IoT-2006-2

門禁系統資安測試規範

-第二部：門禁管理平台

V2.0

行動應用資安聯盟

中華民國 112 年 12 月

目錄

引言

門禁系統近年常見駭客癱瘓門鎖系統、門鎖鎖不住、人臉資訊外洩及使用者個資遭竊等資安威脅，有鑑於此，於經濟部工業局(數位發展部數位產業署承接)支持下制定本系列標準，本系列標準基於國際工控資安標準 IEC 62443 及歐盟資安標準 ETSI EN 303 645，針對智慧門禁系統上相關應用的裝置制定一系列門禁系統相關裝置之資安標準，協助台灣產業接軌國際，提升研發技術及保證產品質量。

「IoT-2006-2 門禁系統資安測試規範-第二部：門禁管理平台」(以下簡稱本測試規範)，依據「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」訂定，同時參照「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」俾利門禁系統裝置製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。本測試規範中具體明列資安檢測之測試項目、測試條件、測試方法及測試標準等事項。

1. 適用範圍

本規範適用於門禁系統中的門禁管理平台(如圖 1)。

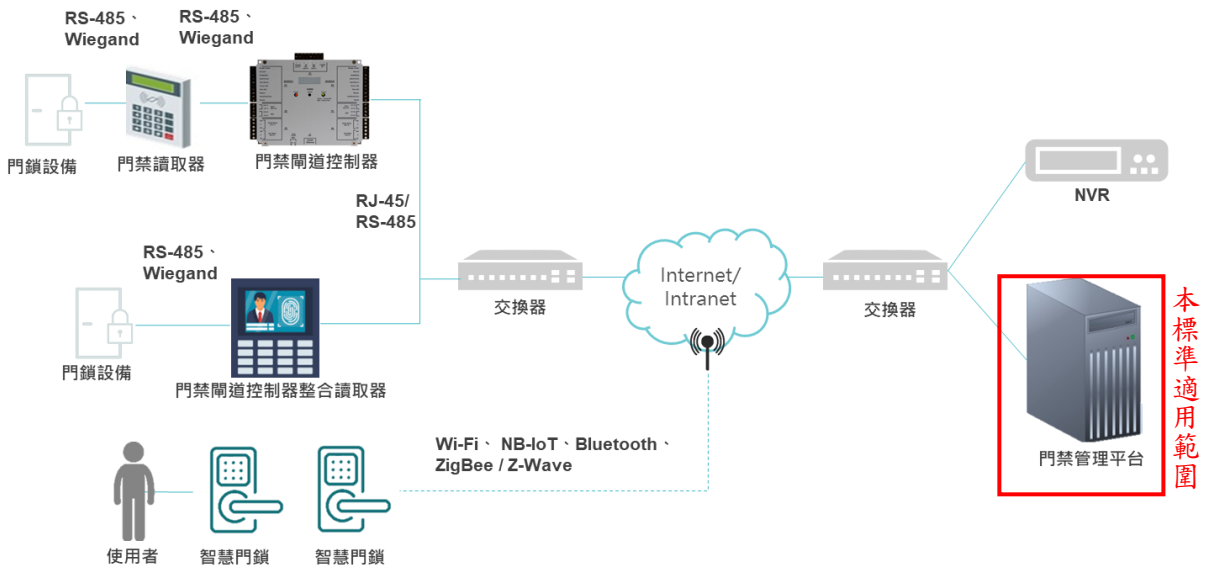

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] IEC 62443-4-2-2019 Security for industrial automation and control systems,Part 4-2: Technical security requirements for IACS components

[2] ETSI EN 303 645 V2.1.1(2020-06) Cyber Security for Consumer Internet of Things:Baseline Requirements

[3] IoT-1006-2 v1.0 門禁系統資安標準-第二部：門禁管理平台

3. 用語及定義

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」所規定之用語及定義適用於本規範。

4. 測試項目分級

本節依據「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」制定相對應之安全測試項目及測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：身分鑑別、識別、授權機制安全、系統完整性、系統機密性、資源可用性、更新安全、警示與紀錄及個人資料/隱私資料安全；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準。其中，關於第三欄安全等級之安全要求項目說明，如下所述：

- 強制性(Mandatory)的安全要求項目，在本欄中僅以編號表示。
- 選擇性(Option)的安全要求項目，在本欄中在編號後加入(O)表示。 (O)之項目不具強制性，可依產品需求及特性選擇是否納入檢測。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品應先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試標準等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
身分鑑別、識別、授權安全	5.1.1 鑑別機制	5.1.1.2 5.1.1.3 5.1.1.4 5.1.1.5 5.1.1.6	-	5.1.1.7
	5.1.2 權限控管	5.1.2.2 5.1.2.3 5.1.2.4 5.1.2.5	5.1.2.6 5.1.2.7	5.1.2.8 5.1.2.9 5.1.2.10 5.1.2.11
	5.1.3 通行碼鑑別	5.1.3.2 5.1.3.3 5.1.3.4 5.1.3.5	-	-
系統完整性	5.2.1 資料完整性	5.2.1.2	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.2.2 安全管理程序	-	-	5.2.2.2
	5.2.3 已知漏洞安全	-	5.2.3.2	-
系統機密性	5.3.1 敏感性資料保護	-	-	-
資源可用性	5.4.1 作業系統與網路服務	5.4.1.2	5.4.1.3	-
	5.4.2 資源管理	-	-	-
更新安全	5.5.1 軟韌體更新	-	-	-
警示與紀錄	5.6.1 安全事件日誌檔與警示	-	-	-
個人資料/隱私資料安全	5.7.1 個人資料/隱私資料保護能力	5.7.1.1(O) 5.7.1.2 5.7.1.3 5.7.1.4(O) 5.7.1.5 5.7.1.6 5.7.1.7 5.7.1.8(O) 5.7.1.9 5.7.1.10(O) 5.7.1.11(O)	-	-

5. 資安測試規範

門禁管理平台為滿足安全功能應依不同級別依循 IoT 1006-1「門禁系統資安標準第一部：一般要求[1]」測試規範及本節所載明之測試規範。

5.1 身分鑑別、識別、授權安全測試

檢視產品有關身分鑑別、識別、授權安全部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.1.1 鑑別機制測試

5.1.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.1.1 節。**

5.1.1.2 **身分鑑別機制測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 產品應保持出廠預設環境狀態。

(3) 若產品支援使用者介面，應提供本地端管理介面。

(4) 廠商應提供產品身分鑑別機制說明文件作為審查依據。

(5) 廠商應提供變更設定需進行身分驗證之產品功能說明文件作為測試依據。

(d) 測試目的：

驗證產品安全相關設定功能進行變更時，是否具備身分鑑別機制。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

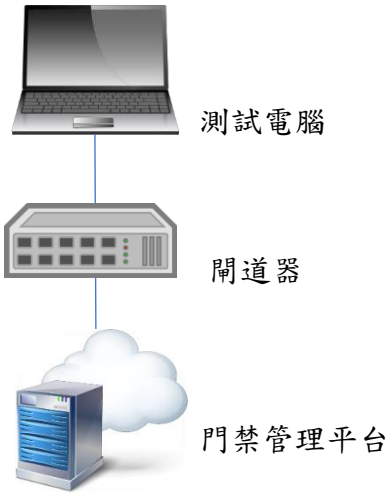

圖 2 測試示意圖

(g) 測試方法：

(1) 審閱廠商提供之說明文件。

(2) 將測試電腦與產品連接，並設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(3) 根據產品使用說明，開啟管理介面之使用者登入頁面。

(4) 以產品之系統管理者帳號、通行碼登入，執行身分鑑別操作。

(5) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。

(6) 檢視身分驗證結果。

(7) 根據說明文件對產品安全相關功能進行設定變更，包括但不限於登入本地端管理介面、實體介面執行通行碼變更或權限角變更。

(8) 檢視產品在開啟功能設定時，是否執行身分驗證機制。

(h) 測試結果：

(1) 產品具備身分鑑別機制，且產品能正常執行身分鑑別機制。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 當變更安全相關設定功能時，產品具備身分驗證機制。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：無。

5.1.1.3 **定期更新身分鑑別碼測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

應提供產品使用手冊，說明身分鑑別碼定期(提醒)更換功能的作法。

(d) 測試目的：

驗證產品之身分鑑別因子定期更新功能是否符合公認資安產業慣例。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品使用手冊。

(2) 根據使用手冊說明，驗證產品更改身分鑑別碼設定。

(h) 測試結果：

(1) 產品使用手冊與身分鑑別碼設定之作法應定期(提醒)更新，或身分鑑別碼管理機制符合 NIST SP 800-63B 之要求。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.1.1.4 使用者帳戶管理功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 產品應提供使用者帳戶管理書面文件，以說明產品如何管理使用者帳戶，作為審查依據。

(d) 測試目的：

驗證產品是否支援管理使用者帳戶的功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品使用者帳戶管理書面資料。

(2) 根據書面資料說明，操作產品使用者帳戶管理功能。

(h) 測試結果：

(1) 產品提供之書面資料證實產品支援管理使用者帳戶的功能，包括但不限於新增/刪除/修改使用者帳戶資訊、使用者權限設定等。

(2) 產品支援使用者帳戶管理功能，將所有使用者帳戶集中管理。

(3) 通過：(1)~(2)項結果符合其一。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.1.1.5 **識別碼管理功能測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

系統管理者帳號、通行碼。

(d) 測試目的：

驗證產品是否具有管理識別碼的功能。

(e) 測試條件：

產品應具備身分鑑別機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 開啟產品之管理頁面。

(2) 檢視是否有管理使用者之識別碼的功能，例如:使用者角色、使用者群組等類別新增、移除、修改等方式。

(h) 測試結果：

(1) 產品之管理介面應提供管理識別碼的功能，例如:對使用者角色、使用者群組等類別作新增、移除、修改等功能。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援身分鑑別機制。

5.1.1.6 **安全警語測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 一般使用者帳號、通行碼。

(3) 產品應提供安全警語資訊，與設定功能相關說明文件作為測試依據。

(d) 測試目的：

驗證產品是否具有安全警語功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

圖 3 測試示意圖

(g) 測試方法：

(1) 根據產品說明文件，以管理者帳號、通行碼登入系統。

(2) 開啟安全警語設定功能，並修改安全警語內容。

(3) 以使用者帳號、通行碼登入之頁面，檢視登入頁面。

(h) 測試結果：

(1) 產品提供之說明文件足以證實與充分讓管理者了解產品具備安全警語設定功能。

(2) 安全警語功能之設定方式包括但不限於內建安全警語供管理者選用，或提供管理者自行輸入警語。

(3) 產品之使用者登入介面顯示所設定之安全警語。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：無。

5.1.1.7 多因子身分鑑別測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.1.7

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品之使用者帳戶及相關鑑別因子(例如:通行碼)已建立，且多因子鑑別功能已啟用。

(2) 產品應提供具多因子鑑別操作之說明文件作為測試依據。

(3) 使用者帳號、通行碼及其他鑑別因子。

(d) 測試目的：

驗證產品是否支援多因子身分鑑別機制。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品使用說明，開啟相對應之使用者存取介面連接工具以執行鑑別。

(3) 執行多因子鑑別操作，查驗每次的鑑別均採用不同種類之鑑別因子。

(4) 查驗鑑別過程中，使用行動裝置作為所持物(something you have)之鑑別因子時，查驗僅可在 1 台行動裝置上獲取鑑別因子。

(h) 測試結果：

(1) 使用者存取介面與產品之間的鑑別，透過多因子鑑別。

(2) 每一階段鑑別皆採用不同鑑別因子，例：第 1 階段為輸入通行碼，而第 2 階段為人臉辨識。

(3) 當行動裝置作為所持物之鑑別因子時，僅可在 1 台行動裝置上獲取鑑別因子。

(4) 通過：(1)~(3)項結果皆符合。

(5) 不通過：(1)~(3)項結果不符合其一。

(6) 不適用：無。

5.1.2 權限控制測試

5.1.2.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.1.2 節。**

5.1.2.2 **使用者權限控管機制測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供使用者角色存取之權限配置宣告作為審查依據。

(2) 提供不同角色類別之使用者帳號、通行碼。

(d) 測試目的：

驗證產品是否具有使用者存取權限管控機制。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱廠商所宣告之使用者權限配置是否以不同的角色類別來分派工作的管理、權限授予及操作系統層級，並查驗實際產品運行與宣告內容是否一致。

(2) 將測試電腦連接產品。

(3) 自使用者存取介面，分別以不同角色登入產品。

(4) 存取產品資料，檢視該帳戶之角色與其對應之權限與產品宣告相符。

(5) 操作產品功能權限，檢視該帳戶之角色與其對應之權限與產品宣告相符。

(h) 測試結果：

(1) 產品所宣告的使用者，其操作所需之身分授權與產品宣告相符。

(2) 產品所宣告的權限控制機制，將不同的使用者角色分派其管理工作、權限授予及系統操作。

(3) 產品所宣告的權限控制機制僅能讓使用者角色存取所必需的產品資料。

(4) 產品所宣告的權限控制機制僅能讓授權的使用者執行符合其角色權限的操作。

(5) 通過：(1)~(4)項結果皆符合。

(6) 不通過：(1)~(4)項結果不符合其一。

(7) 不適用：無。

5.1.2.3 **會話鎖定功能測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供會話鎖定、解鎖與更改閒置時間之操作步驟。

(2) 產品應宣告人員操作之介面(例如:實體及遠端)

(3) 系統管理者帳號、通行碼。

(d) 測試目的：

驗證產品是否具備自動或手動會話鎖定功能，以防止非預期的存取。

(e) 測試條件：

產品應支援人員操作介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品說明，登入產品操作介面。

(3) 進入產品管理介面，嘗試更改閒置時間。

(4) 將產品閒置至設定之時間，檢查產品操作介面是否已鎖定。

(5) 根據 5.1.2.4 項之方法，解除操作介面鎖定。

(6) 以手動方式啟動操作介面鎖定。

(7) 檢查產品操作介面是否已鎖定。

(h) 測試結果：

(1) 產品具閒置時間後自動鎖定功能，且可透過更改閒置時間功能更改。

(2) 產品提供手動會話鎖定功能。

(3) 通過: (1)~(2)項結果符合其一。

(4) 不通過: (1)~(2)項結果皆不符合。

(5) 不適用: 產品不支援人員操作介面。

5.1.2.4 **解除會話鎖定功能測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.4

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 產品應宣告人員操作之介面作為測試依據。

(3) 產品應提供至少 2 筆使用者及解鎖權限紀錄之對應表，第 1 位使用者具會話鎖住及解鎖權限，第 2 位使用者不具解鎖權限，作為測試使用。

(d) 測試目的：

當會話鎖住時，驗證產品是否於相同使用者再次身分認證後，提供解鎖之功能。

(e) 測試條件：

產品應支援人員操作介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 以 5.1.2.3 項之方法使用權限紀錄對應表中之第 1 位使用者，登入產品操作介面後，觸發鎖定功能。

(2) 嘗試以該使用者身分，再次登入並進行存取。

(3) 再次觸發會話鎖定功能。

(4) 嘗試以使用權限紀錄對應表中之第 2 位使用者之身分，登入並進行存取。

(h) 測試結果：

(1) 會話鎖定時，可透過第 1 位使用者之身分登入解鎖並進行存取。

(2) 會話鎖定時，無法以第 2 位使用者身分登入及存取。

(3) 通過: (1)~(2)項結果皆符合。

(4) 不通過: (1)~(2)項結果不符合其一。

(5) 不適用: 產品不支援人員操作介面。

5.1.2.5 **超級使用者權限測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.5

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供具聯網功能之應用程式(Software Application)權限使用說明文件，作為審查依據。

(2) 若存在超級使用者或特權管理者權限為產品運行之必要時，產品應宣告設置超級使用者或特權管理者權限的需求與管理之說明文件，作為審查依據。

(d) 測試目的：

驗證產品之應用程式(Software Application)是否存在超級使用者及特權管理者權限。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱產品所提供具聯網功能之應用程式權限使用說明文件。

(h) 測試結果：

(1) 產品之應用程式，不存在超級使用者權限及特權管理者。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援應用程式。

(5) 不適用：若產品存在超級使用者或特權管理者權限為產品運行之必要時，產品應提供之審查文件足以證實其存在於產品之必要性。

5.1.2.6 **軟體與裝置之權限控管機制測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.6

(b) 安全等級：

2 級。

(c) 測試資料：

廠商應提供軟體與裝置權限配置之宣告作為審查依據，例如：軟體權限對應表，列出各角色所對應之工作管理、權限等級、系統可操作之功能等。

(d) 測試目的：

驗證產品是否具有軟體與裝置之存取權限管控機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商所宣告之軟體與裝置權限配置是否依不同的角色分派其管理工作、授予權限及系統操作，並查驗實際產品運行與宣告內容是否一致。

(2) 審閱廠商所宣告之軟體與裝置權限配置是否僅能讓軟體或裝置存取所必需之資料及/或資源，並查驗實際產品運行與宣告內容是否一致。

(3) 審閱廠商所宣告之軟體與裝置權限配置是否僅能讓合法軟體或裝置執行必要的權限動作，並查驗實際產品運行與宣告內容是否一致。

(h) 測試結果：

(1) 廠商所宣告的軟體與裝置，其執行所需之權限控制與廠商所宣告的一致。

(2) 廠商所宣告的權限控制機制，將管理工作、權限授予、及系統操作分派給不同的角色。

(3) 廠商所宣告的權限控制機制僅能讓軟體、或裝置存取所必需之資料及/或資源。

(4) 廠商所宣告的權限控制機制僅能讓合法軟體、或裝置執行必要的權限動作。

(5) 通過：(1)~(4)項結果皆符合。

(6) 不通過：(1)~(4)項結果不符合其一。

(7) 不適用：無。

5.1.2.7 遠端會話終止功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.7

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 其他裝置之使用者帳號、通行碼。

(3) 產品應提供與產品相接之其他門禁裝置。

(4) 產品應提供其他門禁裝置之操作步驟作為測試依據。

(5) 產品應提供終止會話之操作步驟作為測試依據。

(6) 產品應提供更改閒置時間之操作步驟作為測試依據。

(d) 測試目的：

若產品支持遠程會話(remote session)，驗證產品建立會話後，是否提供自動或手動會話終止功能。

(e) 測試條件：

產品應支援遠端會話功能。

(f) 測試佈局：

如圖 4。

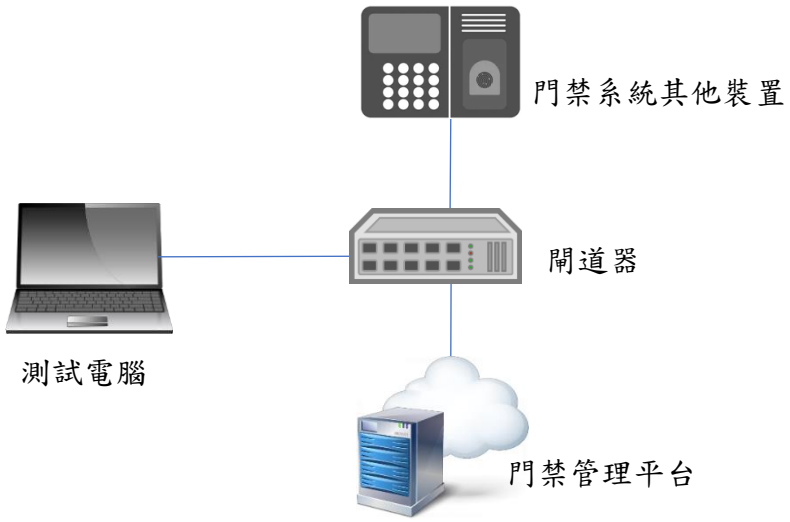

圖 4 測試示意圖

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 登入產品管理介面建立遠程會話。

(3) 嘗試更改閒置時間，並將產品閒置至設定之時間。

(4) 於會話終止時，嘗試以未授權身分之裝置，再次進行存取。

(5) 重新建立遠程會話後，嘗試手動進行會話終止。

(6) 於會話終止時，嘗試以未授權身分之裝置再次進行存取。

(7) 於會話終止時，嘗試重新建立遠程會話，並進行存取。

(8) 透過其他裝置，連上產品並建立遠程會話。

(9) 嘗試於產品更改閒置時間，並將其他裝置閒置至設定之時間。

(10) 透過其他裝置執行(4)~(7)測項。

(h) 測試結果：

(1) 產品提供閒置時間後自動終止功能，且閒置時間可進行更改。

(2) 產品提供手動會話終止功能。

(3) 會話終止後，無法於未授權狀況下存取。

(4) 會話終止後，重新建立會話時，不可再續先前會話之操作。

(5) 通過：(1)~(2)項結果符合其一，且(3)~(4)項結果皆符合。

(6) 不通過：(1)~(2)項結果皆不符合，(3)~(4)項結果不符合其一。

(7) 不適用：產品不支援遠端會話功能，或設備間須持續連線運作。

5.1.2.8 **不受信任網路存取測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.8

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 產品應提供所支援的網路服務與受信任網路之說明文件作為測試依據。

(3) 若產品提供管理者設定外部網路存取的權限，廠商應提供使用手冊作為測試依據。

(4) 產品應保持出廠預設狀態。

(d) 測試目的：

驗證產品是否能拒絕來自不受信任網路的存取。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 依產品使用說明，開啟相應之管理介面連接工具。

(3) 以系統管理者帳號、通行碼登入產品管理介面，設定不允許外部網路存取。

(4) 透過產品不信任的網路連線開啟管理介面，檢視使用者是否可存取產品。

(h) 測試結果：

(1) 產品偵測到來自不受信任網路連線應立即拒絕存取，產品若可由管理者設定允許的存取連線，則應遵循連線設定。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.1.2.9 主管覆蓋功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.9

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 一般使用者帳號、通行碼。

(3) 產品應提供與產品相連之其他門禁裝置。

(4) 產品應提供執行主管覆蓋功能與啟動機制之說明文件作為審查依據。

(d) 測試目的：

驗證產品在緊急情況下，是否支援手動執行主管覆蓋功能(Supervisor manual override)，允許管理者授權使用者對產品自動化控制機制，進行人員手動控制的功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱產品手動主管覆蓋說明文件。

(2) 依據說明文件，以管理者身分登入管理介面，設定主管覆蓋功能予使用者，例如：緊急斷電事件下，授予權限之使用者可手動開啟管制門。

(3) 以使用者身分登入系統。

(4) 啟動緊急事件，使用者是否可手動執行控制。

(h) 測試結果：

(1) 產品提供之說明文件證實產品具備手動主管覆蓋功能，且主管覆蓋功能之功能設定包括但不限於授予使用者權限、權限授予的期限、授予哪些產品操作。

(2) 產品可正確設定主管覆蓋功能，且使用者在緊急狀況下，可手動執行被授予的操作功能。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.1.2.10 雙重確認功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.10

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供說明資料，列出可能會對產品系統運作產生嚴重影響的功能，作為測試依據。

(2) 產品應提供雙重確認機制說明文件作為審查依據。

(d) 測試目的：

若產品存在可能對系統運作造成嚴重影響之功能，驗證產品是否支援雙重確認(Dual approval)功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品提供之雙重確認功能說明文件。

(2) 根據使用說明書，對系統運作會產生嚴重影響的功能進行操作與設定變更，檢視是否啟動雙重確認功能。

(h) 測試結果：

(1) 產品應支援雙重確認功能，且對系統運作會產生嚴重影響的功能執行操作、變更時，產品應啟動雙重確認功能。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無對系統運作具嚴重影響的功能，廠商應提供相關證明文件作為審查依據。

5.1.2.11 限制會話量功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.2.11

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 其他裝置之使用者帳號、通行碼。

(2) 系統管理者帳號、通行碼。

(3) 產品應提供與產品連接之其他門禁裝置。

(4) 產品應提供其他裝置之操作步驟作為測試依據。

(5) 產品應宣告可同時存在的會話數量作為測試依據。

(d) 測試目的：

驗證產品是否提供限制同時存在的會話數量之功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 登入其他裝置管理者介面，並連接產品。

(3) 根據產品宣告，嘗試建立多個會話，直到超過限制之數量。

(h) 測試結果：

(1) 產品具有限制同時存在會話數量的功能，產品無法同時存在超過限制數量的會話。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.1.3 通行碼鑑別測試

5.1.3.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.1.3 節。**

5.1.3.2 **通行碼強度設定測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.3.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 系統管理者帳號、通行碼。

(2) 一般使用者帳號、通行碼。

(3) 產品應提供使用者通行碼安全功能設定相關之使用手冊或安全指南等書面資料作為測試依據。

(d) 測試目的：

驗證產品是否提供更改使用者通行碼強度的安全設定功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

(g) 測試方法：

(1) 根據產品提供之使用者通行碼安全功能設定書面資料，開啟產品安全功能設定，檢視是否可變更使用者通行碼強度之設定。

(2) 更改使用者通行碼強度設定。

(h) 測試結果：

(1) 產品支援使用者通行碼強度安全設定功能。

(2) 產品之使用手冊或安全設定指南提供設定值建議。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1) ~(2)二項結果不符合其一。

(5) 不適用：產品不支援通行碼機制。

5.1.3.3 **通行碼長度測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.3.3

(b) 安全等級：

1 級。

(c) 測試資料：

產品之系統管理者帳號、通行碼。

(d) 測試目的：

驗證產品的通行碼長度原則是否符合至少 8 個字元。

(e) 測試條件：

產品須支援通行碼鑑別機制。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 開啟產品管理介面，建立或變更通行碼。

(3) 檢視通行碼長度設定。

(h) 測試結果：

(1) 通行碼長度設定至少 8 個字元。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援通行碼鑑別機制。

5.1.3.4 **通行碼強度測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.3.4

(b) 安全等級：

1 級。

(c) 測試資料：

系統管理者帳號、通行碼。

(d) 測試目的：

驗證產品的通行碼安全強度是否符合 NIST SP 800-63B[(2)]之規範。

(e) 測試條件：

(1) 產品應支援通行碼鑑別機制。

(2) 產品應提供通行碼鑑別機制說明文件，並列出產品之不合法的通行碼設定規則，以作為審查依據。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 開啟產品管理介面。

(3) 建立或變更通行碼。

(4) 嘗試輸入含使用者的帳戶名稱全名中、3 個以上的連續字元。

(5) 檢查通行碼是否能成功建立或變更。

(a) 測試結果：

(1) 產品之說明文件證實通行碼設定原則符合 NIST SP 800-63B 之規定，包括但不限於使用者名稱、重複字元、連續字元、英文字典字詞等。

(2) 產品應拒絕建立或變更通行碼。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援通行碼鑑別機制。

5.1.3.5 **防暴力破解通行碼功能測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.1.3.5

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之系統管理者帳戶、通行碼。

(2) 廠商應提供使用手冊或安全設定指南等書面資料，以說明產品防止通行碼暴力破解的方法。

(3) 產品應支援通行碼鑑別機制。

(d) 測試目的：

驗證產品是否提供防止暴力破解通行碼之功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品防止通行碼暴力破解的安全功能之使用說明文件。

(2) 檢視產品安全設定是否支援防止通行碼暴力破解的功能。

(h) 測試結果：

(1) 產品使用說明文件證實產品具備防止通行碼暴力破解的功能。

(2) 通行碼防止暴力破解提供之設定功能：1.最高登入失敗次數、2.帳戶鎖定之時限、3.帳戶鎖定時限內不可被存取或由系統管理者解除鎖定。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：產品不支援通行碼鑑別機制。

5.2 系統完整性測試

檢視產品有關系統完整性部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.2.1 資料保護測試

5.2.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.1 節。**

5.2.1.2 **防止惡意程式測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.2.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供書面文件，以說明保護措施如何防止產品受到惡意程式攻擊，例如:使用手冊、安全指南。

(d) 測試目的：

驗證產品是否提供防止惡意程式入侵的保護措施。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

(g) 測試方法：

(1) 審閱產品防止惡意程式保護措施之書面文件。

(2) 檢視產品是否提供保護措施或補償控制措施(Compensating control)。

(h) 測試結果：

(1) 產品之書面文件應說明支援使用的保護措施。

(2) 產品應提供防止惡意程式入侵的保護措施，例如:防毒軟體。

(3) 產品應提供防止惡意程式入侵的補償控制措施，例如:網路封包過濾設備。

(4) 通過：(1)(2)項結果符合，或(1)(3)項結果符合。

(5) 不通過：(1)(2)項結果不符合其一，或(1)(3)項結果不符合其一。

(6) 不適用：無。

5.2.2 安全管理程序測試

5.2.2.1 測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.2 節。

5.2.2.2 匯出安全設定之機器可讀格式報告測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.2.2.2

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供產品匯出安全設定之方法。

(2) 廠商應宣告產品所匯出之安全設定，支援哪些機器可讀(machine-readable)資料格式。

(d) 測試目的：

驗證產品是否提供匯出安全設定的功能，且其支援格式是否為機器可讀取的格式。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

(g) 測試方法：

依據安全設定匯出之操作方法，查驗所匯出之安全設定資料是否為電腦可讀取之格式。

(h) 測試結果：

(1) 產品可匯出安全設定資料。

(2) 產品所匯出之安全設定資料格式支援逗號分隔值(CSV)、JavaScript Object Notation (JSON)或可擴展標記語言(XML)等機器可讀格式。

(3) 通過：(1)(2)項結果皆符合。

(4) 不通過：(1)或(2)項結果不符合其一。

(5) 不適用：無。

5.2.3 已知漏洞測試

5.2.3.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.3 節。**

5.2.3.2 **產品安全監控功能測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.2.3.2

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品應提供書面資料以說明安全監控功能如何提供監控，或對接的安全監控設備符合公認資安產業慣例之證明文件作為審查依據，例如:使用手冊、安全指南。

(2) 若須仰賴其他安全監控設備，則廠商應提供支援對接的安全監控設備相關說明文件。

(d) 測試目的：

驗證產品是否使用產品安全監控的功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品提供的書面資料。

(2) 依據 CAPEC[(5)]所列舉的 Inject Unexpected Items 類及 Subvert Access Control 類的資安攻擊事件，在上述二類攻擊模型中選擇「Likelihood of attack」及

「Typical severity」為「High」的攻擊技術，以此對產品發動攻擊。或由廠商自行列出可防禦之資安攻擊事件及其防禦措施。

(3) 根據書面資料，驗證產品之安全監控功能，或所配置的安全監控設備及其安全監控功能是否能夠偵測、識別或回報。

(h) 測試結果：

(1) 產品所使用的產品安全監控功能，或產品所對接之安全監控設備，對於 CAPEC 所列舉的 Inject Unexpected Items 及 Subvert Access Control 類型的攻擊模型，針對其「Likelihood of attack」及「Typical severity」為「High」的資安攻擊事件能進行偵測、識別或回報。或可防禦廠商自行列出之資安攻擊事件的措施。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.3 系統機密性測試

檢視產品有關系統機密性部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 敏感性資料儲存安全測試

5.3.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.3.1 節。**

5.4 資源可用性測試

檢視產品有關資源可用性部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.4.1 作業系統與網路服務測試

5.4.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.4.1 節。**

5.4.1.2 **防禦 DoS 攻擊測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.4.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供書面資料以說明因應 DoS 攻擊的方法，例如:能防禦 SYN flood、Ping of Death、ARP flood 的資源消耗型 DoS 攻擊，包括但不限於產品安全設計或透過環境面的安全設置與額外部署。若以環境面額外安全部署，廠商應在產品之使用說明書或資安指南中註明產品於現場佈建時額外部署的軟硬體設備，並說明建議部署的軟硬體設備類型。

(2) 廠商應提供書面資料以說明如何在降級模式下維持產品基本功能的運作，作為審查依據。

(d) 測試目的：

驗證產品遭遇 DoS 攻擊時，產品是否能在降級模式(Degrade mode)下維持基本功能運作。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品說明文件。

(2) 使用模擬 DoS 攻擊的工具，檢視產品是否仍能維持基本功能運作。

(h) 測試結果：

(1) 產品應能在降級模式下維持產品基本運作且與說明文件相符，例如: 能防禦 SYN flood、Ping of Death、ARP flood 的資源消耗型 DoS 攻擊。

(2) 當產品以額外設備進行安全部署時，產品之使用說明書或資安指南中註明產品額外部署之軟硬體設備。且證明至少可防禦 SYN flood、Ping of Death、ARP flood 等資源消耗型 DoS 攻擊。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：產品不具備網路介面。

5.4.1.3 **緩解訊息洪泛型 DoS 攻擊能力測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.4.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供書面資料以說明產品預防訊息洪泛 DoS 攻擊的方法，例如:能防禦 UDP flood、ICMP flood 的頻寬消耗型 DoS 攻擊，包括但不限於產品安全設計或透過環境面的安全設置與額外部署。若以環境面額外安全部署，廠商應在產品之使用說明書或資安指南中註明產品於現場佈建時額外部署的軟硬體設備，並說明建議部署的軟硬體設備類型。

(2) 廠商應提供書面資料以說明產品如何減緩受到訊息洪泛 DoS 攻擊的影響，針對訊息洪泛類型 DoS 攻擊的相應測試，包括:威脅減緩測試(Threat mitigation testing)、漏洞測試(Vulnerability testing)作為審查依據。

(d) 測試目的：

驗證產品是否具備減緩受到訊息洪泛(Message flood)類型的 DoS 攻擊影響的能力。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品說明文件是否具備減緩訊息洪泛類型 DoS 攻擊的能力。

(2) 使用模擬訊息洪泛 DoS 攻擊的工具，檢視產品是否仍能減緩攻擊所造成的影響。

(h) 測試結果：

(1) 當產品遭遇訊息洪泛類型的 DoS 攻擊時，例如:UDP flood、ICMP flood，產品應能減緩訊息洪泛 DoS 攻擊對產品的影響。

(2) 當產品以額外設備進行安全部署時，產品之使用說明書或資安指南中註明產品於布建額外部署之軟硬體設備。且證明至少可緩解 UDP flood、ICMP flood 等洪泛型 DoS 攻擊。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(6) 不適用：產品不具備網路介面。

5.4.2 資源管理測試

5.4.2.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.4.2 節。**

5.5 更新安全測試

檢視產品有關更新安全部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.5.1 軟韌體更新測試

5.5.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.5.1 節。**

5.6 警示與紀錄測試

檢視產品有關警示與紀錄部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.6.1 安全事件日誌與警示測試

5.6.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.6.1 節。**

5.7 個人資料/隱私資料安全測試

檢視產品有關個人資料/隱私資料部分之送審資料是否符合 IoT-1006-2 之安全要求，並依下列各測試項目進行實機測試。

5.7.1 個人資料/隱私資料保護能力測試

5.7.1.1 個人資料傳輸安全測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.1

(b) 安全等級：

1 級(O)。

(c) 測試資料：

(1) 廠商應提出產品個人資料傳送所使用的加密演算法書面資料作為審查依據。

(2) 廠商應提出所有個人資料傳輸的邏輯介面之書面資料，邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(d) 測試目的：

驗證產品之個人資料於傳輸中是否加密。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 將測試電腦、門禁管理平台連接產品。

(2) 於相應之邏輯介面輸入產品所需之個人資料(例如:身分證字號、電話號碼)，回傳至門禁管理平台同時側錄封包。

(3) 檢視所側錄之封包。

(h) 測試結果：

(1) 個人資料以加密傳輸，使用的加密技術採用 NIST SP 800-140Cr1 所核可的同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援(或不傳輸)個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用，或不傳輸個人資料。

5.7.1.2 **敏感性個人資料加密傳輸測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提出產品敏感性個人資料傳輸所使用的加密演算法書面資料作為審查依據。

(2) 廠商應提出所有敏感性個人資料傳輸的邏輯介面之書面資料，邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(d) 測試目的：

驗證產品之敏感性個人資料於傳輸中是否加密。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 將測試電腦、門禁管理平台連接產品。

(2) 於相應之邏輯介面輸入產品所需之敏感性個人資料(例如:指紋資料、出勤打卡資料)，回傳至門禁管理平台同時側錄封包。

(3) 檢視所側錄之封包。

(h) 測試結果：

(1) 敏感性個人資料以加密傳輸，使用的加密技術採用 NIST SP 800-140Cr1 所核可的同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援(或不傳輸)敏感性個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用，或不傳輸敏感性個人資料。

5.7.1.3 **刪除使用者資料測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品之刪除使用者資料的功能與操作方法說明文件作為審查依據(包括但不限於產品使用手冊或產品官網等)。

(d) 測試目的：

驗證產品是否告知使用者如何要鋌刪除自身資料的機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品之刪除使用者資料之說明文件。

(2) 根據說明文件之操作說明，查驗產品是否具備刪除使用者資料功能。

(h) 測試結果：

(1) 產品之刪除使用者資料功能說明證實足以協助使用者刪除使用者資料，且提供使用者友善介面以執行資料刪除，且應簡化操作步驟。

(2) 使用者資料刪除功能說明記載於包括但不限於產品使用手冊。

(3) 通過：(1)~(2)項皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：產品不支援使用者資料的應用，廠商應提供相關文件以證明產品不存在任何使用者資料的使用。

5.7.1.4 **刪除個人資料之操作方法測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.4

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供產品之刪除個人資料的功能與操作方法說明文件作為審查依據(包括但不限於產品使用手冊)。

(d) 測試目的：

驗證產品是否告知使用者如何刪除個人資料的方法。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品之個人資料刪除功能之說明文件。

(2) 根據說明文件之操作方式，執行刪除個人資料功能。

(h) 測試結果：

(1) 產品之刪除個人資料刪除方法的說明文件，證實刪除的操作說明方式足以協助使用者正確完成執行個人資料的刪除。

(2) 刪除個人資料的功能操作說明，可記載於包括但不限於產品使用手冊或產品官網。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：產品不支援個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用。

5.7.1.5 個人資料管理機制測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供針對使用者個人資料之收集、利用、處理的管理機制，與管理機制實施範圍宣告之書面文件作為審查依據。

(d) 測試目的：

驗證廠商是否具備收集、利用、處理使用者個人資料的管理機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商提供之使用者個人資料管理機制之說明文件。

(h) 測試結果：

(1) 使用者個人資料的收集、利用與處理之管理機制中應對於收集哪些個人資料、使用目的、提供哪些廠商以外的第三方單位使用及資料保存的政策詳細記載於書面文件。

(2) 管理機制適用範圍包括但不限於產品開發商、系統整合商或第三方廠商。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用。

5.7.1.6 個人資料授權機制測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應基於使用者同意基礎下才能處理個人資料提出建議作法，例：使用手冊或安全指南等。。

(2) 廠商應提供針對使用者個人資料之使用授權機制，與授權機制實施範圍建議之書面文件，例：使用手冊或安全指南等。

(3) 產品應為出廠預設狀態。

(d) 測試目的：

驗證廠商是否具備使用者個人資料之使用授權機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱使用者個人資料使用授權機制之書面文件。

(h) 測試結果：

(1) 廠商於書面文件中應提供個人資料授權機制說明，包括但不限於須經使用者同意下始可處理個人資料。

(2) 授權內容應詳細描述使用個人資料的目的，並提供使用者選擇是否同意授權的機制。

(3) 使用者個人資料之使用授權機制應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網或產品包裝。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：產品不支援個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用。

5.7.1.7 **個人資料使用授權撤銷機制測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.7

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供針對使用者個人資料使用授權之撤銷機制，與機制實施範圍資安指南之書面文件作為審查依據。

(d) 測試目的：

驗證廠商是否具備使用者個人資料之使用授權撤銷機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱撤銷使用者個人資料之使用授權機制之書面文件。

(2) 驗證產品是否提供撤銷個人資料授權之機制。

(h) 測試結果：

(1) 撤銷機制書面文件應詳細說明撤銷方法，且產品可透過取消授權的機制撤銷個人資料使用授權。

(2) 使用者個人資料使用授權之撤銷機制應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網或產品包裝。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用。

5.7.1.8 **遙測數據中個人資料收集最小化測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.8

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供產品所收集遙測數據中個人資料之使用目的及實施範圍的宣告。

(d) 測試目的：

驗證產品是否存在收集預期以外的個人資料。

(e) 測試條件：

產品須支援收集遙測數據。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商提供之產品宣告。

(h) 測試結果：

(1) 產品宣告所列收集個人資料之項目符合該類產品必要之所需，實施範圍包括但不限於產品開發商、系統整合商或第三方廠商應遵守收集原則。

(2) 收集遙測數據之個人資料之使用目的與實施範圍之宣告應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網或產品包裝。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援收集遙測數據。

(6) 不適用：產品收集之遙測數據不支援個人資料的應用，廠商應提供相關文件以證明產品收集之遙測數據不存在任何個人資料的應用。

5.7.1.9 **收集遙測數據測試**

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.9

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供針對遙測數據之收集、利用、處理之宣告，及提供遙測數據的使用者聲明。

(d) 測試目的：

驗證廠商是否具備收集、利用、處理遙測數據宣告，及有哪些產品相關業者是遙測數據使用者之宣告。

(e) 測試條件：

產品須支援收集遙測數據。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商對於遙測數據收集、利用、處理宣告，與遙測數據使用者之聲明資料。

(h) 測試結果：

(1) 廠商遙測數據之宣告應對於遙測數據種類、使用目的及提供予包括但不限產品開發商、系統整合商或第三方廠商使用，資料保存的政策詳細記載於書面文件並告知使用者。

(2) 告知使用者方式包括但不限於產品使用手冊、產品官網或產品包裝。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援收集遙測數據。

(6) 不適用：產品收集之遙測數據不支援資料的應用，廠商應提供相關文件以證明遙測數據不存在任何資料的使用。

5.7.1.10 關聯服務之個人資料刪除功能測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.10

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供產品刪除存於關聯服務之個人資料的功能與操作方法說明文件作為審查依據。

(d) 測試目的：

驗證產品是否提供使用者將存在關聯服務的個人資料之刪除功能。

(e) 測試條件：

產品支援關聯服務。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱刪除存於關聯服務之個人資料的功能與操作之說明文件。

(2) 新增使用者帳戶，輸入個人資料後儲存。

(3) 根據說明文件之操作方式，查驗刪除關聯服務中個人資料的功能。

(4) 利用刪除功能將該筆使用者個人資刪除。

(h) 測試結果：

(1) 產品提供的使用者友善介面執行刪除功能，且能協助使用者以簡便的方式刪除存於關聯服務的個人資料。

(2) 儲存於關聯服務之使用者個人資料確實已被刪除。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援關聯服務。

(6) 不適用：產品之關聯服務不存在個人資料的應用，廠商應提供相關文件以證明產品之關聯服務不存在任何個人資料的使用。

5.7.1.11 回報刪除狀態測試

(a) 測試依據：

「IoT-1006-2 門禁系統資安標準-第二部：門禁管理平台」之 5.7.1.11

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供產品刪除個人資料機制之說明文件作為審查依據，例如:產品使用手冊。

(d) 測試目的：

驗證產品是否具備回報使用者個人資料刪除狀態之機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱刪除個人資料機制之說明文件。

(2) 根據說明文件之操作方式，從產品、關聯服務、應用程式等處刪除個人資料。

(3) 驗證產品是否回報刪除狀態。

(h) 測試結果：

(1) 收到產品回報的刪除狀態，例如:個人資料已自關聯服務刪除。

(2) 產品回報刪除狀態的方式與廠商說明文件相符，例如:電子郵件或簡訊通知等。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援個人資料的應用，廠商應提供相關文件以證明產品不存在任何個人資料的使用。

參考資料

(1) IoT-1006-1 v0.3: 門禁系統資安標準-第一部：一般要求

(2) NIST Special Publication 800-63: Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

(3) ISO/IEC 27039:2015 Information technology - Security techniques - Selection, deployment and operations of intrusion detection and prevention systems (IDPS), https://www.iso.org/obp/ui/#iso:std:iso-iec:27039:ed-1:v2:en

(4) NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), https://csrc.nist.gov/publications/detail/sp/800-94/final

(5) CAPEC, 1000-Mechanisms of Attack, https://capec.mitre.org/data/definitions/1000.html

(6) ETSI TS 103 701 V1.1.1- Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements, https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

版本修改紀錄

版本	時間	摘要
V1.0	111 年 7 月 22 日	版本維持不變，修改內容為編規錯誤及測試一致性問題，如勘誤與修正對照表。
V2.0	112 年 12 月 1 日	內容修訂。