基於生物辨識之強安全認證應用技術實用性研究

陳世仁*、藍紹緯、范雋彥
資訊工業策進會 資安科技研究所
sjchen@iii.org.tw、davidlan@iii.org.tw、ericfan@iii.org.tw

摘要

2020 年將有超過 500 億台設備存取智慧聯網服務，平均每人擁有 6 部以上設備，然而>80% IoT 設備密碼強度及複雜度不足，並且>70%的設備傳輸未加密並可輕易取得帳號資訊，顯示傳統身分認證機制已不足以應付新興的 IoT 應用。由 FIDO 標準聯盟推動新一代認證標準，將身分驗證由機密共享(What you know, What you have)轉成透過生物特徵方式驗證(What you are)，帶動了生物辨識市場蓬勃成長，預估於 2024 年將達到 149 億美元，並廣泛應用於金融、健康醫療、智慧家庭甚至企業安控等領域。因應此一趨勢，本文提出一基於生物辨識之強安全認證應用技術架構，並透過相關場域實證，探究生物辨識技術之實用性及成熟度，供後續應用領域導入此一技術之參考。

關鍵詞：FIDO、生物辨識、強安全認證、智慧聯網

Implementation practices of strong security authentication based on biometrics mechanism

Shih-Jen Chen[1*], Shao-Wei Lan[2], Chuan-Yen Fan[3]
Institute for Information Industry, CyberTrust Technology Institute
sjchen@iii.org.tw、davidlan@iii.org.tw、ericfan@iii.org.tw

Abstract

There will be more than 50 billion connected devices in 2020, It means each one person will have average of more than 6 devices. However, more than 80% of IoT devices using weakness password and more than 70% of devices transfer unencrypted data which could disclosure account information easily. It shows that traditional identity authentication mechanisms are not sufficient for huge IoT applications. Therefore the FIDO(Fast IDentity Online) Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The new authentication standards based on

* 通訊作者 (Corresponding author.)

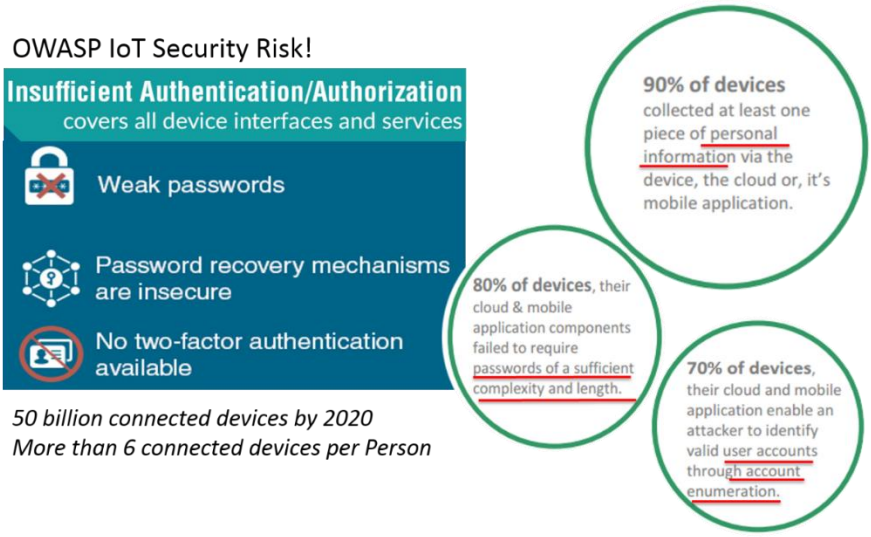
biometric will widely used in finance, health care, smart home and enterprise management. That drives the biometric market grows fast and will reach 14.9 billion in 2024. In this paper, we proposed our implementation of a strong security authentication architecture based on FIDO standards. It has been deploy into IoT application field such as health care and mobile payment to show the adaptability and technology readiness of FIDO.

Keywords: FIDO, biometric authentication, IoT

壹、前言

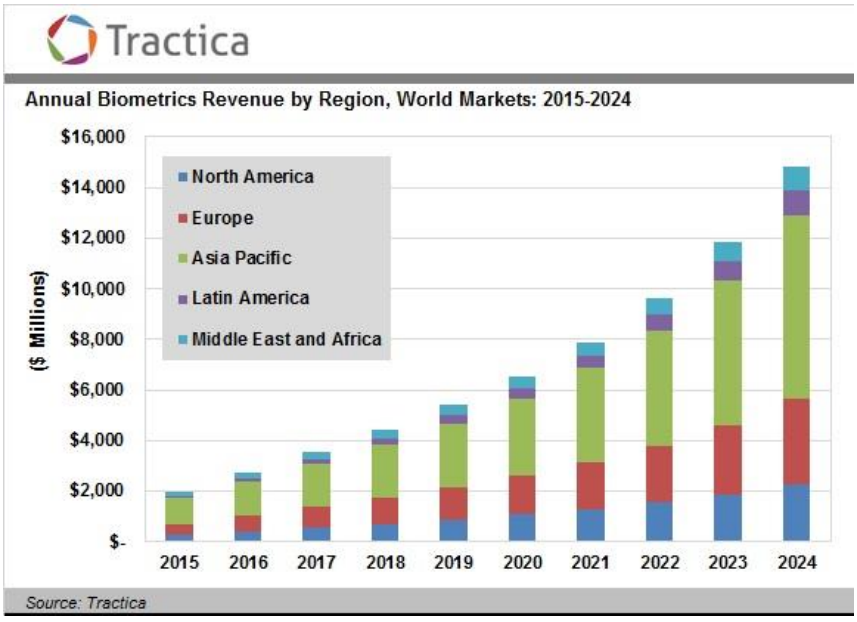
根據 HP 公司 2015 年 IoT 研究報告[2]指出，2020 年將有超過 500 億台設備存取智慧聯網服務，平均每人擁有 6 部以上設備，而>90%的設備會收集使用者個人資訊。因此如何確保 IoT 應用之身分認證授權已成為智慧聯網最關鍵資安課題，然而超過 80% IoT 設備所使用的密碼強度及複雜度不足，甚至 70%以上的設備使用未加密方式傳輸資料，並可輕易取得帳號資訊，都顯示傳統身分管控機制已不足以應付智慧聯網應用需求。整體而言，過去普遍使用的帳號密碼機制存在下列資安問題及挑戰:

- **Forgetful**: 為降低帳號密碼被猜測及盜用，多數應用服務導入強制性複雜密碼原則，如要求大小寫字母、數字及特殊符號組成一定長度並要求前數次已使用之密碼不可重複使用，使得使用者在記憶密碼上形成困擾。
- **Phished**: 即便在強制性複雜密碼原則保護下，使用者仍容易遭受釣魚攻擊(Phishing Attack)如詐欺 E-mail、詐騙電話等而使得帳號密碼被竊取。
- **Key logged**: 雖然部分應用服務已透過加密及 One Time Password(OTP)服務或圖形碼確認等機制強化安全認證，但透過設備端監聽、中間人攻擊(Man in the Middle, MITM)、自動重播 OTP 簡訊，自動辨識圖形碼等等駭客手法還是能取得使用者帳號密碼。
- **Reused**:一般使用為了記憶方便，多數習慣用同一組帳號密碼在多個應用服務平台使用，因此一旦密碼被盜，往往造成所有應用服務都被竊取。



圖一： 智慧聯網資安威脅關鍵因素

身分管控技術隨著科技發展，已由過去機密共享(What you know, What you have)轉成透過生物特徵方式驗證(What you are)，依據 Tractica 市場研究報告[1]指出，生物辨識市場因應智慧聯網需求蓬勃成長，預估於 2024 年將達到 149 億美元，並廣泛應用於金融、健康醫療、智慧家庭甚至企業安控等領域。



圖二：生物辨識市場規模預估

智慧聯網應用如行動金融、車聯網、智慧家庭、健康醫療等，其資安認證存取管控需求及缺口包含:

- **多樣化用戶端設備技術缺口:**
  - 輕量化設備 CPU 運算能力有限，加解密運算負擔高
  - 輸入介面受大小限制，高複雜度密碼輸入困難

- 連網機制以 Internet 為主，OTP/AOTP 等簡訊使用功能受限

• **IoT 行動雲端應用服務技術缺口：**

- 實名制興起，使用者真實身分驗證需求迫切
- 服務建構於多樣設備，D2D 身分驗證/授權標準興起，亟待投入相關技術研發
- IoT 帶動跨領域應用蓬勃發展，跨服務之身分識別轉換技術亟待發展

貳、物辨識產業之現況與發展

生物辨識(Biometric)，是指運用人體身上的特徵來做為識別的密碼，因此在技術的開發上必須選擇準確度高及容易使用的辨識特徵以利使用，其可區分為生理特徵（如臉形、指紋、虹膜）及行為特徵（如聲音、簽名、密碼），以準確度來說，「生理特徵」在唯一性及安全性上明顯優於「行為特徵」。由於不同的生物特徵具差異性，在作為生物辨識上就有不同的優劣勢，整體技術比較如表一，眼球虹膜之辨識方式的專一性最高，但是由於使用上必須以紅外線掃描眼球，在價格及安全性的考慮下，並不容易發展成大眾化的產品，相對的市場占有率也無法迅速拓展。臉部辨識因面積較大，加上特徵點也更多樣、複雜，因此技術難度相對較高，且由於臉部辨識系統容易受到臉部飾品與周圍的光線的影響，相對的精確性便不如其他的辨識系統。而指紋辨識技術使用上較為方便，同時體積小可以附加在現有的資訊設備上，因此指紋辨識技術目前已是生物辨識中接受度最高的技術類別。

表一：生物辨識技術比較

	指紋	臉形	手形	虹膜	語音	靜脈	DNA	步姿
獨特性 (Uniqueness)	高	低	中	高	低	高	高	低
永久性 (Permanence)	高	中	中	高	低	高	高	低
便利性 (Collectability)	高	高	高	中	高	中	低	高
接受度 (Acceptability)	高	高	高	中/低	高	高	低	低
辨識效能 (Performance)	中/高	低/中	中	高	低	中	低	中
技術成熟度 (Maturity)	高	中	中	中/高	中	中	低	中/低

1. 獨特性：所提供的特徵是必須可以與他人分別
2. 永久性：特徵不會隨著時間改變
3. 便利性：特徵是否容易採集
4. 接受度：辨識特徵擷取的安全性
5. 辨識效能：該特徵辨識各種效能的評估
6. 技術成熟度：使用生物辨識技術的應用產品功能成熟度

在 2013 年 9 月，Apple 推出搭載指紋辨識晶片的 iPhone 5s 後，後續 iPhone 型號皆延續此功能，受益於 Apple 公司在 iPhone 整合指紋辨識作為安全防護的措施開始，指紋辨識受到普遍重視，除了 Apple 以外，諸如 Samsung、Sony、華為及 HTC 等國際大廠競相推出搭載指紋辨識功能的智慧型手機。指紋辨識的採樣技術一般以光學及電容式為主。光學技術利用高感光率的電荷耦合元件（CCD）攝取指紋樣本，其品質雖受肯定，但是成本相對昂貴，另外體積較大，較不適用於輕薄的行動裝置。電容式則利用晶片與手指接觸時所感應到電容變化，再利用先進的演算法來找出特徵，加以比對。主要優點是利用晶片感應，解析度高，體積小，適用於以手機為主的應用裝置。

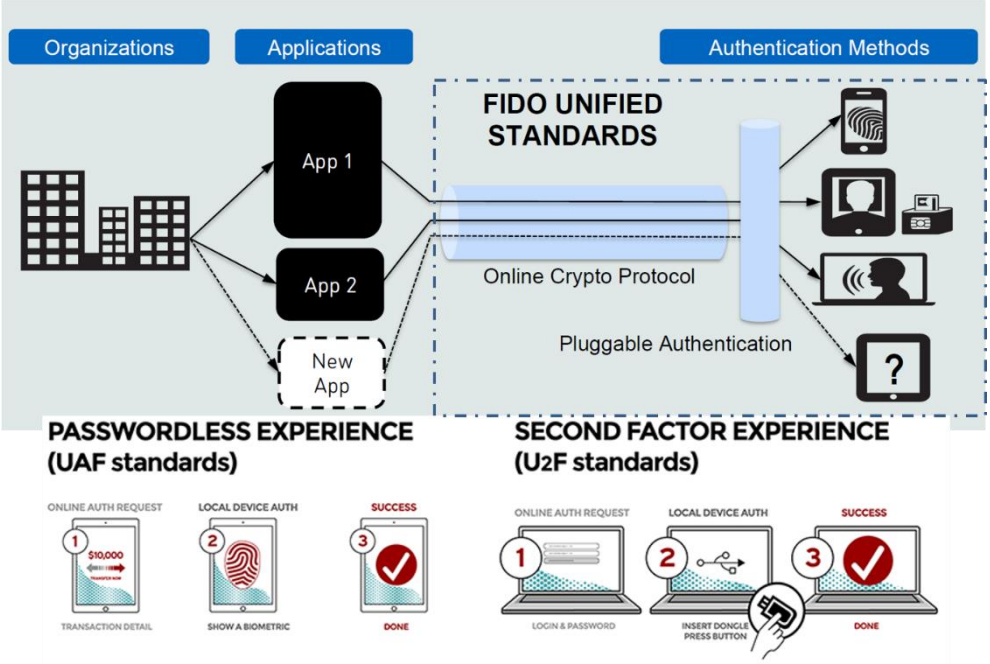
由於無線網路使用環境已日益成熟，未來透過手機作為金融支付或是第三方支付的行動支付方案勢必成為電子商務重要的發展趨勢，而手機搭配指紋辨識的應用，可以兼顧行動支付需要的簡易、便利、安全等特性。因應此一趨勢，指紋辨識儼然成為金融銀行支付平台在驗證使用者的關鍵技術，其導入支付應用之發展里程如下圖:

圖三：指紋辨識切入金融支付之發展里程

參、FIDO 身分認證協定

3.1 FIDO 聯盟及協定概述

有鑑於行動身分認證需求迫切，2012 年由 Google、MasterCard、PayPal 等公司成立 Fast Identification Online (FIDO) 聯盟，透過制定具備 open、scalable、interoperable 特性之新一代認證技術規範減少使用者及應用服務對密碼的依賴，並結合生物辨識等技術以驗證用戶身分。FIDO 主要標準包含完全透過生物辨識技術或其他認證之免密碼認證標準 Universal Authentication Factor (UAF)[3]及降低密碼依賴及強化安全性的雙因子認證標準 Universal Second Factor (U2F)][4]，整體運作機制如下圖：

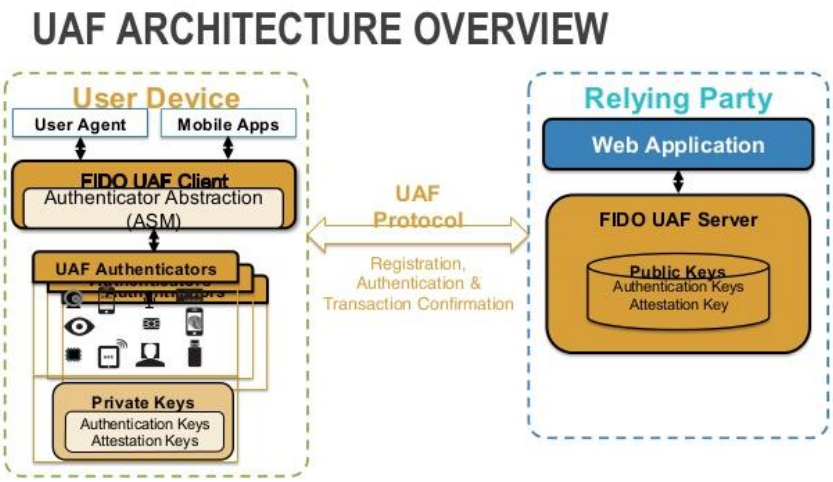


圖四: FIDO 協定運作架構

雖然 FIDO 已制定了 UAF 及 U2F 開放標準，然而對智慧聯網營運商而言，如何將已商轉之服務透過技術介接 FIDO 強化認證機制，並不在標準定義中，而這部份包含因應不同應用認證需求，所需發展的 Relying Party 平台及 Federation 身份識別整合管控技術等等，仍待系統整合商與應用服務商協力推動。

3.2 UAF 運作原理

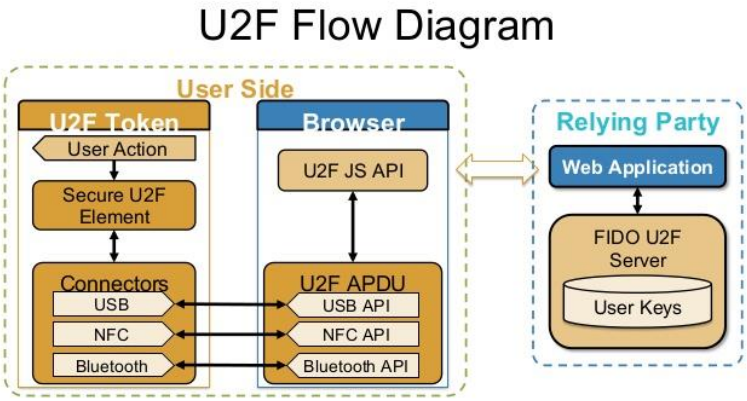
UAF 協定主要針對行動應用發展，適用於具備安全元件及生物辨識晶片之智慧型使用者終端設備如智慧手機、平板、智慧手環等裝置。在用戶端架構分成三層:UAF 認證器層(Authenticator)、UAF 用戶端(Client)及行動應用軟體(Mobile App)。同時為了使生物辨識晶片商能有一致性標準提供 UAF 用戶端介面調用，FIDO 聯盟也定義了認證器抽象介面標準(ASM: Authenticator-specific Module)。在伺服端則包含提供服務(Relying Party)的 Web 應用程式(Web Application)及 UAF 伺服器。當使用者需認證時，會透過行動應用軟體觸發底下的 UAF 用戶端，由它呼叫底層的認證器，認證器包含生物辨識感應器及安全元件，會取樣使用者生物特徵，並透過演算法產生相配對的安全公私鑰(Public-Private Key)，並以此作為驗證使用者依據與 UAF 伺服器溝通，驗證使用者生物特徵所綁定的身分之合法性。其架構如下圖所示:



圖五: FIDO UAF 運作架構

3.2 U2F 運作原理

U2F 協定主要針對個人電腦或筆記型電腦搭配雲端應用發展，透過插入一個具備生物辨識功能的硬體 U2F Token(如 USB Dongle、智慧卡等)於瀏覽器上以生物辨識當第二認證因子(2nd Factor)，降低使用者對密碼的依賴並提高認證安全性。U2F 在用戶端架構分成兩層:UAF Token 驗證器及架構於瀏覽器上的 U2F 用戶端 API。在伺服端則包含提供服務(Relying Party)的 Web 應用程式(Web Application)及 U2F 伺服器。當使用者需認證時，透過瀏覽器觸發以 USB、藍芽或 NFC 連接的 U2F Token，使用者於該認證器上感測其生物特徵，並由其中的安全元件透過演算法產生相配對的安全公私鑰(Public-Private Key)，並以此作為驗證使用者依據與 U2F 伺服器溝通，驗證使用者生物特徵所綁定的身分之合法性。其架構如下圖所示:

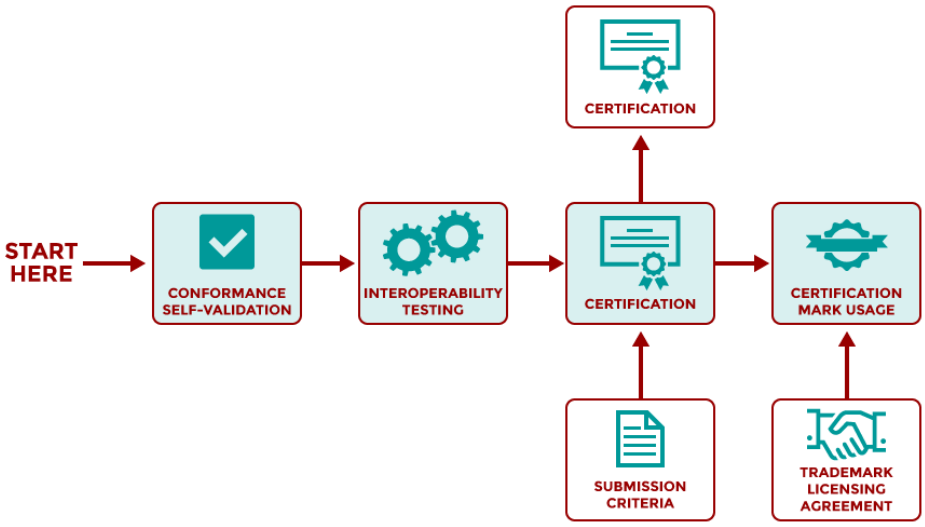


圖六: FIDO U2F 運作架構

3.3 FIDO Certified 標準驗證

隨著 2014 年 12 月 FIDO 聯盟正式推出 FIDO 1.0 標準，使得許多應用及電信商紛紛跟隨並推出免密碼之應用服務，同時為使共通標準能讓不同設備、應用互通，FIDO 聯

盟也推動 FIDO Certified 技術認證[9]，透過此一技術認證驗證不同設備商所推動的認證服務符合 FIDO 標準並支援互通性。其驗證流程如下:



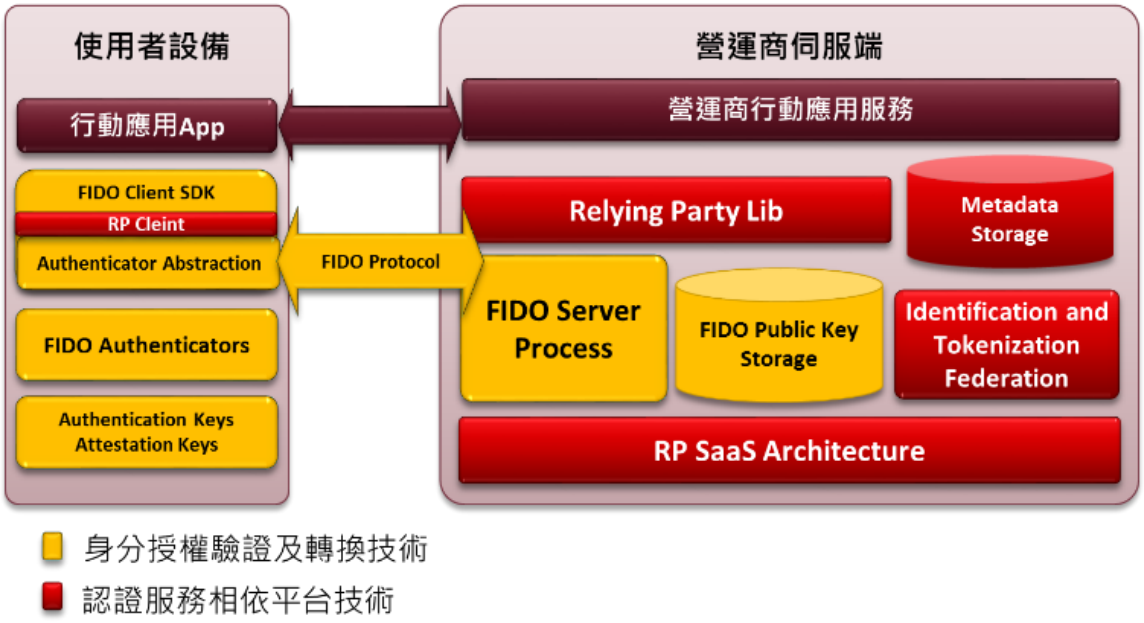
圖七： FIDO Certified 技術認證流程

整體技術認證依產品技術類別區分，目前將技術分為 UAF Client、UAF Server、UAF Authenticator、U2F Authenticator 及 U2F Server 等五大類別，每一種類別測試包含兩部分，一致性自我驗證測試(Conformance Self-Validation)及互通性測試(Interoperability testing)，一致性自我驗證測試可線上遠端存取測試工具進行自主性測試，而互通性測試由聯盟主辦，須先通過 Conformance Self-Validation，於特定指定日期進行異質性產品交互性測試，目前聯盟表定 90 天舉辦一次。截至 2016 年 11 月為止，全球共 57 家廠商產品或技術通過 FIDO 伺服器端 Certified 技術認證。

肆、可行性實作方法

基於前述 FIDO 開放標準，實作研發一套 On Demand Mobile Authentication (ODMA)行動認證服務平台系統，以驗證 FIDO 及生物辨識之實用性及成熟度。使用者可透過行動終端設備如 iPhone/iPad(iOS)、Android 手機或是筆記型電腦作身分登入，而登入的方式可利用手機上或是 USB Dongle 上的生物辨識晶片進行 FIDO UAF/U2F 認證，並依 UAF 或 U2F 協定與平台端的 FIDO 認證伺服器溝通，完成身份認證程序後再將該使用者所能存取的會員及相關資訊透過跨身分識別(Identification Federation)技術轉成不同應用服務所使用的身分識別標準，如 OpenID、OAuth、SAML 或支付服務的 Payment Network 權狀(Tokenization)，同時也將整合現行應用服務已有的多因子身分認證如 OTP、Tokenization 等技術，達到輕量化、易整合，單一存取的應用情境。

基於上述功能架構，本研究技術包含身份授權認驗證及轉換技術及認證服務相依平台技術兩大部分，整體技術架構如下:



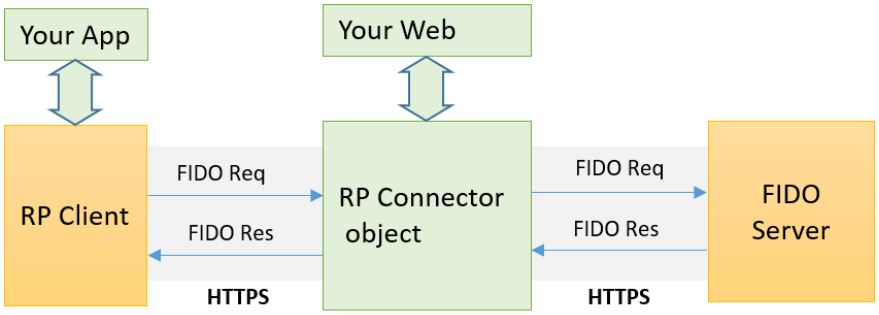
圖八： ODMA 技術架構

4.1 身份授權認驗證及轉換技術

透過服務身份資訊轉換技術(Identification Federation)將由生物辨識所認證之使用者身份，由 FIDO 開放標準資訊對應成應用服務所使用的身份碼及授權權狀(Token)，使得多樣化設備可透過生物辨識認證及 FIDO 標準存取由平台業者所提供的多種應用服務，包含身份認證、支付授權，資訊查詢授權等等。同時透過此一轉換技術亦可介接其他開放式身份認證標準如 OAuth、OpenID、SAML 等應用服務之身份授權，實現單一技術串接整個身份認證應用之目標。

4.2 認證服務相依平台技術

透過認證服務相依平台(Relying Party SaaS Platform)技術與電信業者或支付業者系統介接，提供註冊、認證、授權及管控需求，並透過雲端平台架構保證大量使用者要求之服務交易及擴充性，其運作方式包含建置於營運商服務端的透通模式及獨立雲端服務轉換的 Tokenization Service 模式。以智慧聯網應用場域為例，透過伺服端 RP Connector 可以併入智慧聯網服務商原本服務，並負責與 FIDO Server 溝通，智慧聯網服務不需了解 FIDO 協定，僅需處理進行註冊、認證或註銷等過程中所需記錄的相關資訊，其溝通架構如下:



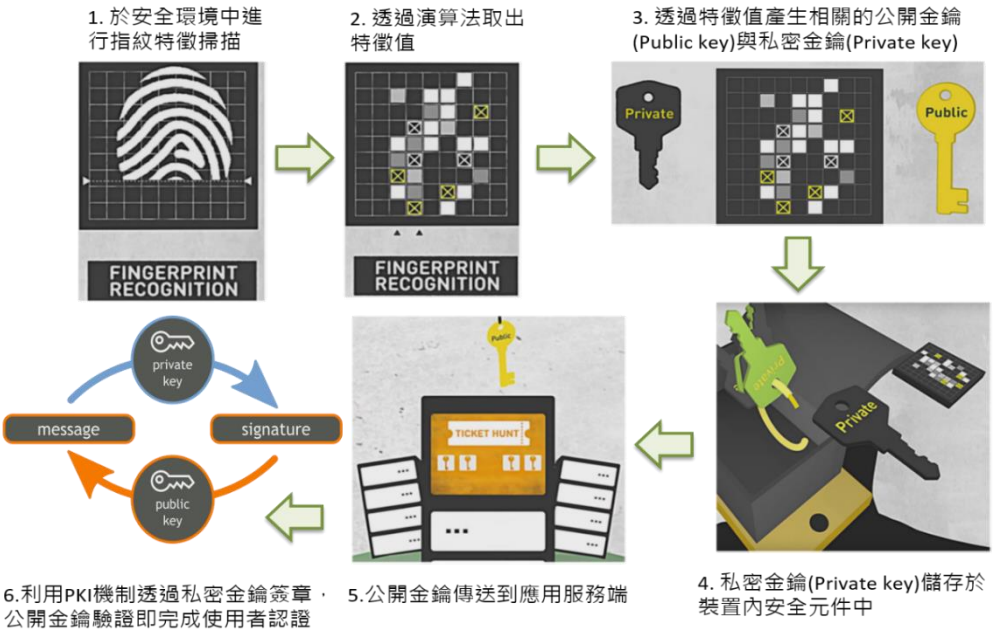
圖九: 智慧聯網服務串接整合架構

在 RP Connector 元件中，服務商可記錄使用者註冊、登入、授權、交易等等動作，並藉此提供服務商掌握使用者行為軌跡。更進一步的來說，服務商可以在過程中實施服務所擬訂的存取政策，透過串接來決定使用者當下的動作是否符合其身分在服務中的授權，並應用於不同的智慧聯網領域。

4.3 強安全認證技術原理

FIDO 所制定的認證機制中，其運作原理是基於兩大條件:1.裝置本身必須具備安全運算環境、2.生物特徵僅由裝置上安全環境運算，且不透過網路傳輸。以智慧手機為例，目前 GP 組織制定了「可信賴執行環境（ Trusted Execution Environment ，簡稱 TEE）」規格[6]。為了建構安全的執行環境，TEE 須有獨立硬體做為安全的作業系統、程式、使用介面、資料儲存空間之使用。除此之外，在 TEE 上運行的軟體稱為可信賴應用程式（Trusted Application， 簡稱 TA），須經授權才可安裝在 TEE 中執行， 而不是在行動裝置的作業系統上運作。因此， TEE 需要晶片廠商與行動裝置廠商配合，方能達成目標。

隨著 iPhone 整合指紋辨識 Touch ID 發展安全認證及 Apple Pay 應用，智慧手機紛紛搭載指紋辨識功能，雖然 Apple 於 iOS 9 開放了 Touch ID API[7]，Google 也在 Android M 上提供 FingerPrint Manager [5]相關 API 供應用軟體開發人員使用，然而這些 API 主要是利用裝置本身已建立的指紋特徵在本地端檢驗(Local Authentication)，並未達到與服務端的認證結合。而 FIDO 所定義的認證為利用驗證器 FIDO Authenticator 所取得的生物特徵產生一對公開\私密金鑰，利用 PKI 原理[8]進行使用者認證。目前 FIDO 所制定的驗證器包含指紋、虹膜、聲紋及安全晶片卡上的 PIN Code 等機制。為達成線上認證需求，FIDO 制定了 6 個步驟來驗證使用者的安全性，當認證時使用者先由安全環境中掃描其特徵，並透過演算法取樣出特徵值，再藉由此特徵值產生相關的公開金鑰(Public Key)及私密金鑰(Private Key)。當使用者註冊所需認證的應用服務時，裝置會將該公開金鑰及使用者相關資訊送到伺服端，因此在後續認證過程中，使用者再次掃描其生物特徵，裝置便可找出其匹配的私密金鑰運算出認證簽章，將此簽章送給應用服務端，再由應用服務端透過註冊的公開金鑰驗證使用者身分，完成整個強安全認證流程。其運作方式如下圖:



圖十: FIDO 強安全認證技術流程

伍、結論

本研究基於 FIDO 身分驗證標準，實作 ODMA 認證服務平台，並透過企業內網安控、金融支付等實證場域驗證 FIDO 強認證服務的成熟度及市場接受度，以金融支付為例，目前支援生物辨識(指紋)的智慧手機搭載率約 40%，主要以具備 Touch ID 的 iPhone 手機及支援 Android M 系統的智慧手機為主。在應用成熟度部分，短期市場仍需整合其他驗證機制如 OTP、PIN 碼等讓所有使用者都能用同樣的認證機制登入服務。而技術門檻在於跨系統整合，包含身分識別跨服務整合及多因子認證整合等。根據相關國際市場研究報告指出，2015 年運用行動生物辨識之交易認證超過 1.2 億次，預估 2020 年運用行動生物辨識之支付交易將超過 160 億次，適合應用在行動及金融服務之生物辨識科技，包括虹膜辨識、視網膜辨識、臉部辨識、指紋辨識、聲音辨識及行為辨識等。整體而言，生物辨識在金融市場應用商機包含下列三個面向:

- **結合安全元件的生物特徵驗證成為終端設備內建安全系統：**

以生物辨識科技進行身份認證，雖然安全性和易用性遠高於密碼系統，惟若以軟體技術實作，基於軟體模組的脆弱及以遭駭客攻擊/侵入的特性，尚不足以達到銀行業要求的安全等級（EAL4+）。尤其生物特徵的不可變性，無法像傳統密碼系統可重置，會讓危險程度更高。因此，必須以無法讀取/修改（tamper resistant）的硬體元件或晶片加強其安全等級，以符合銀行的安控基準。

- **國際標準強化互通性並保障傳輸及加密安全強度:**

在密碼系統已經無法滿足在智慧聯網的安全需求的前提下，龐大的消費族群，會各

自選擇多種各不相同的身份辨識裝置與方式，連結繁雜多樣的網路服務，其所形成的交叉連結關係，其複雜程度將難以相信，若要為這些交叉連結分別建立身份認證機制，所需成本更是難以估量。因此，FIDO 所推動的全球性開放標準將可望大幅削減在 IoT 個應用領域中對身分認證協議的開發、部署成本與時間。

- **生物特徵綁定代用碼機制大幅降低交易過程風險:**

鑑於駭客、惡意木馬技術的無孔不入，為確保網路交易的安全性與不可否認性，我們要保護的對象是使用者/管理者的身份（Identity）及授權範圍。FIDO 要求在安全元件內，儲存/核對使用者/管理者的生物特徵，若能與一次性代用碼機制搭配，當使用者完成身份認證後，同時在安全元件內產生對應代用碼，依此進行後續的授權操作，可確保各項操作行為都是在被認證與授權的條件下進行，將可大幅降低行動金融交易風險。

隨著生物辨識技術發展，「個人資料保護法」已將特徵、指紋列為個人資料，並訂定相關蒐集、處理及利用等規範。內政部「個人生物特徵識別資料蒐集管理及運用辦法」，也規定以電腦或其他科技設備，擷取個人專屬性而足以辨識個別身分之指紋及臉部特徵資料。而銀行公會所訂之「金融機構辦理電子銀行業務安全控管作業基準」，已將雙因素認證機制納入，可採用 3 項技術中任 2 項，包括客戶與銀行所約定的資訊、客戶所持有的設備、客戶所擁有的生物特徵。由上述可預見，未來使用生物辨識作為應用認證機制之趨勢將指日可待，而 FIDO 聯盟所推動的新一代認證協定可解決不同裝置上強安全認證的需求，然而透過本研究實證，在實際運用上仍須針對不同智慧聯網服務的串接，提供跨服務轉換及特徵關聯管理等機制，讓每個使用者身份（Identity）可因應不同服務的要求轉成不同的令牌（tokenization）處理，包含 OpenID、SAML 等身分識別格式。透過這種機制，把使用者的身分藉由生物特徵隱藏，並將真實的個人身份，轉換成一次性使用的虛擬身份（virtual Identity），在不可信的網路環境中使用，才能避免中間人攻擊及駭客竊取，完整確保交易與個人隱私的安全。

參考文獻

[1] Biometrics Market Forecasts: Global Unit Shipments and Revenue by Biometric Modality, Technology, Use Case, Industry Segment, and World Region - 2015-2024, *Tractica*, 2015/06

[2] Ericsson Mobility Report – on the pulse of the network society, *Ericsson* , 2015/06

[3] FIDO Alliance Universal Authentication Framework (UAF) specs, *FIDO Alliance*, 2014, https://fidoalliance.org/specifications/download/

[4] FIDO Alliance Universal 2nd Factor (U2F) specs, *FIDO Alliance*, 2014, https://fidoalliance.org/ specifications/download/

[5] Finger Print Manager Specification, *Android Develops*, https://developer.android.com/hardware/fingerprint/FingerprintManager.html

[6] GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide, *Global Platform*, http://www.globalplatform.org/mediaguidetee.asp

[7] iOS Security White Paper, *Apple Inc.*, https://www.apple.com/business/docs/iOS_Security_Guide.pdf
[8] Public Key Infrastructure, *MSDN*, 2015/03.
[9] The FIDO Certification program, *FIDO Alliance*, https://fidoalliance.org/certification/