IoT-2006-6

門禁系統資安測試規範

-第六部：人臉辨識門禁裝置

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，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-2006-6 門禁系統資安測試規範-第六部：人臉辨識門禁裝置」(以下簡稱本測試規範)，依據「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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中的人臉辨識門禁裝置，如圖 1 所示。

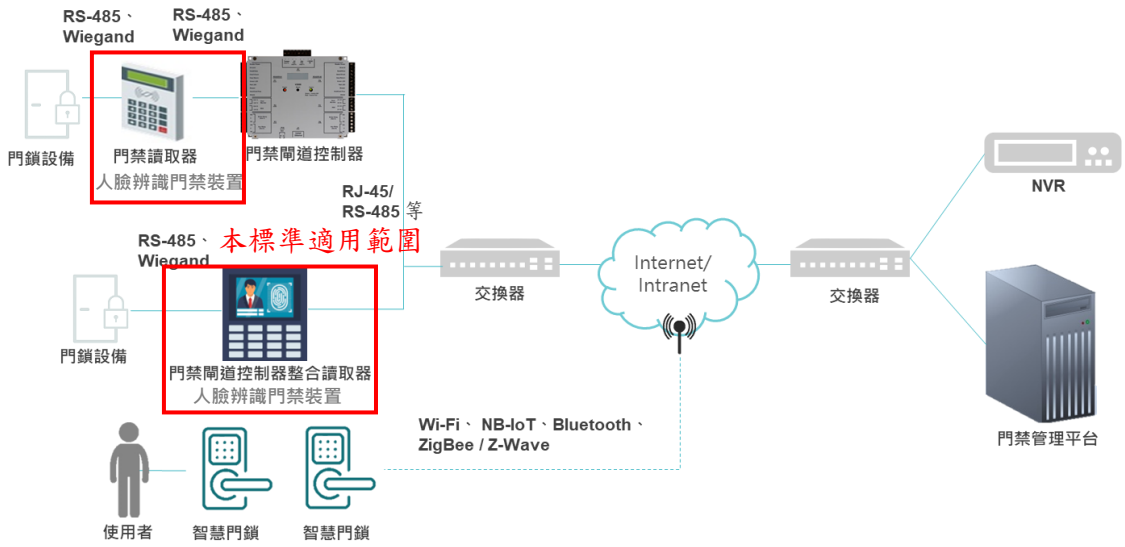

圖 1 適用範圍示意圖

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-1006-6 v1.0 門禁系統資安測試規範-第六部：人臉辨識門禁裝置

3. 用語及定義

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」所規定之用語及定義適用於本規範。

3.1 活體偽冒工具(Presentation attack instrument, PAI)

偽冒攻擊中所使用的生物特徵或物件，例如：2D 的靜態圖像或動態圖像、3D 的面具、複製或變造的指紋、肢解的手指、肢體等。

3.1 活體偽冒攻擊接受率(Impostor Attack Presentation Accept Rate, IAPAR)

係指產品身分驗證功能無法阻擋同類型 PAI 的偽冒攻擊的比例，例如：15 個人臉 PAI 各測試 10 次(共執行 150 次測試)，產品接受 21 次 PAI 使其通過身分驗證，則 IAPAR 為 14%。

4. 測試項目分級

本節依據「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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、個人資料/隱私資料安全及實體安全；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。標示(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
	5.1.2 權限控管	-	-	-
系統完整性	5.2.1 資料完整性	-	-	-
	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	-	5.3.1.2 5.3.1.3	-
資源可用性	5.4.1 作業系統與網路服務	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	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) 5.7.1.12 5.7.1.13 5.7.1.14 5.7.1.15 5.7.1.16 5.7.1.17 5.7.1.18 5.7.1.19	-	-
實體安全	5.8.1 實體入侵防護	5.8.1.1 5.8.1.2	5.8.1.3 5.8.1.4 5.8.1.5	5.8.1.6 5.8.1.7

5. 資安測試規範

人臉辨識門禁裝置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」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-1006-6 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-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.1.1.2

(b) 安全等級：

1 級

(c) 測試資料：

(1) 產品之系統管理者帳密。

(2) 產品應保持出廠預設環境狀態。

(3) 廠商應提供產品身分鑑別機制說明文件。

(4) 廠商應提供變更設定須進行身分驗證之產品功能說明文件。

(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：

產品支援本地端管理介面或實體介面。

(f) 測試佈局：

如圖 2。

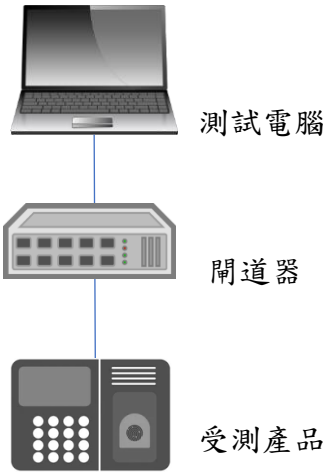

圖 2 測試示意圖

(g) 測試步驟：

(1) 審閱廠商提供之說明文件。

(2) 若產品支援網頁介面、遠端指令介面、API 介面時，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) 以產品之系統管理員帳密登入，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) 檢視身分鑑別結果。

(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色變更。

(8) 檢視產品在開啟功能設定時，是否執行身分驗證機制。

(9) 若產品支援本地端管理介面，以產品之系統管理員帳號登入，執行身分鑑別操作。

(10) 重複步驟(7)~(8)。

(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，產品應執行身分鑑別機制。

(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：產品不支援本地端管理介面及實體介面。

5.1.1.3 活體偽冒檢測功能-初級測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供書面資料以說明活體偽冒檢測功能如何判斷活體偽冒攻擊作為審查依據，例如:使用手冊、產品規格書。

(2) 實驗室應備妥 ISO 或 FIDO 所認可實驗室之 PAD 檢測所使用之活體偽冒工具(PAI)，例如：參閱附錄 A。

(d) 測試目的：

驗證產品是否具備初級活體偽冒檢測(Presentation attack detection, PAD)的防護功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 以測試資料(2)所使用 PAI 之測試對象(真人)在產品上登錄。

(2) 根據附錄 A 之表 A.2 之規定，對產品執行 PAD 測試。

(3) 依攻擊成功次數計算產品 IAPAR。

(h) 測試結果：

(1) 產品之 IAPAR 應小於 15%。

(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 活體偽冒檢測功能-進階測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.1.1.4

(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活體偽冒檢測功能如何判斷活體偽冒攻擊作為審查依據，例如:使用手冊、產品規格書。

(2) 實驗室應備妥 ISO 或 FIDO 所認可實驗室之 PAD 檢測所使用之活體偽冒工具(PAI)，例如：參閱附錄 A。

(3) 廠商可提供經由 ISO 或 FIDO 國際標準組織所認可的實驗室，所核發之 3 年內 ISO 30107 或 FIDO Biometrics Requirements 之檢測評估報告。

(4) 廠商應提供書面資料，以說明產品之人臉辨識功能所支援應用的平台、裝置及其版本等，作為測試使用。

(d) 測試目的：

驗證產品是否具備進階 PAD 的防護功能。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 若廠商提供 PAD 檢測評估報告，查看產品提供的書面資料及檢測報告。

(2) 若廠商未提供 PAD 檢測評估報告，以測試資料(2)所使用活體偽冒攻擊工具之測試對象(真人)在產品上登錄。

(3) 依據測試資料(2)及附錄 A 之表 A.3 之規定，對產品執行 PAD 測試。

(4) 活體偽冒攻擊測試：15 位測試對象依據附錄之定義製作出之攻擊樣態各 14 件 (共 210 件攻擊樣態)，以各攻擊樣態對受測物執行比對測試各 10 次，依攻擊成功次數計算產品之活體偽冒攻擊接受率。

(5) 錯誤拒絕率檢測：同 15 位註冊測試對象(真人)執行比對，各測 20 次。

(h) 測試結果：

(1) 產品之活體偽冒攻擊接受率應小於 7 %，且錯誤拒絕率應小於 10%。

備考 1：活體偽冒攻擊接受率(%)=(比對為成功的數量)/(15 項樣本*各比對 10 次)*100

備考 2：錯誤拒絕率(%)=(比對結果為拒絕的數量或比對不成功的數量)/(15 位測試對象*各比對 20 次)*100

(2) 產品所出具之產品活體偽冒檢測評估報告，足以證明為 ISO 或 FIDO 認可實驗室所發出 FIDO Biometrics Requirements 的 PAD 測試或 ISO/IEC 30107 國際標準之檢測通過報告，且通過條件為活體偽冒攻擊接受率應小於 7%。

(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：無。

5.1.1.5 **多因子身分鑑別測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.1.1.5

(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:臉部特徵辨識、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。

(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兩種(含)以上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) 每次鑑別的不同階段鑑別皆採用不同鑑別因子，例如：第一階段為輸入通行碼、第二階段為人臉辨識。

(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。**

5.2 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-1006-6 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 **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。**

5.2.2 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-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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。

圖 3 測試示意圖

(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機器可讀取之格式。

(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包括但不限於逗號分隔值(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)(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-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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，及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) 若須倚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。

(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。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：不支援網路通訊或網頁介面。

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-1006-6 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。**

5.3.1.2 **信任根保護測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.3.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供產品之信任根功能的操作方法。

(2) 廠商應提供如何保護信任根保護之金鑰及資料的方法。

(3) 廠商應提供信任根功能之設計文件。

(d) 測試目的：

驗證產品之信任根所保護的金鑰及資料是否具有機密性、完整性和真實性的保護。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 依據信任根功能操作方法，查驗是否可提供軟韌體完整性及真實性的保護。

(2) 查驗廠商所保護之信任根所用之金鑰及資料，是否被加密保護。

(3) 查驗廠商所保護之信任根所用之金鑰及資料，是否能防止未授權存取。

(4) 查驗廠商所保護之信任根所用之金鑰及資料，其存取修改都會被記錄。

(h) 測試結果：

(1) 產品具備信任根之功能。

(2) 產品信任根所用之金鑰及資料得到機密性、完整性及真實性的保護，包括但不限於存取時須經身分鑑別、記錄於安全事件紀錄及加密儲存，所使用之加密技術符合 NIST SP 800-140Cr1 所核可的同等或以上等級之要求。

(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。

5.3.1.3 **OSDP 通訊協定傳輸測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.3.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

(4) 產品應支援 OSDP 通訊協定。

(5) 廠商應提供所使用符合 OSDP 通訊協定規格之證明文件，作為測試依據。

(d) 測試目的：

驗證產品所使用 OSDP 通訊協定傳輸是否符合 IEC 60839-11-5:2020 或 SIA OSDP v2.2 所要求之資安規格。

(e) 測試條件：

產品應支援 OSDP 通訊協定。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 查驗廠商提供之 OSDP 通訊協定通過 IEC 60839-11-5:2020 或 SIA OSDP v2.2 驗證之證明文件。

(h) 測試結果：

(1) 產品所提供之證明文件足以證實所使用 OSDP 通訊協定，符合 IEC 60839-11-5:2020 或 SIA OSDP v2.2 所要求之資安規格。

(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 OSDP 通訊協定。

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-1006-6 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。**

5.4.2 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-1006-6 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-1006-6 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-1006-6 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-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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。

(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。

(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。

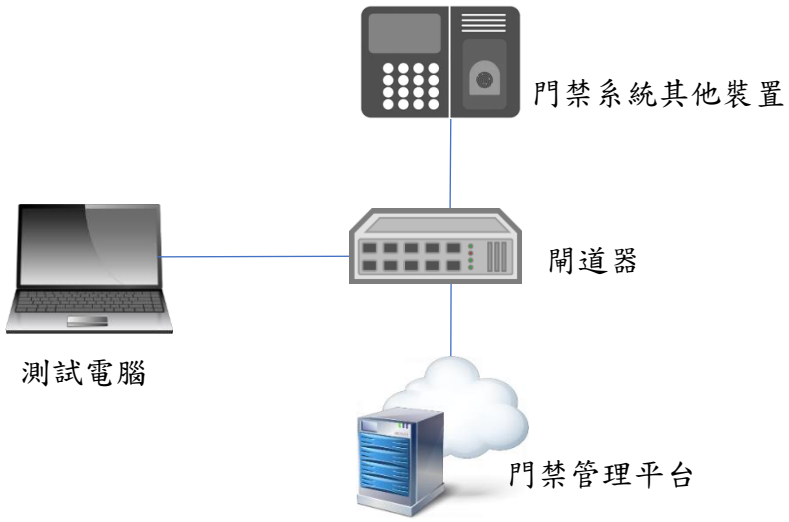

圖 4 測試示意圖

(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) 產品之個人資料傳輸無提供未加密的通訊協定。

(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(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 **人臉辨識資料、敏感性個人資料加密傳輸測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提出產品之人臉辨識資料、敏感性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) 廠商應提出所有人臉辨識資料、敏感性個人資料傳輸的邏輯介面之書面資料，例如：本地端管理介面、網路協定和 API 介面。

(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。

(d) 測試目的：

驗證產品之人臉辨識資料、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。

(4) 若產品之人臉辨識資料須與門禁管理平台同步資料，當執行同步時，同時側錄封包。

(5) 檢視所側錄之封包。

(h) 測試結果：

(1) 人臉辨識資料、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) 產品之人臉辨識資料、敏感性個人資料傳輸無提供未加密的通訊協定。

(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(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 **刪除人臉辨識資料、使用者資料測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品之人臉辨識資料、使用者資料的刪除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刪除人臉辨識資料、使用者資料的機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品人臉辨識資料、使用者資料刪除功能操作之說明文件。

(2) 根據說明文件之操作說明，查驗產品是否具備刪除人臉辨識資料、使用者資料功能。

(h) 測試結果：

(1) 產品之刪除人臉辨識資料、使用者資料功能說明，證實足以協助使用者刪除資料，且提供使用者友善介面以執行資料刪除及檢視已正確清除之功能，並應簡化操作步驟。

(2) 人臉辨識資料、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 刪除人臉辨識資料、個人資料之操作方法測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.4

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供產品之人臉辨識資料、個人資料的刪除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人臉辨識資料、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) 審閱產品之人臉辨識資料、個人資料之刪除功能說明文件。

(2) 根據說明文件之操作方式，執行刪除人臉辨識資料、個人資料功能。

(h) 測試結果：

(1) 產品之人臉辨識資料、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人臉辨識資料、個人資料的刪除。

(2) 刪除人臉辨識資料、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 **人臉辨識資料、個人資料管理機制測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」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人臉辨識資料、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指引之書面文件作為審查依據。

(d) 測試目的：

驗證產品是否具備收集、利用、處理使用者人臉辨識資料、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人臉辨識資料、個人資料管理機制之說明文件。

(h) 測試結果：

(1) 使用者人臉辨識資料、個人資料的收集、利用與處理之管理機制中應符合個人資料保護法第 8 條之規定，包括但不限於：

1. 收集、利用、處理人臉辨識資料與個人資料的目的，

2. 產品的擁有者名稱，

3. 人臉辨識資料、個人資料的類別，

4. 利用的期間、地區、對象及方式，

5. 使用者選擇是否同意授權、撤銷授權及刪除之權利與方式，

6. 擁有者以外的第三方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 **人臉辨識資料、個人資料授權機制測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.6

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供針對使用者人臉辨識資料、個人資料之使用授權機制，與授權機制實施範圍建議之說明文件，例如：使用手冊或安全指南等。

(2) 廠商應提供人臉辨識資料、個人資料授權作法之範例或說明作為審查依據，例如:授權書、授權網頁連結。

(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人臉辨識資料、個人資料之使用授權機制。

(e) 測試條件：

產品應先通過 5.7.1.5 測試。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱使用者人臉辨識資料、個人資料使用授權機制等之書面文件。

(2) 審閱說明文件，產品在使用者操作擷取人臉辨識資料、輸入個人資料前，產品是否提供人臉辨識資料、個人資料授權功能或機制。

(h) 測試結果：

(1) 廠商於書面文件中應提供人臉辨識資料、個人資料授權機制說明，且沒有在未經使用者同意下即逕行收集、利用、處理人臉辨識資料與個人資料。

(2) 使用者人臉辨識資料、個人資料之使用授權機制與授權內容應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網和產品包裝，且使用者授權方式包括但不限於書面同意書、電子郵件或網頁型式。

(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。

5.7.1.7 **人臉辨識資料、個人資料使用授權撤銷機制測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.7

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供對於人臉辨識資料、使用者個人資料的使用授權與撤銷機制，及撤銷機制實施範圍之指引之書面文件，作為審查依據。

(d) 測試目的：

驗證廠商是否具備使用者人臉辨識資料、個人資料之撤銷授權機制。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱撤銷使用者人臉辨識資料、個人資料之使用授權與撤銷機制之書面文件。

(2) 審閱說明文件，產品及與產品連接的其他相關應用或設備是否具備刪除使用者人臉辨識資料、個人資料之功能或機制。

(h) 測試結果：

(1) 撤銷機制書面文件應詳細說明撤銷方法和完成刪除後之告知使用者方式，且產品可透過撤銷授權機制來撤回人臉辨識資料、個人資料的授權，包括但不限於遙測數據、關聯服務等處的人臉辨識資料、個人資料。

(2) 使用者人臉辨識資料、個人資料使用授權之撤銷機制與撤銷方式應公開告知使用者，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 遙測數據之人臉辨識資料、個人資料收集最小化測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.8

(b) 安全等級：

1 級(O)。

(c) 測試資料：

(1) 廠商應提供收集遙測數據中的人臉辨識資料、個人資料之使用目的和實施範圍的宣告。

(2) 廠商應提供產品收集遙測數據所需連接的門禁管理平台或其他門禁設備，和使用說明文件，以供測試使用。

(3) 系統管理者帳號、通行碼。

(d) 測試目的：

驗證遙測數據是否收集非必要的人臉辨識資料、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：

如圖 4。

(g) 測試方法：

(1) 審閱廠商提供之產品宣告文件。

(2) 根據使用說明文件操作，使產品產生各類遙測數據回傳至相連設備或門禁管理平台。

(3) 登入相連的設備或門禁管理平台，查驗遙測數據內容。

(h) 測試結果：

(1) 產品宣告所列收集人臉辨識資料、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最小收集原則。

(2) 遙測數據未收集人臉辨識資料、個人資料，或所收集之人臉辨識資料、個人資料符合必要之所需。

(3) 產品之遙測數據所收集之人臉辨識資料、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。

(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：產品不支援收集遙測數據。

(7) 不適用：產品之遙測數據不支援收集人臉辨識資料，廠商應提供相關文件以證明產品的遙測數據未包括任何人臉辨識資料的取得；且產品之遙測數據不支援收集個人資料，廠商應提供相關文件以證明產品的遙測數據沒有包括任何個人資料的取得。若僅支援人臉辨識資料、個人資料之其中一項時，僅須測試該項。

5.7.1.9 **收集、利用、處理遙測數據之宣告測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.9

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 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。

(2) 廠商應提供產品如何收集遙測數據之說明文件，例如：產品使用手冊、產品說明書等。

(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：

(1) 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。

(1) 根據說明文件執行相關功能操作，產品收集的遙測數據時，側錄傳送遙測數據之封包。

(h) 測試結果：

(1) 廠商遙測數據之宣告應對於遙測數據種類、使用目的及提供予哪些相關對象使用，包括但不限於產品開發商、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) 遙測數據實際所傳送之區域與聲明資料中載明之區域應相同。

(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：產品不支援收集遙測數據。

5.7.1.10 關聯服務之人臉辨識資料、個人資料刪除功能測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.10

(b) 安全等級：

1 級(O)。

(c) 測試資料：

(1) 廠商應提供產品刪除存於關聯服務之人臉辨識資料、個人資料的功能與操作方法說明文件，作為審查依據，例如:產品使用手冊。

(2) 廠商應提供書面資料，以說明使用者如何刪除儲存於關聯服務中的人臉辨識資料、個人資料的方法，作為審查依據，例如:官網、產品使用手冊。

(3) 廠商應提供與產品連接的關聯服務，以供測試使用。

(4) 系統管理者帳號、通行碼。

(5) 關聯服務中已存在至少一名使用者之人臉辨資料、個人資料。

(d) 測試目的：

驗證產品是否提供將存在關聯服務的人臉辨識資料、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：

如圖 4。

(g) 測試方法：

(1) 審閱廠商提供之說明文件。

(2) 根據說明文件之操作方式，查驗刪除關聯服務中人臉辨識資料、個人資料的功能。

(3) 利用刪除功能將一筆使用者的人臉辨識資料、個人資料刪除。

(h) 測試結果：

(1) 審查文件證實產品具備簡便的方法，讓使用者提出刪除關聯服務中的人臉辨識資料、個人資料之請求。

(2) 產品具備管理者易於操作的介面，刪除關聯服務中的人臉辨識資料、個人資料。

(3) 儲存於關聯服務之該筆使用者人臉辨識資料、個人資料確實已刪除。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項項結果不符合其一。

(6) 不適用：產品不支援關聯服務。

(7) 不適用：若產品之關聯服務不支援人臉辨識資料的應用，廠商應提供相關文件以證明不存在任何人臉辨識資料的使用，則產品僅須測試支援個人資料之部分。

(8) 不適用：若產品之關聯服務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，則產品僅須測試支援人辨識資料之部分。

5.7.1.11 **回報刪除狀態測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.11

(b) 安全等級：

1 級(O)。

(c) 測試資料：

廠商應提供自產品及其關聯服務刪除人臉辨識資料、個人資料的刪除狀態回報機制之聲明，作為審查依據，例如:產品使用手冊、官網。

(d) 測試目的：

驗證產品及其關聯服務是否具備刪除狀態之回報機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱刪除狀態回報機制之說明文件。

(h) 測試結果：

(1) 審查文件證實使用者提出刪除人臉辨識資料、個人資料之請求後，產品在完成刪除後回報刪除狀態予使用者，例如:個人資料自關聯服務中刪除完成。

(2) 產品回報刪除狀態的方式，包括但不限於電子郵件或簡訊通知。

(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：產品及其關聯服務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。

5.7.1.12 人臉圖像收集、儲存測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.12

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供人臉辨識功能說明文件，內容須包含人臉圖像的收集、利用、儲存，以作為審查依據。

(2) 廠商應提供產品人臉圖像之收集、利用、儲存等應用之使用者授權機制與宣告，內容應包括但不限於收集、利用、儲存之目的、保存期限、保護與管理能力等，作為審查依據，例如:產品使用手冊等。

(3) 若產品運作須連結其他設備時，廠商應提供與產品連接的門禁管理平台或其他門禁設備，和使用說明文件，以供測試使用。

(4) 系統管理者帳號、通行碼。

(d) 測試目的：

驗證產品沒有收集、儲存未經使用者同意的人臉圖像。

(e) 測試條件：

無。

(f) 測試佈局：

產品應支援收集、儲存人臉圖像。

(g) 測試方法：

(1) 審閱產品授權機制與人臉辨識功能說明文件。

(2) 根據說明文件，新增使用者並建立門禁人臉辨識鑑別資料時，使用者不同意授權人臉圖像。

(3) 產品對使用者執行人臉辨識與身分鑑別。

(4) 根據說明文件，以管理者帳號登入產品，查驗是產品是否存在使用者的人臉圖像。

(h) 測試結果：

(1) 審查文件證實產品對於人臉圖像的收集、利用、儲存具有使用者同意機制，且收集、利用、儲存人臉圖像具有合理的目的、保存期限、保護與管理能力；使用者授權方式包括但不限於書面同意書、電子郵件或網頁型式。

(2) 依據產品人臉圖像授權機制，未取得使用者同意下，應不允許建立未授權人臉圖像之使用者鑑別資料；當執行該名使用者人臉辨識身分鑑別，鑑別不成功。

(3) 使用者不同意人臉圖像的授權時，產品確實沒有收集、儲存其的人臉圖像。

(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：產品不支援人臉圖像之收集及儲存，廠商應提供相關文件以證明產品不存在任何人臉圖像檔的收集及儲存。

5.7.1.13 **人臉辨識資料和人臉圖像收集、利用、處理最小化測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.13

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供人臉辨識資料、人臉圖像之收集、利用、處理和儲存之目的與方法、使用範圍以及利用、處理與保存的期限之宣告，與產品使用說明文件，作為審查依據。

(2) 產品應提供生成人臉辨識資料和產品使用時，所需人臉圖像的數量、類型等說明文件，作為審查依據。

(3) 若產品運作須連結其他設備時，廠商應提供與產品連接的門禁管理平台或其他門禁設備，和使用說明文件，以供測試使用。

(d) 測試目的：

驗證產品對於人臉辨識資料、人臉圖像的收集、利用、處理和儲存是否符合最小化原則。

(e) 測試條件：

產品應支援收集、利用及儲存人臉圖像。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品收集、利用、處理和儲存之宣告文件，和生成人臉辨識資料之說明文件。

(2) 新增使用者並建立門禁人臉辨識鑑別資料。

(3) 比對說明文件與實際產品人臉圖像、人臉辨識資料的收集、利用、處理和儲存情況。

(h) 測試結果：

(1) 產品對人臉辨識資料、人臉圖像的收集、利用、處理和儲存的目的與方法、使用範圍以及利用、處理與保存的期限，符合產品必要之所需(最小化原則)。

(2) 生成人臉辨識資料所需之人臉圖像符合最小化原則，包括但不限於擷取人臉圖像張數最小數量、最少圖像類型。

(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：產品不支援人臉圖像之收集、利用及儲存，廠商應提供相關文件以證明產品不存在任何人臉圖像檔的收集、利用及儲存。

5.7.1.14 **人臉圖像自動刪除測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.14

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供產品之人臉辨識功能說明文件，以供測試使用。

(2) 廠商應提供人臉辨識資料、人臉圖像之收集、利用、處理和儲存之目的與方法、使用範圍以及利用、處理與保存的期限之宣告，作為審查依據。

(3) 產品已完成建立測試人員之人臉辨識資料。

(4) 系統管理者帳號、通行碼。

(5) 若產品運作須連結其他設備時，廠商應提供與產品連接的門禁管理平台或其他門禁設備。

(d) 測試目的：

驗證產品是否在完成鑑別或識別後立刻刪除人臉圖像。

(e) 測試條件：

產品須先通過 5.7.1.13 測試。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 情境一：

(i) 若產品在鑑別或識別所擷取之人臉圖像，有收集、利用、儲存人臉圖像之需要時，查驗 5.7.1.13 是否通過測試。

(2) 情境二：

(i) 根據說明文件，產品偵測與擷取測試人員特徵後，執行人臉辨識以鑑別身分。

(ii) 完成身分鑑別後，以系統管理者帳號登入產品，查驗產品是否存在測試人員的人臉圖像。

(h) 測試結果：

(1) 情境一：若產品在鑑別或識別所擷取之人臉圖像有收集、利用、儲存之需要時，應通過 5.7.1.13 測試。

(2) 情境二：產品在完成身分鑑別後，產品不存在人臉偵測與特徵擷取時的人臉圖像。

(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。

5.7.1.15 人臉辨識資料之可更新、不可逆、不可連結測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.15

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供產品之人臉辨識設計說明文件，作為審查依據。

(2) 產品須先完成建立測試人員之人臉辨識資料。

(d) 測試目的：

驗證產品之人臉辨識資料是否具備可更新、不可逆、不可連結的特性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品人臉辨識說明文件。

(2) 根據產品說明文件，將已建立的測試人員之人臉辨識資料作廢或刪除，嘗試利用同一張測試人員之人臉圖像重新產生人臉辨識資料。

(3) 查驗步驟(2)之 2 筆人臉辨識資料是否有關聯性。

(4) 根據產品說明文件，驗證產品所產生的人臉辨識資料是否可逆向回推人臉圖像。

(h) 測試結果：

(1) 產品所使用之人臉辨識資料在鑑別過程中符合 CNS 29100-2 之去識別化要求，例如:通過 CNS 29100-2 驗證。

(2) 產品可使用同一人臉圖像重新產生人臉辨識資料，且產品說明文件足以實明新產生的人臉辨識資料與原先的人臉辨識資料不具關聯性。

(3) 產品產生的人臉辨識資料無法回復人臉圖像，所使用之技術包括但不限於使用雜湊演算法。

(4) 通過：(1)~(4)四項結果皆符合。

(5) 不通過：(1)~(4)四項結果不符合其一。

(6) 不適用：無。

5.7.1.16 **本地端人臉辨識測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.16

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品之人臉辨識說明文件，作為審查依據，例如:產品使用手冊。

(d) 測試目的：

驗證產品同時支援本地端與遠端人臉辨識時，是否採用本地端人臉辨識。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱產品人臉辨識說明文件。

(h) 測試結果：

(1) 產品之人臉辨識採用本地端(邊緣運算)方式執行身分比對。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品之人臉辨識僅支援透過遠端或管理平台，執行身分比對之非本地端(邊緣運算)人臉辨識門禁裝置。

5.7.1.17 人臉辨識資料、個人資料委外處理測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.17

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供產品之人臉辨識資料、個人資料委外處理政策之宣告，作為審查依據。

(2) 若產品人臉辨識資料、個人資料為委外處理：

(i) 廠商應提供對於委外處理所做的風險評估報告，作為審查依據。

(ii) 廠商應提供如何審核受委託者的風險管理能力之評鑑文件，作為審查依據。

(d) 測試目的：

驗證產品是否未將人臉辨識資料、個人資料委外處理；若為委外處理，則驗證是否對委外處理執行風險評估及對受委託者進行資安風險管理能力審核。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品人臉辨識資料、個人資料委外處理政策之宣告，確認產品的人臉辨識資料、個人資料是否委託第三方處理。

(2) 若產品人臉辨識資料、個人資料為委外處理時，查驗該委外處理行為的風險評估報告，及查驗對受委託者所做的資安風險管理能力之評鑑文件。

(h) 測試結果：

(1) 廠商提供之宣告文件足以證明產品之人臉辨識資料、個人資料未委託第三方處理，且政策宣告公開顯示於，例如:產品官網、產品使用手冊、產品包裝等。

(2) 產品之人臉辨識資料、個人資料委託第三方處理時，廠商有對委外處理的行為完成風險管理評估。

(3) 廠商已確實對受委託者完成風險識別與管理之能力審核。

(4) 通過：(1)項結果符合，或(2)(3)項結果皆符合。

(5) 不通過：(1)項結果不符合，且(2)(3)項結果不符合其一。

(6) 不適用：無。

5.7.1.18 **人臉辨識資料、個人資料之安全管理機制測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.18

(b) 安全等級：

1 級。

(c) 測試資料：

廠商應提供產品之人臉辨識資料、個人資料之管理機制說明文件，作為審查依據。

(d) 測試目的：

驗證產品對於人臉辨識資料、個人資料是否具有安全管理機制文件，且包括發生人臉辨識資料、個人資料遭竊取、洩漏或竄改時告知當事人之規定。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

審閱產品之人臉辨識資料、個人資料安全管理機制文件。

(h) 測試結果：

(1) 廠商對於人臉辨識資料、個人資料的安全管理機制應包括但不限於：

(i) 防止人臉辨識資料、個人資料遭竊取、竄改、毀損、滅失或洩漏的能力。

(ii) 人臉辨識資料、個人資料宣告之目的終止後人臉辨識資料、個人資料之處理方法。

(iii) 發生人臉辨識資料、個人資料發生竊取、洩漏或竄改等侵害時，廠商應主動告知上述資料之當事人，告知的方式，例如：信件、email 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。

5.7.1.19 **跨境傳輸測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.7.1.19

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供產品之人臉辨識資料、個人資料之儲存方式、目的與儲存地之宣告，作為審查依據。

(2) 廠商應提供產品操作說明文件，例如:產品使用手冊，作為測試依據。

(d) 測試目的：

驗證產品之人臉辨識資料、個人資料是否沒有跨境傳輸。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

(g) 測試方法：

(1) 審閱廠商提供之宣告說明文件。

(2) 根據產品說明文件，執行產品人臉辨識資料、個人資料之收集、儲存和備份功能時，側錄產品傳輸封包。

(3) 檢視所側錄之封包。

(h) 測試結果：

(1) 產品之人臉辨識資料、個人資料儲存於國內，無跨境傳輸。

(2) 產品之人臉辨識資料、個人資料須國際傳輸時，應符合個人資料保護法第21條規定。

(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：無。

5.8 實體安全測試

檢視產品有關實體安全部分之送審資料是否符合IoT-1006-6之安全要求，並依下列各測試項目進行實機測試。

5.8.1 實體入侵防護測試

5.8.1.1 啟動階段完整性測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之5.8.1.1

(b) 安全等級：

1級。

(c) 測試資料：

(1) 產品須提供安全啟動功能之設計文件。

(2) 產品須提供未加密的韌體、軟體和組態資料，及其相關安裝步驟之說明文件。

(d) 測試目的：

驗證產品於開機階段是否能確保韌體、軟體及組態資料之完整性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能之書面資料。

(2) 竄改韌體、軟體及組態資料後，重新啟動產品。

(h) 測試結果：

(1) 當韌體、軟體及組態資料經竄改後，產品無法被啟動。

(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。

5.8.1.2 **還原通行碼預設值測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供還原出廠設定操作說明。

(d) 測試目的：

驗證產品實體層的通行碼預設值還原設計是否具備安全防護機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢視產品外觀(不包括設計上應鎖定於牆壁該面)，是否存在徒手(無須特殊工具)即可輕易還原預設通行碼之機制，例如:使用筆或竹籤等非特殊工具強行破解的方式。

(2) 若存在，則測試其還原至出廠設定之功能。

(h) 測試結果：

(1) 產品外觀不存在徒手(無須特殊工具)即可輕易還原回預設通行碼的機制。

(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。

5.8.1.3 實體介面安全管控測試

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供書面資料，說明進入作業系統(若有)除錯模式之方法。

(d) 測試目的：

驗證是否無法透過產品實體介面存取作業系統之除錯模式，或存取實體介面具身分鑑別。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據文件所述連接相應之實體介面。

(2) 若產品支援 USB 埠，則將測試電腦連接產品之 USB 埠，並開啟相應之管理介面連接工具。

(3) 透過 USB 埠存取作業系統之除錯模式。

(4) 若產品支援 UART 埠，則將測試電腦連接產品之 UART 埠，並開啟相應之管理介面連接工具。

(5) 透過 UART 埠存取作業系統之除錯模式。

(6) 若產品支援 JTAG 埠，則將測試電腦連接產品之 JTAG 埠，並開啟相應之管理介面連接工具。

(7) 透過 JTAG 埠存取作業系統之除錯模式。

(h) 測試結果：

(1) 產品透過 USB、UART 或 JTAG 存取作業系統之除錯模式時，產品要求身分鑑別。

(2) 產品不存在可進入作業系統除錯模式之實體介面。

(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。

5.8.1.4 **實體保護測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.4

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 若產品具防拆除保護機制(例：一體成形或機殼防拆螺絲)，或具備防拆偵測設計，則應提供相關說明文件。

(2) 若產品之外殼拆除障礙，是透過現場布建時，額外於產品外殼再裝上支架或防護罩外殼來加以保護，廠商應在產品之使用說明書或資安指引中註明產品於現場布建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件應公告在廠商官網上。

(d) 測試目的：

驗證產品是否建立外殼拆除障礙，或具備防拆偵測設計，以防止實體入侵。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品提供之說明文件。

(2) 檢視產品之外殼是否一體成型。

(3) 檢視產品之外殼是否經防拆螺絲鎖住。

(4) 檢視產品是否具備防拆警示功能之防拆功能。

(h) 測試結果：

(1) 產品採用一體成形或防拆螺絲等機殼防拆除保護設計。

(2) 當產品應額外加裝支架或防護罩外殼，產品之使用說明書或資安指引中註明產品於現場布建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件公告在廠商官網上。

(3) 產品採用本身具有防拆偵測設計或加裝具有防拆偵測功能之防護，防拆警示方式包括但不限於警報聲響、簡訊或 email。

(4) 通過：(1)(3)項結果符合，或(2)(3)項結果符合。

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

(6) 不適用：無。

5.8.1.5 **安全啟動真實性測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.5

(b) 安全等級：

2 級

(c) 測試資料：

產品須提供安全啟動功能之設計文件。

(d) 測試目的：

驗證產品於開機階段是否能確保韌體、軟體及組態資料的真實性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能之書面資料。

(2) 確認產品在開機過程中是否驗證韌體、軟體及組態資料的簽章。

(h) 測試結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 產品在開機過程中驗證韌體、軟體及組態資料的簽章。

(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。

5.8.1.6 **除錯介面偵測測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.6

(b) 安全等級：

3 級。

(c) 測試資料：

產品應提供除錯介面偵測與警示之功能設計說明文件。

(d) 測試目的：

當存取產品除錯介面時，驗證產品是否有能力偵測且產生安全事件日誌紀錄。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據產品提供之說明文件，開啟相對應之管理介面連接工具。

(2) 若產品存在 USB 埠，嘗試存取作業系統除錯模式。

(3) 檢視產品狀態。

(h) 測試結果：

(1) 當產品偵測到存取除錯介面時，產品應產生安全事件日誌紀錄。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品之作業系統無除錯介面。

5.8.1.7 **實體介面偵測警示功能測試**

(a) 測試依據：

「IoT-1006-6 門禁系統資安標準-第六部：人臉辨識門禁裝置」之 5.8.1.7

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供實體介面偵測與警示之功能設計說明文件。

(2) 產品應提供所有實體介面清單之書面文件。

(d) 測試目的：

當產品之實體介面有未經授權存取時，驗證產品是否有能力偵測且發出警示。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據產品提供之說明文件，開啟相對應之管理介面連接工具。

(2) 若產品存在 USB 埠，則插拔外接 USB。

(3) 若產品存在 RJ45 埠，則插拔外接 RJ45。

(4) 檢視產品狀態。

(h) 測試結果：

(1) 當產品偵測實體埠經異常插拔操作時，產品應產生安全事件日誌紀錄，且向使用者和管理者發出警示。

(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。

附錄 A
(參考)
FIDO 活體偽冒工具(PAI)等級說明

PAD 1 級之活體偽冒工具等級劃分[3]，以供測試實驗室與送測廠商參閱：

表 A.1　PAI 等級

等級說明		PAI 示例
A 級	啟動攻擊所需時間:< 1 天 所需專業知識: 無 所需設備: 普通(智慧手機、平板電腦等)	● 照片輸出： 以解析度 1200dpi 之彩色印表機列印，照片主體比例佔 100%、A4 尺寸的白紙、彩色輸出。
		● 數位螢幕顯示： 以解析度 400dpi 之 10 吋平板顯示，照片主體比例佔 75%、彩色顯示。
	生物特徵來源: 即時、簡單	樣本來源為模擬竊取的照片或來自社群媒體的照片。
B 級	啟動攻擊所需時間: < 7 天 所需專業知識: 精通 所需設備: 普通、專業(智慧手機、平板電腦等)	● 數位影片以行動裝置顯示： 以解析度 400dpi 之 6.5 吋智慧手機播放，影像主體比例佔 75%、彩色顯示。
		● 數位影片以 4K 螢幕顯示： 以 24 吋 4K 螢幕播放，影像主體比例佔 100%、彩色顯示。
		● 2.5D 紙面具： 以解析度 1200dpi 之雷射印表機列印之面具由測試人員配戴，照片主體比例佔 100%、A4 尺寸白貼紙、彩色輸出及半身樣式。 註：2.5D 紙面具應至少二處以上露出配戴者之五官，例如:眼、口、鼻等。
	生物特徵來源: 中等	樣本來源為模仿證件照(國際民航組織規定格式)之高畫質照片、影片。

表 A.2　1 級 PAD 測試資料與設置

測試參數	值	說明
樣本數 (人數)	15	足夠的覆蓋率，包括年紀、性別、種族等。依據 FIDO Biometrics Requirements 6.1.2 所規定。
PAI 等級 A	2	見表 A.1 之 A 級。
PAI 等級 B	3	見表 A.1 之 B 級。
每一樣本測試次數	10	確保可重複性。
測試環境	1	在一般照明光源之相同測試場所。

A.3 2 級 PAD 測試資料與設置

測試參數	值	說明
樣本數(人數)	15	足夠的覆蓋率，包括年紀、性別、種族等。依據 FIDO Biometrics Requirements 6.1.2 所規定。
PAI 等級 A	6	參照表 A.1 之 A 級。
PAI 等級 B	8	參照表 A.1 之 B 級。
每一樣本測試次數	10	確保可重複性。
測試環境	1	在一般照明光源之相同測試場所。

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 SP 800-140C Rev.1, 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) FIDO Alliance, FIDO Biometrics Requirements (2021, December 6), https://fidoalliance.org/specs/biometric/requirements/

(4) ISO/IEC 30107-3:2017 Information Technology-Biometric Presentation Attack Detection-Part 3: Testing and reporting, https://www.iso.org/standard/67381.html

(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
V2.0	112 年 12 月 4 日	內容修訂。