IoT-1006-2

門禁系統資安標準

-第二部：門禁管理平台

V2.0

行動應用資安聯盟

中華民國 112 年 11 月

目錄

引言

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裝置制定資安標準，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，本標準之適用範圍為門禁管理平台，門禁管理平台為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，與門禁系統中其他門禁產品連接，其應用包括但不限於收集來自管制出入口門禁讀取器之出入資料、傳送控制指令。

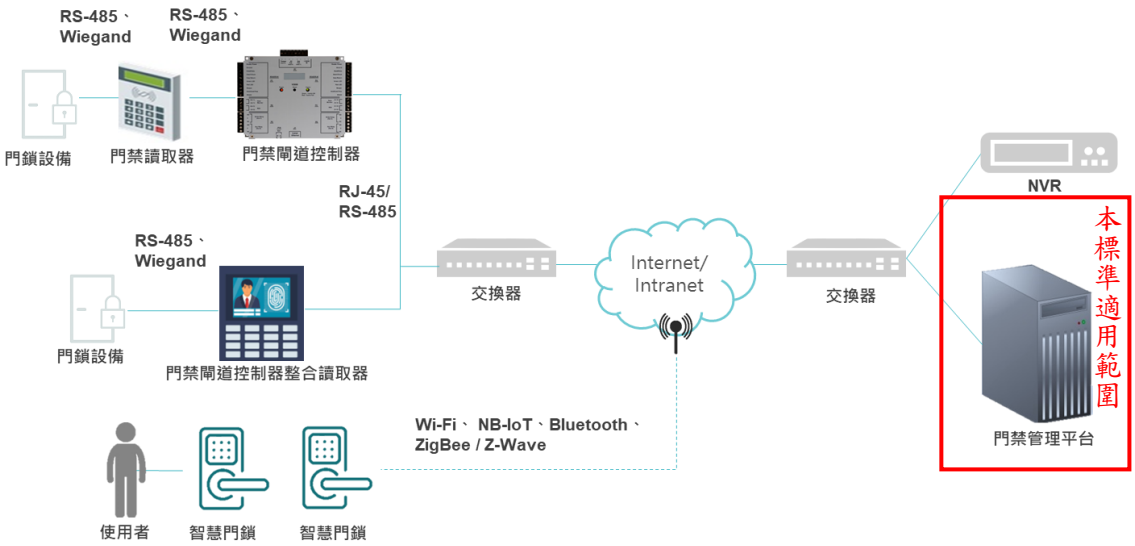

圖 1 門禁系統架構示意圖

按產品功能設計，產品適用標準說明：

- 產品為門禁管理平台，須依循 IoT-1006-1「門禁系統資安標準-第一部：一般要求」標準規範及本標準所載明之標準規範。

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] IoT-1006-1 v1.0	**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」所述及下列用語及定義適用於本標準。

3.1 降級模式(Degrade mode)

係產品發生故障時，產品為繼續提供必要功能運作而設計的操作模式。

3.2 使用者資料(User Data)

係指儲存於產品中的所有敏感性資料和使用者權限配置。

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、(6)警示與紀錄及(7)個人資料/隱私資料安全；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 5.7 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。(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	5.1.1.2 5.1.1.3 5.1.1.4 5.1.1.5 5.1.1.6	-	5.1.1.7
	5.1.2 權限控管	5.1.2.2 5.1.2.3 5.1.2.4 5.1.2.5	5.1.2.6 5.1.2.7	5.1.2.8 5.1.2.9 5.1.2.10 5.1.2.11
	5.1.3 通行碼鑑別	5.1.3.2 5.1.3.3 5.1.3.4 5.1.3.5	-	-

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	5.2.1.2	-	-
	5.2.2 安全管理程序	-	-	5.2.2.2
	5.2.3 已知漏洞安全	-	5.2.3.2	-
系統機密性	5.3.1 敏感性資料保護	-	-	-
資源可用性	5.4.1 作業系統與網路服務	5.4.1.2	5.4.1.3	-
	5.4.2 資源管理	-	-	-
更新安全	5.5.1 軟韌體更新	-	-	-
警示與紀錄	5.6.1 安全事件日誌檔與警示	-	-	-
個人資料/隱私資料安全	5.7.1 個人資料/隱私資料保護能力	5.7.1.1(O) 5.7.1.2 5.7.1.3 5.7.1.4(O) 5.7.1.5 5.7.1.6 5.7.1.7 5.7.1.8(O) 5.7.1.9 5.7.1.10(O) 5.7.1.11(O)	-	-

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。

(g) 個人資料/隱私資料：產品須具有個人隱私的保護機制。

4.1.2 安全要求分項：

IoT-1006-1 之第 4.1.2 節之規定適用於本標準。

4.1.3 安全等級：

IoT-1006-1 之第 4.1.3 節之規定適用於本標準。

5. 一般要求

門禁管理平台為滿足安全功能，門禁系統之門禁管理平台應依不同級別依循 IoT 1006-1 「門禁系統資安標準 第一部：一般要求」標準規範及本節所載明之標準規範。

5.1 身分鑑別、識別、授權安全

5.1.1 鑑別機制

5.1.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.1.1 節之要求。

5.1.1.2 產品應具備身分鑑別機制，變更產品安全相關設定之功能應執行身分認證，例如:設定時間、門禁權限、解除警示功能等，包括但不限於本地端管理介面、實體介面執行通行碼變更或權限角色變更。(1 級)

5.1.1.3 產品定期更新身分鑑別碼的功能應符合公認資安產業慣例，例如: NIST SP 800-63B。(1 級)

5.1.1.4 產品應支援管理所有使用者帳戶的功能，或將使用者帳戶整合到管理帳戶系統的能力。(1 級)

5.1.1.5 產品應提供依據使用者、角色、群組，及/或介面來管理識別碼之功能。(1 級)

5.1.1.6 產品之使用者登入介面應顯示安全警語，且該安全警語可更改。(1 級)

5.1.1.7 使用者存取產品時應採用多因子身分鑑別機制。(3 級)

5.1.2 權限控管

5.1.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.1.2 節之要求。

5.1.2.2 確保使用者存取所需之權限控管與廠商所宣告的一致，且廠商所宣告的權限控管機制宜滿足職責分離(Separation of duty)、應需所知(Need to know)和最小化特權(Minimization of privilege)的原則。(1 級)

5.1.2.3 當產品使用者介面閒置時，應提供自動會話鎖定(Session lock)或使用者手動啟動會話鎖定，以防止其他存取。(1 級)

5.1.2.4 當使用者與產品建立之會話鎖定(Session)，應提供解除鎖定機制。(1 級)

5.1.2.5 產品之應用程式不應存在超級使用者權限，以避免因應用程式被攻陷而導致整個系統權限被取得。(1 級)

5.1.2.6 確保軟體與裝置的執行所需之權限控管與廠商所宣告的一致，且廠商所宣告的權限控管機制宜滿足職責分離(Separation of duty)、應需所知(Need to know)和最小化特權(Minimization of privilege)的原則。(2 級)

5.1.2.7 當產品遠端指令介面網路連線閒置時，應具備遠端會話終止(Remote session termination)功能。(2 級)

5.1.2.8 產品應拒絕來自不受信任網路的存取，但取得管理者認可之連線不在此限。(3 級)

5.1.2.9 產品應具備可配置時間或事件次序(Sequence of events)的主管覆蓋(Supervisor manual override)功能，例如:所授予之使用者、授予權限的期限、授予操作的功能等。 (3 級)

5.1.2.10 若產品的功能對系統運作具嚴重影響時，產品功能之操作、修改應支援雙重確認(Dual approval)。(3 級)

5.1.2.11 產品的所有介面應提供限制建立會話(Session)數量的功能。(3 級)

5.1.3 通行碼鑑別

5.1.3.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.1.3 節之要求。

5.1.3.2 產品須提供更改使用者通行碼強度安全設定功能。(1 級)

5.1.3.3 產品之通行碼長度設定原則應至少 8 碼。(1 級)

5.1.3.4 產品之通行碼安全強度設定建議，應符合 NIST SP 800-63B[(1)]之規範。(1 級)

5.1.3.5 產品應有防止暴力破解通行碼之功能，且最高嘗試登入失敗次數及帳戶鎖定之時限應可設定，其帳戶鎖定時限內不應被存取或可由系統管理者解除鎖定。(1 級)

5.2 系統完整性

5.2.1 資料完整性

5.2.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.1 節之要求。

5.2.1.2 產品應提供防止惡意程式的保護措施。(1 級)

5.2.2 安全管理程序

5.2.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.2 節之要求。

5.2.2.2 產品應提供匯出安全設定的功能且其支援格式應為機器可讀取的格式。(3 級)

5.2.3 已知漏洞安全

5.2.3.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.3 節之要求。

5.2.3.2 產品應使用公認資安產業慣例之產品安全監控之功能，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 級)

5.3 系統機密性

5.3.1 敏感性資料保護

5.3.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.3.1 節之要求。

5.4 資源可用性

5.4.1 作業系統與網路服務

5.4.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.4.1 節之要求。

5.4.1.2 當產品遭遇 DoS 攻擊時，產品應能在降級模式(Degrade mode)下維持基本功能運作。(1 級)

5.4.1.3 產品應具備減緩受到訊息洪泛(Message flood)類型之 DoS 攻擊影響的能力。(2 級)

5.4.2 資源管理

5.4.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.4.2 節之要求。

5.5 更新安全

5.5.1 軟韌體更新

5.5.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.5.1 節之要求。

5.6 警示與紀錄

5.6.1 安全事件日誌檔與警示

5.6.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.6.1 節之要求。

5.7 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 產品之個人資料應加密傳輸，保護資料的加密方式應符合 5.3.1.1 項之要求。(1 級)(O)

5.7.1.2 產品之敏感性個人資料應加密傳輸，保護資料的加密方式須採用 5.3.1.1 之同等或以上之加密演算法。(1 級)

5.7.1.3 產品應提供使用者簡便的功能以刪除使用者資料(user data)，例如:使用者友善介面且操作步驟盡可能減少至必要的步驟。(1 級)

5.7.1.4 產品應提供使用者明確的刪除個人資料之操作方法說明，例如:產品使用手冊中說明刪除使用者資料的功能和方法。(1 級)(O)

5.7.1.5 廠商應具備對於收集、利用、處理使用者個人資料的管理機制，管理機制適用於包括但不限於產品開發商、系統整合商或第三方廠商。(1 級)

5.7.1.6 產品應具備使用者個人資料之使用授權機制，在收集、利用、處理使用者個人資料前應由經使用者同意。(1 級)

5.7.1.7 產品應提供使用者個人資料使用授權之撤銷機制。(1 級)

5.7.1.8 產品所收集之遙測數據若包含個人資料時，該個人資料之內容宜為廠商必要之所需，包括但不限於產品開發商、系統整合商或第三方廠商。(1 級)(O)

5.7.1.9 產品所收集之遙測數據，應提供說明遙測數據之種類、使用目的，遙測數據使用者包括但不限於產品開發商、系統整合商或第三方廠商。(1 級)

5.7.1.10 產品應提供使用者簡便的功能以刪除儲存於關聯服務中的個人資料。(1 級)(O)

5.7.1.11 產品所提供之刪除個人資料機制，從產品及其關聯服務完成刪除後應告知使用者刪除狀態。(1 級)(O)

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]
	CR1.2 – Software process and device identification and authentication	
5.1.1.2		5.5-5 - Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.
5.1.1.3	CR 1.5C - Authenticator management - change/refresh all authenticators periodically	5.1-4 - Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
5.1.1.4	CR1.3 - Account managemen	-
5.1.1.5	CR1.4 - Identifier management	-
5.1.1.6	CR 1.12 - System use notification	-
5.1.1.7	CR1.1RE(2) - Multifactor authentication for all interfaces	-
5.1.2.2	CR2.1 - Authorization enforcement	-
5.1.2.3	CR2.5A - Session lock - initiation	-
5.1.2.4	CR2.5B - Session lock - removal	-
5.1.2.5	-	-
5.1.2.6	CR2.1RE(1) - Authorization enforcement for all users	5.6-7 - Software should run with least necessary privileges, taking account of both security and functionality.
5.1.2.7	CR2.6 - Remote session termination	-
5.1.2.8	NDR1.13RE(1) - Explicit access request approval	-
5.1.2.9	CR2.1RE(3) - Supervisor override	-
5.1.2.10	CR2.1RE(4) - Dual approval	-
5.1.2.11	CR2.7 - Concurrent session control	-
5.1.3.2	CR1.7 - Strength of password-based authentication	-

本標準 要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
	CR1.2 – Software process and device identification and authentication	
5.1.3.3	-	-
5.1.3.4	-	-
5.1.3.5	CR1.11A - Unsuccessful login attempts - limit number	5.1-5 - When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.
	CR1.11B - Unsuccessful login attempts - response	
5.2.1.2	NDR3.2 - Protection from malicious code	-
5.2.2.2	CR7.6RE(1) - Machine-readable reporting of current security settings	-
5.2.3.2	CR6.2 - Continuous monitoring	-
5.4.1.2	CR 7.1 - Denial of service protection	-
5.4.1.3	CR7.1 RE(1) - Manage communication load from component	5.12-2(partial) - The manufacturer should provide users with guidance on how to securely set up their device.
		5.12-3(partial) - The manufacturer should provide users with guidance on how to check whether their device is securely set up.
5.7.1.1	-	5.8-1 - The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.
5.7.1.2	-	5.8-2 - The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.
5.7.1.3	-	5.11-1(partial) - The user shall be provided with functionality such that user data can be erased from the device in a simple manner.
5.7.1.4	-	5.11-3 - Users should be given clear instructions on how to delete their personal data.
5.7.1.5	-	6.1 - The manufacturer shall provide consumers with clear and transparent information about what personal data is

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
	CR1.2 – Software process and device identification and authentication	
		processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.
5.7.1.6	-	6.2 - Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.
5.7.1.7	-	6.3 - Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.
5.7.1.8	-	6.4 - If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.
5.7.1.9	-	6.5 - If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.
5.7.1.10	-	5.11-2 - The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.
5.7.1.11	-	5.11-4 - Users should be provided with clear confirmation that personal data has been deleted from services,devices and applications.

參考資料

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

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。