無密碼 FIDO 落實「零信任」資安

■文：任芷萍


照片人物：數位發展部部長唐鳳

疫後生活、消費習慣急遽數位化，卻也讓網路詐騙有機可乘，日前由數位發展部 (簡稱：數發部) 數位產業署主辦的《2023 網路信賴基礎環境應用導入論壇》對於無密碼數位環境有深入探討。數位發展部部長唐鳳開場致詞：數位信任等同於數位韌性，密碼容易成為詐騙標的，惟有「FIDO」(Fast IDentity Online) 這種快速認證身分的機制才能建置真正的「零信任」(Zero Trust) 資安——包含生物特徵、設備裝置與連線行為是三道「防盜門」。數位發展部亦於今年 1 月加入國際身分辨識標準組織 FIDO 聯盟，目前台灣分會已有 27 個會員。

數位信任、數據隱私、網路安全，建構可信賴網路環境

數位發展部去年成立之初即率先採用 TWFidO (中華民國行動自然人憑證) 用來登錄內部網站、系統簽公文等，內政部今年 8 內亦修正通過「內政部行動自然人憑證系統介接申請要點」，擬將 TWFidO 系統的服務對象從原本電信、醫療等行業，擴大至行動自然人憑證系統、到適用個人資料保護法的機關或非公務機關。TWFidO 不只簽章、認證身分功能，它跟卡式的自然人憑證一樣，還有加、解密功能，惟現階段還在測試中；之後紙本公文可利用 TWFidO 進行端到端加密實現數位化，公務活動也可不必限於特定地點進行。

工研院資訊與通訊研究所副所長黃維中表示，可信賴的網路環境由數位信任、數據隱私與網路安全三者構成安全機制——數位信任是網路信賴的核心，又可概分為數位身分識別 (身份證明、驗證) 和簽章兩大塊；數據隱私保護著重於遮罩及去識別化；網路安全藉由軟體、防火牆、滲透測試等達陣。密碼技術存在已久，但它其實很脆弱：運算加速及人工智慧 (AI) 進步，讓它越來越容易遭到破解；而隨著網路釣魚活動的智慧化、組織化、平台化、服務化，厲害到可自動化破解雙因子認證 (2FA) 及 OTP (一次性動態密碼)，更為金融業帶來大規模災情。


照片人物：工研院資訊與通訊研究所副所長黃維中

「追本溯源，問題出在共享密碼的身分驗證機制，讓存放共享秘密的主機成為攻擊目標，驗證過程容易遭到中間人攔截和釣魚

攻擊——FIDO 就是為此而生」，黃維中說。他解釋，FIDO 是一種安全便利的身分識別機制，結合終端比對生物特徵，提升使用的便利性，且生物特徵、密鑰皆存放於裝置安全儲存模組，保障隱私與安全性；主機僅用來存放公鑰，能降低成為攻擊目標的風險，且使用非對稱式密碼技術，可完全防止中間人和釣魚攻擊。更重要的是，FIDO 是唯一符合美國 (SP 800-63) 與歐盟 (eIDAS) 國家之政府與產業「高」等級身分證之產業標準！


照片人物：Mercari 資安長 (CISO) 市原尚久 (Naohisa Ichihara)

FIDO Passkeys 可抵擋「釣魚攻擊」

黃維中說明，FIDO 除了符合國際規範 ISO 29115:2003 四個身分驗證與識別等級 (Level 1 ～ 4)，還同時覆蓋美國 NIST SP 800-63 (2017)、Revision 4 (2023) 明訂三個身分驗證等級、三個身分確認等級及三個身分聯邦等級 (皆分為：低、中、高三等)，簽章法規則有 ESIGN/UETA、NIST FIPS 186-5；而歐盟 eIDAS (2015) 有低／中／高，三個身分驗證及識別等級，eIDAS2 (2023) 則是簽章／進階／合格三個簽章等級。但他特別提醒：採用 FIDO 不見得就符合 NIST SP 800-63 或 eIDAS 規範！技術符合與取得認證是兩回事。

在 2019 年推出智能手機支付服務 Merpay 的 C2C 市集日本廠商 Mercari，就曾身受密碼所苦：容易被遺忘、破解、攻擊或洩露，且會被某些服務拒絕，因而決定採用生物驗證、密碼管理、簡訊 OTP 等多因子驗證 (MFA)。資安長 (CISO) 市原尚 (Naohisa Ichihara) 剖析，雖說 MFA 可強化使用者認證，但有些 MFA 用例仍透露不夠堅固的訊息，只有能「抵擋釣魚攻擊」(phishing-resistant) 的 FIDO 金鑰 (Passkeys) 是最佳解，並預言未來十年將快速成長——這是因為大約在 2020 年 FIDO 處於快速擴張期，FIDO2 與 WebAuthn 也開始擴散。

市原尚久指出，FIDO 發展大致可分為三個階段來看：2013 年由 UAF/U2F 帶頭、2019 年由 FIDO2/WebAuthn 啓動、2022 年後將由金鑰展開第三階段的成長。他並提到帳號恢復議題：當使用者購買新手機、或是設備遺失／被偷／損壞時，若要恢復程序，需輔以額外的 ID 驗證、認證及提示程序才行；此時，不良的使用者介面恐成大問題，甚至無法抵擋釣魚攻擊。FIDO 密鑰配對可作為多裝置憑證 (Credential)——可在不同裝置或瀏覽器之間同步運作，並經由谷歌 (Google) Password Manager 和蘋果 (Apple) iCloud Keychain 管理，冀可解決帳號恢復爭議。

防堵時下駭客，ZTA 才是根本解決之道！

露天市集技術處協理陳贊元陳述，以往資安防護只靠三招克敵制勝：政策、演練、稽核。首先是建立全方位的資訊安全管理，確保企業和客戶的數據安全；然後定期進行資安演練，包括漏洞評估、滲透測試、DDoS 模擬和紅隊演練，以增強資安意識和檢驗防護能力；最後進行資安稽核，評估現有資安措施的效果，以及潛在威脅。然而，要防堵時下駭客非法行動，傳統作為顯然已不足以應對，惟有零信任架構 (ZTA) 才是根本解決之道！事實上，OTP 簡訊發送即是 ZTA 入門手段之一，優點是立即見效且使用者體驗一致。


照片人物：露天市集技術處協理陳贊元

不過，OTP 有三大缺點：1. 使用量越大，費用越高，成本是變動的、不易控制預算；2. 仰賴電信產業，在控管上效果有限；3. 使用者購物流程會被打擾或中斷，影響消費體驗。陳贊元認為，未來資安防護有兩大走向：一是設置專責安全操作中心 (SOC)，不僅可強化入侵偵測，還能提供數位鑑識記錄留存；二是持續迭代 ZTA，不斷提升安全技術和保護措施，以保障企業和客戶的龐大資料安全。因此，「FIDO2 ＋ Passkeys」的組合拳，將是大勢所趨，擁有以下好處：

■使用體驗優，登入過程更簡便；
■無密碼傳輸，改採公私鑰驗證；
■成本合理，且趨近於固定成本；
■政策支持，數發部大力推動導入。

每年處理交易金額達新台幣 900 億元的藍新科技，對上述觀點亦表認同。藍新科技產品規劃處處長林承勳分享，他們確實觀察到電商客戶有加強身分識別的需求，但對於導入 FIDO 常遭遇「3 門檻＋1 難關」：

■導入的進入門檻：不認識 FIDO，無法想像導入價值，FIDO 註冊前的身分核驗難以選擇強驗證或弱驗證，缺少可依循的作業指引、擔憂導入後無所適從；
■應用的技術門檻：對身分識別服務信賴者 (RP) 與身分識別服務提供者 (IDP) 之間的技術實作不熟悉，對 RP FIDO 伺服器的建置、維護與管理沒有經驗，對 FIDO 與現行身分識別技術的分工、導入應用或服務方式欠缺完整想法；
■驗證的成本門檻：投入成本是最關鍵要素，導入 FIDO 的效益是否夠高是權衡重點，擔心 FIDO 發展的不確定性造成成本難估算，於是，「繼續觀望」便成了安全選項。

FIDO 應用擴至一般大眾的日常生活

「支付服務亦存在驗證難關」，林承勳說。這是因為第三方支付業者缺乏合適的驗證工具，且信用卡驗證支援 FIDO 仍在發展中，加上身分識別在電商用戶端和支付端整合不易所造成。所幸，基於以下理由仍看到改變契機：1. 政府積極推廣 FIDO 並建立相關作業指引；2. 以 TW FIDO 為典範，突破 FIDO 註冊前的驗證門檻；3. 透過服務規模化降低技術與成本門檻；4. 主管機關願意協助支付業者爭取驗證工具。在會中最後座談階段，主持人無店面零售商業同業公會秘書長許生忠引言：「登入」是駭客竊取數據最常借道的破口。

文化部資訊處處長莊舜清接棒：有鑑於 80% 資料外洩都是肇因於弱密碼設置，幾經思量，導入 FIDO 是最好選擇。甫經修正的「內政部行動自然人憑證系統介接申請要點」已將該系統的服務對象擴大至適用個人資料保護法之公務機關或非公務機關，並以行動自然人憑證作為網路中之身分識、數位簽章及加解密用途，一般民眾只要手機


照片人物：藍新科技產品規劃處處長林承勳

下載應用程式 (APP)、連線至系統平台完成認證後，這支手機就能成為身分憑證。藍新科技副總經理李偉琪就第三方支付業者立場提到，如何借助 FIDO 為買、賣雙方打造「防詐」的交易環境是值得深思的議題。

FIDO 聯盟台灣分會會長暨神盾公司副總經理張心玲介紹，FIDO 聯盟成立於 2013 年，迄今全球有逾 300 個會員、認證產品 (FIDO Certified Products) 已突破千項。FIDO 是很好的生態系，組成非常多元，參與其中有助於了解諸多國際標準並與國際龍頭廠商結緣；據 Yahoo! Japan 統計，導入 FIDO 後可降低 25% 的客服成本、使顧客上線購物時間增加 2.6 倍，而使用 FIDO 上線的消費者更高達 74% ！露天市集技術處協理陳贊元總結，做資安就像在買保險，做得越多、風控就越周全；惟考慮到並非所有裝置都支援 FIDO，採用分段實施將是較理想方式。