A.4.2.M	手機系統內建軟體應具備資料隱碼攻擊字串的處理能力。
	A.4.3.M	手機系統內建軟體應具備延伸標記語言攻擊字串的處理能力。

必測項目-檢測細項(3/6)

檢測項目	檢測編號	檢測細項
P.1協定使用授權	P.1.1.B	手機應提供使用者可開啟及關閉無線傳輸技術功能之介面。
	P.1.2.B	當手機之無線傳輸技術功能確認開啟時，應給予使用者相對應的提示狀態。
	P.1.3.B	手機以無線傳輸技術功能與其他設備進行第一次連接時，須經使用者同意後才可建立連線。
	P.1.4.B	手機應提供使用者可開啟及關閉近場通訊技術功能之介面。
P.2協定傳輸保護	P.2.1.B	手機系統內建軟體透過無線傳輸技術功能傳輸敏感性資料時，應使用加密傳輸，以確保敏感性資料安全。
	P.2.2.M	手機系統內建軟體應避免交談識別碼遭重送攻擊。
	P.2.3.M	手機系統內建軟體與付費功能伺服器間之加密傳輸，應使用安全之加密演算法。
P.3協定執行安全	P.3.1.M	手機系統應具備通訊協定內容的錯誤處理能力。

必測項目-檢測細項(4/6)

檢測項目	檢測編號	檢測細項
O.1系統操作授權	O.1.1.B	手機系統之更新來源應與「廠商自我宣告表」中所宣告之「資料連結伺服器之IP/DN/公司主機名稱」相符。
	O.1.2.B	手機系統於下載或安裝更新作業系統時應提供更新資訊，並告知使用者更新內容。
O.2系統身分辨識	O.2.1.B	手機系統應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。
	O.2.2.B	手機系統應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。
	O.2.3.B	手機系統應提供至少72種密碼輸入值，包含英文大寫、英文小寫數字及特殊符號等，且密碼長度應可達14碼以上。
	O.2.4.M	手機系統之螢幕鎖定解鎖資料，不應以明文方式儲存於手機上，以避免遭未經授權的使用。

必測項目-檢測細項(5/6)

檢測項目	檢測編號	檢測細項
O.3系統執行安全	O.3.1.B	手機系統應提供回報安全性問題之管道。
	O.3.2.M	手機系統應具備記憶體配置保護機制，以避免程式與參考函式在記憶體中的位址被不當應用。
	O.3.3.H	手機系統應建立與通訊目標間受信任的傳輸通道，作為傳輸期間資料保護使用。
	O.3.4.H	手機開機過程應提供密碼功能測試與系統軟體完整性自我測試機制
	O.3.5.H	手機系統應具備驗證錯誤計數機制，當嘗試錯誤超過手機設定門檻值時，應抹除受保護之資訊。

必測項目-檢測細項(6/6)

檢測項目	檢測編號	檢測細項
H.1金鑰管理保護	H.1.1.H	手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合NIST、ANSI或IEEE發布之金鑰使用及管理標準。
	H.1.2.H	手機所有儲存於行動裝置之金鑰，都應對其機密性與完整性提供額外保護。
	H.1.3.H	金鑰不得以明文方式存放於非揮發性之記憶體，且不得以明文型態用任何方式匯出或直接對外傳輸。
H.2演算法強度要求	H.2.1.H	手機實作之加密、解密及簽章演算法，應符合NIST、ANSI或IEEE發布之金鑰演算法標準。
	H.2.2.H	手機實作之演算法，應依據各模式要求，產生初始化向量，並符合NIST發布之初始化向量要求。
	H.2.3.H	金鑰使用之亂數，應符合NIST或ANSI發布之隨機位元產生規範要求。

檢測細項 -資料層 範例

檢測項目	D.1資料使用授權
檢測細項	D.1.1.B手機系統內建軟體於存取敏感性資料**前**，應取得使用者同意。
檢測條件：	■受測軟體具備存取敏感性資料的功能 ■資料型別：第1型資料及第2型資料 ■受測軟體屬性：出廠預載、銷售商加載

檢測方法	**判定標準**
(1)開啟受測系統。 (2)檢查受測系統之隱私權政策或使用聲明中，是否提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。 (3)如未符合步驟(2)，則執行受測軟體，並存取使用者敏感性資料。 (4)檢查受測軟體是否提供相對應的使用者同意機制。	步驟(2)中，隱私權政策或使用聲明中有提供受測軟體存取敏感性資料之相對應說明和使用者同意機制。 或步驟(4)中，受測軟體有提供相對應的使用者同意機制。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

檢測細項 -應用程式層 範例

檢測項目	A.1 程式身分辨識	
檢測細項	A.1.1.B手機系統內建軟體在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限以確保內建軟體具備該帳戶使用權限。	
	檢測條件： ■受測軟體具備連接使用者帳戶功能 ■資料型別：無 ■受測軟體屬性：出廠預載、銷售商加載	
	檢測方法	**判定標準**
	(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體之使用者帳戶認證功能。 (4)檢查受測軟體是否提供使用者登入確認並取得授權之機制。	步驟(4)中，受測軟體於存取使用者帳戶時有提示使用者認證與授權機制。 若「符合」判定標準，則本檢測細項通過；若「不符合」判定標準，則本檢測細項不通過。

檢測細項 -通訊協定層 範例

檢測項目	P.3 協定執行安全	
檢測細項	P.3.1.M手機系統內建軟體應具通訊協定內容的錯誤處理能力。	
	檢測條件： ■受測的無線傳輸技術：藍牙及WLAN ■資料型別：無 ■受測軟體屬性：無	
	檢測方法	**判定標準**
	(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)執行受測軟體之網路傳輸功能。 (4)在受測的無線傳輸環境下，於通訊連線交涉(Negotiation)起，採用模糊測試方法，針對使用的通訊協定逐一發送不同錯誤封包達一萬次。 (5)檢查無線傳輸技術介面或受測系統是否仍正常運作。	步驟(4)中，受測系統均可正常進行通訊連線與資料傳輸，且正常運作。 若「符合」判定標準，則本檢測細項通過 若「不符合」判定標準，則本檢測細項不通過。

檢測細項 -作業系統層 範例

檢測項目	O.3 系統執行安全	
檢測細項	O.3.1.B手機系統內建軟體應提供回報安全性問題之管道。	
	檢測條件： ■資料型別：無 ■受測軟體屬性：無	
	檢測方法	**判定標準**
	(1)開啟受測系統。 (2)檢查受測系統、官方網站或使用說明書是否提供問題回報管道。	步驟(2)中，受測系統發現的問題可透過問題回報管道回報。 若「符合」判定標準，則本檢測細項通過 若「不符合」判定標準，則本檢測細項不通過。

檢測細項 -硬體層 範例

檢測項目	H.1 金鑰管理保護
檢測細項	H.1.1.H 手機之金鑰管理，包含加密及通訊密鑰之產生、交換、合併與銷毀，應符合NIST、ANSI或IEEE發布之金鑰使用及管理標準。相關標準臚列如下： ANSI X9.31-1998、IEEE 802.11-2012、IEEE 802.11ac-2013、IEEE 802.1X、NIST SP 800-38A, 38C~F, 56A~B, 57, 90B
檢測條件：	■ 申請者須提供書面資料作為審查依據 ■ 必要時請申請者進行功能示範 ■ 資料型別：無 ■ 受測軟體屬性：無

檢測方法	**判定標準**
(1)依書面資料審查是否具備此功能。 (2)當無充分資料顯示具備此功能時，則請申請者做功能示範。	於步驟(1)或(2)中，受測硬體之金鑰管理符合機密性與完整性之要求。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過。

選測項目

選測項目介紹與範例

選測項目

- 選測項目分為資料層(Information/Data)選測、應用程式層(APPs)選測以及無圖示軟體檢測，此類檢測細項可由送測單位**自由選擇**是否檢測
- 資料層(Information/Data)選測、應用程式層(APPs)選測
  - 於規範中標示(+)
- 無圖示軟體選測
  - 如遇開啟出廠預設或銷售商加載軟體所連動至無圖示軟體部分，則依該檢測細項判定標準檢測之

選測項目-檢測細項

檢測項目	檢測編號	檢測細項
D.1資料使用授權	D.1.2.M(+)	手機系統內建軟體經使用者設定拒絕存取敏感性資料後，該軟體不應仍可存取。
D.2資料儲存保護	D.2.2.M(+)	手機系統內建軟體於儲存敏感性資料時應提供資料加密功能，以避免遭不正當方式取得敏感性資料。
	D.2.3.M(+)	手機系統內建軟體與遠端伺服器溝通之帳號及密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。
A.3程式執行授權	A.3.4.M(+)	手機系統內建軟體不應在未取得使用者同意之情況下，於背景撥打電話或發送簡訊。
	A.3.5.M(+)	手機系統內建軟體於使用者設定關閉時，應停止該內建軟體所有相關程序。

選測項目-應用程式層 範例

檢測項目	D.2資料儲存保護	
檢測細項	D.2.3.M(+) 手機系統內建軟體與遠端伺服器溝通之帳號及密碼不應以明文方式存在於執行檔中，以避免遭不正當的方式存取。	
	檢測條件： ■申請者須提供智慧型手機管理者權限 ■受測軟體具備帳號密碼登入功能 ■資料型別：帳號及密碼 ■受測軟體屬性：出廠預載、銷售商加載	
	檢測方法	**判定標準**
	(1)開啟受測系統。 (2)確認已符合檢測條件。 (3)使用資料讀取工具對受測軟體執行檔進行資料讀取。 (4)檢查步驟(3)之受測軟體執行檔中是否以明文方式儲存與遠端伺服器溝通之帳號及密碼。	步驟(4)中，執行檔中未以明文方式儲存與遠端伺服器溝通之帳號及密碼。 若「符合」判定標準，則本檢測細項通過； 若「不符合」判定標準，則本檢測細項不通過

各安全等級檢測數量

- 目前檢測項目共有44項;含10個選擇檢測項目（其中4個屬無圖示軟體選測）
- 註：(+)為選擇檢測項目數，可由送測單位與檢測實驗室討論是否進行檢測

檢測細項數量		安全等級						
		初級		中級			高級	
		必測細項	無圖示軟體選測細項	必測細項	無圖示軟體選測細項	選測細項	必測細項	選測細項
五個層別	資料層 (Data, D)	5	-	-	-	3(+)	-	-
	應用程式層 (Application, A)	6	(1)	3	(1)	2(+)	-	-
	通訊層 (Protocol, P)	5	(1)	3	(1)	-	-	-
	作業系統層 (Operation, O)	6	-	2	-	-	3	-
	硬體層 (Hardware, H)	0	-	0	-	-	6	-
各級填測	初級(B)	必測22(含無圖示選測2)						
	中級(M)	必測30(含無圖示選測4) + 選測5						
	高級(H)	必測39(含無圖示選測4) + 選測5						
		總計44個檢測細項						

申請方式

- 送件地址：高雄郵政59-26號信箱
- 收件者：E.S.S.標章審查小組
- 聯絡窗口：藍淵 小姐
- 聯絡電話：07-5250558 或 07-5252000#4317
- 聯絡Email：ccisapa01@gmail.com

簡報完畢
敬請指教