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 106 年 3 月 3 日

目錄

智慧型手機系統內建軟體資通安全檢測技術規範

1. 概說

網路與通訊無遠弗屆，智慧型手機基於高度可攜性與便利性，有效提升生產力與工作效率，但隨之而來，使用者也必須面對智慧型手機上網後所帶來的資安威脅。有鑒於此，國家通訊傳播委員會（下稱本會）爰參考國際標準及歐美等國作法，研議訂定「智慧型手機系統內建軟體資通安全檢測技術規範」（以下簡稱「本規範」），作為智慧型手機製造商、經銷商、電信業者及資通安全檢測實驗室辦理檢測之依據。

2. 適用範圍

本規範適用於智慧型手機系統及其系統內建軟體，以確保其符合現階段資訊安全要求，但不包含使用者於內建軟體中自行下載之附加服務或內容。

資通安全本質為風險控管概念，智慧型手機系統內建軟體經本規範檢測通過後，並不能保證受測後之智慧型手機於使用時不會被惡意破解或遭到駭客攻擊，使用者應搭配良好的使用習慣，並隨時提高資安警覺，以降低資安問題所帶來的風險與影響程度。

2.1 內建軟體屬性

智慧型手機系統內建軟體（以下簡稱內建軟體）分為出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，其中無圖示軟體得由申請檢測者（以下簡稱申請者）自行選擇是否檢測：

- 出廠預載軟體：智慧型手機出廠時已預設安裝之應用軟體，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。

2.2 檢測層別

本規範依據國際間對智慧型手機安全之分層概念，將智慧型手機區分為資料層、應用程式層、通訊協定層、作業系統層及硬體層五個層別，考量不同層別可能面臨的資訊安全風險有所不同，故對各層別分別訂定檢測項目。各檢測層別之安全性說明如下：

- 資料層（Information/Data）：資料之安全性主要包含資料的傳送、儲存或使用等相關安全，並應確保使用者資料避免遭系統內建軟體未經授權之蒐集、分享、使

用、刪除、竄改及儲存。

- 應用程式層（APPs）：應用程式之安全性主要包含程式信任來源、執行授權等相關安全，並應確保內建軟體避免未經授權存取系統資源。
- 通訊協定層（Protocol）：通訊協定之安全性主要包含無線傳輸技術及通訊協定等相關安全，並應確保使用者對資料之傳輸、周邊設備之連接的可控管性。
- 作業系統層（Operating System）：作業系統之安全性主要包含作業系統相關服務與身分辨識等相關安全，並應確保作業系統對系統資源之保護、提醒，並讓使用者於知情的狀況下進行更新。
- 硬體層（Hardware）：硬體之安全性主要包含金鑰與演算模組等安全，並應確保金鑰管理、存放之保護，及演算法之安全強度符合國際規範，並讓使用者於知情的狀況下進行更新。

3. 安全等級

為配合不同安全需求，本規範將智慧型手機系統內建軟體資通安全等級區分為初級、中級及高級 3 種，各等級之要求及說明如表 1。

表 1 資通安全等級之要求及說明

資通安全等級	要求	說明
初級 (B)	智慧型手機應提供個人隱私相關的資料安全，包含手機安全性功能和敏感性資料相關保護，如蒐集敏感性資料的行為必須明確告知使用者。	為智慧型手機基本隱私保護之最低要求。
中級 (M)	智慧型手機應提供完整資料保護機制，包含所有資料在使用、儲存及傳輸時，皆可被安全保護。	除須符合初級之所有必測細項外，並增加資料進階保護之檢測細項。
高級 (H)	智慧型手機應確保核心底層不被竄改或被不正當的擷取資訊。	為確保智慧型手機之核心底層不會被竄改或不正當地擷取資訊，除須符合初級與中級之所有必測細項外，並增加手機設計相關安全性文件審查之檢測細項。

4. 參考標準

ISO/IEC 15408 共同準則(Common Criteria for Information Technology Security Evaluation, CC)。

5. 用語釋義

5.1 加密（Encryption）

係指利用數學演算法處理電子資料，使資料不會以原來的形式呈現，達到保密的目的，並且可透過解密方式取得加密資料原文內容。

5.2 通訊埠（Port）

係指內建軟體因服務需求開啟之通訊埠。

5.3 交談識別碼（Session Identification，Session ID）

係指在建立連接時，指派給每個使用者連接的唯一工作階段識別碼。當連接結束時，即釋出該識別碼，讓伺服器重新指派給新的使用者連接。

5.4 近場通訊技術（Near Field Communication，NFC）

係指一種近距離（通常小於 10 公分）的無線通訊技術，主要運作頻率是 13.56 百萬赫茲(MHz)，資料傳輸速度每秒最高可達 424 Kbps。NFC 包含三種模式，分別為點對點模式（Peer-to-Peer Mode）、讀寫模式（Read/Write Mode）及卡片模擬模式（Card Emulation Mode），其中卡片模擬模式可模擬多種實體卡片功能，如信用卡、悠遊卡等，當近場通訊技術使用卡片模擬模式時，可在無電力供應情況下使用。

5.5 非作業系統保護區（Non-Operating System Protection Area）

係指使用者透過外部裝置（如電腦）連接手機，在非管理者權限下可存取之空間，包含手機本身儲存空間和出廠時提供的外接記憶卡。

5.6 資料隱碼攻擊（Data Injection）

係指利用資料輸入欄位或資料庫的漏洞執行非預期之外部程式或指令，進而取得未經授權資料之攻擊。

5.7 延伸標記語言隱碼攻擊（XML Injection）

係指一種網路攻擊手法，XML 格式的檔案常用來作為應用程式的輸入和輸出，當應用程式以 XML 格式作為執行作業的輸入時，攻擊者可能透過變更 XML 格式的結構或資料，以此來篡改重要檔案或資料之內容，達到入侵目的。

5.8 個人資料（Personal Data）

指自然人之姓名、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、社會活動及其他得以直接或間接方式識別該個人之資料。

5.9 敏感性資料（Sensitive Data）

指內容遭外洩或竄改將可能導致個人或資料擁有者的權益受損之個人資料或手機相關資訊。

5.10 資料型別 （Data Type）

本規範依資料之敏感性與是否為使用者輸入等兩個因素分成第 1 型、第 2 型、第 3 型及第 4 型（如表 2）其中第 1 型及第 2 型為敏感性資料。

表 2 資料型別分類表

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	1.本規範用語釋義之個人資料。 2.手機相關資訊：簡訊內容、通話錄音、裝置密碼、帳號密碼、相片。
第 2 型	是	否	IMEI、IMSI[註]、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	無法判斷	無法判斷	資料加密、協定加密、無加密但內容未知。
[註] IMEI 碼及 IMSI 碼須與行動通信業者或手機廠商之銷售保固連結，該 IMEI 碼及 IMSI 碼才具備個資識別性，但使用人與登錄人可能不同，故歸類為第 2 型。			

5.11 穩固性測試（Robustness Testing）

係指透過製造錯誤或不可預期的輸入來驗證程式的穩固性，主要對於作業系統、行動應用程式或網路服務在執行過程中，遭遇輸入、運算等異常時，其錯誤處理程序或演算法繼續正常執行能力的測試。

5.12 國際行動用戶識別碼（International Mobile Subscriber Identity，IMSI）

係指結合所有 GSM 與 UMTS 網路行動裝置用戶的唯一識別碼。IMSI 由一串 10 進位數組成，最大長度為 15 位，在行動電話裡面的 SIM 卡上所標示前三位數代表行動裝置國碼(Mobile Country Code， MCC)；接續是行動裝置網路碼(Mobile Network Code，MNC)，它是 3 位數（北美標準式）或 2 位數（歐洲標準式）；其餘的位數代表行動訂閱辨識碼（Mobile Subscription Identification Number，MSIN），該數值由營運商自行分配，因此 IMSI 是由 MCC、MNC 及 MSIN 三種代表碼依次連接而成。

5.13 國際行動設備識別碼（International Mobile Equipment Identity，IMEI）

係指行動網路中識別每一部獨立的行動通訊裝置，相當於該裝置之身分證。序列號共有 15 位數字，前 6 位（Type Approval Code，TAC）是型號核准號碼，代表手機類型；接著 2 位(Final Assembly Code，FAC)是最後裝配號，代表產地；後 6 位(Serial Number, SNR）是序號，代表生產順序號；最後 1 位（SP）是檢驗碼，一般為 0。國際行動設備識別碼一般貼於機身背面與外包裝上，同時也存在於手機記憶體中。

5.14 密碼（Password）

係指為特定應用中，用於保護特定資料的一組字串，通常用於身分識別及資料加密。

5.15 使用者同意 （User Agrees）

使用者同意機制係指系統透過訊息提示方式提供使用者選擇「同意」或「不同意」的機制。使用者同意則係指包含使用者主動操作之行為和系統透過使用者同意機制取得使用者同意之情況。

5.16 無線傳輸技術（Wireless Transfer Technology ）

係指透過無線通訊標準的連接，讓智慧型手機透過網路或點對點等連線方式來傳輸資料。手機使用的無線傳輸技術包括如藍牙、WLAN、NFC、行動通訊網路、GPS（定位服務）、紅外線及無線充電等。

5.17 無線區域網路（Wireless Local Network，WLAN）

係指透過無線電波、雷射光或紅外線作為傳輸資料的媒介與網路連線，其功能與有線區域網路相同。

5.18 智慧型手機系統內建軟體（Embedded Software of Smartphone）

係指手機製造商、行動通信服務業者或應用軟體開發商，於使用者初次使用智慧型手機或初次啟用網路服務時，強制安裝之軟體。

5.19 網際網路通訊協定位址（Internet Protocol Address，IP Address）

係指可唯一識別網際網路上主機的位址，簡稱為 IP 位址，分為 IPv4 及 IPv6 二種。

5.20 網域名稱（Domain Name ）

係指用以與網際網路位址相對映，便於網際網路使用者記憶網路主機所在位址（即 IP 位址）之文字或數字組合。

5.21 數位簽章（Digital Signature）

係指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，再以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰進行驗證。

5.22 緩衝區溢位攻擊（Buffer Overflow）

係指一種攻擊手法，惡意攻擊者利用程式設計漏洞，輸入超過預定長度的字串或資料，造成程式發生非預期情況，產生緩衝區溢位問題；惡意攻擊者以帶有惡意目的之程式語法或資料插入原有程式碼中，可能導致程式異常停止、執行任意程式碼或取得系統權限等影響。

5.23 憑證（Certificate）

係指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

5.24 憑證機構（Certification Authority，CA）

係指簽發憑證之機關、法人，為使用者所信任之公正機構，其業務為簽發並管理 X.509 格式之公開金鑰憑證、憑證機構註銷清冊及憑證廢止清冊。

5.25 位址空間配置隨機化（Address Space Layout Randomization，ASLR）

係指於執行程序中將關鍵元件的記憶體位置打亂，使得攻擊方難以定位執行的基址、函式庫、記憶體堆疊（stack）及堆積（heap）等關鍵位址，使其難以正確地執行惡意程式。

5.26 共同準則（Common Criteria，CC）

係指國際資通安全產品評估及驗證之標準（ISO/IEC 15408），依其定義之評估保證等級（Evaluation Assurance Level，簡稱 EAL） 判定產品之安全等級，EAL 共有 7 個等級，最低等級為 EAL 1，最高等級為 EAL 7，提供申請者/贊助者、檢測實驗室與驗證機關（構）評估及驗證資通安全產品安全與功能性，參考網址 http://www.commoncriteriaportal.org。

5.27 評估標的（Target of Evaluation，TOE）

係指申請資通安全評估及驗證之產品及其相關使用手冊。

5.28 保護剖繪（Protection Profile，PP）

係指滿足資通安全產品評估標的（TOE）製作之安全基本需求文件。

5.29 安全標的（Security Target，ST）

係指資通安全產品能符合保護剖繪（PP）或特定安全需求製作之規格文件。

5.30 安全功能需求（Security Functional Requirement，SFR）

係指共同準則第二部分（Common Criteria，Part 2）所定義之安全相關需求條文，用以描述一資通安全產品之安全功能（TSF）所需滿足的各項要求。此要求條文會被引用於保護剖繪及安全標的中，用以具體陳述該產品功能於安全方面的需求。

5.31 安全功能（TOE Security Functions，TSF）

係指資通安全產品用於實現安全標的(ST)所要求安全功能需求（Security Functional Requirement，SFR）之相關功能。

5.32 安全功能介面（TOE Security Functions Interface，TSFI）

係指評估標的（TOE）用於實現安全功能需求（SFR）之對外溝通介面。

5.33 安全領域（Security Domain）

係指一主動式個體（人或機器）被授權存取的資源集合，為安全架構的屬性之一。

5.34 自我保護（Self-Protection）

係指安全功能可以自動識別自身並加以保護，無法被無關的程式碼或設施破壞，為安全架構的屬性之一。

5.35 防止繞道（Non-Bypassibility）

係指防止避開待測物安全功能檢查之技巧（如：未經過身分鑑別，無法進入稽核功能介面）。

6. 技術要求

檢測實驗室應依本規範所說明之適用範圍及檢測項目，對申請者檢附之相關資料及智慧型手機樣品進行書面審查與實機測試。

6.1 申請檢測應檢附之資料

申請者應填具檢測申請書（附件 1）、廠商自我宣告表（附件 2）及內建軟體摘要表（附件 3），並提供智慧型手機樣品向檢測實驗室申請檢測。申請檢測之資通安全等級為高級者，應額外另填具安全功能規格表（附件 4）、設計安全性表（附件 5）及安全架構表（附件 6）。

6.1.1 檢測申請書

內容包括申請者、製造商相關資訊、送測智慧型手機相關規格（包含廠牌、型號、名稱、作業系統版本、定位功能、無線傳輸技術、生物辨識、外接記憶體等）。

6.1.2 廠商自我宣告表

內容包括系統內建軟體名稱、發行商、版本、套件名稱、屬性、功能說明、權限說明、存取資料類型、通訊埠等詳細資訊。

6.1.3 內建軟體摘要表

內容包括系統內建軟體名稱、發行商、版本、屬性、功能說明及權限說明。本摘要表應可供本會引用及公開。

6.1.4 安全功能規格表

內容包括安全功能介面(TSFI)之名稱、目的、可實現的安全功能需求、操作方式、參數、執行的動作以及錯誤訊息。申請者應完整填列及說明，俾檢測實驗室檢視安全功能介面是否可確實實現安全功能（TSF）需求。

6.1.5 設計安全性表

內容包括如何以子系統組成安全功能規格之安全功能介面，以及安全功能子系統之名稱、目的、子系統隸屬之安全功能介面、子系統行為說明。

6.1.6 安全架構表

內容應依據安全功能規格表、設計安全性表之內容，說明送測設備安全架構如何滿足安全功能需求（SFR），並針對安全功能介面及子系統，提出安全架構的設計概念與操作安全建議。安全架構應說明送測設備因執行安全功能區隔的安全領域、安全功能的安全初始程序、安全功能的自我保護機制，以及安全功能執行如何避免被繞道。

6.2 檢測項目

本規範依檢測層別訂定檢測項目，再按照各檢測項目之安全需求訂定檢測細項。檢測項目及安全需求說明如表3,檢測項目、檢測細項與資通安全等級對應關係如表4。各檢測項目之檢測編碼原則說明如下：

- 檢測編碼：

  層別代碼.檢測項目編碼.檢測細項編碼.資通安全等級代碼 (+)

- 說明：

(1)層別代碼如下表：

層別	代碼
資料層	D
應用程式層	A
通訊協定層	P
作業系統層	O
硬體層	H

(2)資通安全等級代碼如下表：

資通安全等級	代碼
初級	B
中級	M
高級	H

(3)檢測編碼標記(+)符號者，為選測細項，由申請者自行選擇是否檢測。

- 範例：

(1)資料層中第 1 個檢測項目的第 1 個檢測細項為初級，且為必測項目，是以其檢測編碼為 D.1.1.B。

(2)資料層中第 2 個檢測項目的第 2 個檢測細項為中級，且為選測項目，是以其檢測編碼為 D.2.2.M(+)。

表 3 檢測項目及安全需求說明

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。
	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。
	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	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。
	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。
	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

(A)		意，並與其宣告之內容相符。
	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。
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。
	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。
	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。
	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。
	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。
	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。

表 4 檢測項目、檢測細項與資通安全等級對應關係

層別	檢測項目	檢測細項	資通安全等級	檢測編碼
資料層(D)	1.資料使用授權	1.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。	B	D.1.1.B
		2.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。	M	D.1.2.M(+)
	2.資料儲存保護	1.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。	B	D.2.1.B
		2.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。	M	D.2.2.M(+)

		3.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。	M	D.2.3.M(+)
	3. 資料遺失保護	1.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。	B	D.3.1.B
		2.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。	B	D.3.2.B
		3.手機系統應提供資料備份功能。	B	D.3.3.B
應用程式層 (A)	1. 程式身分辨識	1.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。	B	A.1.1.B
	2. 程式信任來源	1.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。	B	A.2.1.B
		2.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。	B	A.2.2.B
	3. 程式執行授權	1.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。	B	A.3.1.B
		2.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。	B	A.3.2.B
		3.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。	M	A.3.3.M
		4.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。	M	A.3.4.M(+)
		5.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。	M	A.3.5.M(+)
	4. 程式執行安全	1.手機系統內建軟體應提供回報安全性問題之管道。	B	A.4.1.B
		2.手機系統內建軟體應具備資料隱碼攻擊字串的處理能力。	M	A.4.2.M

		3.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。	M	A.4.3.M
通訊協定層(P)	1.協定使用授權	1.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。	B	P.1.1.B
		2.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。	B	P.1.2.B
		3.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。	B	P.1.3.B
		4.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。	B	P.1.4.B
	2.協定傳輸保護	1.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。	B	P.2.1.B
		2.手機系統內建軟體應避免交談識別碼遭重送攻擊。	M	P.2.2.M
		3.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。	M	P.2.3.M
	3.協定執行安全	1.手機系統應具備通訊協定內容的錯誤處理能力。	M	P.3.1.M
作業系統層(O)	1.系統操作授權	1.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。	B	O.1.1.B
		2.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。	B	O.1.2.B
	2.系統身分辨識	1.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。	B	O.2.1.B
		2.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。	B	O.2.2.B
		3.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。	B	O.2.3.B
		4.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	M	O.2.4.M

		免遭未經授權的使用。		
	3. 系統執行安全	1.手機系統應提供回報安全性問題之管道。	B	O.3.1.B
		2.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。	M	O.3.2.M
		3.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。	H	O.3.3.H
		4.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。	H	O.3.4.H
		5.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。	H	O.3.5.H
硬體層 (H)	1. 金鑰管理保護	1.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	H.1.1.H
		2.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	H.1.2.H
		3.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	H.1.3.H
	2. 演算法強度要求	1.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	H.2.1.H
		2.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	H.2.2.H
		3.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。	H	H.2.3.H

6.3 初級檢測項目

本規範檢測方法與判定標準說明中，統一將手機系統稱為受測系統，手機系統內建軟體簡稱為受測軟體。檢測實驗室應依下列檢測細項對智慧型手機樣品進行測試，以確保符合本規範之檢測項目。

6.3.1 必測項目

內建軟體包含出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，本節就出廠

預載軟體與銷售商加載軟體，說明初級必測項目之檢測條件、檢測方法與判定標準。

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。	
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。

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。	
檢測條件： ■ 受測軟體具備帳號密碼登入功能 ■ 資料型別：帳號之密碼 ■ 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) 執行受測軟體，輸入帳號密碼、同意儲存帳號密碼並成功	步驟(5)中，受測軟體未將帳號之密碼以明文型態存放於非作業系統保護區內。

登入。 (4) 對受測軟體在非作業系統保護區內所存放的檔案進行資料讀取。 (5) 檢查受測軟體是否將帳號之密碼以明文型態存放於非作業系統保護區內。	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。

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。	
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) 設定並執行受測系統的遠端鎖定功能。 (3) 檢查受測系統是否被遠端鎖定。	步驟(3)中，受測系統已被遠端鎖定。 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。
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。	
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) 輸入測試資料後並儲存。 (3) 執行受測系統的遠端刪除功能，並執行遠端刪除步驟(2)輸入之測試資料。	步驟(4)中，測試資料已被遠端刪除。 若「符合」判定標準，則本檢測細項通過；

(4) 檢查步驟(2)輸入之測試資料是否被刪除。	若「不符合」判定標準，則本檢測細項不通過。

D.3.3.B 手機系統應提供資料備份功能。	
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) 檢查受測系統是否有提供資料備份功能。	步驟(2)中，受測系統有提供資料備份功能。 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。

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。	
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。

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。

檢測條件：

- ■ 受測軟體具備付費功能
- ■ 伺服器類型：付費功能的伺服器
- ■ 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) 受測軟體透過網路傳輸資料至遠端伺服器。 (4) 檢查伺服器端提供給受測軟體之憑證資料是否過期。	步驟(4)中，伺服器端提供給受測軟體的憑證資料未過期。 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。

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。

檢測條件：

- ■ 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) 檢查受測軟體或廠商自我宣告表是否提供受測軟體的發行商和版本資訊。	步驟(3)中，受測軟體或廠商自我宣告表有提供受測軟體的發行商和版本資訊。 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。

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。

<table>
<tr><td colspan="2">檢測條件：
■ 受測軟體具備付費功能
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1) 開啟受測系統。
(2) 確認已符合檢測條件。
(3) 執行受測軟體，並開啟付費功能。
(4) 檢查受測系統或受測軟體是否經使用者同意才執行付費。</td><td>步驟(4)中，受測系統或受測軟體經使用者同意才執行付費。

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。</td></tr>
<tr><td colspan="2">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。</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須填寫「廠商自我宣告表」中之「功能說明」與「權限說明」欄位
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1) 開啟受測系統。
(2) 確認已符合檢測條件。
(3) 執行及操作受測軟體，並列舉受測軟體所使用的功能及存取權限。
(4) 比對步驟(3)列舉之內容是否與廠商自我宣告之內容相符。</td><td>步驟(4)中，步驟(3)列舉之內容與廠商自我宣告之內容相符。

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。</td></tr>
</table>

<table>
<tr><td>A.4 程式執行安全</td></tr>
<tr><td>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。</td></tr>
<tr><td>檢測條件：
■ 資料型別：無
■ 受測軟體屬性：銷售商加載</td></tr>
</table>

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) 檢查受測軟體、官方網站或使用說明書是否提供問題回報管道。	步驟(3)中，受測軟體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。

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。	
檢測條件： ■ 受測的無線傳輸技術：藍牙、WLAN 、行動通訊網路及 GPS(定位服務) ■ 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) 檢查手機是否提供無線傳輸技術功能的開啟及關閉介面，並確認手機狀態是否與顯示狀態相符。	步驟(3)中，手機有提供無線傳輸技術功能的開啟及關閉介面，且手機狀態與顯示狀態相符。 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。
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。	
檢測條件： ■ 受測的無線傳輸技術：藍牙、WLAN、NFC(Peer-to-Peer 模式和 Read/Write 模式)、行動通訊網路及 GPS(定位服務) ■ 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) 開啟手機之無線傳輸技術功能。 (4) 檢查手機是否提供相對應的提示狀態。	步驟(4)中，手機有提供使用者相對應的提示狀態。 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。
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。	
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) 開啟手機之無線傳輸技術功能。 (4) 開啟另一臺具備無線傳輸技術對應可被連線之設備，並與手機連接。 (5) 於受測系統選擇拒絕或不接受連線功能。 (6) 檢查受測系統是否能與步驟(4)之設備建立連線。	在步驟(6)中，受測系統無法與步驟(4)之設備建立連線。 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。
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。	
檢測條件： ■ 受測的無線傳輸技術：近場通訊技術（Near Field Communication，簡稱 NFC） ■ 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。	步驟(3)中，手機有提供近場通訊技術功能的開啟及關閉介面（含軟體

(3) 檢查手機是否提供近場通訊技術功能的開啟及關閉介面，並確認手機狀態是否與顯示狀態相符。	綁定方式），且手機狀態與顯示狀態相符。 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。

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。	
檢測條件： ■ 軟體支援之無線傳輸技術：藍牙、WLAN 及行動通訊網路 ■ 資料型別：第 1 型資料(不包含相片)及定位資訊 ■ 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，並以無線傳輸技術功能傳輸敏感性資料。 (4) 檢查受測軟體是否以明文方式傳輸敏感性資料。	步驟(4)中，受測軟體未以明文方式傳輸敏感性資料。 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。

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。
檢測條件： ■ 受測系統具備作業系統更新功能 ■ 申請者須填寫「廠商自我宣告表」中之「資料連結伺服器之 IP/DN/公司主機名稱」欄位 ■ 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) 透過受測系統內建作業系統更新功能執行作業系統更新。 (4) 取得作業系統更新之連線目的地位址。 (5) 檢查步驟(4)中目的地位址是否與廠商自我宣告之內容相符。	步驟(5)中，目的地位址與廠商自我宣告之內容相符。 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。
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。	
檢測條件： ■ 受測系統具備作業系統更新功能 ■ 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) 檢查受測系統或官網是否提供作業系統更新資訊，並告知使用者更新之內容。	步驟(3)中，受測系統或官網有提供作業系統更新資訊，並告知使用者更新內容。 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。

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。	
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。	步驟(5)中，可以步驟(2)所設定之

(2) 開啟受測系統之螢幕鎖定設定功能介面，並設定螢幕鎖定方式及解鎖資料。 (3) 鎖定受測系統(包含關閉螢幕及關閉受測系統)。 (4) 喚醒受測系統(包含開啟螢幕及開啟受測系統)，並操作解鎖方式。 (5) 檢查是否可以步驟(3)所設定的解鎖資料喚醒受測系統。	密碼喚醒受測系統。 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。
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。	
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) 開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。 (3) 鎖定受測系統。 (4) 喚醒受測系統，並重複輸入數次錯誤的解鎖資料。 (5) 檢查受測系統是否顯示強制鎖定的訊息。	步驟(5)中，受測系統有顯示強制鎖定的訊息。 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。
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。	
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) 開啟輸入密碼設定介面。 (3) 檢查受測系統提供之密碼輸入	步驟(3)中，受測系統提供之密碼輸入值有包含英文大寫、英文小寫、數字及特殊符號，且達 72 種以上。

值，是否包含英文大寫、英文小寫、數字及特殊符號，且達72種以上。 (4) 檢查密碼長度是否可達14碼以上。	且步驟(4)中，密碼長度可達14碼以上。 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。

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。	
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。

6.3.2 選測項目

如申請者希望了解無圖示軟體之安全性，可自行選擇檢測無圖示軟體之初級檢測項目如表5，詳細檢測內容請參閱6.3.1。

表 5 無圖示軟體之初級檢測項目與檢測細項

層別	檢測項目	檢測細項	資通安全等級	檢測編碼
應用程式	2.程式信任來源	1.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	B	A.2.1.B(+)

層 (A)		交易之安全。		
通訊協定層 (P)	2. 協定傳輸保護	1. 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。	B	P.2.1.B(+)

6.4 中級檢測項目

6.4.1 必測項目

本節就出廠預載軟體與銷售商加載軟體，說明中級必測項目之檢測條件、檢測方法與判定標準。

A.3 程式執行授權	
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。	
檢測條件： ■ 受測軟體具備開啟網路連接埠進行網路連線功能 ■ 申請者須填寫「廠商自我宣告表」中之「通訊埠」欄位 ■ 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) 執行受測軟體並開始通訊，取得受測軟體開啟之網路埠號。 (4) 檢查步驟(3)取得之網路埠號是否與廠商自我宣告表所宣告之「通訊埠」相符。	步驟(4)中，取得之網路埠號與廠商自我宣告表所宣告之「通訊埠」相符。 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。

A.4 程式執行安全	
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。	
檢測條件： ■ 受測軟體具備可供使用者輸入資料之欄位 ■ 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，並輸入至少 50 組常見且不同之資料隱碼攻擊字串。 (4) 檢查步驟(3)之受測軟體是否執行隱碼攻擊字串。	步驟(4)中，受測軟體未執行資料隱碼攻擊字串。 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。
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。	
檢測條件： ■ 受測軟體可接收延伸標記語言 ■ 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) 執行受測軟體之網路傳輸功能。 (4) 攔截遠端主機傳送至受測軟體之通訊封包。 (5) 將至少 10 組不同之延伸標記語言攻擊字串逐一注入步驟(4)攔截之通訊封包中後，傳送至受測軟體。 (6) 檢查受測軟體是否執行注入攻擊字串。	步驟(6)中，受測軟體未執行注入攻擊字串。 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。

<table>
<tr><td colspan="2">P.2 協定傳輸保護</td></tr>
<tr><td colspan="2">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。</td></tr>
<tr><td colspan="2">檢測條件：
■ 受測軟體透過網路傳輸資料時具備交談識別碼
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(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) 側錄受測軟體與遠端主機間之通訊封包，並擷取交談識別碼。
(5) 將步驟(4)中之交談識別碼，透過電腦主機執行重送攻擊。</td><td>步驟(5)中，電腦主機使用交談識別碼執行重送攻擊並無效果。

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。</td></tr>
<tr><td colspan="2">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。</td></tr>
<tr><td colspan="2">檢測條件：
■ 伺服器類型：付費功能的伺服器
■ 申請者可提供書面資料作為審查依據
■ 必要時，檢測實驗室得請申請者進行功能示範
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(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) 檢查受測軟體所存取之伺服器，其使用之加密演算法是否為 FIPS 140 核准之加密編譯演算法或由申請者提供同等安全性之佐證資料。</td><td>步驟(4)中，受測軟體與伺服器端之通訊加密演算法為 FIPS 140 核准之加密編譯演算法或申請者提供足以證明達同等安全性之佐證資料。

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。</td></tr>
</table>

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。	
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。

O.2 系統身分辨識	
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。	
檢測條件： ■ 申請者須提供智慧型手機管理者權限 ■ 螢幕鎖定功能：圖形、密碼及生物特徵 ■ 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) 開啟螢幕鎖定設定功能介面並設定螢幕鎖定方式及解鎖資料。	步驟(4)中，未以明文方式將螢幕鎖定解鎖資料儲存於手機上。 若「符合」判定標準，則本檢測細項通過；

(4) 以管理者權限身分確認解鎖資料是否以明文方式儲存於手機上；若未能提供管理者權限者，得提供足以證明符合本測試細項之詳細說明、畫面及截圖等佐證資料，必要時檢測實驗室得要求申請者做功能示範。	若「不符合」判定標準，則本檢測細項不通過。

O.3 系統執行安全	
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。	
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，受測系統具備記憶體配置保護機制。 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。

6.4.2 選測項目

6.4.2.1 出廠預載軟體與銷售商加載軟體選測項目

本節就出廠預載軟體與銷售商加載軟體，說明中級選測項目之檢測條件、檢測方法與判定標準。

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。
檢測條件： ■ 受測軟體具備拒絕存取敏感性資料的功能 ■ 申請者可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：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) 如步驟(2)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，則選擇拒絕隱私權政策或使用聲明，並檢查受測系統能否繼續操作。 (4) 如步驟(2)中無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，則執行受測軟體，並拒絕受測軟體存取敏感性資料。 (5) 檢查受測軟體是否仍可存取敏感性資料。 (6) 當無充分資料顯示具備此功能時，則請申請者做功能示範。	步驟(3)中，受測系統無法繼續操作。 或於步驟(5)、(6)中，受測軟體無法繼續操作或無法存取使用者敏感性資料。 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。

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。
檢測條件： ■ 申請者須提供智慧型手機管理者權限

■ 受測軟體具備儲存敏感性資料的功能 ■ 資料型別：第 1 型資料(不包含相片) ■ 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，並儲存敏感性資料。 (4) 以管理者權限檢查步驟(3)之受測軟體是否以明文方式儲存敏感性資料。	步驟(4)中，受測軟體未以明文方式儲存敏感性資料。 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。
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。

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。
檢測條件： ■ 申請者須提供智慧型手機管理者權限 ■ 資料型別：無

<table>
<tr><td colspan="2">■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1) 開啟受測系統。
(2) 確認已符合檢測條件。
(3) 執行受測軟體，並操作其功能。
(4) 透過比對通話紀錄、簡訊資料檔案之檔案時間戳記等方式，檢查是否有背景撥打電話、發送簡訊等紀錄。</td><td>步驟(4)中，未發現有背景撥打電話、發送簡訊之紀錄。

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。</td></tr>
<tr><td colspan="2">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。</td></tr>
<tr><td colspan="2">檢測條件：
■ 申請者須提供智慧型手機管理者權限
■ 受測軟體為非常駐程式
■ 資料型別：無
■ 受測軟體屬性：出廠預載、銷售商加載</td></tr>
<tr><td>檢測方法</td><td>判定標準</td></tr>
<tr><td>(1) 開啟受測系統。
(2) 確認已符合檢測條件。
(3) 以管理者權限取得所有執行中的應用程式清單。
(4) 執行並操作受測軟體。
(5) 關閉步驟(4)執行之受測軟體，並再次以管理者權限取得所有執行中的應用程式清單。
(6) 檢查步驟(5)之清單是否與步驟(3)之清單相同。</td><td>步驟(6)中，步驟(5)之清單與步驟(3)之清單相同。

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。</td></tr>
</table>

6.4.2.2 無圖示軟體選測項目

如申請者希望了解無圖示軟體之安全性，可自行選擇檢測無圖示軟體之中級檢測項目如表 6，詳細檢測內容請參閱 6.4.1。

表 6 無圖示軟體之中級檢測項目與檢測細項

層別	檢測項目	檢測細項	資通安全等級	檢測編碼
應用程式層 (A)	3. 程式執行授權	3. 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。	M	A.3.3.M(+)
通訊協定層 (P)	2. 協定傳輸保護	3. 手機系統內建軟體與付費功能伺服器間之資料加密傳輸，應使用安全之加密演算法。	M	P.2.3.M(+)

6.5 高級檢測項目

6.5.1 必測項目

本節就出廠預載軟體與銷售商加載軟體，說明高級必測項目之檢測條件、檢測方法與判定標準。

O.3 系統執行安全	
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。	
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	於步驟(1)或(2)中，受測系統之傳輸過程具備安全通道。

時，則請申請者做功能示範。	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。
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。	
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，受測系統之開機過程具備自我安全功能測試。 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。
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。	
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，受測系統之認證失敗處理方式符合資料覆蓋方式，可安全抹除受保護之資料。 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。

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。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。
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。	
檢測條件： ■ 申請者須提供書面資料作為審查依據 ■ 必要時請廠商進行功能示範 ■ 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，受測硬體之金鑰儲存保護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。
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。	
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，受測硬體之金鑰傳輸保護符合不匯出或傳輸之要求。金鑰若需以加密方式匯出或傳輸，加密之強度須為原演算法金鑰強度等級（含）以上。加密強度參考 NIST、ANSI 或 IEEE 發布之資料。 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。

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。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，受測硬體之演算法符合技術要求。 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。

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。相關標準為：
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，受測硬體之初始向量符合技術要求。 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。

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。相關標準臚列如下：

NIST SP 800-90A、 ANSI X9.31-1998	
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，受測硬體之亂數符合技術要求。 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。

附件 1　智慧型手機系統內建軟體資通安全檢測申請書

申請日期：　年　月　日

<table>
<tr><td colspan="2">申請者
(公司、商號名稱)</td><td colspan="2">☐製造商 ☐電信業者
☐我國代理商</td><td colspan="2">○○○股份有限公司</td><td rowspan="5">申請者用印
(大、小章)</td></tr>
<tr><td colspan="2">統一編號</td><td colspan="4"></td></tr>
<tr><td colspan="2">營業所地址</td><td colspan="4">☐☐☐-☐☐</td></tr>
<tr><td colspan="2">代表人姓名</td><td colspan="4"></td></tr>
<tr><td rowspan="2">聯絡人</td><td>姓名及職稱</td><td></td><td>電子信箱</td><td colspan="2"></td></tr>
<tr><td>聯絡電話</td><td></td><td>傳真機</td><td colspan="2"></td></tr>
<tr><td colspan="2">製造商及地址</td><td colspan="5">○○○股份有限公司
☐☐☐-☐☐</td></tr>
<tr><td colspan="3">智慧型手機之廠牌/型號/名稱</td><td colspan="4">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">智慧型手機申請檢測之作業系統版本</td><td colspan="4">○○○-○○○-○○○</td></tr>
<tr><td colspan="2">申請檢測安全等級</td><td colspan="5">☐初　☐中　☐中(含選擇檢測項目)　☐高　☐高(含選擇檢測項目)</td></tr>
<tr><td colspan="2" rowspan="5">智慧型手機具備功能資訊</td><td>定位功能</td><td colspan="4">☐ 美國全球定位系統 GPS　☐ 歐盟伽利略 Galileo
☐ 俄羅斯格洛納斯 GLONASS　☐ 其他，_____
☐ 中國北斗衛星導航(☐可雙向傳輸)</td></tr>
<tr><td>無線傳輸技術</td><td colspan="4">☐ 藍牙　☐行動通訊網路 (☐2G ☐3G ☐4G)
☐ WLAN　☐其他，_____
☐ NFC (☐ Peer-to-Peer Mode ☐ Read/Write Mode)</td></tr>
<tr><td>生物辨識</td><td colspan="4">☐ 無　☐ 有，指紋辨識、…</td></tr>
<tr><td>外接記憶體</td><td colspan="4">☐ 無　☐ 有，microSD card、…</td></tr>
<tr><td colspan="2"></td><td colspan="4"></td></tr>
<tr><td colspan="2" rowspan="3">檢附智慧型手機樣品數量</td><td>初級</td><td colspan="4">☐ 受測樣品 2 支</td></tr>
<tr><td>中級</td><td colspan="4">☐ 受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td>高級</td><td colspan="4">☐ 受測樣品 2 支，並配合檢測項目需要提供管理者權限</td></tr>
<tr><td colspan="2">檢附文件
(正本或影本)</td><td colspan="5">☐1.中文或英文之使用手冊或說明書
☐2.中文或英文之規格資料
☐3.公司登記證明文件或商業登記證明文件；申請者為外國製造商者，應檢附該製造商之設立相關證明文件
☐4.廠商自我宣告表、內建軟體摘要表
☐5.安全功能規格表、設計安全性表及安全架構表(申請高級者須檢附)
☐6.光碟片乙份(含檢測申請書及第 1 項至第 5 項內容)</td></tr>
<tr><td colspan="7">[註]檢測實驗室除留存本申請書正本及光碟片外，應將檢測申請書影本、智慧型手機樣品及其餘文件於出具檢測報告時一併發還申請者。</td></tr>
<tr><td colspan="2" rowspan="4">檢測實驗室
(由實驗室填寫)</td><td colspan="5">檢測實驗室名稱：</td><td rowspan="4">檢測實驗室用印</td></tr>
<tr><td colspan="5">出具檢測報告乙份：
1.檢測報告編號：_____
2.安全等級：☐初級 ☐中級 ☐高級</td></tr>
<tr><td>受理日期</td><td></td><td>完成日期</td><td colspan="2"></td></tr>
<tr><td>聯絡人</td><td></td><td>聯絡電話</td><td colspan="2"></td></tr>
</table>

附件 2　廠商自我宣告表-1 （範例）

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	受測軟體名稱	是否存取敏感性資料	是否支援無線傳輸技術	是否具帳號密碼登入
1	電話	company 1.2.2	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____	☐否 ☐是

附件 2　廠商自我宣告表-2 （範例）

受測軟體基本資訊			應用層			
項次	受測軟體名稱	發行商及版本	功能說明	權限說明	資料連結伺服器之IP/DN/公司名稱及伺服器類型	是否開啟通訊埠
1	電話	company 1.2.2	☐常駐軟體 ☐非常駐軟體 說明： 可從通訊錄中撥打電話。	READ_CONTACTS：用於訊息分享功能 ACCOUNT_MANAGER：用於新增帳號到社群 CAMERA：用於圖片紀錄功能 INTERNET：用於連線主機，取得最新公告	apPchat. example.net：一般主機 111.112. 113.114：付費功能主機	☐否 ☐是， 埠號：____

[註] 伺服器類型包含一般主機及付費功能主機。

附件 3　內建軟體摘要表

內建軟體摘要表

1.智慧型手機之廠牌/型號/名稱：APPLE / a16xx / iPhone 6s

2.智慧型手機之作業系統版本：○○○-○○○-○○○

3.智慧型手機之內建軟體資訊如下：

編號	名稱	發行商及版本	屬性	功能說明	權限說明
APP01	電話	Company 1.2.2	■出廠預載 □銷售商加載 □無圖示	(1)從通訊錄中撥打電話	(1)READ_CONTACTS：用於訊息分享功能 (2)ACCOUNT_MANAGER：用於新增帳號到社群 (3)CAMERA：用於圖片紀錄功能 (4)INTERNET：用於連線主機，取得最新公告
APP02	…		□出廠預載 □銷售商加載 □無圖示		
…	…		□出廠預載 □銷售商加載 □無圖示		
			□出廠預載 □銷售商加載 □無圖示		
			□出廠預載 □銷售商加載 □無圖示		

附件 4　安全功能規格表

安全功能介面名稱 TSFI	目的 Purpose	安全功能介面可實現之安全功能需求 SFR	操作方式 Method of Use	參數 Parameter	執行動作 Actions	錯誤訊息 Error Message
列出所有安全功能介面。	說明各安全功能介面之安全功能目的。	說明各安全功能介面如何實現附檢測項目之 O.7~O.11 以及 H.1~H.5 所列之安全功能需求。	說明如何使用各安全功能介面。	說明各安全功能介面所有參數及其意義。	說明各安全功能介面如何運作及其執行細節。	說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。
範例： *TSFI_CLI*	*範例：* *提供命令列模式操作介面*	*範例：* *SFR_安全管理:提供安全管理功能*	*範例：* *以 ssh 連接待測物，即提供命令列模式操作介面*	*範例：* *ID & password*	*範例：* *可下達管理命令操作待測物*	*範例：* *連接失敗* *認證失敗*

附件 5　設計安全性表

子系統名稱 Subsystem	目的 Purpose	子系統隸屬之安全功能介面 TSFI	子系統行為說明 Behavior Description
列出各安全功能介面之子系統。	說明各子系統之安全功能目的。	說明各子系統隸屬於附件 3 所列之安全功能介面。	說明各子系統行為如下： (1) 如何實現安全功能介面的功能。 (2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。
範例： *Subsystem_ssh*	*範例：* *提供 ssh 服務*	*範例：* *TSFI_CLI*	*範例：* *(1) 提供 TSFI_CLI 命令列模式操作介面* *(2) 與其他子系統之互動：* *(A) Subsystem_auth: 傳遞認證資訊給 Subsystem_auth，並由回覆訊息確認認證是否成功* *(B) Subsystem_terminal: ...*

附件 6　安全架構表

項目	說明	
	安全領域名稱	**安全領域說明**
1.安全領域 Security Domain	列出各安全功能介面對應之安全領域 *範例：* *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 *範例：* *透過 TSFI_GUI 來執行管理功能石，該 TSFI 同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。*

項目	說明	
	相關元件	**初始程序說明**
2.初始程序 Secure Initialization	操作待測物的相關元件/環境 *範例：* *待測物網路連接程序*	提供安全啟動待測物之相關元件啟始步驟及安裝程序。 *範例：* *1. 從端口標記為 0/ 0(ethernet0 / 0 接口)連接一個 RJ- 45 電纜到交換機或路由器 Trust 安全區。* *2. 從端口標記為 0/ 1(ethernet0 / 1 接口)連接一個 RJ- 45 電纜到交換機或路由器中的 DMZ 安全區。*

項目	說明		
	自我保護功能	**與外部設備之關係**	**自我保護機制說明**
3.自我保護 Self-Protection	列出各安全功能介面對應之自我保護機制 *範例：* *TSFI_WEB:* *自我保護 1:身分驗證* *自我保護 2:遠端連線加密*	說明安全功能及其介面與外部設備之資料交換動作 *範例：* *遠端以瀏覽器連線待測物進行管理功能時，以 TSFI_WEB GUI 介面進行身分認驗證*	需說明安全功能介面提供實體上或邏輯上的自我保護機制 *範例：* *1. 應輸入通行碼才能進入介面。* *2. 資料傳輸機制：TLS/SSL。* *3. 特殊執行方式：指紋辨識。* *4. 特殊設備需求：指紋辨識器。*

項目	說明	
4.防止繞道 Non-Bypassibility	**防止繞道功能**	**防止繞道機制說明**
	列出各安全功能對應之防止繞道機制 *範例：* *TSF_Authentication 身分驗證功能*	1. 列舉可能繞道之手法 2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 *範例：* *可能直接以維護介面不經身分認證操控待測物。* *防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。*