IoT-1006-1

門禁系統資安標準

-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

近來全球物聯網資安法規、標準、規範、指引相繼出籠，2018 年美國加洲法案 SB-327，2019 年美國 NIST 發布 NISTIR 8259，2021 年更是陸續發布 8259 系列標準，2020 年歐洲 ETSI 發布 ETSI EN 303 645 等，說明物聯網資安是刻不容緩極需面對的議題，全球資安認驗證的意識已明顯浮現，例如: 2019 年歐盟推出的 EU cybersecurity Act、2021 年美國即將推出的 Cybersecurity Labeling Program，面對可能造成國際出口貿易障礙的隱憂，數位發展部數位產業署協助各產業訂定資安標準，包括：影像監控系統系列資安標準、智慧巴士資通訊系列資安標準、智慧路燈系列資安標準、空氣品質微型感測裝置、消費性網路攝影機資安標準，引導產業轉型升級，增加國際競爭力。

根據 Marketsandmarkets 市調報告中指出，門禁系統的全球市場規模將從 2018 年的 75 億美元，每年以 8.24% CAGR (複合成長率)速度上升，預測到 2024 年達到 121 億美元。與 Mordor Intelligence 研究顯示，預估 2019-2024 年北美為全球門禁系統需求最大市場，與亞太地區皆為成長率最高的區域。然而門禁系統遭受各式各樣的資安威脅，主要可分為 4 大類: (1)駭客癱瘓門鎖系統、(2)門鎖鎖不住、(3)人臉資訊外洩、(4)用戶個資遭竊，這些威脅將使原本讓群眾安全安心的門禁服務不再被信任。

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產品制定資安標準，包括門禁系統上的門禁管理平台、門禁閘道控制器、門禁讀取器與智慧門鎖，以緩解門禁系統遭遇之資安威脅。

1. 適用範圍

本系列標準規定門禁系統產品之資安要求。門禁系統為於通道出入口管制人員進出所使用的軟硬體產品所組成的系統，本標準適用範圍包括門禁讀取器、門禁閘道控制器、門禁管理平台及智慧門鎖。其相關應用為辦公室各出入口、廠房、軍事或醫院特定區域出入口等。

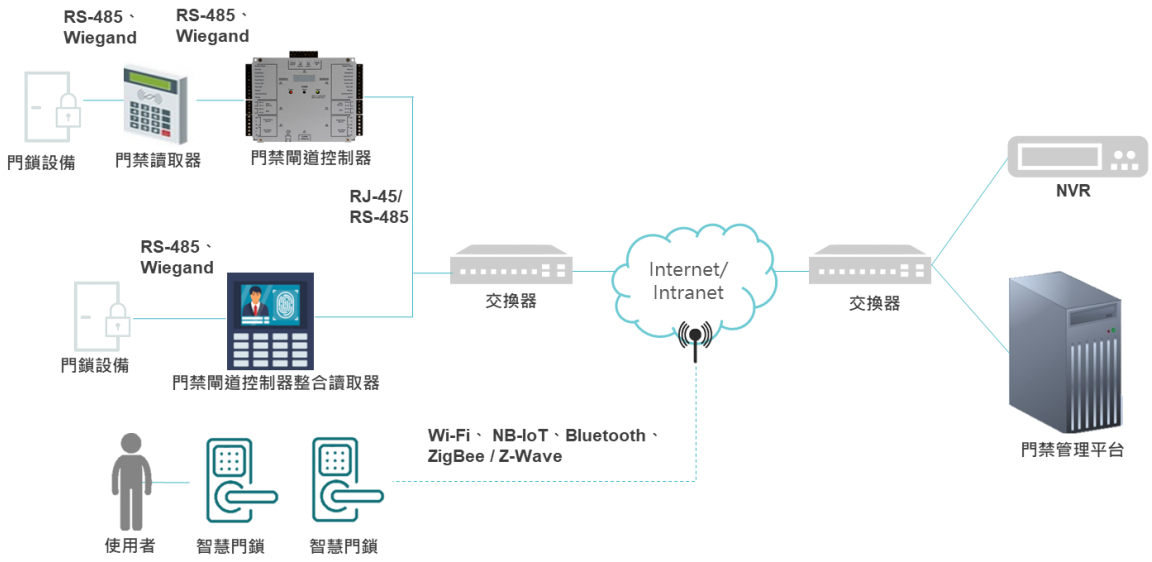

圖 1 門禁系統架構示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。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. 用語及定義

下列用語與定義適用於本系列標準。

3.1 門禁讀取器(Access control reader)

在門禁系統中的重要組成產品之一，裝設於管制通道出入口，門禁系統信號輸入的關鍵設備。例如：感應卡式門禁讀取器、按鍵型門禁讀取器、指紋型讀取器。

3.2 門禁閘道控制器(Access controller)

係為門禁系統的核心，結合場域閘道器與管理平台連接，作為門禁讀取器與門禁管理平台資料傳輸之出入口，用於將門禁讀取器接收之卡片、指紋、通行碼、人臉等資料傳送至門禁管理平台，及接收門禁管理平台發送之控制指令予以令管制出入門開啟或關閉。

3.3 門禁管理平台(Access control management system)

係指具有管理門禁系統使用者功能的後台伺服器、軟體或邏輯介面，用於與門禁閘道控制器或智慧門鎖連接，傳送控制指令至門禁閘道控制器或智慧門鎖，以及收集來自管制出入口門禁讀取器所回傳之出入資料，提供管理單位即時監控、管理與記錄。

3.4 智慧門鎖(Smart lock)

係指安裝於門上以代替傳統只能鑰匙上鎖開鎖之設置，智慧門鎖普遍可透過感應卡、通行碼、指紋等方式解鎖，透過連網功能具備遠端操控或監控開鎖紀錄。

3.5 不可否認性(Non-repudiation)

確保網路交易的雙方無法否認曾進行過的交易、或通訊參與的雙方皆無法否認曾進行資料傳輸或接收訊息，證明所宣稱事件(或動作)之發生及其發起個體的能力。

備考：不可否認性旨在解決關於事件(或動作)是否發生，以及於該事件中個體是否參與之爭議。

3.6 信任根(Root of trust)

係指安全的根本，在密碼系統中始終可以信任的來源。它可以是用來加解密的金鑰、資料，或是硬體模組，用它來生成和保護金鑰並在其安全環境中執行加密功能。

3.7 行動碼(Mobile code)

係指不需要接收者明確安裝即可在資產之間傳輸的軟體程式(Software programs)。例如：JavaScript、VBScript、Java applets、ActiveX controls、Flash animations、Shockwave movies、Microsoft Office macros 等。

3.8 安全敏感性資料(Secure sensitive data)

係指身份鑑別資料(例如:生物特徵、通行碼、金鑰)，當此資料遭到揭露或修改時，可能會損害產品的安全性。例如：產品進行 OTA 更新時，更新伺服器發送之憑證金鑰遭到惡意人士的竄改或竊取，可能造成更新失敗或韌體遭竊取。

3.9 敏感性資料(Sensitivity data)

本標準之敏感性資料是指，安全敏感性資料、敏感性個人資料與個人資料的統稱。

3.10 敏感性個人資料(Sensitive personal data)

係指其被揭露後極有可能對個人造成人身傷害或財產損害的資料。敏感性個人資料之內容因產品和使用案例而異，例如：家用影像攝影機(IP camera)的視訊串流、支付資訊、通訊資料內容帶有時間戳記的位置座標。

3.11 個人資料(Personal data)

係指對於已識別或可識別自然人有關的任何資訊，包括識別個人身分之隱私資料，例如：身分證字號、電話號碼、住址、車牌及生物辨識相關之影像等。

備考：依個人資料保護法第 2 條第 1 款之定義。

3.12 關聯服務(Associated services)

係指產品所提供之功能所需的數位服務，包括行動應用程式(App)、雲服務(雲端運算、雲端儲存)、第三方 API 及傳輸遙測數據的第三方服務等。

3.13 遙測數據(Telemetry data)

係指蒐集來自產品的資訊，雖可以提供廠商用以識別問題或改善產品服務所需之相關的訊息，例如：產品 crash 回報、產品座標(GPS)、使用習慣紀錄等資訊，但可能洩漏使用者之隱私。

3.14 通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)[2]

由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)提供的漏洞評分系統，目前發展至第 3 版，以衡量軟體漏洞的特徵和嚴重性進行評分，包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度，都被列入計分。自 0 分至 10 分，0 代表無風險，而 10 則代表最高風險。

3.15 常見漏洞揭露(Common Vulnerabilities and Exposures, CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

3.16 美國國家漏洞資料庫(National Vulnerabilities Database, NVD)

係指美國國家標準技術研究所(National Institute of Standards and Technology)提供的美國國家漏洞資料庫，負責常見漏洞如 3. 15 所述之資料的發布及更新。

3.17 遠端證明(Remote attestation)

係指系統用以驗證前端產品身分的方法，通常透過憑證機制與公鑰加密結合，來保證發出的資訊只能被發出證明要求的電腦或設備讀取，而非其他竊聽者。

3.18 安全通道(Security tunnel)

網際網路通訊端點與端點(End-to-End)間，並達到資料隱密性及完整性所建立之通道，如：目前常見之實作通訊協定為安全套接層(Secure Sockets Layer, SSL)和傳輸層安全性(Transport Layer Security, TLS)。

3.19 會話(Session)

係指在二個或多個通信實體(例如:主機設備、網路設備、軟體/應用程式、嵌入式設備)之間進行半永久性、有狀態的資訊相互交換，通常會話具有明確定義的開始和結束過程。

備考：通常會話具明確定義之開始過程及結束過程。

3.20 安全事件日誌(Security event log)

係指記錄每個稽核規則所定義的活動，用以察覺威脅或攻擊事件的發生，本標準之安全事件即指使用者登入系統、硬體拆卸等的行為。

3.21 日誌滾動(Log rotation)

日誌滾動是指系統管理中一個自動化歸檔過期日誌文件的過程，每次增加新日誌文件時，舊日誌文件名後面的數字就會增加，當舊日誌文件後面的數字超過設定臨界值時，可以被刪除或者存到他處來釋放儲存空間。日誌滾動提供了一個有效的方法來限制日誌文件的大小，同時保留近期的日誌用於分析。

3.22 軟體物料清單(Software bill of materials，SBOM)

係指代碼庫(codebase)中存在的所有開放原碼和第三方組件的列表，透過 SBOM 來管理代碼庫中所使用組件的版本、漏洞修補狀態及這些組件的授權。其主要目的為明確地識別各組件與其他組件之間相互關係。

3.23 預定義狀態(Predetermined state)

係指產品為防止控制系統在受到攻擊、失去網路訊號等無法維持正常運作的情況下，產品提供針對上述情況可進行預先設定應變狀態定義的功能。例如:預定義狀態設定為火災警報作用時門鎖裝置解除鎖定、安全更新失敗則回復至更新前的門禁控制狀態。

3.24 使用者(User)

係由系統或裝置管理者授予一般存取權限之個人、團隊或組織，但不具有安全組態設定、監控等管理者(Administrator)權限。

3.25 使用者資料(User data)

係指儲存於產品中之所有敏感性資料及使用者權限配置資料。

3.26 一體成型(Integrated molding)

係指產品的外殼非由零件組合而成，而是整體不分割地直接製成。

3.27 防拆螺絲(Tamper resistant screws)

係指在螺絲設計上採用各種特殊頭型及沖針設計等，需要用特殊工具固定和拆卸，無法透過一般販售之公版螺絲起子及板手拆卸。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

安全等級總表，如表 1 所示，第一欄為安全構面，包括：(1)身分鑑別、識別、授權安全、(2)系統完整性、(3)系統機密性、(4)資源可用性、(5)更新安全及(6)警示與紀錄；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。本安全等級總表各欄的關連性，須依循本節 5.1 至 5.6 之技術規範內容。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)引用國際標準之安全要求等級、(2)相關資安風險高低，分為 1 級、2 級與 3 級三個等級。產品應先通過較低安全等級之測試，始可進級高階等級之測試。

表 1 安全要求等級總表

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

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
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 5.2.1.9 5.2.1.10(O)	5.2.1.11 5.2.1.12 5.2.1.13	5.2.1.14
	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	5.2.3.8
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	-	-

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

4.1.1 安全構面：

(a) 身分鑑別與授權機制安全：溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，應確保鑑別與授權相關機制。

(b) 系統完整性：產品的資料保護，監控與修補產品已知漏洞及預防與處置機制的資訊安全管理。

(c) 系統機密性：敏感性資料之儲存與通訊安全，通訊服務存在未知之資安漏洞與否。

(d) 資源可用性：產品須確保服務可維持正常運作的能力。

(e) 更新安全：產品之作業系統及韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(f) 警示與紀錄：產品日誌紀錄須有管理機制，且於發生安全事件須具有警示能力。

4.1.2 安全要求分項：

依安全構面所設計對應之安全要求要項，且每一安全要求分項包含一個以上之安全要求。

4.1.3 安全等級：

安全等級依(1)引用國際標準之安全要求等級、(2)相關資安風險高低之綜合考量，分為 1 級、2 級、3 級三個等級。其對應之列即其所應符合的安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求必須先滿足較低安全等級要求。

4.1.3.1 安全 1 級，適用於消費性產品，運行期間所產生之資料為敏感的個人資料，需要基本資安防護來避免消費者隱私受侵害，並確保系統基本完整性及高度可用性以保護人身財產安全，建議一般居家環境或較無機敏資料之商辦的區域使用，如：社區大樓、智慧宅、商辦。

4.1.3.2 安全 2 級，適用於商業、工業用產品，運行期間所產生之安全且敏感之資料，需要進階防護來避免商業機密外洩與危及使用安全，且須確保系統中度完整性及高度可用性以保護人身財產安全，建議企業商辦或工廠管制區域使用，如：私人公司、工廠。

4.1.3.3 安全 3 級，適用於關鍵基礎設施用產品，需要花費較高成本來嚴格防護產品運行期間所產生之機密資料，且須確保系統高度完整性及高度可用性以保護人身財產安全，建議具有高度管制區域使用，如：能源、交通等關鍵基礎設施。

5. 一般要求

本節詳盡載明門禁系統之產品為滿足安全功能應採取的共通方法，所有門禁系統產品應符合本節中所有安全要求。

5.1 身分鑑別、識別、授權安全

5.1.1 鑑別機制

5.1.1.1 廠商所生產之產品，其身分鑑別所使用之預設安全敏感性資料(例:通行碼、金鑰)都須相異；抑或首次成功取得產品存取之授權，須強制更改預設安全敏感性資料。(1 級)

5.1.1.2 鑑別錯誤訊息不應顯露出合法使用者名稱。(1 級)

5.1.1.3 當產品使用公開金鑰架構時，應遵循公認資安產業慣例之最佳技術，包括但不限於 ISO/IEC 國際標準、歐盟國際標準、美國國家標準等普遍業界所接受的作法。(2 級)

5.1.1.4 當產品使用公開金鑰身分鑑別機制時，應具備：(2 級)

(a)憑證為受信任根憑證所發行。

(b)自簽憑證者，應驗證憑證串鏈的功能。

(c)驗證憑證撤銷狀態的功能。

(d)私鑰的儲存與權限控管的功能。

(e)驗證憑證與相應之使用者身分的功能。

(f)簽章演算法應符合 5.3.1.1 項之要求。

5.1.1.5 當產品使用對稱金鑰身分鑑別機制時，應符合：(2 級)

(a)通話的雙方應提供交互認證的功能。

(b)該組件應提供安全儲存雙方所協商一致對稱共享密鑰的功能。

(c)該組件應提供限制訪問共享密鑰的功能。

(d)該組件應提供確保用於對稱密鑰認證的演算法和密鑰符合 5.3.1.1 項之要求。

5.1.1.6 產品應具備遠端證明(Remote Attestation)功能，使智慧門鎖、門禁讀取器、門禁閘道控制器向門禁管理平台證明自身的真實性。(3 級)

5.1.1.7 產品應具備使用者通行碼生命週期與通行碼定期提醒更換功能，該功能應符合公認資安產業慣例之規格，包括但不限於 ISO/IEC 國際標準、歐盟國際標準、美國國家標準等普遍業界所接受的作法。(3 級)

5.1.1.8 產品的身分鑑別用之安全敏感性資料，除短生命週期私鑰外，應使用硬體機制保護，例如:安全晶片。(3 級)

5.1.1.9 產品應提供所有存取介面之使用者識別和身分鑑別功能。(1 級)

5.1.1.10 產品應提供使用者之唯一識別。(2 級)

5.1.1.11 產品應有唯一的識別碼。(3 級)

5.1.2 權限控管

5.1.2.1 當產品支援行動碼執行，產品應驗證行動碼的完整性，且不應執行或傳輸未經授權之行動碼(mobile code)。(1 級)

5.1.2.2 當產品支援行動碼執行時，應驗證行動碼的真實性。(2 級)

5.1.3 通行碼鑑別

5.1.3.1 產品應提供強制設定使用者通行碼最小和最大生命週期的功能。(3 級)

5.2 系統完整性

5.2.1 資料完整性

5.2.1.1 產品於傳輸過程中應鑑別所接收安全敏感性資料的完整性。(1 級)

5.2.1.2 產品應確保安全敏感性資料於儲存、使用與傳輸的完整性。(1 級)

5.2.1.3 產品所使用之安全敏感性資料應具唯一性，例如:產品金鑰。(1 級)

5.2.1.4 當產品完整性偵測到有未經授權的軟體變更時，產品應向管理者或使用者發出警示，且直接或間接皆不應連結到超出執行告警功能所需的網路範圍。(1 級)

5.2.1.5 產品之所有介面應驗證輸入的語法和內容，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)。(1 級)

5.2.1.6 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，例如:回復至產品最後一次備份之組態設定狀態。(1 級)

5.2.1.7 產品所揭露予使用者之錯誤訊息之內容，不應有可能被攻擊利用之敏感性安全資料。(1 級)

5.2.1.8 當產品出於安全為目的將產品唯一識別碼以硬編碼(Hard code)方式儲存，應防止實體或軟體等方式竄改。(1 級)

5.2.1.9 當產品出於安全為目的，應禁止安全敏感性資料以硬編碼方式儲存。(1 級)

5.2.1.10 產品應支援硬體等級的記憶體存取控制機制，例如:MMU、MPU 技術進行空間保護。(1 級)(O)

5.2.1.11 產品於傳輸過程中應鑑別所接收敏感性資料的真實性，如使用密碼演算法應符合 5.3.1.1 項之要求。(2 級)

5.2.1.12 軟體/韌體、組態或影響到功能執行的資料(例如:感測資料)變更時，應具備真實性檢查且產生安全事件日誌。(2 級)

5.2.1.13 產品應具備通信會話(Session)完整性的機制，應：(2 級)

(a)會話識別碼應具唯一性。

(b)會話識別碼的生成機制應足夠隨機，所使用之生成機制應符合公認之資安產業慣例之演算法。

(c)當使用者會話終止或使用者註銷會話識別碼時，會話識別碼應立即失效。

5.2.1.14 當產品完整性偵測到有未經授權的軟體、組態或影響到功能執行的資料(例如:感測資料)變更時，產品應主動發出警示予使用者與管理者。(3 級)

5.2.2 安全管理程序

5.2.2.1 產品應具備良好之金鑰管理程序，以確保金鑰管理的品質。(1 級)

5.2.2.2 產品應提供安全設定指南以協助使用者完成最佳安全設置，安全設定指南內容包括但不限於:應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。(1 級)

5.2.2.3 產品管理介面與網路服務應僅提供產品必要服務之所需。(1 級)

5.2.2.4 產品應具備漏洞揭露政策，政策內容包括但不限於：(1 級)

(a)回報漏洞問題的連絡資訊。例如:使用說明書記載廠商之漏洞回報專線或電子信箱。

(b)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。

(c)問題的處理至解決各階段之狀態更新。例如:廠商可運用平台的漏洞回報與處理流程機制。

5.2.2.5 廠商應及時處理已被揭露的漏洞，例如:在漏洞修正計畫中載明漏洞風險等級、等級對應之修復處理時間之界定等漏洞處理原則。(1 級)(O)

5.2.2.6 產品所有之網路與安全功能於交付前應通過審查(review)或評估(evaluate)，審查內容包括但不限於廠商已識別之漏洞修補結果，評估內容包括廠商所識別的必要安全措施及緩解措施。(1 級)(O)

5.2.2.7 產品之密碼演算法及相關資訊須可被更新，若產品為不可更新設備時，產品的建議使用年限不得超過密碼演算法建議使用期限。(1 級)(O)

5.2.2.8 廠商應提供產品安全開發說明文件，包括但不限於開發人員安全培訓、軟體需求設計階段、安全程式設計技術、實施階段的安全收費(security

tolling)、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。(1 級)(O)

5.2.2.9 廠商應具備產品之軟體物料清單(SBOM)，軟體物料清單內容欄位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、建立清單之作者。(1 級)

5.2.2.10 產品應提供查閱產品資訊之功能，例如：產品名稱、型號、軟韌體版本及支援傳輸類型等。(2 級)

5.2.3 已知漏洞安全

5.2.3.1 廠商對其產品已揭露之安全漏洞應持續監控、識別與修正。(1 級)(O)

5.2.3.2 產品之作業系統與網路服務(Network Service)，不應存在美國國家漏洞資料庫所公開的常見漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為重大風險。(1 級)

5.2.3.3 產品之網站服務(web service)不應存在 OWASP 所揭露之最新網站 10 大資安風險[4]，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為高風險。(1 級)

5.2.3.4 產品所引用網路相關之第三方函式庫不應存在美國國家漏洞資料庫所公開的常見漏洞資料，且漏洞評鑑系統 CVSSv3 嚴重性等級評比為重大風險。(1 級)

5.2.3.5 產品之作業系統與網路服務，不應存在美國國家漏洞資料庫所公開的常見漏洞資料，且漏洞評鑑系統 CVSSv3 嚴重性等級評比為高風險。(2 級)

5.2.3.6 產品之網站服務不應存在 OWASP 所揭露之最新網站 10 大資安風險，且漏洞評鑑系統 CVSS v3 嚴重性等級評比為中風險。(2 級)

5.2.3.7 產品所引用網路相關之第三方函式庫不應存在美國國家漏洞資料庫所公開的常見漏洞資料，且漏洞評鑑系統 CVSSv3 嚴重性等級評比為高風險。(2 級)

5.2.3.8 產品所引用網路相關之第三方函式庫不應存在美國國家漏洞資料庫所公開的常見漏洞資料，且漏洞評鑑系統 CVSSv3 嚴重性等級評比為中風險。(3 級)

5.3 系統機密性

5.3.1 敏感性資料保護

5.3.1.1 產品所使用之密碼演算法應根據國際公認 NIST SP 800-140Cr1 [(1)]所核可的同等或以上等級之密碼演算法。(1 級)

5.3.1.2 產品所儲存、傳輸之安全敏感性資料、敏感性資料不應明文儲存，而保護資料的加密方式應符合 5.3.1.1 項之要求。(1 級)

5.3.1.3 產品應提供刪除安全敏感性資料之安全機制。(2 級)

5.3.1.4 產品應確保釋出記憶體後，已完全消除暫存於揮發性共享記憶體資源(例如:RAM)之敏感性資料。(3 級)

5.4 資源可用性

5.4.1 作業系統與網路服務

5.4.1.1 產品應具備資源管理功能，提供限制安全功能使用資源之設定，以防止資源耗盡。(1 級)

5.4.1.2 在系統中斷或故障後，產品應提供還原至預設的安全狀態的功能。(1 級)

5.4.1.3 產品在初始狀態下的網路服務，所揭露給未認證方的訊息應為廠商提供必要服務之所需。(1 級)

5.4.1.4 產品預載之軟體服務應為廠商提供必要服務之所需。(1 級)(O)

5.4.1.5 產品之原始碼應最小化且為必要功能之所需。(1 級)(O)

5.4.1.6 產品應提供備份功能，以確保失效或錯誤設置時可以恢復正常狀態，且備份過程不應影響產品正常運作。(1 級)

5.4.1.7 當產品還原備份前，應確保備份檔之完整性。(2 級)

5.4.2 資源管理

5.4.2.1 產品若有外部感測功能應清楚告知使用者，告知方式包括但不限於記載於產品使用說明書或產品包裝等。(1 級)

5.4.2.2 針對網路和電源中斷的情況，產品應設置因應網路和電源中斷的彈性機制，例如:設置備用電源、資料即時備份等。(1 級)(O)

5.4.2.3 產品應在網路中斷時仍可保持本地端運作，且在網路恢復後，系統能回復正常運作。(1 級)(O)

5.4.2.4 產品應具備保持連線穩定與功能正常運作之能力，包括但不限於產品分批線上更新、產品於恢復網路連線時連線。(1 級)(O)

5.5 更新安全

5.5.1 軟韌體更新

5.5.1.1 產品應支援軟韌體更新的能力，且具備安全更新的部署管理程序。(1 級)

5.5.1.2 產品應在更新安裝前驗證任何軟韌體更新檔的真實性和完整性。(1 級)

5.5.1.3 產品之軟/韌體應具備安全更新功能，更新之安全功能包括但不限於防止安裝舊版本、傳輸加密演算法符合 5.3.1.1 之加密演算法或更新傳輸安全通道。(1 級)

5.5.1.4 產品應通知使用者進行更新，且更新資訊應說明該更新所能緩解的風險，通知方式包括但不限於使用彈跳視窗、推播訊息或電子郵件。(1 級)(O)

5.5.1.5 當產品更新過程，若會中斷產品基本功能，則須於更新前告知使用者。(1 級)(O)

5.5.1.6 廠商應提供使用者產品支援期限，且敘述應淺顯易懂，支援期限公告於包括但不限在產品網站、包裝或使用說明書等。(1 級)

5.5.1.7 產品更新作業異常中斷時，系統應能恢復正常運作。(1 級)

5.6 警示與紀錄

5.6.1 安全事件日誌檔與警示

5.6.1.1 產品應提供與安全相關的日誌記錄功能，安全事件日誌應包括但不限於時間戳、來源(原始設備、軟體程序或使用者帳號)、類別、型式、事件 ID 和安全事件結果。(1 級)

5.6.1.2 當產品設置於低度風險等級環境時，安全事件日誌檔之儲存容量配置應遵循 NIST SP 800-92[(3)]建議，儲存容量應至少可保存 1 至 2 週的日誌檔儲存空間，容量配置之評估因素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。(1 級)

5.6.1.3 產品之事件日誌檔應具備日誌滾動(log rotate)機制，以防止因安全相關之處理程序發生錯誤時，產品仍能維持正常運作。(1 級)

5.6.1.4 當產品發生日誌記錄失敗(audit processing failure)的情況時，日誌記錄失敗事件應被記錄且應向使用者或管理者發出警示。(1 級)

5.6.1.5 產品應具有建立時間戳(包括日期和時間)的功能，以供後續稽查事件紀錄之用，應依據 ISO/IEC 8601:2019 之格式。(1 級)

5.6.1.6 產品應至少具備日誌用於確認使用者存取資料的不可否認性。(1 級)

5.6.1.7 產品之安全事件日誌須具備權限控管機制，應提供僅授權者得以唯讀方式讀取安全事件日誌之設定功能。(1 級)

5.6.1.8 日誌檔中不應存在明文或可被還原回復之安全敏感性資料。(1 級)

5.6.1.9 當產品設置於中度風險等級環境時，安全事件日誌檔之儲存容量配置應遵循 NIST SP 800-92 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，容量配置之評估因素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。(2 級)

5.6.1.10 產品產生的時間戳應具備與系統時間同步的功能，例如：網路時間協定(NTP)或全球定位系統(GPS)。(2 級)

5.6.1.11 產品應保護安全日誌，以防止未經授權的存取、修改和刪除。(2 級)

5.6.1.12 當產品設置於高度風險等級環境時，安全事件日誌檔之儲存容量配置應遵循 NIST SP 800-92 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，容量配置之評估因素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。(3 級)

5.6.1.13 當產品之安全事件日誌的儲存量達到配置的容量時，產品應具備主動告警功能。(3 級)

5.6.1.14 時間同步機制應偵測未授權之變更，且在變更時應主動告警。(3 級)

5.6.1.15 產品應確認使用者、軟體、設備存取特定功能的不可否認性。(3 級)

5.6.1.16 產品之安全事件日誌應儲存於硬體強制單次寫入媒體(Hardware-enforced write-once media)，例如：NIST SP 800-53[(5)]所述之 CD-R, BD-R, DVD-R 裝置。(3 級)

5.6.1.17 產品應提供 API 介面以查看安全事件日誌。(3 級)

附錄 A
(參考)
技術要求事項與各標準規範對照表

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.1.1.1	CR 1.5A - Authenticator management – initialize authenticator content	5.1-1 - Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
	CR 1.5B - Authenticator management – change default authenticators	
5.1.1.2	CR1.10 - Authenticator feedback	-
5.1.1.3	CR1.8 - Public key infrastructure (PKI) certificates	-
5.1.1.4	CR1.9A - Strength of public key-based authentication - check validity of signature of a given certificate	-
	CR1.9B - Strength of public key-based authentication -validate certificate chain	
	CR1.9C - Strength of public key-based authentication - check certificate's revocation status	
	CR1.9D - Strength of public key-based authentication - establish user control of private key	
	CR1.9E - Strength of public key-based authentication - map authenticated identity to a user	
	CR1.9F - Strength of public key-based authentication - use of cryptography	
5.1.1.5	CR1.14A - Strength of symmetric key-based authentication - establish the mutual trust using the symmetric key	-
	CR1.14B - Strength of symmetric key-based authentication - secure storage for shared secret	
	CR1.14C- Strength of symmetric key-based authentication - restrict access to shared secret	
	CR1.14D - Strength of symmetric key-based authentication - ensure that the	

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
	algorithms and keys used for the symmetric key	
5.1.1.6	CR 1.2 - Software process and device identification and authentication CR1.2RE(1) - Unique identification and authentication	-
5.1.1.7	CR1.7RE(1) - Password generation and lifetime restrictions for human users	-
5.1.1.8	CR1.5RE(1) - Hardware security for authenticators	-
	CR1.9RE(1) - Hardware security for public key-based authentication	
	CR1.14RE(1) - Hardware security for symmetric key-based authentication	
5.1.1.9	CR 1.1 - Human user identification and authentication CR 1.2 - Software process and device identification and authentication	5.5-4 - Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.
5.1.1.10	CR 1.1RE(1) - Human user identification and authentication - Unique identification and authentication	5.1-2 - Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
5.1.1.11	CR1.2RE(1) - Software process and device identification and authentication- Unique identification and authentication	-
5.1.2.1	NDR2.4A - Mobile code - control execution	-
	NDR2.4B - Mobile code - control upload by user	
	NDR2.4C - Mobile code - integrity check	
5.1.2.2	NDR2.4RE(1) - Mobile code authenticity check	-
5.1.3.1	CR1.7RE(2)- - Password lifetime restrictions for all users	-
5.2.1.1	CR3.1 - Communication integrity	-
5.2.1.2	CR1.5D - Authenticator management - protect authenticators	5.4-1(partial) - Sensitive security parameters in persistent storage shall be stored securely by the device.

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.2.1.3	-	5.4-4 - Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.
5.2.1.4	CR3.4 - Software and information integrity	5.7-2 - If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.
5.2.1.5	CR3.5 - Input validation	5.13-1 - The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.
5.2.1.6	CR3.6 - Deterministic output	-
5.2.1.7	CR3.7 - Error handling	-
5.2.1.8	-	5.4-2 - Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.
5.2.1.9	-	5.4-3 - Hard-coded critical security parameters in device software source code shall not be used.
5.2.1.10	-	5.6-8 - The device should include a hardware-level access control mechanism for memory.
5.2.1.11	CR3.1RE(1) - Communication authentication	5.3-10(partial) - Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.
5.2.1.12	CR3.4RE(1) - Authenticity of software and information	-
5.2.1.13	CR3.8A - Session integrity - invalidate session identifiers CR3.8B - Session integrity - generate and recognize session identifiers	-

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
	CR3.8C - Session integrity - random session identifiers	
5.2.1.14	CR3.4RE(2) - Automated notification of integrity violations	-
5.2.2.1	-	5.5-8 - The manufacturer shall follow secure management processes for critical security parameters that relate to the device.
5.2.2.2	CR7.6 - Network and security configuration settings	5.12-1(partial) - Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.
		5.12-2(partial) - The manufacturer should provide users with guidance on how to securely set up their device.
5.2.2.3	CR7.7 - Least functionality	5.6-1 - All unused network and logical interfaces shall be disabled.
5.2.2.4	-	5.2-1 - The manufacturer shall make a vulnerability disclosure policy publicly available.
5.2.2.5	-	5.2-2 - Disclosed vulnerabilities should be acted on in a timely manner.
5.2.2.6	-	5.5-2 - The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.
5.2.2.7	-	5.5-3 - Cryptographic algorithms and primitives should be updateable.
5.2.2.8	-	5.6-9 - The manufacturer should follow secure development processes for software deployed on the device.
5.2.2.9	-	-
5.2.2.10	CR7.8 - Control system component inventory	5.3-16(partial) - The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.
5.2.3.1	-	5.2-3 - Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
		they operate during the defined support period.
		5.10-1 - If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.
5.2.3.2	-	-
5.2.3.3	-	-
5.2.3.4	-	-
5.2.3.5	-	-
5.2.3.6	-	-
5.2.3.7	-	-
5.2.3.8	-	-
5.3.1.1	CR4.3 - Use of cryptography	5.1-3(partial) - Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.
		5.5-1(partial) - The consumer IoT device shall use best practice cryptography to communicate securely.
		5.3-7(partial) - The device shall use best practice cryptography to facilitate secure update mechanisms.
5.3.1.2	CR4.1A - Information confidentiality - at rest	5.5-1 - The consumer IoT device shall use best practice cryptography to communicate securely.
	CR4.1B- Information confidentiality - in transit	5.5-6 - Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.
5.3.1.3	CR4.2 - information persistence	-
5.3.1.4	CR4.2RE(1) - Information persistence - Erase of shared memory resources	-
	CR4.2RE(2) - Information persistence - Erase verification	
5.4.1.1	CR7.2 - Resource management	-
5.4.1.2	CR7.4 - Control system recovery and reconstitution	-

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.4.1.3	-	5.6-2 - In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.
5.4.1.4	-	5.6-5 - The manufacturer should only enable software services that are used or required for the intended use or operation of the device.
5.4.1.5	-	5.6-6 - Code should be minimized to the functionality necessary for the service/device to operate.
5.4.1.6	CR7.3 – Control system backup	
5.4.1.7	CR7.3 RE(1) – Control system backup - Backup integrity verification	
5.4.2.1	-	5.8-3 - All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.
5.4.2.2	-	5.9-1 - Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.
5.4.2.3	-	5.9-2 - Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.
5.4.2.4	-	5.9-3 - The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.
5.5.1.1	NDR3.10 - Support for updates	5.3-1 - All software components in consumer IoT devices should be securely updateable.
		5.3-8 - Security updates shall be timely.
5.5.1.2	NDR3.10RE(1) - Update authenticity and integrity	5.3-9 - The device should verify the authenticity and integrity of software updates.
		5.3-10(partial) - Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.5.1.3	-	5.3-2 - When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.
5.5.1.4	-	5.3-11 - The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.
5.5.1.5	-	5.3-12 - The device should notify the user when the application of a software update will disrupt the basic functioning of the device.
5.5.1.6	-	5.3-13 - The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.
5.5.1.7	-	-
5.6.1.1	CR2.8A - Auditable events - categories CR2.8B - Auditable events - data fields	-
5.6.1.2	CR2.9A - Audit storage capacity - allocation	-
5.6.1.3	CR2.9B - Audit storage capacity - exceeded CR2.10A - Response to audit processing failures - maintain essential functions	-
5.6.1.4	CR2.10A - Response to audit processing failures - maintain essential functions CR2.10B - Response to audit processing failures - actions taken	-
5.6.1.5	CR2.11 - Timestamps	-
5.6.1.6	CR2.12 - Non-repudiation	-
5.6.1.7	CR6.1 - Audit log accessibility	-
5.6.1.8	-	-
5.6.1.9	CR2.9A - Audit storage capacity - allocation	-
5.6.1.10	CR2.11RE(1) - Time synchronization	-
5.6.1.11	CR3.9 - Protection of audit information	-
5.6.1.12	CR2.9A - Audit storage capacity - allocation	-
5.6.1.13	CR2.9RE(1) - Warn when audit record storage capacity threshold reached	-

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.6.1.14	CR2.11RE(2) - Protection of time source integrity	-
5.6.1.15	CR2.12RE(1) - Non-repudiation for all users	-
5.6.1.16	CR3.9RE(1) - Audit records on write-once media	-
5.6.1.17	CR6.1RE(1) - Programmatic access to audit logs	-

附錄 B
(參考)
門禁系統網路安全參考模型

門禁系統系列產品為滿足本系列標準之安全要求，當產品受限於市場定位或客製化要求之限制，以至於產品本身無法滿足安全要求時，藉由環境面的安全設置與部署以助於達到產品所需之安全能力，如圖 B1 與圖 B2 之參考模型作為建置門禁系統之參考。

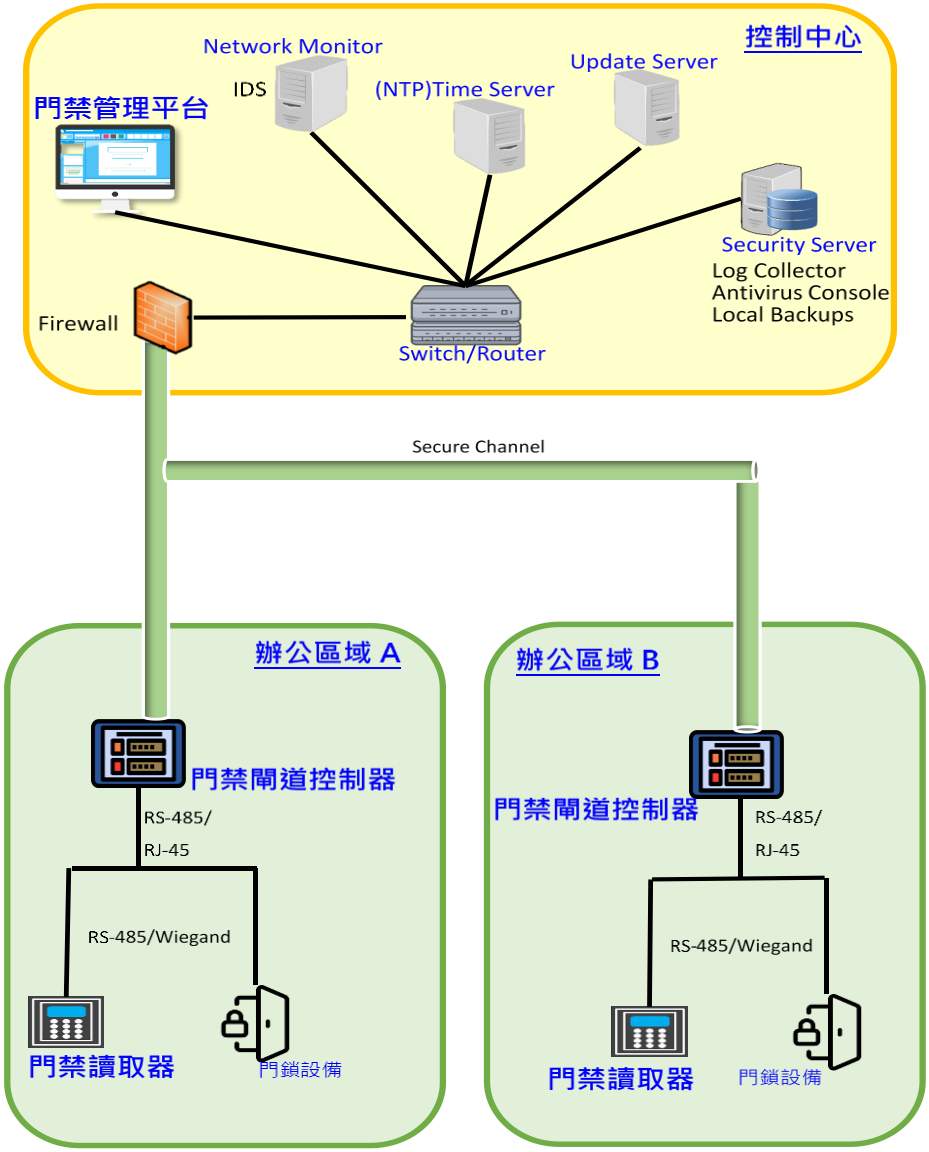

圖 B1 以相同建築內之企業門禁系統為例

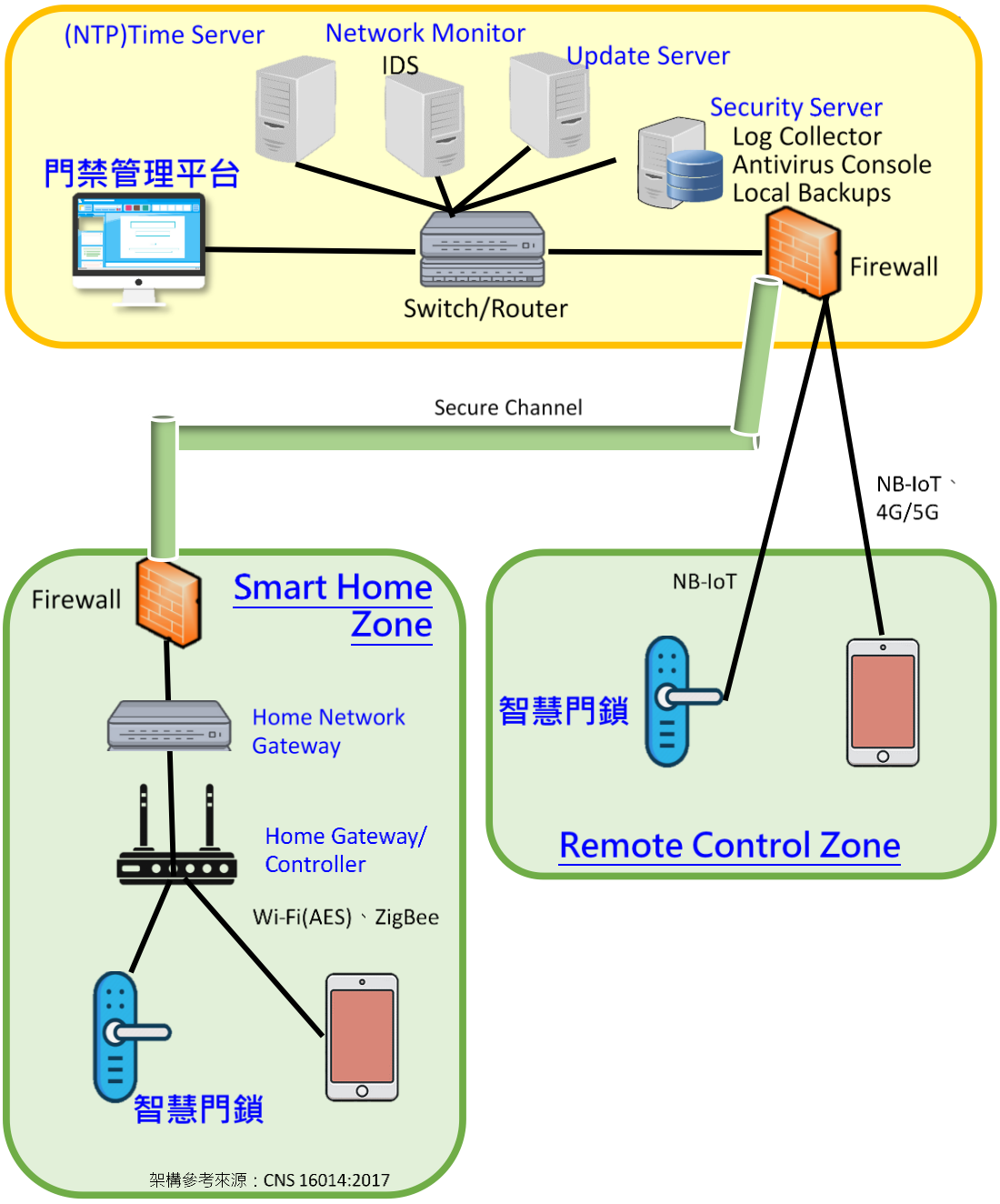

圖 B2 智慧門鎖參考模型

參考資料

(1) 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

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

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

(4) 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

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

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 27 日	修訂內容。