IoT-1006-6

門禁系統資安標準

-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 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。

本標準所定義之人臉辨識門禁裝置係指，裝設於管制門禁外，以偵測與擷取人類臉部特徵，以臉部特徵進行人員身分比對的門禁產品。在人臉辨識產品的檢測中，涉及了「人臉特徵識別」和「欺騙攻擊(Spoofing attack)」兩大類，其中「人臉特徵識別」區分為功能正確性驗證與辨識效能測試；而「欺騙攻擊」檢測則為活體偽冒檢測(Presentation attack detection)。本標準著重於門禁系統中人臉辨識裝置之資訊與網路安全，不包括人臉特徵識別之正確性、可靠性與辨識效能的能力。

為防範門禁系統上的資安威脅與欺騙攻擊，本系列標準在數位發展部數位產業署的支持下，基於國際工控資安標準 IEC 62443 及歐盟資安標準 ETSI EN 303 645 之資訊與網路安全要求，以及引用了我國個人資料保護法與 PAD 測試標準 ISO/IEC 30107-3，亦對產品的個人資料、人臉特徵資料的保護和人臉欺騙攻擊的防範程度之安全要求，而制定人臉辨識門禁裝置資安產業標準，以緩解人臉辨識門禁裝置可能遭遇的資安威脅並提升產品防護能力，人臉識別的功能正確性驗證與辨識效能測試不在本標準所規範之範圍。

1. 適用範圍

本標準之適用範圍為人臉辨識門禁裝置。

人臉辨識門禁裝置的組成包括以偵測與擷取人體臉部特徵，以臉部特徵進行人員身分比對之邊緣運算(本地端)人臉辨識門禁裝置；與人臉辨識須透過後端或雲端管理平台執行身分比對之非邊緣運算人臉辨識門禁裝置。

人臉辨識門禁裝置之架構，如下圖所示。

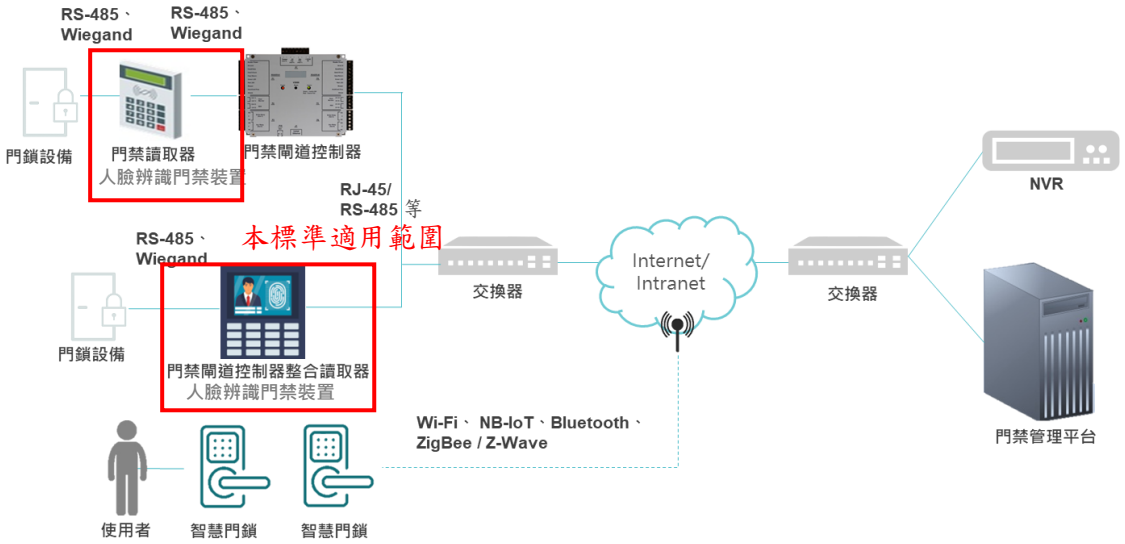

圖 1 人臉辨識門禁裝置架構示意圖

按產品功能設計，產品適用標準說明：

- 產品為邊緣運算類型之人臉辨識門禁裝置，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。
- 產品為非邊緣運算類型之人臉辨識門禁裝置，須依循 IoT 1006-1「門禁系統資安標準 第一部：一般要求」、IoT 1006-2「門禁系統資安標準 第二部：門禁管理平台」及本標準之標準規範。

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 人臉辨識門禁裝置(Face recognition access control device)

在門禁系統中組成產品之一，裝設於管制通道出入口，透過偵測與擷取人體臉部特徵，並以臉部特徵執行人員身分比對的關鍵設備。

3.2 活體偽冒(presentation attack, PA)

以偽造活體之生物特徵的偽冒攻擊，例如:複製或變造的指紋、面具、影片等人工製品，以干擾生物辨識系統執行判斷操作，冒充已授權之人員以達成身分驗證通過為目的之行為。

3.3 活體偽冒檢測(Presentation attack detection, PAD)

自動偵測活體偽冒的功能，對感測器所擷取的目標物之各項特徵進行測量與分析，以確認所擷取的目標物為真實存在的活體對象。

3.4 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。

3.5 人臉辨識資料(Face recognition data)

係指自人臉圖像或影像中提取可識別、可重複的特徵資料(值)，或是前述之特徵資料與其他資訊結合後以便自動識別自然人身分的資料。

3.6 一體成型(Integrated molding)

係指產品的外殼不是由零件組合而成，而是整體不分割地直接製成。

3.7 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和板手拆卸。

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、(6)警示與紀錄、(7)個人資料/隱私資料安全及(8)實體安全；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 5.8 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	5.1.1.2 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	-	-	-
	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	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
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

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：產品須確保服務可回復正常運作的能力。

(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：產品日誌紀錄須具有管理機制，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。

(h) 實體安全：產品輕易被拆解與否，或產品資料存儲與測試用連接埠的處置，應視為實體安全要求的標的。

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：

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，適用於一般行號、商店用產品，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，建議較無機敏資料之商辦的區域使用，如：商店、商辦、小型工作室。

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

人臉辨識門禁裝置為滿足安全功能，門禁系統之邊緣運算類型之人臉辨識門禁裝置產品應依不同級別依循 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。若產品為非邊緣運算類型之人臉辨識門禁裝置，須依循 IoT 1006-1「門禁系統資安標準 第一部：一般要求」、IoT 1006-2「門禁系統資安標準 第二部：門禁管理平台」及本節之標準規範。

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鑑別，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 產品應具備公認資安產業慣例之活體偽冒檢測(PAD)之初級防護等級，例如 FIDO Biometrics Requirements、ISO/IEC 30107 國際標準等普遍業界所接受的作法。(1 級)

5.1.1.4 產品應具備公認資安產業慣例之活體偽冒檢測(PAD)之進階防護等級，例如 FIDO Biometrics Requirements、ISO/IEC 30107 國際標準等普遍業界所接受的作法。(2 級)

5.1.1.5 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。

5.2 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。

5.2.2 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安全監控作法。(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。

5.3.1.2 產品應確保自身信任根所使用之金鑰及資料均符合其機密性、完整性及真實性。(2 級)

5.3.1.3 當產品使用 OSDP 通訊協定傳輸時，應符合 IEC 60839-11-5:2020 或 SIA OSDP v2.2 所要求之資安規格。(2 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。

5.4.2 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 產品之人臉辨識資料、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 產品應提供簡便的功能以刪除人臉辨識資料、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人臉辨識資料、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 產品應具備對於收集、利用、處理使用者人臉辨識資料、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 產品應具備使用者人臉辨識資料、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經使用者同意。(1 級)

5.7.1.7 產品應提供使用者人臉辨識資料、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人臉辨識資料、個人資料時，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，應提供遙測數據之種類、使用目的之說明，遙測數據之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 產品應提供簡便的功能以刪除儲存於關聯服務中的人臉辨識資料、個人資料。(1 級)(O)

5.7.1.11 產品所提供之刪除人臉辨識資料與個人資料機制，從產品及其關聯服務完成刪除後應告知刪除狀態。(1 級)(O)

5.7.1.12 產品不應收集、儲存未經當事人授權的人臉圖像。(1 級)

5.7.1.13 產品收集、利用、處理和儲存人臉辨識資料、人臉圖像應為系統運作必要之所需。(1 級)

5.7.1.14 產品應於完成鑑別或識別後立即刪除人臉圖像，若產品鑑別或識別所擷取的人臉圖像有收集、利用、儲存人臉圖像之必要時，應符合 5.7.1.13 之要求。(1 級)

5.7.1.15 人臉辨識資料應具備可更新、不可逆、不可連結之特性。(1 級)

備考：可更新：人臉辨識資料遭洩露時，可重新產生相異之人臉辨識資料。

不可逆：無法從人臉辨識資料回復到人臉圖像。

不可連結：同一張人臉圖像產生的相異之人臉辨識資料間，不具有關聯性；且在產品應符合 CNS 29100-2 之去識別化鑑別要求事項。

5.7.1.16 產品同時支援本地端與遠端人臉辨識方式時，應採用在本地端進行人臉辨識。(1 級)

5.7.1.17 產品之人臉辨識資料、個人資料不應進行委外處理；若產品需要將人臉辨識資料、個人資料委外處理時，應對委外處理行為進行風險評估，並審核受委託者是否對前述之風險具備風險管理的能力。(1 級)

5.7.1.18 產品對於人臉辨識資料、個人資料的安全管理機制，應依個人資料保護法施行細則第 12 條之規定，若人臉辨識資料、個人資料發生竊取、洩漏或竄改等侵害時，應依個人資料保護法第 12 條規定告知當事人。(1 級)

5.7.1.19 產品收集或產生的人臉辨識資料、個人資料應在其國境內儲存。(1 級)

5.8 實體安全

5.8.1 實體入侵防護

5.8.1.1 產品於啟動階段應確保韌體、軟體及組態資料的完整性。(1 級)

5.8.1.2 產品外部不應有徒手(無須特殊工具)即可還原通行碼預設值的功能。(1 級)

5.8.1.3 產品預設應無法透過實體介面存取產品作業系統之除錯模式。若需經實體介面存取，則應通過身分鑑別作業始得執行。(2 級)

5.8.1.4 產品應採用一體成形或防拆螺絲等機殼防拆除保護，及具備防拆偵測設計。(2 級)

5.8.1.5 產品於啟動階段應確保韌體、軟體及組態資料的真實性。(2 級)

5.8.1.6 產品當偵測到除錯介面之存取行為時，應產生安全事件日誌。(3 級)

5.8.1.7 產品偵測到實體遭未經授權存取時，應向使用者及管理者發出警示且應產生安全事件日誌。(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	對應標準規範	
要求事項	IEC 62443-4-2[1]	ETSI EN 303 645[2]
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	-	-
5.1.1.4	-	-
5.1.1.5	CR1.1RE(2) - Multifactor authentication for all interfaces	-
5.2.2.2	CR7.6RE(1) - Machine-readable reporting of current security settings	-
5.2.3.2	CR6.2 - Continuous monitoring	-
5.3.1.2	NDR3.12 - Provisioning product supplier roots of trust NDR3.13A - provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust NDR3.13B - support the capability to provision without reliance on components that may be outside of the device’s security zone.	5.4-1(partial) - Sensitive security parameters in persistent storage shall be stored securely by the device.
5.3.1.3	-	-
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.

本標準	對應標準規範	
要求事項	IEC 62443-4-2[1]	ETSI EN 303 645[2]
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.
5.7.1.4	-	6.1 - The manufacturer shall provide consumers with clear and transparent information about what personal data is 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.
5.7.1.5	-	6.2 - Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.
5.7.1.6	-	6.3 - Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.
5.7.1.7	-	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.
5.7.1.8	-	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.
5.7.1.12	-	-
5.7.1.13	-	-
5.7.1.14	-	-

本標準	對應標準規範	
要求事項	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.7.1.15	-	-
5.7.1.16	-	-
5.7.1.17	-	-
5.7.1.18	-	-
5.7.1.19	-	-
5.8.1.1	NDR3.14 - Integrity of the boot process	-
5.8.1.2	-	-
5.8.1.3	NDR 2.13 - Use of physical diagnostic and test interfaces	5.6-4 - Where a debug interface is physically accessible, it shall be disabled in software.
5.8.1.4	NDR3.11 - Physical tamper resistance and detection	-
5.8.1.5	NDR3.14 RE(1) - Authenticity of the boot process	5.7-1 - The consumer IoT device should verify its software using secure boot mechanisms.
5.8.1.6	NDR2.13RE(1) - Use of physical diagnostic and test interfaces -Active monitoring	-
5.8.1.7	NDR3.11RE(1) - Communication authentication	-

參考資料

(1) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, https://csrc.nist.gov/projects/cryptographicmodule-validation-program

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

(3) ISO/IEC 19989-3:2020 Information Security-Criteria and methodology for security evaluation of biometric systems -Part 3: Presentation attack detection, https://www.iso.org/standard/73721.html

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

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

版本修改紀錄

版本	時間	摘要
V2.0	112 年 11 月 27 日	內容修訂。