IoT-2006-1

門禁系統資安測試規範

-第一部：一般要求

V2.0

行動應用資安聯盟

中華民國 112 年 11 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-2006-1 門禁系統資安測試規範-第一部：一般要求」(以下簡稱本測試規範)，依據「IoT-1006-1 門禁系統資安標準-第一部：一般要求」訂定，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、測試資料、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系列產品之共通要求，適用範圍包括門禁讀取器、門禁閘道控制器、門禁閘道控制器整合讀取器、門禁管理平台及智慧門鎖。 (如圖 1)。

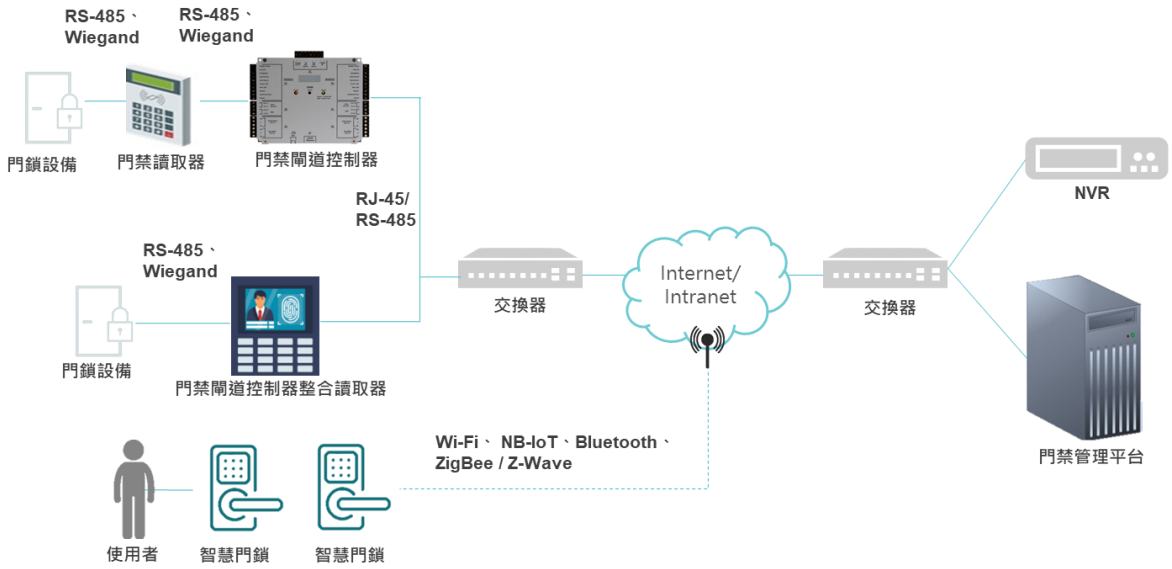

圖 1 適用範圍示意圖

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。

CNS 62443-4-2 工業自動化及控制系統之安全性,Part 4-2: IACS 組件之技術安全要求事項

CNS 16190 消費者之網宇安全：基準要求事項

IoT-1006-1 門禁系統資安標準-第一部：一般要求

3. 用語及定義

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」所規定之用語及定義適用於本規範。

3.1 本地端管理介面(Local Management Interface)

使用者直接存取與控制產品的操作介面，不需要連接網際網路經由門禁管理平台操控產品，例如產品應用程式或透過電腦與產品連接並以 IP 地址開啟的管理頁面等。

3.2 除錯模式(Debug mode)

係指一個以釐清產品故障原因為目的程式，其允許開發者透過該介面進行除錯或設定，亦稱作工程模式。

3.3 死碼刪除(Dead code elimination)

係一種最佳化技術，其用途為刪除對程式執行結果無任何影響的程式碼，這類的程式碼包括不會被執行到的程式碼，以及只影響無關程式執行結果的變數。

3.4 受限制設備(Constrained device)

係指此類設備預期用途受限於實體而產生的限制，包括但不限於處理資料的能力、通訊的能力、資料儲存的能力或與使用者互動的能力。例如感測器，它可能是實體限制的設備，可能因電源、電池壽命、運算處理能力、實體的存取、功能有限、記憶體有限或網路頻寬有限，這些限制在設備運行時可能需要搭配另一設備來支援；或者，可能是透過同一實體線路供電與資料傳輸，此設備的通訊協定與加密方式就受限於該線路配置。

4. 測試項目分級

本節依據「IoT-1006-1 門禁系統資安標準-第一部：一般要求」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、更新安全及警示與紀錄；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	5.1.1.1 5.1.1.2 5.1.1.9	5.1.1.3 5.1.1.4 5.1.1.5 5.1.1.10	5.1.1.6 5.1.1.7 5.1.1.8 5.1.1.11
	5.1.2 權限控管	5.1.2.1	5.1.2.2	-
	5.1.3 通行碼鑑別	-	-	5.1.3.1
系統完整性	5.2.1 資料完整性	5.2.1.1 5.2.1.2 5.2.1.3 5.2.1.4 5.2.1.5 5.2.1.6 5.2.1.7 5.2.1.8	5.2.1.11 5.2.1.12 5.2.1.13	5.2.1.14

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
		5.2.1.9 5.2.1.10(O)		
	5.2.2 安全管理程序	5.2.2.1 5.2.2.2 5.2.2.3 5.2.2.4 5.2.2.5(O) 5.2.2.6(O) 5.2.2.7(O) 5.2.2.8(O) 5.2.2.9	5.2.2.10	-
	5.2.3 已知漏洞安全	5.2.3.1(O) 5.2.3.2 5.2.3.3 5.2.3.4	5.2.3.5 5.2.3.6	5.2.3.7
系統機密性	5.3.1 敏感性資料保護	5.3.1.1 5.3.1.2	5.3.1.3	5.3.1.4
資源可用性	5.4.1 作業系統與網路服務	5.4.1.1 5.4.1.2 5.4.1.3 5.4.1.4(O) 5.4.1.5(O) 5.4.1.6	5.4.1.7	-
	5.4.2 資源管理	5.4.2.1 5.4.2.2(O) 5.4.2.3(O) 5.4.2.4(O)	-	-
更新安全	5.5.1 軟韌體更新	5.5.1.1 5.5.1.2 5.5.1.3 5.5.1.4(O) 5.5.1.5(O) 5.5.1.6 5.5.1.7	-	-
警示與紀錄	5.6.1 安全事件日誌檔與警示	5.6.1.1 5.6.1.2 5.6.1.3 5.6.1.4 5.6.1.5	5.6.1.9 5.6.1.10 5.6.1.11	5.6.1.12 5.6.1.13 5.6.1.14 5.6.1.15

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
		5.6.1.6 5.6.1.7 5.6.1.8		5.6.1.16 5.6.1.17

5. 資安測試規範

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 CNS XXX-1-1 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 預設鑑別碼測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.1

(b) 安全等級：

1 級

(c) 測試資料：

(1) 若產品存在預設鑑別碼，應提供產品預設鑑別碼之設計文件作為審查依據。

(2) 產品應為出廠預設組態。

(3) 廠商應提供至少 2 件產品供測試使用。

(d) 測試目的：

驗證產品是否沒有相同的預設鑑別碼，若有相同預設鑑別碼或無預設鑑別碼，則查證鑑別碼是否在首次上線後強制要求更改。

(e) 測試條件：

產品應支援鑑別碼鑑別機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品之預設鑑別碼設計文件，檢視產品是否存在相同之預設鑑別碼，或無預設鑑別碼。

(2) 將測試電腦或行動裝置連接產品。

(3) 根據使用說明文件，從管理介面輸入鑑別碼。

(4) 確認若存在相同之預設鑑別碼，或無預設鑑別碼時，在未設定新鑑別碼的情況下，不可存取產品。

(h) 測試結果：

(1) 產品之預設鑑別碼皆不同。

(2) 未經設定新鑑別碼前無法存取。

(3) 通過：(1)~(2)項結果符合其一。

(4) 不通過：(1)~(2)項皆不符合。

(5) 不適用：產品不支援鑑別碼鑑別機制。

5.1.1.2 **身分鑑別錯誤訊息測試**

(a) 網頁介面

(1) 測試依據：

「 IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者帳號搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

驗證鑑別錯誤之訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品支援網頁介面。

(6) 測試佈局：

如圖 2。

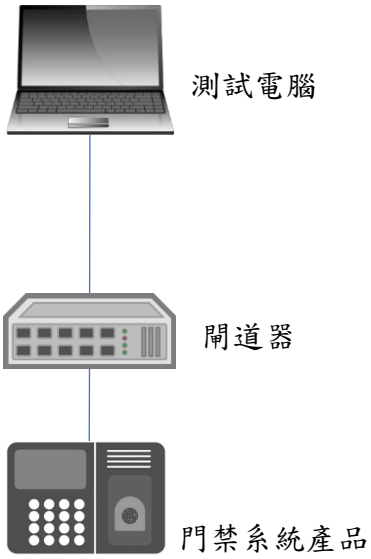

圖 2 測試示意圖

(7) 測試方法：

(i) 將測試電腦連接產品。

(ii) 根據產品使用說明，開啟網頁介面。

(iii) 輸入產品已存在之使用者帳號搭配錯誤的通行碼。

(iv) 檢視鑑別錯誤訊息。

(v) 輸入不存在之使用者帳號和通行碼。

(vi) 檢視鑑別錯誤訊息。

(8) 測試結果：

(i) 從鑑別錯誤訊息無法推斷出合法使用者名稱。

(ii) 通過：(i)項結果符合。

(iii) 不通過：(i)項結果不符合。

(iv) 不適用：產品不支援網頁介面。

(b) 實體介面

(1) 測試依據：

「 IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.2

(2) 安全等級：

1 級

(3) 測試資料：

(i) 產品之已存在使用者帳號搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品支援實體介面。

(6) 測試佈局：

如圖 3。

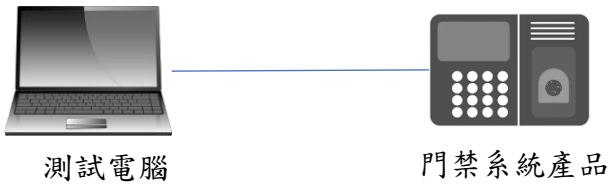

圖 3 測試示意圖

(7) 測試方法：

(i) 將測試電腦連接產品。

(ii) 若產品支援 UART，將測試電腦連接產品之 UART。

(iii) 透過 UART 埠存取作業系統之除錯模式 。

(iv) 輸入產品之已存在使用者帳號搭配錯誤的通行碼。

(v) 檢視鑑別錯誤訊息。

(vi) 輸入不存在之使用者帳號和通行碼。

(vii) 檢視鑑別錯誤訊息。

(viii)若產品支援 JTAG ，將測試電腦連接產品之 JTAG 。

(ix) 透過 JTAG 埠存取作業系統之除錯模式。

(x) 重複(iv)~(vii)之步驟。

(xi) 若產品支援 USB，將測試電腦連接產品之 USB 。

(xii) 透過 USB 埠存取作業系統之除錯模式。

(xiii)重複(iv)~(vii)之步驟。

(8) 測試結果：

(i) 從鑑別錯誤訊息中，無法推斷出使用者名稱是否存在。

(ii) 通過：(i)項結果符合。

(iii) 不通過：(i)項結果不符合。

(iv) 不適用：產品不支援實體介面。

(c) 遠端指令介面

(1) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者帳號搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(4) 測試目的：

驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品支援遠端指令介面。

(6) 測試佈局：

如圖 2。

(7) 測試方法：

(i) 將測試電腦經由網路連接產品。

(ii) 根據產品使用說明，開啟遠端指令介面。

(iii) 輸入產品之已存在使用者帳號搭配錯誤的通行碼。

(iv) 檢視鑑別錯誤訊息。

(v) 輸入不存在之使用者帳號和通行碼。

(vi) 檢視鑑別錯誤訊息。

(8) 測試結果：

(i) 從鑑別錯誤訊息中，無法推斷出使用者名稱是否存在。

(ii) 通過：(i)項結果符合。

(iii) 不通過：(i)項結果不符合。

(iv) 不適用：產品不支援遠端指令介面。

(d) API 介面

(1) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.2

(2) 安全等級：

1 級。

(3) 測試資料：

(i) 產品之已存在使用者帳號搭配錯誤的通行碼。

(ii) 不存在之使用者帳號、通行碼。

(iii) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(4) 測試目的：

驗證鑑別錯誤訊息不會造成安全敏感性資料的洩漏。

(5) 測試條件：

產品支援 API。

(6) 測試佈局：

如圖 4。

(7) 測試方法：

(i) 將測試電腦與門禁管理平台連結在同一個區域網路中。

(ii) 依據產品使用說明，將產品連結門禁管理平台。

(iii) 根據產品使用說明，開啟遠端指令介面。

(iv) 輸入產品之已存在使用者帳號搭配錯誤的通行碼。

(v) 檢視鑑別錯誤訊息。

(vi) 輸入不存在之使用者帳號和通行碼。

(vii) 檢視鑑別錯誤訊息。

(8) 測試結果：

(i) 從鑑別錯誤訊息中，無法推斷出使用者名稱是否存在。

(ii) 通過：(i)項結果符合。

(iii) 不通過：(i)項結果不符合。

(iv) 不適用：產品不支援 API 或 API 不支援通行碼鑑別。

5.1.1.3 **公開金鑰架構測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.3。

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 若產品支援公開金鑰架構(Public Key Infrastructure, PKI)，應提供所使用公開金鑰身分鑑別技術書面文件作為審查依據，例如：IETF Request for Comment (RFC) 3647 for X.509-based PKI 等。

(2) 若產品須與系統整合後方能運行之情況，廠商應提供使用手冊、安全指南等說明文件，以揭露產品如何支援系統公開金鑰架構。

(d) 測試目的：

驗證產品使用公開金鑰架構，是否遵循公認資安產業慣例之最佳技術。

(e) 測試條件：

產品支援公開金鑰架構。

(f) 測試佈局：

無。

(g) 測試方法：

審閱具備所使用公開金鑰架構鑑別技術之書面資料。

(h) 測試結果：

(1) 提供之書面資料文件足以證明所使用之技術符合公認資安產業慣例之技術，例如：IETF Request for Comment (RFC) 3647 for X.509-based PKI 等包括但不限於 ISO/IEC 國際標準、歐盟國際標準或美國國家標準等普遍業界所接受的作法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援公開金鑰架構。

5.1.1.4 公開金鑰身分鑑別機制之強度測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.4。

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供已過期的憑證。

(2) 廠商應提供未過期但已撤銷的憑證。

(3) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(4) 廠商應提供所使用公開金鑰身分鑑別技術之書面文件作為審查依據。

(5) 若不是採用自簽憑證，廠商應提供產品所使用之憑證鏈(certification path)架構說明文件作為審查依據。

(6) 廠商應出具「供使用者、軟體或裝置其所屬金鑰之儲存保護說明」文件作為審查依據。

(d) 測試目的：

驗證產品所使用之公開金鑰身分鑑別機制，是否具備安全功能。

(e) 測試條件：

產品支援公開金鑰身分鑑別機制。

(f) 測試佈局：

如圖 4。

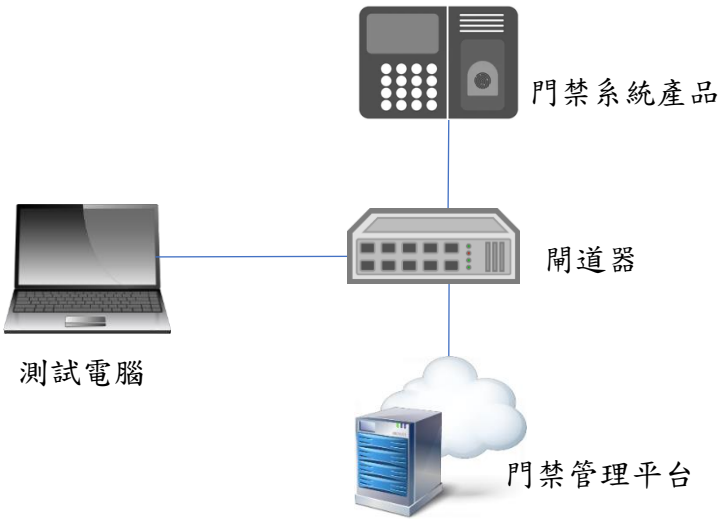

圖 4 測試示意圖

(g) 測試方法：

(1) 依據廠商宣告，開啟產品有使用公開金鑰身分鑑別機制之介面。

(2) 於該介面上，傳送合法簽章之憑證予產品，查驗身分鑑別是否成功。

(3) 於該介面上，傳送不合法簽章之憑證予產品，查驗身分鑑別是否成功。

(4) 審閱廠商所宣告之憑證鏈架構，並於產品上查驗憑證鏈資訊是否與宣告一致。

(5) 於該介面上，傳送過期之憑證予產品，查驗身分鑑別是否成功。

(6) 於該介面上，傳送效期內但已撤銷之憑證予產品，查驗身分鑑別是否成功。

(7) 審閱供使用者、軟體或裝置其所屬金鑰之儲存保護說明文件，並於該公開金鑰身分鑑別架構下申請憑證，查鑰申請過程中及申請憑證後，申請者所屬金鑰之存取權限。

(8) 於帳戶管理功能，查驗通過公鑰認證之識別碼是否可對應出使用者、軟體或裝置。

(h) 測試結果：

(1) 產品僅接受合法簽章憑證之連線。

(2) 產品之憑證鏈資訊與宣告一致。

(3) 產品可偵測及回報已撤銷之憑證。

(4) 只有金鑰擁有者可以存取所屬金鑰。

(5) 通過公鑰認證之識別碼可對應出使用者、軟體或裝置。

(6) 通過：(1)~(5)項皆符合。

(7) 不通過：(1)~(5)項不符合其一。

(8) 不適用：產品不支援公開金鑰身分鑑別機制。

5.1.1.5 **對稱金鑰身分鑑別測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.5。

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供所使用對稱金鑰身分鑑別技術書面文件，列出所使用之對稱金鑰演算法及其支援的金鑰長度，作為審查依據。

(2) 廠商應提供說明文件，說明如何使用對稱金鑰建立雙向認證，作為審查依據。

(3) 廠商應提供說明文件，說明保護共享秘密之方式，作為審查依據。

(d) 測試目的：

驗證產品所使用之對稱金鑰身分鑑別機制，是否具備安全功能。

(e) 測試條件：

產品支援對稱金鑰身分鑑別機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱建立雙向信任之說明文件，並根據廠商聲明之方法查驗是否僅受信任之對象可建立連線。

(2) 審閱共享秘密保護方法之說明文件，並根據廠商聲明之方法查驗共享秘密是否有加密儲存。

(3) 審閱建立保護共享秘密之說明文件，並根據廠商聲明之方法查驗共享秘密是否僅限共享秘密擁有者可以存取。

(4) 審閱對稱金鑰身分鑑別技術文件，查驗對稱金鑰之演算法及金鑰長度，是否符合 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(h) 測試結果：

(1) 對稱金鑰所建立之連線，僅受信任雙方可存取。

(2) 共享秘密有加密儲存。

(3) 共享秘密僅限擁有者有權限可存取。

(4) 對稱金鑰之演算法及金鑰長度符合 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(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：產品不支援對稱金鑰身分鑑別機制。

5.1.1.6 門禁裝置身分證明測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.6。

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供與產品相連的門禁管理平台或其他門禁設備，以供測試使用。

(2) 產品應提供說明文件，說明如何以信任根提供遠端證明功能之真實性核對的作法，作為審查依據。

(d) 測試目的：

驗證產品是否具有向相連接之門禁管理平台或門禁裝置(智慧門鎖、門禁讀取器、門禁控制器)證明自身之真實性的能力。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱具備遠端證明功能之設計文件。

(2) 將產品與門禁管理平台建立連線。

(3) 使用測試電腦側錄之間的封包。

(4) 檢視產品遠端證明身分之機制是否有核對身分之真實性。

(h) 測試結果：

(1) 產品具備遠端證明功能且能確保身分之真實性。

(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。

5.1.1.7 **通行碼生命週期測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.7。

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供使用者通行碼生命週期與通行碼更換之書面說明文件，作為審查依據。

(2) 產品應為原廠預設狀態。

(d) 測試目的：

驗證產品使用者通行碼是否具備生命週期，與通行碼更換功能。

(e) 測試條件：

產品支援通行碼功能。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱具備使用者通行碼生命週期功能之說明文件。

(2) 連結測試電腦與產品。

(3) 根據產品說明文件，開啟相應之使用者登入介面以執行身分鑑別。

(4) 調整測試時間至使用者通行碼生命週期即將期滿之時間，相應之使用者登入介面以執行身分鑑別，觀察期滿前提醒之行為。

(h) 測試結果：

(1) 產品具有使用者通行碼生命週期功能，且應符合公認資安產業慣例包括但不限於歐盟國際標準、美國國家標準或ISO/IEC國際標準等普遍業界所接受的作法。

(2) 產品於使用者通行碼生命週期期限屆滿前，提示提醒使用者更換。

(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：產品不支援通行碼功能。

5.1.1.8 **安全敏感性資料硬體保護機制測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.8

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供產品所使用硬體保護機制設計文件作為審查依據。

(2) 產品應提供所有安全敏感性資料清單，與以硬體保護之安全敏感性資料清單，作為審查依據。

(d) 測試目的：

驗證產品是否有使用硬體機制，來保護安全敏感性資料(短生命週期私鑰除外)。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱保護產品安全敏感性資料 (除短生命週期私鑰)之硬體機制安全設計文件或晶片型號規格，與產品以硬體機制保護之資料清單。

(h) 測試結果：

(1) 書面資料證實產品以硬體機制 (例如：安全晶片)方式保護所有具身分鑑別用之安全敏 感性資料。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品為非實體設備，例如:軟體、應用程式、網頁。

(5) 不適用：產品無安全敏感性資料，且廠商應提供佐證資料足以證明產品不存在安全敏感性資料。

5.1.1.9 **使用者身分識別與鑑別功能測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.9

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品所提供之系統管理者帳號和通行碼。

(2) 若產品為讀取器，則應提供讀取器與門禁卡之間所使用的身分鑑別機制設計之說明文件。

(3) 若產品本地端管理介面支援門禁卡：合法可通行的門禁卡及其卡片相關規格說明文件、空白門禁卡。

(d) 測試目的：

驗證產品是否具有身分識別與鑑別功能。

(e) 測試條件：

產品支援網頁介面或遠端指令介面或 API 介面或本地端管理介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 網頁介面

(i) 將測試電腦連接產品。

(ii) 於未登入的狀況下，存取身分鑑別頁面外之頁面，確認是否要求身分鑑別。

(iii) 根據產品使用說明，開啟網頁介面。

(iv) 以產品之系統管理者帳號和通行碼執行身分鑑別操作。

(2) 遠端指令與 API 介面

(i) 將測試電腦連接產品。

(ii) 根據產品使用說明，開啟所支援控制主要功能之遠端指令介面。

(iii) 以產品之系統管理者帳號和通行碼執行身分鑑別操作。

(iv) 根據產品使用說明，開啟所支援 API 介面。

(v) 以產品之 API 驗證連接方式執行身分鑑別操作。

(3) 本地端管理介面

(i) 啟動產品之本地端管理介面(UI)。

(ii) 於未登入狀況下，存取身分鑑別外之操作頁面，確認是否要求身分鑑別。

(iii) 以產品之系統管理者帳號和通行碼執行身分鑑別操作。

(h) 測試結果：

(1) 產品於網頁介面能正常執行身分鑑別機制。

(2) 產品於遠端指令介面能正常執行身分鑑別機制。

(3) 產品於 API 介面能正正常執行身分鑑別機制。

(4) 產品於本地端管理介面能正常執行身分鑑別機制。

(5) 通過：若產品支援網頁介面，則(1)項結果符合。

(6) 通過：若產品支援遠端指令介面，則(2)項結果符合。

(7) 通過：若產品支援 API 介面，則(3)項結果符合。

(8) 通過：若產品支援本地端管理介面，則(4)項結果符合。

(9) 不通過：若產品支援網頁介面，(1)項結果不符合。

(10) 不通過：若產品支援遠端指令介面，則(2)項結果不符合。

(11) 不通過：若產品支援 API 介面，則(3)項結果不符合。

(12) 不通過：若產品支援本地端管理介面，則(4)項結果不符合。

(13) 不適用：產品不支援網頁介面、遠端指令介面、API 介面和本地端管理介面。

5.1.1.10 使用者唯一識別碼測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.10

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品所提供之系統管理者帳號和通行碼。

(2) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(3) 產品應提供識別碼生成機制之書面資料作為審查依據。

(4) 產品應提供使用者身分鑑別機制之說明文件作為審查依據。

(d) 測試目的：

驗證產品之使用者識別碼是否唯一且產品是具有身分鑑別功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱具備說明唯一識別碼之生成機制的書面證明文件。

(2) 審閱以識別碼驗證之使用者身分鑑別機制的書面資料。

(3) 新增使用者帳號，檢驗使用者識別碼。

(4) 開啟產品管理介面，確認產品是否要求身分鑑別。

(h) 測試結果：

(1) 產品之使用者唯一識別碼採用至少 4 位元組長度之合理不重覆的編碼方式。

(2) 產品應具備使用者身分鑑別功能。

(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：產品不支援網頁介面、遠端指令介面、API 介面及本地端管理介面。

5.1.1.11 **產品唯一識別碼測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.1.11

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供識別碼生成機制之書面資料作為審查依據。

(2) 產品應提供產品對其他裝置身分鑑別機制之說明文件作為審查依據。

(d) 測試目的：

驗證產品之識別碼是否唯一且產品是否具身分鑑別功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備說明唯一識別碼之生成機制的書面證明文件。

(2) 審閱以識別碼驗證之身分鑑別機制的書面資料。

(h) 測試結果：

(1) 產品之唯一識別碼採用產品唯一識別碼採用 IMEI、IMSI、UUID 同等或以上重覆概率的編碼方式。

(2) 產品應具備身分鑑別功能。

(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：門禁管理平台不適用。

5.1.2 權限控管測試

5.1.2.1 行動碼完整性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.2.1。

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品支援行動碼。

(2) 廠商應提供門禁管理平台中，具有傳輸與執行行動碼權限之管理者帳號和通行碼。

(3) 廠商應提供門禁管理平台中，不具傳輸與執行行動碼權限之使用者帳號和通行碼。

(4) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(5) 廠商應提供保護行動碼完整性之方式及演算法書面資料，作為審查依據。

(d) 測試目的：

驗證產品是否具備驗證門禁管理平台所傳送行動碼完整性之功能，並限制未授權行動碼的執行。

(e) 測試條件：

產品支援行動碼。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱保護行動碼所採用之雜湊演算法。

(2) 將測試電腦與門禁管理平台連結在同一個區域網路中，將產品與門禁管理平台連接。

(3) 以使用者帳號和通行碼登入門禁管理平台，傳送行動碼至相連的產品。

(4) 確認產品是否收到行動碼。

(5) 以管理者帳號和通行碼登入門禁管理平台，傳送行動碼至相連的產品。

(6) 確認產品是否收到行動碼。

(7) 進入產品作業系統，竄改所接收之行動碼。

(8) 確認產品是否能正常執行行動碼。

(9) 將相連的產品設定為禁止執行行動碼。

(10) 確認產品是否可執行行動碼。

(h) 測試結果：

(1) 行動碼完整性保護，採用 NIST SP 800-140Cr1 [(2)]所核可之同等或以上強度之雜湊演算法。

(2) 以不具行動碼傳輸權限的帳號無法傳送行動碼，產品未收到行動碼。

(3) 產品無法執行遭竄改過的行動碼。

(4) 限制禁止執行行動碼的產品，接收到行動碼後仍無法執行。

(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：產品不支援行動碼、產品不下載行動程式碼至門禁裝置，或無法執行行動程式碼功能。

5.1.2.2 **行動碼真實性測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.2.2。

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 行動碼封包。

(2) 竄改後的行動碼封包。

(3) 門禁管理平台之具傳輸行動碼權限之管理者帳號和通行碼。

(4) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(5) 廠商應提供保護行動碼真實性之方式及演算法書面資料，作為審查依據。

(d) 測試目的：

驗證產品是否具備驗證門禁管理平台所傳送行動碼真實性之功能。

(e) 測試條件：

產品支援行動碼。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 方法 1：

(i) 審閱簽章所採用之演算法。

(ii) 將測試電腦與門禁管理平台連結在同一個區域網路中。

(iii) 將產品連結門禁管理平台，透過管理者登入門禁管理平台後，傳送行動碼至產品。

(iv) 擷取傳送中的行動碼封包。

(v) 置換簽章後，發送至產品。

(vi) 檢視竄改過之封包是否被接受。

(2) 方法 2：

(i) 將測試電腦與門禁管理平台連結在同一個區域網路中。

(ii) 將產品連結門禁管理平台，透過管理者登入門禁管理平台後，傳送行動碼至產品。

(iii) 使用封包側錄工具，側錄門禁管理平台與產品之間的封包。

(iv) 檢視所側錄之封包。

(h) 測試結果：

(1) 產品不接受遭置換過簽章之行動碼封包，且簽章演算法應採用 NIST SP 800-140Cr1 所核可之同等或以上強度之演算法。

(2) 以安全通道傳輸行動碼封包，且安全通道所使用之密碼件如附錄 A 所建議，或符合 NIST SP 800-140Cr1 所核可之同等或以上等級之密碼演算法。

(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：產品不支援行動碼、產品不下載行動程式碼至門禁設備裝置，或不支援執行行動碼的功能。

5.1.3 通行碼鑑別測試

5.1.3.1 設定通行碼生命週期測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.1.3.1

(b) 安全等級：

3 級。

(c) 測試資料：

產品應提供使用者通行碼生命週期設定功能之說明文件作為審查依據，例如:使用手冊、安全設定指南。

(d) 測試目的：

驗證產品是否支援強制設定使用者通行碼最小和最大生命週期的功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品使用者通行碼生命週期說明文件。

(2) 根據說明文件，檢視產品設定頁面是否提供強制設定使用者通行碼最小和最大生命週期的功能。

(h) 測試結果：

(1) 產品支援設定使用者通行碼最小和最大生命週期的功能，且此功能應為強制設定項目。

(2) 產品之通行碼最小和最大生命週期應與產品說明文件一致。

(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：不支援以使用者通行碼作為身分鑑別。

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-1006-1 之安全要求，並依下列各測試項目進行實機測試。

5.2.1 資料完整性測試

5.2.1.1 接收安全敏感性資料之完整性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 產品應保持出廠預設環境狀態。

(3) 產品應提供接收安全敏感性資料之完整性檢查的說明文件，供測試使用。

(4) 產品應提供敏感性資料傳輸保護之完整演算法書面文件作為審查依據。

(d) 測試目的：

驗證產品是否對所接收之安全敏感性資料具有完整性檢查。

(e) 測試條件：

產品應存在敏感性資料。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審查廠商所提供之接收安全敏感性資料之完整性檢查說明文件。

(2) 根據說明文件，將安全敏感性資料自門禁管理平台或其他門禁裝置傳送至產品，檢視產品是否核對其完整性。

(h) 測試結果：

(1) 產品在接收安全敏感性資料時有檢查完整性，且完整性核對錯誤時拒絕接收。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無安全敏感性資料，或不傳送及接收安全敏感性資料廠商應提供佐證資料足以證明產品不存在安全敏感性資料，或不傳送及接收安全敏感性資料。

(5) 不適用：產品為無法連接外部網路之門禁讀取器，廠商應提供足以佐證之資料。

5.2.1.2 **安全敏感性資料的完整性測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 廠商應提供安全敏感性資料之完整性檢查的說明文件作為審查依據。

(d) 測試目的：

驗證產品是否確保安全敏感性資料之完整性。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱能證明符合此安全要求之安全敏感性資料之完整性檢查的說明文件。

(2) 產品讀取所儲存的安全敏感性資料、接收其他設備所傳送的安全敏感性資料時，檢視是否驗證其完整性。

(3) 檢視安全敏感性資料之完整性演算法。

(h) 測試結果：

(1) 書面資料證實產品在儲存、使用與傳輸過程中，有驗證檔案的完整性。

(2) 產品安全敏感性資料之完整性演算法，採用 NIST SP 800-140Cr1 所核可之同等或以上強度的演算法。

(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：產品無安全敏感性資料，且廠商應提供佐證資料足以證明產品不存在安全敏感性資料。

(6) 不適用：若產品為無法連接外部網路之門禁讀取器，廠商應提供足以佐證之資料。

(7) 不適用：產品不支援作業系統(例:Windows、Linux)且無除錯介面。

5.2.1.3 **安全敏感性資料唯一性測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供所使用安全敏感性資料之宣告作為審查依據。

(2) 產品應提供具唯一性的安全敏感性資料生成機制之說明文件，作為審查依據。

(d) 測試目的：

驗證產品於更新，及與關聯服務間傳輸所使用的安全敏感性資料(例如:產品金鑰)，是否具唯一性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱具備能證明安全敏感性資料具唯一性的生成機制證明文件。

(h) 測試結果：

(1) 產品提供之文件證實產品所使用的安全敏感性資料(例如:產品金鑰)具唯一性。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不存在安全敏感性資料。

5.2.1.4 **軟體未經授權變更測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供未加密的韌體、軟體，及其變更的方法。

(2) 廠商應提供進入作業系統層之使用者帳號及通行碼。

(3) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(4) 產品應提供軟體完整性保護，與完整性檢查的方法作為審查依據。

(5) 產品應提供安全事件告警機制之設計說明文件作為測試依據。

(d) 測試目的：

驗證產品發生未經授權之軟體變更時，是否能向管理者或使用者發出警示。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱產品軟體完整性之演算法證明文件。

(2) 透過實體埠或遠端管理介面，變更產品軟體。

(3) 根據安全事件告警機制文件，檢視產品警示狀態。

(h) 測試結果：

(1) 保護產品之軟體完整性演算法採用 NIST SP 800-140Cr1 所核可之同等或以上等級雜湊演算法。

(2) 當產品軟體完整性受到變更時，產品發出之警示應符合產品自我宣告，包括但不限於向管理者或使用者發出告警訊息或電子郵件警示，且產品發出警示所使用的網路不應使用超出執行告警功能的網路範圍，例如:外部網路。

(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：產品不支援作業系統(例：Windows、Linux)、遠端管理介面或無實體埠。

5.2.1.5 **輸入驗證測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之 IP 位址。

(2) 產品應提供說明文件以說明支援的使用者介面，包括但不限於本地端管理介面、網路服務介面、應用程式介面(APIs)，作為測試依據。

(3) 產品應提供說明文件以說明支援的通訊協定(Protocol)作為測試依據。

(d) 測試目的：

驗證產品所有介面，是否有對使用者輸入的資料進行驗證。

(e) 測試條件：

廠商須提供產品輸入驗證相關之檢測報告；若無法提供輸入驗證相關之檢測報告時，則由檢測單位執行有效輸入之測試。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 驗證廠商提供之輸入驗證相關檢測報告是否有輸入驗證之漏洞，例：跨站腳本(cross-site scripting)、SQL 注入、遠端程式碼執行(remote code exection)。

(2) 若廠商未提供源碼檢測報告，根據廠商提供之說明文件，使用輸入合法性測試工具執行測試，例如:網頁弱掃工具、模糊測試工具。

(h) 測試結果：

(1) 輸入驗證相關之檢測報告應無輸入驗證之漏洞。

(2) 執行輸入合法性測試未發現輸入驗證之漏洞。

(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。

5.2.1.6 異常狀態回復預定義機制測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品所提供之系統管理者帳號和通行碼。

(2) 產品應提供導致產品無法維持使用者設定的運作狀態之步驟、查看狀態的方法、運作狀態設定之步驟等說明文件，作為測試依據。

(3) 產品提供說明文件應包括列出所有產品之狀態的狀態列表、預定義狀態之宣告，作為測試依據

(d) 測試目的：

當產品無法正常維持使用者設定的運作狀態時，產品應可自動恢復為預定義狀態。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 查看產品狀態。

(2) 嘗試設定運作狀態。

(3) 依據產品說明文件，嘗試執行導致產品無法維持使用者設定的運作狀態之方法。

(4) 再次查看運作狀態。

(h) 測試結果：

(1) 產品無法維持使用者設定的運作狀態時，有進入預定義之狀態。

(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。

5.2.1.7 錯誤訊息測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.7

(b) 安全等級：

1 級。

(c) 測試資料：

產品須提供錯誤訊息列表，列出產品所有的錯誤訊息，及其相對應之使用情境的說明文件，作為測試使用。

(d) 測試目的：

產品提供予使用者所使用之所有錯誤訊息之內容，不應包含可能遭攻擊者利用之敏感性安全資料。

(e) 測試條件：

產品應支援使用者介面。

(f) 測試佈局：

無。

(g) 測試方法：

審閱錯誤訊息列表中顯示予使用者的錯誤訊息。

(h) 測試結果：

(1) 錯誤訊息表列不包含敏感性安全資料。

(2) 通過: (1)項結果符合。

(3) 不通過: (1)項結果不符合。

(4) 不適用: 產品不支援使用者介面，廠商應提供佐證資料足以證明產品不支援任何使用者介面。

5.2.1.8 硬編碼測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.8

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供保護唯一識別碼以硬編碼儲存，防止其遭篡改之安全設計書面資料作為審查依據。

(d) 測試目的：

驗證若產品之唯一識別碼以硬編碼(Hard code)方式儲存時，是否具備防篡改能力。

(e) 測試條件：

產品的唯一識別碼因安全目的以硬編碼方式儲存。

(f) 測試佈局：

無。

(g) 測試方法：

審閱防止產品唯一識別碼硬編碼儲存遭篡改之安全設計。

(h) 測試結果：

(1) 書面資料證實產品具備防止篡改之安全設計。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援以硬編碼方式儲存產品唯一識別碼。

5.2.1.9 安全敏感性資料禁用硬編碼測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.9

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 未加密的軟/韌體檔案。

(2) 產品應提供所使用安全敏感性資料之宣告以作為測試依據。

(d) 測試目的：

驗證產品之原始碼中是否存在安全敏感性資料。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 對產品之韌體/軟體檔案進行拆解。

(2) 搜尋檔案之內容，確認是否存在安全敏感性資料。

(h) 測試結果：

(1) 無法被解析出產品所宣告之安全敏感性資料。

(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。

5.2.1.10 記憶體存取控制測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.10

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供所使用記憶體存取控制機制之說明文件作為審查依據，例如: Memory Management Unit (MMU)、Memory Protection Unit (MPU)等技術。

(d) 測試目的：

驗證產品是否使用為硬體等級的記憶體存取控制機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商提供產品使用之記憶體控制機制之書面佐證資料。

(h) 測試結果：

(1) 書面資料證實產品使用硬體等級之記憶體存取控制機制進行空間保護，例如:MMU、MPU 技術。

(2) 通過：(1)項結果皆符合。

(3) 不通過：(1)項結果皆不符合。

(4) 不適用：產品為非實體設備，例如:軟體、應用程式、網頁。

5.2.1.11 敏感性資料來源真實性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.11

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 測試用假憑證。

(2) 廠商應提供與產品相連的門禁管理平台或其他門禁設備，以供測試使用。

(d) 測試目的：

驗證產品是否具備驗證傳輸資料來源身分的真實性。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 將產品與門禁管理平台或其他門禁設備連接，並啟動安全通道之建立程序。

(2) 當其他門禁管理平台或其他門禁設備發送憑證至產品時，攔截此憑證，並置換憑證公鑰或憑證資訊(包括發證單位、有效期限、格式及憑證簽章)。

(3) 發送已竄改之憑證至產品，並在安全通道建立的交握過程中監聽封包。

(4) 檢視所側錄的封包。

(h) 測試結果：

(1) 當資料傳輸用之安全通道憑證遭竄改後，經產品驗證後無法建立安全通道。

(2) 資料傳輸用之安全通道所使用之密碼套件如附錄 A 所建議，或符合 NIST SP 800-140Cr1 所核可之同等或以上等級之密碼演算法。

(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：無敏感性資料，或使用專屬連接線路，廠商須提供線路保護之證明文件。

5.2.1.12 **軟體、組態、資料變更之真實性測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.12

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供與產品相連的門禁管理平台或其他門禁設備，以供測試使用。

(2) 產品應提供變更軟體、組態檔、資料的真實性檢查的方法作為審查依據。

(3) 產品應提供軟體、組態、資料所使用之簽章演算法說明文件作為審查依據。

(d) 測試目的：

驗證影響到功能執行的軟體、組態、資料(例如:感測資料)變更時，產品是否能具備真實性檢查且產生安全事件日誌。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱能證明符合此安全要求之會影響到功能執行的軟體、組態檔、資料的簽章演算法說明文件。

(2) 產品讀取所儲存影響到功能執行的軟體、組態檔、資料時，檢視存取前是否驗證簽章。

(3) 檢視影響功能執行之軟體、組態檔、資料所採用之簽章演算法。

(4) 查詢產品是否建立安全事件日誌。

(h) 測試結果：

(1) 產品驗證簽章失敗後，無法存取影響到功能執行的軟體、組態檔、資料。

(2) 產品真實性檢查之簽章演算法採用 NIST SP 800-140Cr1 所核可之同等或以上強度的簽章演算法。

(3) 產品於存取影響到功能執行的軟體、組態檔和資料時，產生相應之安全事件日誌。

(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：產品不支援組態檔、軟體及影響功能執行之資料。

備考:若產品功能須提供使用者更改組態檔，若為公開金鑰機制則需提供公開金鑰給業主將組態檔簽章加密儲存，並於使用手冊中說明作法；若產品本身為軟體，則需提供符合安裝平台之簽章機制的介面，並於使用手冊中說明作法。

(7) 不適用：產品不支援連接外部網路。

(8) 不適用：產品不支援作業系統。

5.2.1.13 **會話完整性測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.13

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 系統管理者帳號和通行碼。

(2) 提供會話清單(Session list)。

(3) 產品須提供會話識別碼生成之演算法作為審查依據。

(d) 測試目的：

驗證產品是否具備會話(Session)完整性機制。

(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) 開啟封包側錄工具，並側錄封包。

(3) 登入管理者介面，並執行提供之功能。

(4) 紀錄會話 ID，並截錄封包。

(5) 登出或終止會話。

(6) 嘗試重送封包。

(7) 嘗試以紀錄且應註銷之會話 ID，執行須授權之功能。

(8) 審閱產品會話識別碼生成之演算法。

(9) 多次登入管理者介面，並分析會話識別碼。

(10) 嘗試生成類似之識別碼，或透過相同演算法生成會話識別碼。

(11) 透過生成之識別碼，嘗試存取產品。

(h) 測試結果：

(1) 產品無法於登出或會話終止後，以應註銷之會話 ID 進行存取。

(2) 產品會話識別碼生成之演算法，符合 NIST SP 800-140Cr1 之同等或以上等級密碼演算法。

(3) 產品只接受自行生成之會話識別碼。

(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：不支援會話機制

5.2.1.14 **軟體、組態、資料未經授權變更測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.1.14

(b) 安全等級：

3 級。

(c) 測試資料：

產品應提供影響到功能執行的軟體、組態設定、資料的完整性檢查的方法作為審查依據。

產品應提供安全事件告警機制之設計說明文件作為測試依據。

(d) 測試目的：

驗證產品發生未經授權之影響到功能執行的軟體、組態設定、資料變更時，產品是否能向管理者或使用者發出警示。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 以未授權之使用者透過實體埠或遠端管理介面，變更產品會影響到功能執行的軟體、組態設定和資料(例如:感測資料)。

(2) 依據產品提供之說明文件，當產品完整性偵測到產品會影響到功能執行的軟體、組態設定和資料遭未經授權變更時，檢視產品警示狀態。

(h) 測試結果：

(1) 產品完整性偵測到產品會影響到功能執行的軟體、組態設定和資料遭未經授權變更時發出之警示，包括但不限於向管理者或使用者發出告警訊息或電子郵件警示。

(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。

5.2.2 安全管理程序測試

5.2.2.1 金鑰之安全管理程序測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.1

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供產品包含金鑰及其安全管理程序之說明文件作為審查依據。

(d) 測試目的：

驗證產品對於金鑰的管理是否遵循安全管理程序。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱金鑰與其安全管理程序之書面文件。

(h) 測試結果：

(1) 產品有制定金鑰生成、交換、儲存、使用、銷毀及更換之程序，且該程序應達到監督、保證及證明金鑰得到妥善管理之紀錄。(可參考 NIST SP 800-57[4])

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援金鑰驗證機制。

5.2.2.2 **安全設定指南測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品安全設定指南作為審查依據，其內容應清楚記載在包括但不限於產品使用說明書。

(d) 測試目的：

驗證產品是否提供使用安全設定指南以協助完成產品最速安全設置。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供的產品安全設定指南說明文件。

(2) 驗證產品的安全性設置功能，依產品安全性設置程序完成安全設定。

(h) 測試結果：

(1) 產品應有安全設定指南說明書，且內容包括但不限於以簡易的安全性設定步驟設置使用安全設定、步驟中的最佳安全建議有醒目提示、具有安全性的預設設定參數等。

(2) 產品應具備安全性設置功能(例如:設定精靈)提供使用者設定。

(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。

5.2.2.3 **網路服務最小化測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 產品應提供所啟用之網路服務與對應埠之宣告作為審查依據。

(d) 測試目的：

驗證產品是否存在預期以外之網路埠。

(e) 測試條件：

無。

(f) 測試佈局：

圖 4

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具網路埠掃描功能之工具。

(3) 對產品執行 TCP 埠 0~65535 之掃描。

(4) 檢視掃描結果所呈現之網路服務與對應埠。

(5) 對產品執行 UDP 埠 0~65535 之掃描。

(6) 檢視掃描結果所呈現之網路服務與對應埠。

(h) 測試結果：

(1) 產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

(2) 產品未開啟自我宣告以外之網路服務。

(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：產品無網路服務之功能。

5.2.2.4 漏洞揭露政策測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.4

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供漏洞揭露與改善措施政策文件，作為審查依據。

產品應提供廠商之漏洞揭露與改善措施政策之連結，作為審查依據。

(d) 測試目的：

驗證產品是否具有漏洞揭露政策宣告。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供漏洞揭露與改善措施政策文件。

(2) 驗證產品漏洞揭露與改善措施政策頁面或連結。

(3) 核對該頁面內容及廠商提供之漏洞揭露與改善措施政策文件。

(h) 測試結果：

(1) 廠商應提供產品之漏洞揭露與改善政策。

(2) 漏洞揭露與改善措施政策之內容應包括但不限於：

1. 回報漏洞問題的連絡資訊。例如:廠商提供漏洞回報的專線或電子信箱。

2. 接收漏洞問題後的初步確認程序。例如: 漏洞揭露政策中訂定收到漏洞後多久時間內須完成問題確認。

3. 問題的處理至解決各階段之狀態更新。例如:廠商可透過與漏洞賞金平台合作，運用漏洞賞金平台的漏洞回報與處理流程機制。

(3) 通過：(1)~(2)項結果符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.2.2.5 **漏洞處理測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.5

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供處理產品之漏洞修正計畫相關書面文件作為審查依據，例如:包括但不限於產品計畫書、產品程序書。

(d) 測試目的：

驗證廠商是否具備處理產品已揭露漏洞之漏洞修正計畫。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商提供漏洞修正計畫之書面文件。

(h) 測試結果：

(1) 產品之漏洞修正計畫內容應載明包括但不限於：漏洞風險等級、等級對應之修復處理時間之界定等漏洞處理原則。

(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。

5.2.2.6 **安全開發驗證測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.6

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供產品所使用的網路和安全功能清單，及其已通過審查或評估的佐證資料作為審查依據。

(d) 測試目的

驗證產品所使用之網路與安全功能在上線/出廠前是否通過審查(review)或評估(evaluate)。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱產品之審查或評估佐證資料。

(h) 測試結果

(1) 佐證資料應可證實產品確實於上線 /出廠前已通過審查或評估，且 1.審查之內容包括但不限於，廠商已識別之資安缺陷及漏洞修補結果、2.評估內容包括但不限於，供應商所識別的必要安全措施及緩解措施。

(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。

5.2.2.7 密碼演算法和密碼基元使用期限測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.7

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供產品的密碼演算法及密碼基元更新說明文件，或產品與密碼演算法及密碼基元建議使用年限之書面資料作為審查依據。

(d) 測試目的

驗證產品建議的使用年限是否不超過所使用之密碼演算法及密碼基元(cryptographic primitives)的建議使用期限。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱廠商提供之產品使用密碼演算法及密碼基元書面文件。

(2) 若產品為非受限制設備產品，則檢視書面文件的內容是否包括但不限於：1.使用的密碼演算法及密碼基元、2.密碼演算法及密碼基元的更新計畫與方法。

(3) 若產品為受限制設備產品，則檢視書面文件的內容是否包括但不限於：1.使用的密碼演算法及密碼基元、2.產品建議使用期限與密碼演算法及密碼基元的建議使用期限。

(h) 測試結果

(1) 非受限制設備產品：書面資料證實產品所使用的密碼演算法及密碼基元可被更新。

(2) 受限制設備產品：書面資料證實產品的建議使用期限不超過密碼演算法建議使用期限。

(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。

5.2.2.8 **安全開發測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.8

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供相關說明文件(參見附錄 C)作為審查依據。

(d) 測試目的

驗證產品開發流程是否符合安全開發要求。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱產品安全開發說明文件。

(h) 測試結果

(1) 說明文件證實產品符合安全開發之規定。

(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。

5.2.2.9 **軟體物料清單測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.9

(b) 安全等級

1 級。

(c) 測試資料

廠商應提供軟體物料清單(SBOM)之書面文件作為審查依據，例：以 SBOM 工具匯出產品之 SBOM 文件。

(d) 測試目的

查驗產品是否具備軟體物料清單(SBOM)。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱產品之軟體物料清單，軟體物料清單內容欄位應包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記。

(h) 測試結果

(1) 產品具備軟體物料清單且內容包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者及時間戳記。

(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。

5.2.2.10 **產品標示測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.2.10

(b) 安全等級

2 級。

(c) 測試資料

產品應提供產品資訊說明以作為審查依據，產品資訊載明方式包括但不限於產品管理介面、使用說明書、產品包裝、或產品官網。

(d) 測試目的

驗證產品是否載明產品名稱、型號、產品所使用之軟韌體版本及產品支援傳輸類型於使用者易於辨識之處。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

查閱產品資訊。

(h) 測試結果

(1) 產品應提供使用者查閱產品名稱、型號、產品所使用之軟韌體版本及產品支援傳輸類型，上述產品資訊應顯示在包括但不限於產品管理介面、使用說明書、產品包裝或產品官網。

(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。

5.2.3 已知漏洞安全測試

5.2.3.1 漏洞監控測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.1

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供漏洞揭露與改善措施政策文件，作為審查依據。

產品應提供廠商之漏洞揭露與改善措施政策之連結，作為審查依據。

(d) 測試目的：

驗證產品漏洞揭露政策宣告是否包含維護期間的安全漏洞監控、識別和修正聲明。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供漏洞揭露與改善措施政策文件。

(2) 檢視產品漏洞揭露與改善措施政策頁面或連結。

(3) 核對該頁面內容及廠商提供之漏洞揭露與改善措施政策文件。

(h) 測試結果：

(1) 漏洞揭露政策聲明之內容應包括維護期間內對其產品之安全漏洞持續監控、識別與修正。

(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。

5.2.3.2 測試作業系統與網路服務是否存在 CVSS v3 評分為 9.0 分以上之常見資安漏洞

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 產品須提供系統管理者帳號和通行碼。

(d) 測試目的：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3[(3)]重大資安風險之漏洞。

(e) 測試條件：

產品應支援作業系統與網路服務。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具。

(3) 設定產品之 IP 位址及系統管理者帳號和通行碼。

(4) 對產品執行工具掃描。

(h) 測試結果：

(1) 作業系統與網路服務無檢測出美國國家漏洞資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

(2) 若作業系統與網路服務存在美國國家漏洞資料庫評分 CVSS v3 為 9.0 分以上之資安漏洞，產品應提出包括但不限於漏洞風險評估、修復處理時間及複驗之漏洞修正計畫。

(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：產品不支援作業系統(例:Windows、Linux)或網路服務功能。

5.2.3.3 網頁管理介面高風險等級漏洞測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之 IP 位址。

(2) 產品應提供系統管理者權限供測試用。

(3) 產品之管理者帳號和通行碼。

(d) 測試目的：

驗證產品之網頁管理介面是否存在 OWASP web TOP 10 高風險等級漏洞。

(e) 測試條件：

產品應支援網頁介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。

(3) 啟動具備網頁弱點掃描功能之工具 。

(4) 設定產品 IP 位址，對產品網頁介面執行弱點掃描。

(5) 檢視該弱點掃描工具所產生之報告，是否存在 OWASP web TOP 10 之高風險等級漏洞。

(h) 測試結果：

(1) 產品之網頁管理介面，不存在引發 OWASP web Top 10[(6)]之高風險風險等級漏洞。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援網頁介面。

5.2.3.4 **第三方函式庫漏洞初級測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.4

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供所引用網路功能相關之第三方函式庫清單(包括函式庫名稱與版本號)，作為審查依據。

(d) 測試目的：

驗證產品所引用網路功能相關之第三方函式庫未潛藏來源 CVSS v3 評分為 9.0 分以上之資安漏洞。

(e) 測試條件：

產品支援第三方函式庫。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱第三方函式庫清單。

(2) 根據該版本函式庫所可能潛藏 CVSS v3 評分為 9.0 分以上之資安漏洞，實際驗證是否確實存在。

(h) 測試結果：

(1) 實測後未發現 CVSS v3 評分為 9.0 分以上之資安漏洞。

(2) 若第三方函式庫存在 CVSS v3 評分為 9.0 分以上之資安漏洞，產品應提出包括但不限於漏洞風險評估、補救方法、更換第三方函式庫及複驗之漏洞修正計畫。

(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：若產品未使用網路功能相關第三方函式庫，廠商應提供足以佐證之資料。

5.2.3.5 測試作業系統與網路服務是否存在 CVSS v3 評分為 7.0 分以上之常見資安漏洞

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.5

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品 IP 位址。

(2) 產品應保持出廠預設環境狀態。

(3) 設定產品之 IP 位址及系統管理者帳號和通行碼。

(d) 測試目的：

驗證產品之作業系統與網路服務是否存在已知 CVSS v3 高資安風險之漏洞。

(e) 測試條件：

產品應支援作業系統與網路服務。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具作業系統及網路服務弱點掃描功能之工具。

(3) 設定產品之 IP 位址及系統管理者帳號和通行碼。

(4) 對產品執行工具掃描。

(h) 測試結果：

(1) 作業系統與網路服務無檢出美國國家漏洞資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞；當檢測出之資安漏洞不具有 CVSS v3 評分時，以 CVSS v2 評分為依據。

(2) 若作業系統與網路服務存在美國國家漏洞資料庫評分 CVSS v3 為 7.0 分以上之資安漏洞，產品應提出包括但不限於漏洞風險評估、修復處理時間及複驗之漏洞修正計畫。

(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：產品不支援作業系統或網路服務功能。

5.2.3.6 網頁管理介面中風險等級漏洞測試

(i) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.6

(j) 安全等級：

2 級。

(k) 測試資料：

(4) 產品之 IP 位址。

(5) 產品應提供系統管理者權限供測試用。

(6) 產品之管理者帳號和通行碼。

(l) 測試目的：

驗證產品之網頁管理介面是否存在 OWASP web TOP 10 中風險等級漏洞。

(m) 測試條件：

產品支援網頁介面。

(n) 測試佈局：

如圖 2。

(o) 測試方法：

(6) 將測試電腦連接產品。

(7) 開啟網頁管理介面，檢視網頁是否使用超文本傳輸協定。

(8) 啟動具備網頁弱點掃描功能之工具 。

(9) 設定產品 IP 位址，對產品網頁介面執行弱點掃描。

(10) 檢視該弱點掃描工具所產生之報告，是否存在 OWASP web TOP 10 之中風險等級漏洞。

(p) 測試結果：

(5) 產品之網頁管理介面，不存在引發 OWASP web Top 10[(6)]之中風險等級漏洞。

(6) 通過：(1)項結果符合。

(7) 不通過：(1)項結果不符合。

(8) 不適用：產品不支援網頁介面。

5.2.3.7 第三方函式庫漏洞中級測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.7

(b) 安全等級：

2 級。

(c) 測試資料：

產品須提供所引用網路功能相關之第三方函式庫清單(包括函式庫名稱與版本號)，作為審查依據。

(d) 測試目的：

驗證產品所引用網路功能相關之第三方函式庫來源未潛藏 CVSS v3 評分為 7.0 分以上之資安漏洞。

(e) 測試條件：

產品支援第三方函式庫。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱第三方函式庫清單。

(2) 根據該版本函式庫所可能潛藏 CVSS v3 評分為 7.0 分以上之資安漏洞，實際驗證是否確實存在。

(h) 測試結果：

(1) 實測後未發現 CVSS v3 評分為 7.0 分以上之資安漏洞。

(2) 若第三方函式庫存在 CVSS v3 評分為 7.0 分以上之資安漏洞，產品應提出包括但不限於漏洞風險評估、補救方法、更換第三方函式庫及複驗之漏洞修正計畫。

(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：若產品未使用網路功能相關第三方函式庫，廠商應提供足以佐證之資料。

5.2.3.8 **第三方函式庫漏洞高級測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.2.3.8

(b) 安全等級：

3 級。

(c) 測試資料：

產品須提供所引用網路功能相關之第三方函式庫清單(包括函式庫名稱與版本號)，作為審查依據。

(d) 測試目的：

驗證產品所引用網路功能相關之第三方函式庫來源未潛藏 CVSS v3 評分為 4.0 分以上之資安漏洞。

(e) 測試條件：

產品支援第三方函式庫。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱第三方函式庫清單。

(2) 根據該版本函式庫所可能潛藏 CVSS v3 評分為 4.0 分以上之資安漏洞，實際驗證是否確實存在。

(h) 測試結果：

(1) 實測後未發現 CVSS v3 評分為 4.0 分以上之資安漏洞。

(2) 若第三方函式庫存在 CVSS v3 評分為 4.0 分以上之資安漏洞，產品應提出包括但不限於漏洞風險評估、補救方法、更換第三方函式庫及複驗之漏洞修正計畫。

(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：若產品未使用網路功能相關第三方函式庫，廠商應提供足以佐證之資料。

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-1006-1 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 敏感性資料保護測試

5.3.1.1 密碼演算法測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.3.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品所使用密碼演算法之技術書面文件作為審查依據。

(d) 測試目的：

驗證產品所使用之密碼演算法是否採用符合國際公認 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱產品所使用的密碼演算法之技術書面文件。

(h) 測試結果：

(1) 產品所使用的密碼演算法符合 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援加密機制，或不存在敏感性資料及不傳輸敏感性資料。

5.3.1.2 安全敏感性資料、敏感性資料保護測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.3.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 產品應保持出廠預設環境狀態。

(3) 廠商應提供書面資料以說明產品有哪些敏感性資料，以作為審查依據。

(4) 產品應提供安全敏感性資料、敏感性資料儲存保護之加密演算法書面文件作為審查依據。

(5) 產品應提供安全敏感性資料、敏感性資料傳輸保護之加密演算法書面文件作為審查依據。

(d) 測試目的：

驗證產品之安全敏感性資料、敏感性資料的儲存、傳輸是否加密保護。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 情況 1：(安全敏感性資料、敏感性資料儲存)

(i) 審閱能證明符合此安全要求之書面資料。

(ii) 將測試電腦連接產品。

(iii) 若產品支援 UART，將測試電腦連接產品之 UART。

(iv) 透過 UART 埠存取作業系統之除錯模式 。

(v) 根據廠商提供之存放位置，查找安全敏感性資料、敏感性資料。

(vi) 檢視保護安全敏感性資料、敏感性資料所採用的加密演算法。

(vii) 若產品支援 JTAG，將測試電腦連接產品之 JTAG。

(viii)透過 JTAG 埠存取作業系統之除錯模式 。

(ix) 重複(v)~(vi)之步驟。

(x) 若產品支援 USB，將測試電腦連接產品之 USB。

(xi) 透過 USB 埠存取作業系統之除錯模式。

(xii) 重複(v)~(vi)之步驟。

(xiii)若產品支援遠端指令介面，開啟並連接遠端指令介面。

(xiv)重複(v)~(vi)之步驟。

(2) 情況 2：(安全敏感性資料、敏感性資料傳輸)

(i) 開啟安全通道掃描工具，對門禁管理平台進行掃描。

(ii) 比對掃描結果是否為附錄 A 中所包含之密碼套件。

(iii) 將測試電腦連接產品。

(iv) 將產品與門禁管理平台連線，分別傳送安全敏感性資料、敏感性資料至門禁管理平台，同時側錄封包。

(v) 檢視所側錄之封包是否採用安全通道。

(h) 測試結果：

(1) 產品的安全敏感性資料、敏感性資料不應以明文方式儲存，且加密方式採 NIST SP 800-140Cr1 所核可的同等或以上等級之加密演算法。

(2) 產品以安全通道傳輸安全敏感性資料、敏感性資料，安全通道所使用之密碼件如附錄 A 所建議，或應符合 NIST SP 800-140Cr1 所核可之同等或以上等級之密碼演算法。

(3) 通過：(1)~(2)項結果符合。

(4) 不通過：(1)~(2)項結果不符合。

(5) 不適用：若產品為無法連接外部網路之門禁讀取器或其他門禁設備，則情況 2 不適用，且廠商應提供足以佐證之資料。

(6) 不適用：產品不支援儲存安全敏感性資料及敏感性資料。

(7) 不適用：產品不支援作業系統(例:Windows、Linux)。

5.3.1.3 **刪除安全敏感性資料測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.3.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供產品之刪除安全敏感性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)。

(2) 廠商應提供書面資料以說明產品有哪些安全敏感性資料，作為測試依據。

(d) 測試目的：

驗證產品是否告知使用者如何刪除安全敏感性資料的方法。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品之刪除安全敏感性資料之說明文件。

(2) 根據說明文件之操作方式，檢視刪除安全敏感性資料功能。

(h) 測試結果：

(1) 產品之刪除安全敏感性資料功能說明證實足以協助使用者刪除安全敏感性資料。

(2) 安全敏感性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。

5.3.1.4 **確認消除暫存於揮發性共享內存資源的敏感性資料測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.3.1.4

(b) 安全等級：

3 級。

(a) 測試資料：

(1) 產品應提供書面資料以說明產品如何完全消除暫存於揮發性共享內存資源(例如:RAM)之敏感性資料的方法，作為審查依據。

(2) 廠商應提供設計相關文件以說明如何透過實體方式檢驗揮發性共享內存資源之資料儲存狀態(例如:指出腳位)，作為測試依據。

(b) 測試目的：

驗證產品是否提供確認暫存於揮發性共享內存資源的資料是否完全消除的功能。

(c) 測試條件：

無。

(d) 測試佈局：

無。

(e) 測試方法：

(1) 根據審查文件，啟動產品所有功能。

(2) 傾印(Dump)揮發性共享內存資源(RAM)中的資料，檢查是否存在敏感性資料。

(3) 若產品存在敏感性資料，關閉或再次啟動產生敏感性資料之程式後，傾印其(RAM)中的資料。

(4) 檢查是否存在敏感性資料。

(f) 測試結果：

(1) 產品應提供可完全消除暫存於揮發性共享內存資源(例如:RAM)之資料的方法。

(2) 產品之揮發性共享內存資源(例如:RAM)中已完全不存在敏感性資料。

(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。

5.4 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-1006-1 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 資源管理功能測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.1

(b) 安全等級

1 級。

(c) 測試資料

廠商應提供產品設計書面文件，以說明有哪些安全功能及如何控制其所使用的資源，作為審查依據。若產品須以額外裝置進行部署達到資源管理功能時，則廠商應提供相關說明文件，供測試使用。

(d) 測試目的

驗證產品是否提供設定安全功能使用產品資源的資源管理功能。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 審閱產品書面文件，檢視資源管理功能(例如:安全事件記錄、病毒掃描) 之設計。

(2) 根據書面文件說明，驗證產品執行安全功能時門禁功能仍可維持正常運作。

(h) 測試結果

(1) 廠商提供之書面文件證實產品具備資源管理功能，或產品透過額外裝置進行資源管理，各安全功能可設定其運作時所使用的資源優先權與使用量。

(2) 當執行安全功能造成 CPU 負載過高或記憶體使用率過量時，產品功能仍可維持正常運作。

(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：當產品之安全功能所使用的資源使用量固定的情況下，不會造成 CPU 負載過高或記憶體使用率過量，廠商應提供足以佐證之資料。

5.4.1.2 **中斷或故障回復功能測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.2

(b) 安全等級

1 級。

(c) 測試資料

產品應提供還原功能之說明文件作為審查依據，且說明預期還原的安全狀態。

(d) 測試目的

驗證產品在系統中斷或故障後是否能還原至預設安全狀態。

(e) 測試條件

無。

(f) 測試佈局

如圖 2。

(g) 測試方法

(1) 審閱產品還原功能說明文件。

(2) 根據說明文件，觸發產品系統異常中斷。

(3) 產品重啟後，檢視產品是否回復至安全狀態。

(h) 測試結果

(1) 產品應回復至原先設定的預設安全狀態，例如以下情況：1.所有系統參數(預設或可組態設定)皆設置為預設之安全值、2.重新安裝安全修補程式、3.系統資料和操作程序仍可用、4.重新安裝組件且亦使用預設的設定、5.安裝最新的已知安全備份等。

(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。

5.4.1.3 **網路服務所提供資訊最小化測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.3

(b) 安全等級

1 級。

(c) 測試資料

(1) 產品之 IP 位址。

(2) 產品應提供相連的門禁管理平台或其他門禁設備，以供測試使用。

(3) 產品應保持出廠狀態。

(4) 產品應提供初始未身分鑑別前之網路傳輸所需公開敏感性資訊之宣告，以作為測試依據。

(d) 測試目的

驗證產品在初始狀態下網路服務公開與敏感性相關的資訊是否為服務必要之所需。

(e) 測試條件

無。

(f) 測試佈局

如圖 4。

(g) 測試方法

(1) 將產品與門禁管理平台或其他門禁設備連接，產品連線初始狀態下，透過測試電腦開啟封包側錄工具進行側錄。

(2) 檢視側錄到的封包，確認其提供之資訊與廠商宣告是否相符。

(h) 測試結果

(1) 產品未公開自我宣告以外之敏感性資訊，例如:email 地址、WiFi 通行碼等。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無網路服務之功能。

5.4.1.4 **軟體服務最小化測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.4

(b) 安全等級

1 級(O)。

(c) 測試資料

(1) 產品應保持出廠預設環境狀態。

(2) 廠商提供進入產品系統層之方法。

(3) 產品應於文件中列出啟用的軟體服務並說明其功用、使用方式與其必要性，作為審查依據，例如:SSH daemon。

(d) 測試目的

驗證產品是否存在預期以外之軟體服務。

(e) 測試條件

無。

(f) 測試佈局

如圖 3。

(g) 測試方法

(1) 審閱啟用之軟體服務的說明文件。

(2) 開啟產品各軟體服務。

(3) 比對產品軟體服務與說明文件內容。

(h) 測試結果

(1) 產品所啟用之軟體服務皆與產品說明文件相符。

(2) 產品不存在非說明文件所述的軟體服務。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.4.1.5 原始碼最小化測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.5

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供產品原始碼檔案，版本應與產品送驗相同。

廠商應提出已完成產品的完成死碼刪除(Dead code elimination)之證明與使用工具，作為審查依據。

(d) 測試目的

驗證產品是否存在預期以外之程式碼。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱廠商提供之程式最小化的證明文件。

(2) 使用檢測工具檢驗產品程式碼。

(h) 測試結果

(1) 產品已確實移除程式碼中非產品功能或服務所需的程式，例如:不必要的字符、註解或註銷的程式片段等。

(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。

5.4.1.6 備份能力測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供備份功能之使用說明文件。

(d) 測試目的：

驗證產品是否支援備份功能，以防止失效或錯誤設定時可恢復正常狀態。

(e) 測試條件：

產品應支援備份功能。

(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，開啟相應之管理介面連接工具。

(3) 啟動備份功能，檢視功能是否正常運行。

(4) 啟動還原功能，檢視是否回復至該備份點之狀態。

(h) 測試結果：

(1) 產品應提供備份功能，以保護產品狀態資訊(檔)，且備份過程不應影響產品正常運作。

(2) 產品應可正確還原至該備份點之狀態。

(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：產品不存在組態設定。

5.4.1.7 備份檔案完整性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.1.7

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品應提供備份還原功能之使用說明。

(2) 產品之還原備份檔案。

(d) 測試目的：

產品應在還原備份前是否確認備份檔的完整性。

(e) 測試條件：

產品應支援備份/還原功能。

(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，開啟相應之管理介面連接工具。

(3) 竄改備份檔案。

(4) 啟動還原功能，檢視功能是否正常運行。

(h) 測試結果：

(1) 產品還原失敗。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不存在組態設定。

5.4.2 資源管理機制

5.4.2.1 外部感測功能測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.2.1

(b) 安全等級

1 級。

(c) 測試資料

廠商應提供產品之外部感測功能說明文件作為審查依據(包括但不限於產品使用手冊或包裝說明等)。

(d) 測試目的

驗證產品是否存在有外部感測功能且告知使用者。

(e) 測試條件

產品支援外部感測功能。

(f) 測試佈局

無。

(g) 測試方法

檢視產品之外部感測功能宣告。

(h) 測試結果

(1) 產品之外部感測功能說明方式應清楚記載在包括但不限於產品使用說明書、產品包裝或產品官網。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援外部感測功能。

5.4.2.2 備援機制測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.2.2

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供設置預防網路和電源中源的備援機制，與其之環境面部署說明文件作為審查依據。

(d) 測試目的

驗證產品是否設置因應網路或電源中斷的備援機制。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

(1) 審閱預防網路和電源中斷備援機制書面文件。

(2) 根據說明文件，中斷產品網路，檢視產品運作情況。

(3) 中斷網路，檢視產品運作情況。

(4) 中斷電源，檢視產品運作情況。

(h) 測試結果

(1) 產品備援機制或額外安全部署足以確保產品能正常關閉或停止，以防止資料未正確儲存，且門禁安全功能保持運行狀態等。

(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。

5.4.2.3 **網路中斷應變測試**

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.2.3

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(d) 測試目的

驗證當網路異常中斷時是否可保持本地端運作，且在網路恢復後能回復正常運作。

(e) 測試條件

無。

(f) 測試佈局

如圖 4。

(g) 測試方法

(1) 若受測產品非門禁管理平台，則開啟門禁管理平台監控產品，觸發網路連線中斷(例:拔除產品網路線路)。

(2) 若受測產品為門禁管理平台，則開啟遠端管理介面監控產品，觸發網路連線中斷(例:拔除產品網路線路)。

(3) 檢視產品運作情況。

(4) 恢復產品網路連線。

(h) 測試結果

(1) 網路連線中斷產品應仍可正常運作。

(2) 恢復產品網路連線，管理介面應回復監控狀態。

(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：無網路連線功能之受限制設備。

5.4.2.4 保持連線穩定及功能持續正常運作測試

(a) 測試依據

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.4.2.4

(b) 安全等級

1 級(O)。

(c) 測試資料

廠商應提供設置保持產品穩定連線與功能持續運作的運作機制書面文件作為審查依據。

(d) 測試目的

驗證產品是否具備保持連線穩定與功能持續正常運作的運作機制。

(e) 測試條件

無。

(f) 測試佈局

無。

(g) 測試方法

審閱產品運作機制之書面文件。

(h) 測試結果

(1) 運作機制證實讓產品保持連線與功能正常運作，運作機制包括但不限於產品批次線上更新、產品在恢復網路連線時須隨機依序連線。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無網路連線功能之受限制設備。

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-1006-1 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 更新功能測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 若產品支援線上更新，須由廠商負責觸發線上更新。

(2) 產品應具備更新機制，並提供更新機制說明文件。

(3) 廠商應說明包括但不限於漏洞處理、安全更新政策宣告與安全更新部署與管理程序之安全更新計畫書面文件，作為審查依據，例如:產品安全更新計畫書、產品安全更新程序書、漏洞修正計畫等。

(d) 測試目的：

驗證產品是否支援軟韌體更新功能且是否具備安全更新政策與部署程序。

(e) 測試條件：

產品應支援更新功能，包括但不限於線上更新或手動更新方式。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供之書面說明文件。

(2) 觸發產品更新。

(3) 驗證產品更新結果。

(h) 測試結果：

(1) 廠商提供之書面文件證實產品具備軟韌體安全更新、漏洞處理、及時安全更新部署與管理程序。

(i) 安全更新機制內容包括但不限於：更新方式、支援更新之軟體組件，或不支援更新之軟體組件，並說明不支援更新的原因。

(ii) 書面文件之漏洞修正計畫應包括但不限於產品漏洞風險等級定義、各風險等級所對應之漏洞處理時間。

(2) 產品具備更新功能，可正確更新軟韌體，且安全更新功能與說明文件相符，不支援更新的軟體組件不影響產品安全性。

(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。

5.5.1.2 更新檔真實性與完整性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之更新韌體檔。

(2) 產品所使用之軟/韌體。

(3) 若選擇測試方法 1，廠商提供測試用私鑰予實驗室。

(4) 若選擇測試方法 1，則廠商應提供產品之數位簽章使用機制作為審查依據。

(5) 若選擇測試方法 2，實驗室提供自簽公私鑰予廠商。

(d) 測試目的：

驗證產品安裝更新檔是否採用簽章驗證機制，以確保更新檔案之真實性與完整性

(e) 測試條件：

產品應支援更新機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 測試方法 1 (廠商提供測試用私鑰予實驗室)：

(i) 廠商提供原始軟/韌體並提供簽章方法，實驗室使用廠商提供之自簽私鑰簽章該軟/韌體，檢視更新結果。

(ii) 實驗室使用自簽私鑰簽章該軟/韌體，實驗室執行軟/韌體更新，檢視更新結果。

(2) 測試方法 2 (實驗室提供自簽公私鑰予廠商)：

(i) 實驗室提供自簽公私鑰予送測廠商，廠商利用該私鑰簽署軟/韌體，並將公鑰植入於產品。

(ii) 實驗室執行軟/韌體更新，檢視更新結果。

(iii) 受測廠商將實驗室所提供之測試私鑰加入產品之受信任私鑰列表。

(iv) 實驗室執行軟/韌體更新，檢視更新結果。

(h) 測試結果：

(1) 若採用測試方法 1:

(i) 實驗室使用廠商提供之私鑰簽章該軟/韌體，實驗室執行軟/韌體更新，軟/韌體更新成功。

(ii) 實驗室使用自簽私鑰簽章軟/韌體，軟/韌體更新不成功。

(2) 若採用測試方法 2，廠商使用實驗室提供之自簽公私鑰，軟/韌體更新成功。

(3) 通過：(1)或(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：產品為不支援軟/韌體更新之受限制設備，則廠商應提供相關設計文件以證明產品無法直接更新軟/韌體 ，必須以其他方式更新(例如:硬體更換、召回等)。

5.5.1.3 **安全更新功能測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 若產品支援線上更新，須由廠商負責觸發線上更新。

(2) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(3) 廠商應提出採用安全更新機制作法與加密演算法之書面文件，作為審查依據。

(d) 測試目的：

驗證產品是否具備不可降為較舊之軟/韌體版本、軟/韌體傳輸加密、軟/韌體線上更新路徑是否採用安全通道。

(e) 測試條件：

產品支援更新機制。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 安全功能 1：(防止安裝舊版本)

(i) 使用舊軟/韌體版本執行更新安裝。

(ii) 檢視產品是否完成軟/韌體安裝。

(2) 安全功能 2：(軟/韌體加密傳輸)

(i) 將測試電腦與門禁管理平台連結在同一個區域網路中。

(ii) 將產品連結門禁管理平台並啟動更新。

(iii) 攔截傳送中之封包。

(iv) 檢視封包加密機制是否採用 NIST SP 800-140Cr1 同等或以上強度之雜湊演算法。

(3) 安全功能 3：(更新路徑)

(i) 將測試電腦、產品與更新伺服器/門禁管理平台連結在同一個區域網路中。

(ii) 啟動軟/韌體更新。

(iii) 使用工具側錄更新伺服器/門禁管理平台與產品之間的封包。

(iv) 檢視所側錄之封包。

(h) 測試結果：

(1) 產品安裝舊版軟/韌體不成功。

(2) 若產品支援線上更新，軟/韌體加密機制採用 NIST SP 800-140Cr1 同等或以上強度之雜湊演算法。

(3) 若產品支援線上更新，產品之線上更新路徑通過安全通道，且安全通道所使用之密碼件如附錄 A 所建議，或應符合 NIST SP 800-140Cr1 所核可之同等或以上等級之密碼演算法。

(4) 通過：(1)、(2)項結果皆符合，或(1)、(3)項結果皆符合。

(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：產品為無法自行/自動更新之受限制設備，則廠商應提供相關文件以證明的產品安全更新方式(例如:硬體更換、召回等)。

5.5.1.4 **更新通知功能測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.4

(b) 安全等級：

1 級(O)。

(c) 測試資料：

(1) 若產品支援線上更新，廠商須協助觸發產品軟/韌體更新。

(2) 廠商於測試時，須協助發布更新通知。

(3) 廠商應提供產品更新功能說明文件作為測試依據。

(d) 測試目的：

驗證產品之更新通知是否有清楚說明更新資訊。

(e) 測試條件：

產品應支援更新機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 廠商觸發產品軟/韌體更新。

(2) 檢視產品之更新功能。

(3) 檢視產品之更新通知內容。

(h) 測試結果：

(1) 產品之軟/韌體更新以於產品本地端管理介面使用彈跳視窗、推播訊息或寄送電子郵件等方式通知。

(2) 軟/韌體更新通知的內容應包括：更新版本、該次更新所能緩解的風險、修正的錯誤。

(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：產品為無法自行/自動更新之受限制設備，則廠商應提供相關文件以證明的產品安全更新方式(例如:硬體更換、召回等)。

5.5.1.5 **更新警語測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.5

(b) 安全等級：

1 級(O)。

(c) 測試資料：

(1) 廠商須協助觸發產品軟/韌體更新。

(2) 廠商應提供產品更新功能說明文件或產品使用手冊，作為審查依據。

(d) 測試目的：

驗證產品若在更新期間會造成產品基本功能中斷，在進入更新程序前是否有提示警語。

(e) 測試條件：

產品應支援更新機制。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供之更新說明文件中的更新警語功能。

(2) 廠商觸發產品軟/韌體更新。

(3) 檢視產品在進入更新程序前是否有警示。

(h) 測試結果：

(1) 更新警語功能證實與廠商提供之說明文件相符，更新警語的內容包括但不限於：什麼情況下中斷功能或哪些情況下不會完全關閉、預計更新持續多少時間、更新期間可能中斷連線的時間等。

(2) 產品在更新程序開始前，產品本地端管理介面或連接之門禁管理平台應顯示更新警語提示。

(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：產品為更新過程中不會造成產品基本功能中斷。

(6) 若產品為無法自行 /自動更新之受限制設備，則廠商應提供相關文件以證明的產品安全更新方式 (例 :硬體更換、召回等)。

5.5.1.6 **支援更新期限說明測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品支援期限之聲明文件作為審查依據，文件的形式包括但不限於產品官網、使用手冊或包裝等公告方式。

(d) 測試目的：

驗證產品具有產品支援期限之宣告。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱廠商所提供之產品支援宣告文件或網頁連結。

(h) 測試結果：

(1) 產品支援期限與廠商提供之宣告文件相符，且宣告之敘述應淺顯易懂。

(2) 產品支援期限之宣告方式，包括但不限於產品官網、產品使用手冊或產品包裝等處。

(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。

5.5.1.7 **更新中斷恢復功能測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.5.1.7

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供軟/韌體更新檔案。

(2) 若產品支援線上更新，廠商須負責觸發線上更新。

(d) 測試目的：

驗證當更新作業異常中斷時，產品仍可恢復正常運作狀態。

(e) 測試條件：

產品應支援軟/韌體更新。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 啟動/執行產品更新。

(2) 於更新過程中(非軟/韌體檔案下載階段)，觸發更新中斷。

(h) 測試結果：

(1) 更新中斷後，產品仍可恢復正常運作狀態。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品為無法自行/自動更新之受限制設備，則廠商應提供相關文件以證明的產品安全更新方式(例如:硬體更換、召回等)。

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-1006-1 之安全要求，並依下列各測試項目進行實機測試。

5.6.1 安全事件日誌檔與警示測試

5.6.1.1 安全事件日誌功能測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 廠商應提供書面文件以說明產品發生哪些安全事件及如何記錄安全事件，作為測試依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台記錄安全事件，以何方式通知門禁管理平台進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證產品是否具備安全事件紀錄功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 情況 1：(產品具備安全事件日誌)

(i) 將測試電腦與產品連接。

(ii) 根據廠商提供之說明文件，觸發安全事件。

(iii) 根據產品使用說明，開啟相應之管理介面連接工具。

(iv) 瀏覽安全事件日誌。

(v) 確認日誌內容是否記載步驟(ii)的安全事件紀錄。

(vi) 檢視該日誌是否具時間戳、來源(原始設備名稱、軟體程式或使用者帳號)、類別、型式、安全事件 ID 和安全事件後果。

(vii) 將產品重新開機，開啟相應之管理介面連接工具，瀏覽安全事件日誌。

(2) 情況 2：(由門禁管理平台或其他門禁裝置記錄產品之安全事件日誌)

(i) 觸發設備所定義的安全事件。

(ii) 以系統管理者帳號和通行碼登入門禁管理平台瀏覽安全事件日誌。

(iii) 或側錄傳送往門禁管理平台之封包，檢視傳送往門禁管理平台之安全事件日誌。

(h) 測試結果：

(1) 產品具有安全事件日誌功能或產品之安全指引/使用手冊闡明由門禁管理平台(或其他門禁裝置)記錄安全事件日誌。

(2) 安全事件日誌或定期事件回傳的資料應包含時間戳、來源(原始設備名稱、軟體程式或使用者帳號)、類別、型式、事件 ID 和安全事件後果。

(3) 重開機後之安全事件日誌仍可查詢。

(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。

5.6.1.2 **安全事件日誌儲存容量-初級測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供審查文件以說明產品設置環境及安全事件日誌儲存空間之宣告，作為審查依據。

(2) 廠商應提供安全日誌儲存容量設置評估報告，用以分析設置容量大小之評估因素須包括但不限於每筆日誌的平均大小、日誌生成速率、預期之日誌保留期，作為審查依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證當產品設置於低度風險等級環境時，是否有針對安全事件日誌檔配置合理的儲存容量。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供之說明文件與容量評估報告。

(2) 檢視產品安全事件日誌儲存容量。

(3) 若產品安全事件日誌儲存於門禁管理系統，則檢視門禁管理系統之產品安全事件日誌儲存容量。

(h) 測試結果：

(1) 產品的設置環境與安全事件日誌儲存容量應遵循 NIST SP 800-92[(5)]之低度風險等級建議，儲存容量應至少可保存 1 至 2 週的日誌檔儲存空間。

(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。

5.6.1.3 安全事件日誌滾動功能測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供系統管理者權限之帳號、通行碼，以供測試用。

(2) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證產品是否具備處理日誌儲存空間不足之異常狀況。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 不斷觸發安全事件。

(2) 填充儲存容量，直到儲存空間不足。

(3) 檢視產品是否正常記錄安全事件，產品功能是否維持運作。

(h) 測試結果：

(1) 產品不會發生儲存空間不足現象。

(2) 產品仍可正常記錄安全事件，且產品功能皆能正常運作。

(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) 不適過：無。

5.6.1.4 安全事件記錄失敗測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.4

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 廠商應提供書面文件以說明產品發生哪些安全事件及如何記錄安全事件，說明文件應包括定義日誌記錄失敗有哪些情況其處理機制，作為審查依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，以何方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證日誌記錄失敗時，產品是否有能力記錄該失敗紀錄且發出警示。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱安全事件記錄功能書面文件。

(2) 根據書面文件之日誌記錄失敗情況，以觸發產品日誌記錄失敗。日誌記錄失敗情況，例如：1.日誌空間不足，無法繼續儲存日誌、2.前端設備失聯無

繼續回傳日誌資料、3.從前端設備傳送來的日誌時間不正確、4.從前端設備傳送來的日誌內容不完整或被竄改、5.日誌程式 crash 至無法重啟。

(3) 確認產品在日誌記錄失敗情況下，產品是否有應變機制。

(h) 測試結果：

(1) 當產品發生日誌記錄失敗時，日誌記錄失敗事件應被記錄且產品應能向特定人員(例:使用者或管理者)發出警示。

(2) 產品應持續維持必要功能運作。

(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。

5.6.1.5 **日誌時間戳功能測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.5

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供與產品連接的門禁管理平台或其他門禁設備，以供測試使用。

(2) 產品應提供系統管理者權限之帳號、通行碼，以供測試用。

(3) 廠商應提供書面文件以說明產品發生哪些安全事件及如何記錄安全事件，作為測試依據。

(4) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，以何方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證產品安全事件日誌功能是否具有建立時間戳功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 情況 1：(產品具備安全事件日誌)

(i) 將測試電腦與產品連接。

(ii) 根據廠商提供之說明文件，觸發安全事件。

(iii) 根據產品使用說明，開啟相應之管理介面連接工具。

(iv) 瀏覽安全事件日誌。

(v) 確認日誌內容是否記載步驟(ii)的安全事件紀錄。

(vi) 檢視該日誌是否具有時間戳。

(2) 情況 2：(由門禁管理平台(或其他門禁裝置)記錄產品之安全事件日誌)

(i) 觸發設備所定義的安全事件。

(ii) 以系統管理者帳號和通行碼登入門禁管理平台瀏覽安全事件日誌。

(iii) 或側錄傳送往門禁管理平台之封包，檢視傳送往門禁管理平台之安全事件日誌。

(h) 測試結果：

(1) 產品之安全事件記錄功能或定期事件回傳的資料應可在每個安全事件日誌建立時間戳，且安全事件日誌時間戳之格式應符合 ISO/IEC 8601:2019[7]所規範之格式。

(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。

5.6.1.6 使用者存取資料之不可否認性測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供系統管理者/使用者(若支援)權限之帳號、通行碼，以供測試用。

(2) 廠商應宣告產品安全事件日誌記錄發生哪些安全事件及如何記錄安全事件，作為測試依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，以何方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據

(d) 測試目的：

驗證使用者存取產品時，產品是否能記錄使用者所有操作。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 以管理者/使用者權限(若支援)權限之帳號登入產品管理介面。

(2) 開啟產品設定及查閱門禁系統使用者資料。

(3) 根據產品使用說明，開啟相應之管理介面連接工具。或若安全事件日誌儲存於門禁管理平台，以系統管理者帳號和通行碼登入門禁管理平台瀏覽安全事件日誌。

(4) 瀏覽安全事件日誌。

(h) 測試結果：

(1) 當該管理者權限/使用者權限(若支援)帳號執行廠商所宣告之事件操作時，產品會產生安全事件日誌。

(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。

5.6.1.7 **安全事件日誌檔存取權限設定測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.7

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 管理者與使用者帳號、通行碼。

(2) 產品之使用者帳號和通行碼已經建立，並且存在管理者及一般使用者不同類別之帳號。

(3) 產品應提供設定安全事件日誌存取權限之說明文件作為測試依據。

(4) 廠商應提供書面文件以說明，若由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄。

(d) 測試目的：

驗證產品之安全事件日誌是否具備權限控管。

(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，開啟相應之管理介面連接工具。

(3) 以產品之管理者帳號和通行碼登入。

(4) 瀏覽安全事件日誌。

(5) 根據說明文件，將一般使用者帳號的安全事件日誌存取權限，設定為唯讀。

(6) 登出後以產品之一般使用者帳號和通行碼登入。

(7) 瀏覽安全事件日誌，並修改安全事件日誌。

(h) 測試結果：

(1) 產品具備安全事件日誌檔的讀取權限設定功能。

(2) 一般使用者帳號僅能瀏覽安全事件日誌。

(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：若產品之安全事件日誌是由門禁管理平台(或其他門禁裝置)記錄，且無法由產品之使用者介面存取門禁管理平台(或其他門禁裝置)瀏覽安全事件日誌。

5.6.1.8 日誌紀錄安全敏感性資料外洩測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.8

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供管理者權限之帳號、通行碼。

(2) 廠商應提供書面文件以說明，若由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄。

(d) 測試目的：

驗證日誌紀錄是否會洩露安全敏感性資料。

(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) 若產品支援網頁介面，開啟並以產品之管理者身分登入。

(3) 瀏覽安全事件日誌。

(4) 檢視安全事件日誌是否存在明文或可還原恢復之安全敏感性資料。

(5) 若產品可存取作業系統之介面 ，開啟該介面並以產品之管理者身分登入。

(6) 重複(3)~(4)步驟。

(h) 測試結果：

(1) 日誌紀錄不存在明文或可還原恢復之安全敏感性資料。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品無存取安全事件日誌之介面。

5.6.1.9 安全事件日誌儲存容量-中級測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.9

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供審查文件以說明產品設置環境及安全事件日誌儲存空間之宣告，作為審查依據。

(2) 廠商應提供安全日誌儲存容量設置評估報告，用以分析設置容量大小之評估因素須包括但不限於每筆日誌的平均大小、日誌生成速率、預期之日誌保留期，作為審查依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證當產品設置於中度風險等級環境時，是否有針對安全事件日誌檔配置合理的儲存容量。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供之說明文件與容量評估報告。

(2) 檢視產品安全事件日誌儲存容量。

(3) 若產品安全事件日誌儲存於門禁管理系統，則檢視門禁管理系統之產品安全事件日誌儲存容量。

(h) 測試結果：

(1) 產品的設置環境與安全事件日誌儲存容量應遵循 NIST SP 800-92 之低中度風險等級建議，儲存容量應至少可保存 1 至 3 個月的日誌檔儲存空間。

(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。

5.6.1.10 安全事件日誌之系統時間同步功能測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.10

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供審查文件以說明產品安全事件日誌之生成時間戳與時間同步之功能設計，作為審查依據。

(2) 廠商應提供書面文件以說明，若由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄。

(d) 測試目的：

驗證安全事件日誌之時間戳是否具備與系統時間同步功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱安全事件日誌功能設計文件。

(2) 變更產品日期/時間，檢視產品安全事件日誌之時間戳。

(h) 測試結果：

(1) 產品之安全事件日誌具備與系統時間同步的功能，例如:使用網路時間協定(NTP) 或全球定位系統(GPS)。

(2) 若產品無法產生時間或無連網功能時，應於使用指南說明產品系統時間同步之設置方法，例如:透過相連之閘道器、管理平台同步等其他相連設備。

(3) 通過：(1)~(2)項項結果符合其一。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.6.1.11 未經授權存取安全事件日誌測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.11

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供一組已授權之管理者類別的帳號和通行碼。

(2) 廠商應提供一組未經授權之使用者類別的帳號和通行碼。

(3) 產品應提供安全事件日誌檔存取權限說明文件作為測試依據。

(4) 廠商應提供書面文件以說明，若由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄。

(d) 測試目的：

驗證產品之安全事件日誌檔是否具備防止未經授權的存取、修改和刪除。

(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，開啟相應之管理介面連接工具。

(3) 以廠商提供之管理者帳號和通行碼登入。

(4) 瀏覽安全事件日誌，選擇一筆安全事件日誌檔試圖修改、刪除它。

(5) 登出後，以廠商提供之使用者帳號和通行碼登入。

(6) 瀏覽安全事件日誌，選擇一筆安全事件日誌檔試圖修改、刪除它。

(7) 檢視帳號之上述二種身分類型對安全事件日誌檔的存取行為。

(h) 測試結果：

(1) 以管理者身分登入時可瀏覽安全事件日誌，但無法對安全事件日誌檔執行修改或刪除。

(2) 以使用者身分登入時無法瀏覽安全事件日誌，亦無法對安全事件日誌檔執行修改或刪除。

(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：產品不支援管理者帳戶以外之使用者帳戶登入(僅需測試管理者帳戶)，廠商應提供登入角色與權限設計相關文件作為證明。

(6) 不適用：產品不支援存取安全事件日誌之介面。

5.6.1.12 **安全事件日誌儲存容量-高級測試**

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.12

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供審查文件以說明產品設置環境及安全事件日誌儲存空間之宣告，作為審查依據。

(2) 廠商應提供安全日誌儲存容量設置評估報告，用以分析設置容量大小之評估因素須包括但不限於每筆日誌的平均大小、日誌生成速率、預期之日誌保留期，作為審查依據。

(3) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為測試依據。

(d) 測試目的：

驗證當產品設置於高度風險等級環境時，是否有針對安全事件日誌檔配置合理的儲存容量。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱廠商提供之說明文件與容量評估報告。

(2) 檢視產品安全事件日誌儲存容量。

(3) 若產品安全事件日誌儲存於門禁管理系統，則檢視門禁管理系統之產品安全事件日誌儲存容量。

(h) 測試結果：

(1) 產品的設置環境與安全事件日誌儲存容量應遵循 NIST SP 800-92 之高度風險等級建議，儲存容量應至少可保存 3 至 12 個月的日誌檔儲存空間。

(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。

5.6.1.13 日誌儲存容量不足與警示測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.13

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供審查文件以說明產品安全日誌儲存空間配置、容量偵測與警示功能，作為測試依據。

(2) 廠商應提供書面文件以說明，若由門禁管理平台或其他門禁裝置記錄安全事件，則以何種方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄。

(d) 測試目的：

驗證產品具有偵測安全事件日誌儲存容量不足與警示功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 不斷觸發安全事件。

(2) 試圖填充安全事件日誌的儲存空間，直到達到產品設定之儲存空間不足警示的容量。

(3) 檢視產品是否發出容量不足之警示。

(h) 測試結果：

(1) 產品應具備安全事件日誌儲存容量設定，且安全事件日誌容量達到配置的容量時，產品應發出警示。

(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。

5.6.1.14 未經授權變更時間同步機制測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.14

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供 1 組管理者及使用者之帳號與通行碼。

(2) 廠商應提供產品時間同步機制之設計說明文件作為測試依據。

(d) 測試目的：

驗證產品的時間同步機制是否具備偵測未授權變更與告警功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 根據說明文件之設定權限，以一般使用者帳號和通行碼登入管理介面。

(2) 變更時間同步功能之時區設定。

(3) 根據產品使用說明，開啟相應之管理介面連接工具。

(4) 以管理者帳號和通行碼登入，檢視產品時間及是否有發出警示。

(5) 檢視產品時間是否變更及是否已發出警示。

(h) 測試結果：

(1) 產品之時間同步機制應具備未經授權變更之偵測功能。

(2) 當產品時間同步機制遭未經授權更改時間後，產品應自動發出警示。

(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。

5.6.1.15 使用者、軟體、設備存取之不可否認測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.15

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供與產品相連的設備、軟體。

(2) 廠商應提供可操作特定功能(例如:安全功能設定、發送 e-mail 的能力等)之使用者帳號和通行碼。

(3) 廠商應提供產品書面文件以說明使用者、軟體、設備可對產品哪些功能進行操作及如何記錄安全事件，作為審查依據。

(4) 廠商應提供書面文件以說明若是由門禁管理平台或其他門禁裝置記錄安全事件，以何方式通知門禁管理平台或其他門禁裝置進行安全事件的記錄，作為審查依據。

(d) 測試目的：

驗證產品針對使用者、軟體、設備對產品的特定功能進行操作時是否記錄該安全事件日誌。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據書面文件說明，以廠商提供之使用者帳號和通行碼登入產品並操作特定功能。

(2) 以書面文件說明查閱安全事件方法，檢視產品安全事件日誌。

(3) 根據書面文件說明，以廠商提供之軟體連結產品並操作特定功能。

(4) 以書面文件說明查閱安全事件方法，檢視產品安全事件日誌。

(5) 根據書面文件說明，以廠商提供之設備連結產品並操作特定功能。

(6) 以書面文件說明查閱安全事件方法，檢視產品安全事件日誌。

(h) 測試結果：

(1) 產品之安全事件日誌應包括自使用者登入開始之所有操作行為並保存日誌檔。

(2) 產品之安全事件日誌應包括自軟體連接產品開始之所有操作行為並保存日誌檔。

(3) 產品之安全事件日誌應包括自設備連接產品開始之所有操作行為並保存日誌檔。

(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。

5.6.1.16 硬體強制單次寫入媒體測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.16

(b) 安全等級：

3 級。

(c) 測試資料：

廠商應提供產品設計文件以說明安全事件日誌之儲存方式，作為審查依據。

(d) 測試目的：

驗證產品之安全事件日誌是否儲存在硬體強制單次寫入媒體(Hardware-enforced write-once media)。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

(g) 測試方法：

(1) 審閱說明文件。

(2) 根據文件內容，檢視產品的安全事件日誌是否儲存在硬體強制單次寫入的儲存媒體。

(h) 測試結果：

(1) 產品之安全事件日誌檔應存在硬體強制單次寫入媒體，例如:NIST SP 800-53 所述之 CD-R、DVD-R、BD-R。

(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。

5.6.1.17 使用 API 介面查閱安全事件日誌測試

(a) 測試依據：

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」之 5.6.1.17

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品之管理者帳號和通行碼。

(2) 廠商應提供產品設計文件以說明查閱安全事件日誌的方法，作為測試依據。

(d) 測試目的：

驗證是否可透過 API 介面查閱產品安全事件日誌。

(e) 測試條件：

(1) 產品應支援 API 介面。

(2) 若不支援 API 介面，產品應支援安全事件日誌傳送至集中管理系統/門禁管理平台。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 根據產品說明文件，執行具 API 功能之操作。

(2) 輸入管理者帳號和通行碼，檢視產品安全事件日誌。

(3) 若不支援 API 介面，根據產品說明文件，以管理者帳號和通行碼登入門禁管理平台檢視是否可查閱安全事件日誌。

(h) 測試結果：

(1) 產品應提供 API 介面查閱安全事件日誌。

(2) 產品應支援安全事件日誌傳送至集中管理系統/門禁管理平台，管理者可透過集中管理系統/門禁管理平台查閱安全事件日誌。

(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。

附錄 A
(規定)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
    - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_SHA256
    - TLS_ DHE_RSA_AES128_GCM_SHA256
    - TLS_ DHE_RSA_AES256_GCM_SHA384
- TLSv1.3
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
    - TLS_AES_128_CCM_SHA256
    - TLS_AES_128_CCM_8_SHA256

附錄 B
(參考)
產品概述說明(範例)

送測產品應檢附產品概述表，以供測試實驗室參閱：

表 B.1 設備概述表

製造商	XX 公司
設備名稱	XXX
廠牌	XXX
型號	XX-XXX
韌(軟)體版本	XX.XXX.XX
通訊介面	XXX
網路服務(埠號)	https (443)
網路服務平台(IP)	XX 雲端平台 (XX.XX.XX.XX)
日誌存取權限	User A : 唯讀
日誌檔保存期限	90 天
角色存取權限	Administrator : User A :
管理者帳號/通行碼	Admin 帳號 : Admin 通行碼 :
外觀	<picture>

附錄 C
(參考)
安全功能規格說明(範例)

送測產品應檢附安全功能規格表，以供測試實驗室參閱：

表 C.1 安全功能規格表

項目	說明	申請者填寫內容
1. 除錯模式	詳細描述進入產品除錯模式之方法，或提供佐證文件。	
2. 網路協定	詳細描述產品支援之網路協定，或提供說明文件。	
3. 加密演算法	列出產品所提供之加密演算法及其應用，及提供佐證文件。	
4. 日誌與警示機制	說明安全事件警示機制與警示方式，或提供佐證資料。	
5. 安全通道憑證	驗證安全通道安全要求項目之產品應提供。	
6. 安全開發證明	出示相關認證證明，或包括但不限於以下文件：開發人員安全培訓、軟體需求設計階段、安全編碼技術、實施階段的安全收費、安全測試、安全審查、與軟體安全維護有關的資產和資訊的保存、安全部署、安全事件應變流程和管理第三方軟體供應商。	
7. 個人資料收集	詳細描述收集哪些個人資料及其使用情境和提供誰利用、機密保護作法與存取/	

	存放位置。	
8. 遙測數據收集	詳細描述收集哪些遙測數據及其使用目的和提供誰利用、個資/隱私資料保護作法與存取/存放位置。	

參考資料

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

(2) SP 800-140C Rev. 1:2022 CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/final

(3) FIRST, Common Vulnerability Scoring System version 3.1: Specification Document, https://www.first.org/cvss/specification-document

(4) NIST Special Publication 800-57: Recommendation for Key Management, https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

(5) NIST Special Publication 800-92: Guide to Computer Security Log Management, https://csrc.nist.gov/publications/detail/sp/800-92/final

(6) Open Web Application Security Project (OWASP) org., OWASP Top Ten 2017 Project [viewed 2018-05-16]. Available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

(7) ISO/IEC 8601-1:2019 Date and time — Representations for information interchange — Part 1: Basic rules, https://www.iso.org/standard/70907.html

(8) 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 11 月 28 日	內容修訂。