IoT-2006-4

門禁系統資安測試規範

-第四部：門禁讀取器

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-2006-4 門禁系統資安測試規範-第四部：門禁讀取器」(以下簡稱本測試規範)，依據「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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讀取器、門禁閘道控制器整合讀取器(如圖 1)。

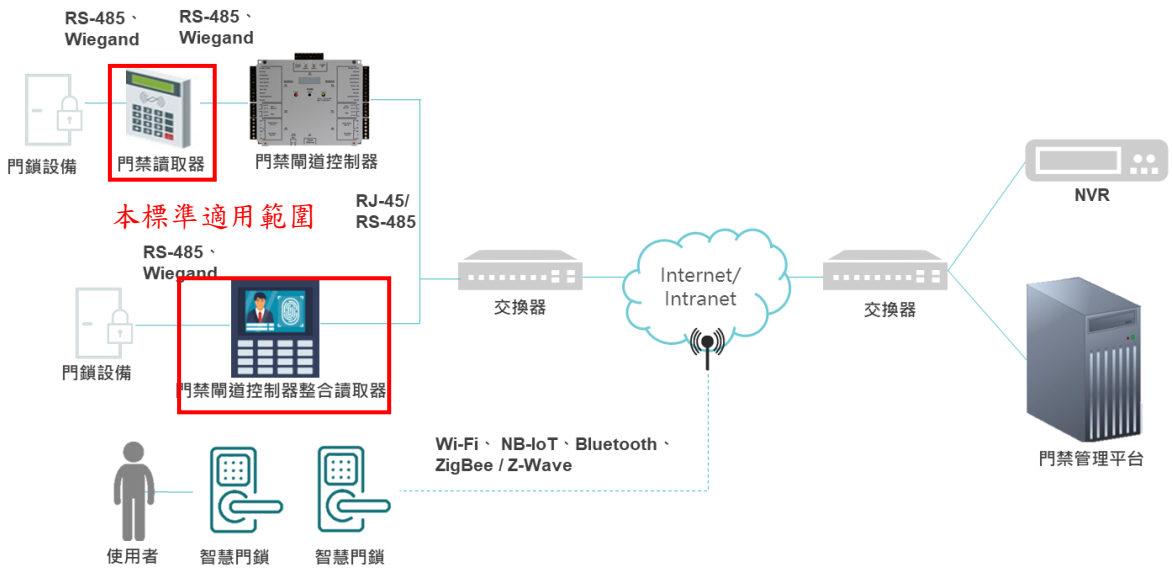

圖 1 適用範圍示意圖

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-1006-4 v1.0 門禁系統資安測試規範-第四部：門禁讀取器

3. 用語及定義

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」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。 (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	-	-
	5.1.2 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	-
資源可用性	5.4.1 作業系統與網路服務	-	-	-
	5.4.2 資源管理	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
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)	-	-
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 5.8.1.8

5. 資安測試規範

門禁讀取器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-1006-4 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 **安全警語測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.1.1.3

(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供測試使用，例：使用手冊。

(d) 測試目的：

驗證產品是否在使用者登入時具有安全警語功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

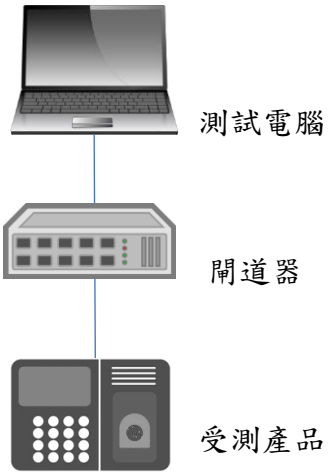

圖 2 測試示意圖

(g) 測試方法：

(1) 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) 以使用者帳號及通行碼開啟登入頁面，檢視登入頁面。

(h) 測試結果：

(1) 產品提供之說明文件足以讓管理者充分了解產品使用安全警語設定功能。

(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) 若產品支援使用者介面，產品之使用者登入介面應顯示所設定之安全警語。

(4) 若產品未支援使用者介面，安全警語應張貼實體通知，例如:貼紙、標籤等。

(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 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-1006-4 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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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)(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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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，或對接的安全監控裝置符合公認資安產業慣例之證明文件，供測試使用，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：

產品應具網路通訊或網頁等介面。

(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[(4)]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裝置，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：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-1006-4 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 信任根安全測試

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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：

驗證產品之信任根的金鑰及資料是否具有機密性、完整性和可用性的保護。

(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。

(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-1006-4 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-1006-4 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-1006-4 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-1006-4 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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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。

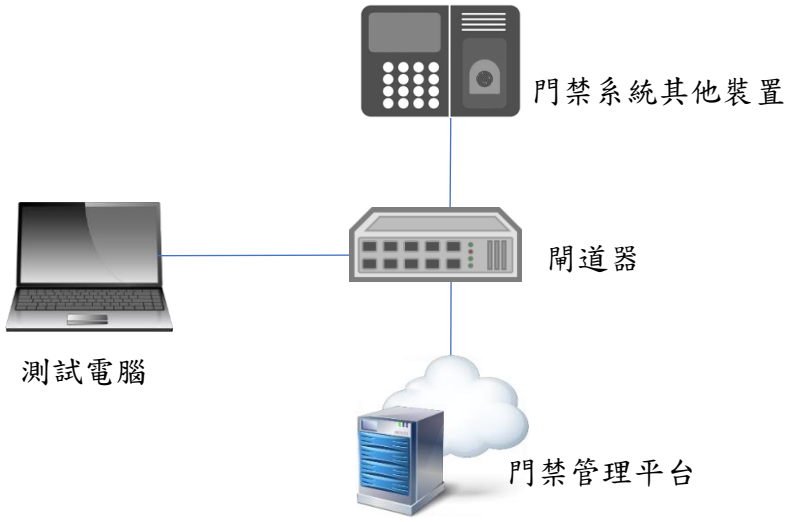

圖 4 測試示意圖

(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) 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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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) 廠商應提出所有敏感生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敏感性個人資料的利用，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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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求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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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的之說明文件。

(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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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、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、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才可處理個人資料。

(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。

(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 **個人資料授權測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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 **遙測數據收集之個人資料收集最小化測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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最小收集原則。

(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個人資料的利用。

5.7.1.9 **收集遙測數據測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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、使用目的及提供予哪些相關對象使用，包括但不限產品開發者、系統整合者或第三方廠商使用，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產品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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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料刪除。

(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) 儲存關聯服務之使用者個人資料確實被刪除。

(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的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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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、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。

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-1006-4 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-1006-4 門禁系統資安標準-第四部：門禁讀取器」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) 廠商應提供未加密韌體檔案與韌體安裝說明文件。

(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 還原預設卡號或通行碼測試

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」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：

驗證產品實體層的預設卡號或通行碼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)，是否存在無須特殊工具即可輕易還原預設卡號或通行碼之機制，例如:使用一支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) 產品外觀不存在無須特殊工具即可輕易還原回預設卡號或通行碼的機制。

(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 藍牙傳輸保護測試

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品藍牙是否使用安全的藍牙加密傳輸。

(e) 測試條件：

產品應支援藍牙傳輸。

(f) 測試佈局：

如圖 5。

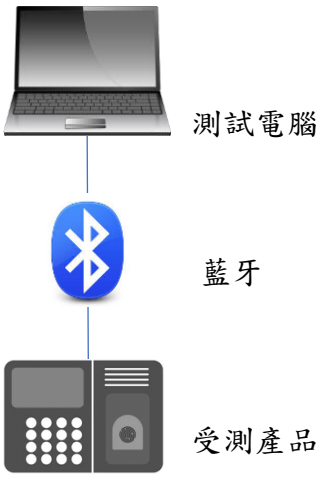

圖 5 測試示意圖

(g) 測試方法：

(1) 使用藍牙傳輸側錄工具，擷取受測物之藍牙封包，確認裝置所使用之藍牙傳輸是否加密。

(2) 藍牙傳輸是否採用符合 NIST SP 800-140Cr1 [(2)]所核可之同等或以上等級之加密演算法。

(h) 測試結果：

(1) 產品之藍牙傳輸採用符合 NIST SP 800-140Cr1 所核可之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：產品不支援藍牙。

5.8.1.4 實體介面安全管控測試

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.4

(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) 若產品支援透過 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。

5.8.1.5 **實體保護測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.5

(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)(2)項結果皆不符合，或(3)項結果不符合。

(6) 不適用：無。

5.8.1.6 **安全啟動真實性測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.6

(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) 書面資料證實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。

5.8.1.7 **除錯介面偵測測試**

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.7

(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。

(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之紀錄。

(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。

5.8.1.8 實體介面偵測警示功能測試

(a) 測試依據：

「IoT-1006-4 門禁系統資安標準-第四部：門禁讀取器」之 5.8.1.8

(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) 產品應提供實體介面清單。

(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 埠。

(3) 若產品存在 RJ45 埠，則插拔外接 RJ45 埠。

(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。

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) 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) FIDO Alliance, FIDO Biometrics Requirements (2021, December 6), https://fidoalliance.org/specs/biometric/requirements/

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

(5) 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 25 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 4 日	內容修訂。