

# FIDO2 安全金鑰

## AuthTron Security Key



FIDO2 強認證  
(FIDO2 & U2F)



企業一站式導入  
(Turnkey solution)



客製密碼引擎功能



金鑰管理介面

# 81% 的駭客入侵，來自密碼問題

為何應該汰換掉密碼框架

- 是導致資料外洩的關鍵破口
- 企業不易管理

為了建立信任機制，並且確保在違規或意外發生時可究責，企業與政府單位制定了許多繁雜的程序。數位化讓狀況更糟，因為數位資料非肉眼可見，我們不知道惡意內容是否藏在一般檔案，因此我們透過帳號密碼、簡訊、安全政策和其他方法來確認「身分」。驗證是必要的，但當我們要開始管理和記住愈來愈多帳號密碼，同時又面對更先進的網路及釣魚攻擊的威脅，提升密碼強度就如老鼠跑滾輪一般無濟於事。根據 Verison 2017 年的報告 (Verizon Data Breach Investigations Report, 2017)，有 81% 的駭客入侵是來自於密碼產生的漏洞。即使密碼强度高，「管理密碼」本身就成了問題，因此必須跳脫既有框架，才能兼顧安全性與易用性。

## 信任根基 (Root-of-Trust) 的典範轉移

從「密碼」到「密碼學」

當密碼已經開始危及我們的生產力和安全性時，典範已經轉移到以公鑰密碼學為核心的信任根基。我們不再相信密碼，而是相信密碼學 (cryptography)。我們將信任奠基於「存在於安全晶片內的私鑰」。

匯智安全科技於 2021 年正式加入 FIDO (Fast Identity Online) 聯盟，為 FIDO Japan 與 FIDO Taiwan 組織成員。我們和國內知名雲端服務廠商合作，協助企業和政府導入 FIDO 認證框架，從雲端到設備端打造強認證生態系，抵擋釣魚網站和身分偽造的威脅。



## WiSECURE AuthTron™——企業一站式導入

AuthTron™ 如何解決問題

- 朝向企業導入設計
- 實現無密碼與多因素認證
- 可客製化多種密碼功能

匯智安全的 AuthTron™ 是通過 U2F 與 FIDO2 L2 認證的安全金鑰 (security key)，支援無密碼及多因素認證。AuthTron™ 提供企業等級的發行管理及使用管理機制，透過一站式 (turnkey) 雲到點解決方案，包含 RP server、FIDO server 與硬體安全模組 (hardware security module, HSM)，滿足企業對於監理、安全維運以及設備授權管控的需求。Google 早期便是實施此措施，解決企業內部資料洩漏及非法存取的問題。此外，我們還提供 AuthTron™ 客製化服務，能依照使用情境實現認證以外的功能，如資料加密、交易簽章、區塊鏈應用等。



您也可以用 AuthTron™ 登入 (包含但不限於) 如 Microsoft、Google、Amazon、Dropbox 等網站。



## 產品規格

支援應用	<ul style="list-style-type: none"><li>· FIDO2 Authenticator</li><li>· Hardware Cryptographic Module</li></ul>
金鑰管理功能	<ul style="list-style-type: none"><li>· Multiple Application Key Domains (Up to 8 applications / Up to 128 keys per application)</li><li>· Support ECC (NIST P-256, P-384, P-521, Brainpool 512 ), RSA (2048) keys</li></ul>
認證服務	<ul style="list-style-type: none"><li>· Security policy for limited password attempts (FIDO only)</li><li>· Touch pattern for user presence (FIDO only)</li></ul>
密碼演算法與功能	<ul style="list-style-type: none"><li>· ECDSA / ECMQV / EdDSA / RSA</li><li>· ECDH / ECIES</li><li>· HMAC-SHA2 / HMAC-SHA3</li><li>· SHA2 / SHA3 (Host Software Library)</li><li>· Key Wrapping and Unwrapping</li><li>· PBKDF</li><li>· Random Number Generation<ul style="list-style-type: none"><li>– DRBG with TRNG as seed</li></ul></li></ul>
API	<ul style="list-style-type: none"><li>· PKCS#11</li><li>· Native API</li></ul>
傳輸介面	<ul style="list-style-type: none"><li>· USB 2.0</li></ul>
安規認證	<ul style="list-style-type: none"><li>· FIDO2 level 1, level 2 and U2F level 1</li><li>· CC EAL5+ certified security chip</li><li>· CE</li><li>· FCC</li><li>· RoHS</li></ul>

# 為什麼選擇 WiSECURE FIDO2 解決方案？



## 周邊產品組合完整

我們提供產品導入與顧問服務，協助客戶釐清應用情境的風險，並具備雲端、手機端密碼模組，能依需求組建最佳性價比之方案



## 密碼實作與 ODM 服務

我們從底層密碼實作到硬體開發一手包辦，除了打造自有產品，也有能力提供 ODM 服務，打造客戶專屬安全金鑰 (security key)



## 認知行為認證

我們使用獨家的「認知型身分驗證」(cognition-based user presence)，使用者不需提供生物特徵，卻能達同等安全識別效果

## FIDO2 強認證產品組合，實現高強度資料安全

匯智安全以密碼學為核心，致力於保障客戶寶貴資料的可用性與安全。我們透過同樣經過 FIDO2 認證、內嵌輕量加密引擎的 CryptoAir® 產品，與 AuthTron® 整合打造 FileAegis® 檔案安全儲存作業平台，透過該方案，您可以：

### 相信自己的資料被妥善保護

不論是內部攻擊、外部攻擊或人為疏失，本地資料都已經被加密保護

### 相信公司員工的資料存取被妥善控管

FIDO2 安全金鑰可以阻止未經授權的訪問並強制紀錄操作稽核日誌，此外還可客製簽章功能確保資料真實性

### 相信客戶的資料被妥善存放

這能幫助您避免洩漏客戶的資料與後續的鉅額罰款

FileAegis 保護靜態資料 (data at rest) 與傳輸中資料 (data in transit) 免於惡意軟體、中間人攻擊及未經授權的訪問，提供完善密鑰機制，加密過程不需傳輸金鑰。而 FIDO2 認證框架在本解決方案中可強制執行「最低權限管理」和「紀錄稽核日誌」，落實公司資料管控政策。

想更瞭解我們的解決方案或 FIDO2 其他應用可能，歡迎與我們聯繫：

<https://www.wisecure-tech.com/contact/>

+886-2-29343166