實 務

行動自然人憑證應用於公文及檔案管理資訊系統之實驗性研究

An Experimental Research on Applying Taiwan Fast IDentity Online to the Electronic Documents and Records Management System

徐綉茹 Hsu, Hsiu-Ju
國家發展委員會檔案管理局文書檔案資訊組高級分析師
Senior Systems Analyst, Archives Information Division, National Archives Administration, National Development Council

胡治民 Hu, Chih-Ming
國家發展委員會檔案管理局文書檔案資訊組分析師
Systems Analyst, Archives Information Division, National Archives Administration, National Development Council

李秉澤 Li, Ben-Zor
國家發展委員會檔案管理局文書檔案資訊組分析師
Systems Analyst, Archives Information Division, National Archives Administration, National Development Council

江偉良 Chiang, Wei-Liang
國家發展委員會檔案管理局文書檔案資訊組助理設計師
Assistant Systems Designer, Archives Information Division, National Archives Administration, National Development Council

壹、前言

近年因嚴重特殊傳染性肺炎影響，政府機關及民間企業紛紛採取遠距辦公措施，疫後該工作型態亦將漸成常態，本文透過瞭解我國公文及檔案管理資訊系統（以下簡稱文檔系統）導入內政部行動自然人憑證 (Taiwan Fast IDentity Online, TW FidO) 之效益及可行性，盼能為機關施行遠距辦公覓得更佳出路，使機關建置文檔系統線上簽核功能得與實務作業緊密結合，並提供國家發展委員會檔案管理局（以下簡稱檔案局）改善文書及檔案管理資訊化相關制度參考。

經本文技術實作結果顯示，導入 TW FidO 應用模式於線上簽核作業確實可行，且符合電子簽章法要求及數位簽章之不可否認性，藉由導入 TW FidO 可大幅提升政府機關遠距辦公之線上簽核應用效益。

貳、技術簡介

行政院研究發展考核委員會（現國家發展委員會）於 2010 年開始推廣行政院及所屬各機關實施公文線上簽核作業，從公文製作、管理及簽核全程採電子化處理，期能帶動各機關改造辦公

作業流程，提升行政效率，並確保辦公同仁可於網路環境中，採用身分識別措施安全傳送資料。內政部核發之自然人憑證作為公文線上簽核之安全認證機制，可鑑別身分並配合應用電子憑證數位簽章加密技術，確保電子公文之真實性、完整性及滿足法律信證需要。

內政部於 2019 年鑒於行動裝置越來越普及，且使用自然人憑證還須使用讀卡機讀取實體卡片，爰以國際標準 Fast IDentity Online（FIDO）結合行動裝置的生物特徵辨識功能，推出 TW FidO 行動身分識別服務，並續於 2022 年在原本已具備身分驗證的基礎上加入電子簽章功能，使 TW FidO 服務應用更為多元。以文檔系統為例，現行使用者以自然人憑證簽核公文時，須以讀卡機讀取實體憑證卡，並輸入密碼後才能簽核線上公文，如文檔系統導入 TW FidO 技術，則透過行動裝置的生物特徵辨識，便可不須再使用實體憑證卡簽核線上公文，讓辦公型態的改變更具彈性。以下將介紹公文線上簽核技術、檢測公文線上簽核產出電子檔案之電子封裝檔工具箱及 TW FidO 技術。

一、公文線上簽核技術

公文線上簽核是在紙本公文管理的基礎上，整合電子簽章、憑證加密、電子公文製作及公文流程控管等技術，使公文傳遞更加迅速。然而，傳統紙本公文可透過蓋章或簽名辨識文件簽核者，進而確認文件之真實性，但線上簽核公文因電子文件之簽章或簽名很容易被複製偽造，便須以數位簽章作為驗證身分的鑑別技術。

憑證作為特定身分的證明，係運用非對稱加密機制進行數位簽章（digital signature）。所謂非對稱是指加密與解密分別利用不同私鑰（private key）與公鑰（public key）。當傳送電子文件時，其內容會先經雜湊（hash）演算法轉成一定長度雜湊值，再以傳送者憑證之私鑰對該雜湊值加密形成數位簽章，並連同原本的電子文件傳送給接收者；當接收者收到電子文件及其數位簽章後，會使用相同的雜湊演算法將電子文件轉成雜湊值，並使用憑證頒發機構發布在網路上用以配對的傳送者公鑰，對數位簽章解密取得雜湊值，經比對後若結果相符即證明該訊息源自某特定人員且電子文件未被竄改，滿足數位簽章之完整性（integrity）及不可否認性（non-repudiation）需求（如圖 1）。

公文線上簽核即以上述原理，利用訊息摘要函數（message digest function）將準備加密的公文（包括公文及其附件）製成訊息摘要（message digest），再以簽核者之憑證私鑰加密。由於使

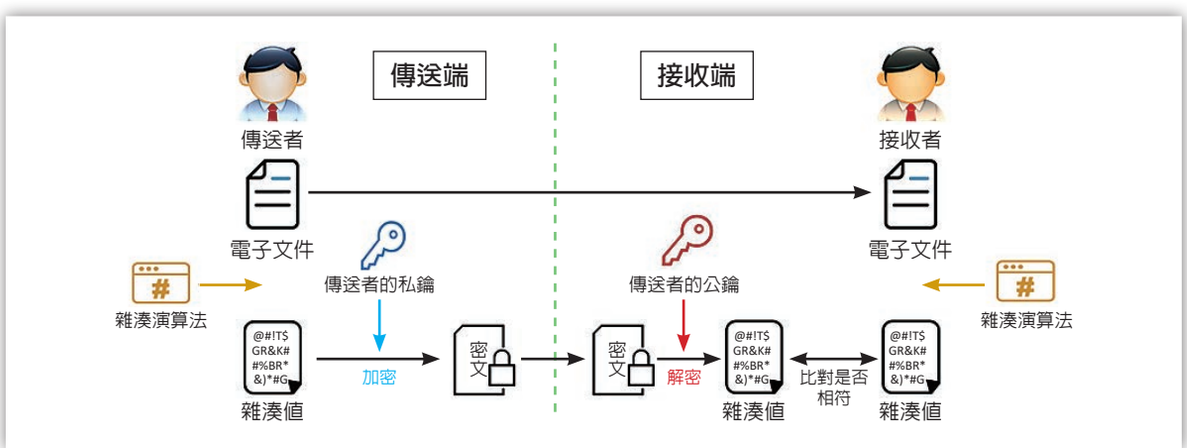

圖 1　數位簽章加密過程

資料來源：作者整理

用非對稱金鑰進行加、解密較耗時，尤其當傳輸訊息容量越大，時間將更冗長，故先製成訊息摘要可節省處理時間。將透過憑證私鑰加密的訊息摘要寫入簽核電子檔（sign instance, SI）後，下一個公文流程可利用各簽核點的公鑰，反向推算其訊息摘要，再與實際文件算得訊息摘要比較，如無差異即可確認各簽核點真實性；反之，如該簽核點的公鑰無法算出訊息摘要，或算出的訊息摘要與實際文件不同，便可推定該文件不是從該簽核點簽發的原始文件（如圖 2）。

二、電子封裝檔工具箱

依文書及檔案管理電腦化作業規範（以下簡稱文檔規範）第 18 點規定，完成線上簽核之電子檔案，應於點收時確認簽核電子檔載明資訊無誤後，附加機關憑證電子簽章，並以簽核電子檔產生電子檔案封裝檔。為檢測文檔系統導入 TW FidO 技術的電子檔案封裝檔是否符合文檔規範，本文使用檔案局電子檔案保存實驗室委外開發的「電子封裝檔工具箱」單機版軟體，檢測每個簽核點憑證簽署時間、憑證效期、外部檔案雜湊值

圖 2　SI 檔範例

資料來源：作者整理

及比對驗章，以驗證其真實性（authenticity）及完整性（integrity）。

電子封裝檔工具箱可指定檢測單筆封裝檔或批次檢測特定資料夾下所有封裝檔，檢測項目包含封裝檔格式、外部檔案格式與雜湊值、憑證等，並可產出檢測報表（如圖 3）。

三、TW FidO 憑證技術

TW FidO 係依循國際標準 FIDO 提供使用者無密碼驗證服務，其是同名國際組織「FIDO 聯盟（FIDO Allience）」制定的網路識別標準。傳統帳戶登入是藉由使用者輸入帳號及密碼比對伺服器端驗證資料進行身分識別（identification）與身分驗證（verification）才允許登入，代表只需要知道帳號及密碼，即使不是本人也能夠通過驗證，而 FIDO 則是透過公開金鑰加密（public key cryptography）進行多重要素驗證（multi-factor authentication, MFA）及生物辨識登入以嚴密保護資料安全（如圖 4）。

內政部自 2019 年起規劃試辦 TW FidO 行動

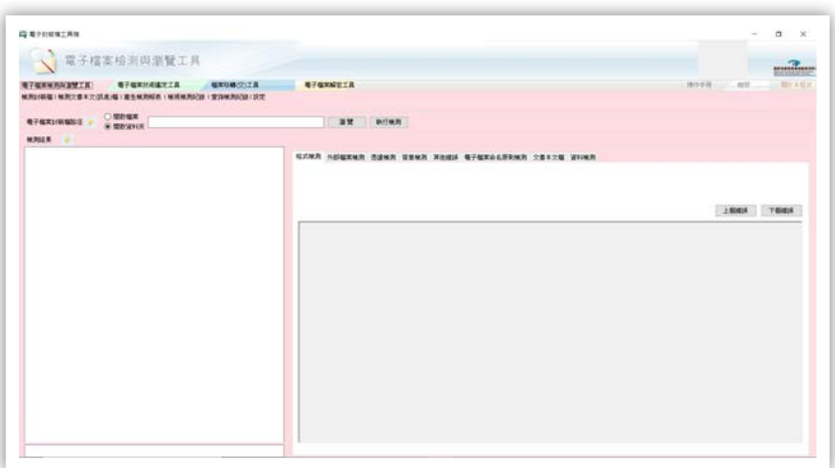

圖 3　電子封裝檔工具箱

資料來源：作者整理

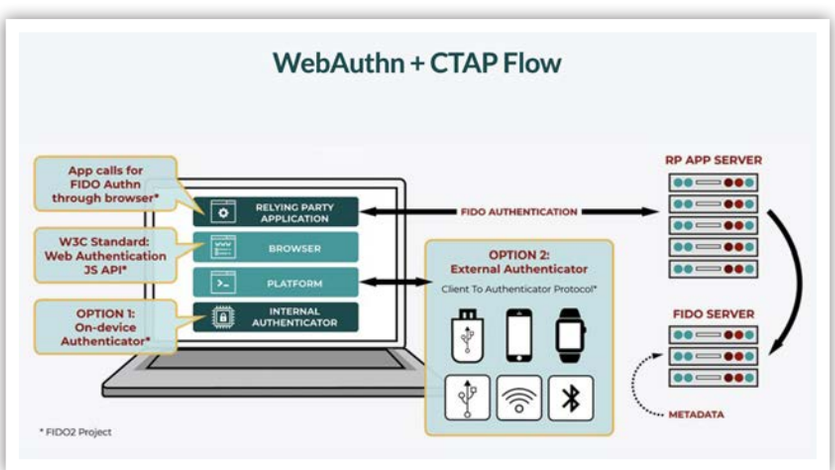

圖 4 FIDO 2.0 架構

資料來源：FIDO Alliance (n.d.)

身分識別機制並進行先期驗證，目標是透過行動裝置的生物辨識功能（例如指紋辨識、臉部辨識）驗證使用者身分，實現便利性、安全性及隱私保護的新時代無密碼身分識別機制。同年 10 月 TW FidO 行動身分識別服務正式上線，並陸續導入多項線上應用，例如繳納地價稅、牌照稅及房屋稅等。2022 年 2 月內政部在原本的基礎上導入 FIDO2 標準，並加入自然人憑證簽章功能（如圖 5），結合行動裝置的生物特徵辨識，發展條碼（QR Code）、推播、行動裝置網頁對 App、網頁轉導及 App 對 App 等 5 種模式提供系統介接應用。

參、研究方法

本章說明研究構思及以雛型系統架構驗證文檔系統線上簽核導入 TW FidO 之可行性方法。

一、研究構思

研究方法主要採用文獻探討及雛型系統架構實驗，並利用第三方驗證工具「電子檔案工具箱」檢驗系統建置可行性。前面章節介紹了文檔系統線上簽核功能及 TW FidO 技術帶來的衝擊及相關運用原理，透過雛型系統架構實驗及第三方工具之驗證結果，提供文檔系統在遠距辦公運

圖 5　行動自然人憑證簽章服務

資料來源：作者整理

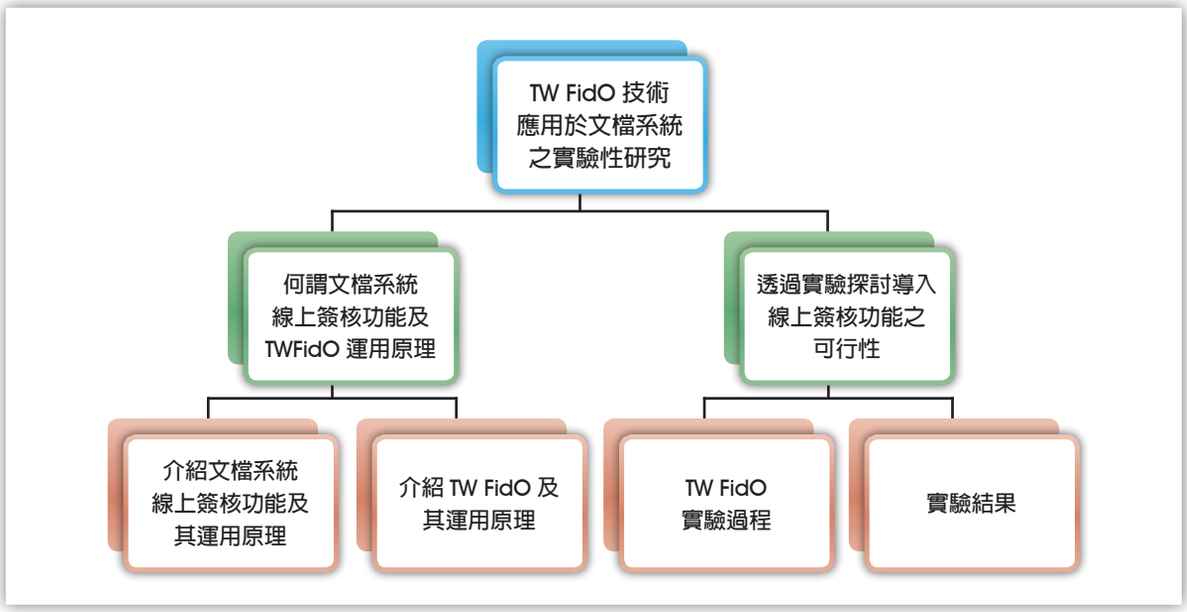

圖 6　研究構思示意圖

資料來源：作者整理

用 TW FidO 執行公文線上簽核，並確保其法律效力、安全性、不可否認性，以及提供事後稽評使用參考，研究構思示意圖如圖 6。

二、研究流程

本研究以檔案局使用的電子公文檔案管理系統（以下簡稱系統 A）及授權他機關使用之公版公文製作系統（以下簡稱系統 B）為對象，驗證雛型概念模組（proof of concept, POC）功能實作，提出系統 A 及系統 B 可搭配情境之行動憑證線上簽核模式，並向內政部提出介接服務，以驗證及確認模擬情境可行性，最後根據實作結果提出結論及建議，以供各機關（構）及文檔系統廠商參考（如圖 7）。

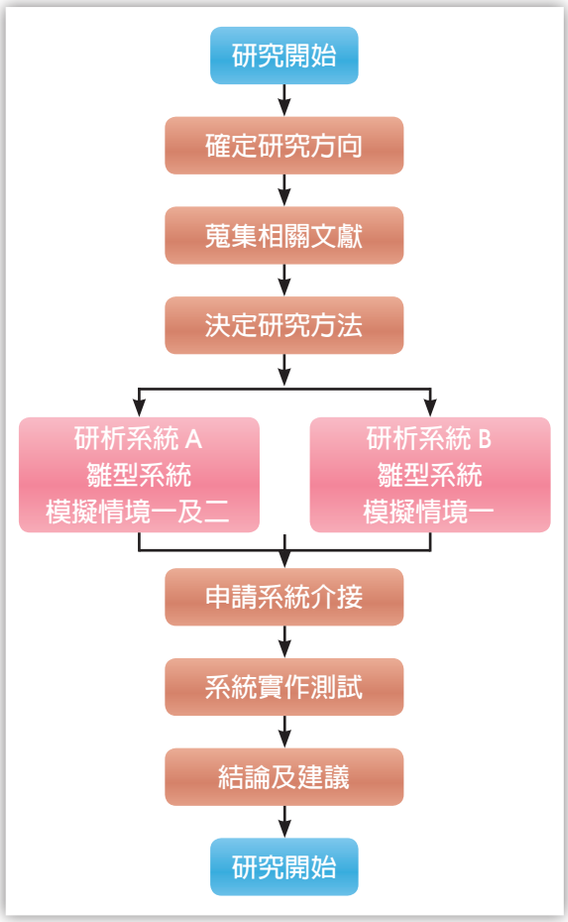

圖 7　研究流程圖

資料來源：作者整理

肆、文檔系統導入 TW FidO

為辦理文檔系統導入 TW FidO 實作驗證，前置作業包括：使用者須先以實體憑證於 TW FidO 網站註冊，並於可攜式裝置（需具生物識別

及連網功能）下載安裝 TW FidO App。此外，行動憑證效期為 1 年，使用者每年須重新申請。

一、文檔系統導入 TW FidO 實作方式

本文將系統 A 及系統 B 導入 TW FidO，並依據不同情境，採用內政部發布之 TW FidO 一致性應用程式介面（application programming interface, API），取得簽署資料並利用電子封裝檔工具箱驗證。

（一）系統 A 導入 TW FidO 實作說明：

1. 依據情境一公文流程加簽作業（如圖 8），使用者於桌上型電腦之文檔系統擬稿送出加簽，分為無設定身分（系統設定輸入身

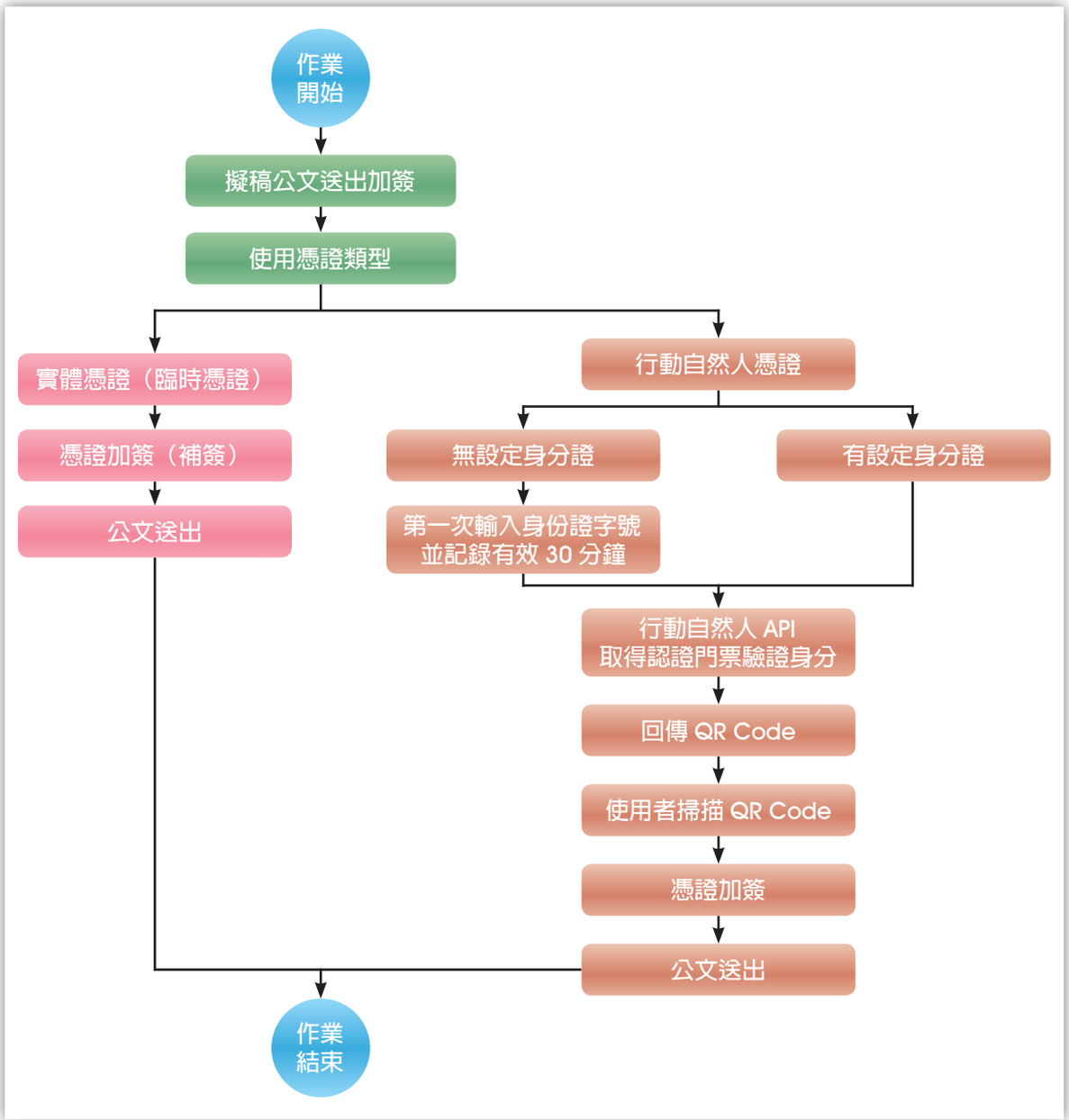

圖 8　系統 A 情境一公文流程加簽案例流程

資料來源：作者整理

分證字號後可以記憶身分資訊 30 分鐘，此期間無需再輸入）及有設定身分（系統設定每次都要輸入身分證字號），掃描桌上型電腦顯示之 QR Code 驗證及簽章後，便完成憑證加簽。

2. 依據情境二公文流程加簽作業（如圖 9），使用者使用平板電腦或手機之文檔系統擬稿送出加簽，同樣分為無設定身分及有設定身分，使用者透過平板電腦或手機 API 取得認證後，跳轉至 TW FidO App，並使用手機生物辨識驗證及簽章即完成。

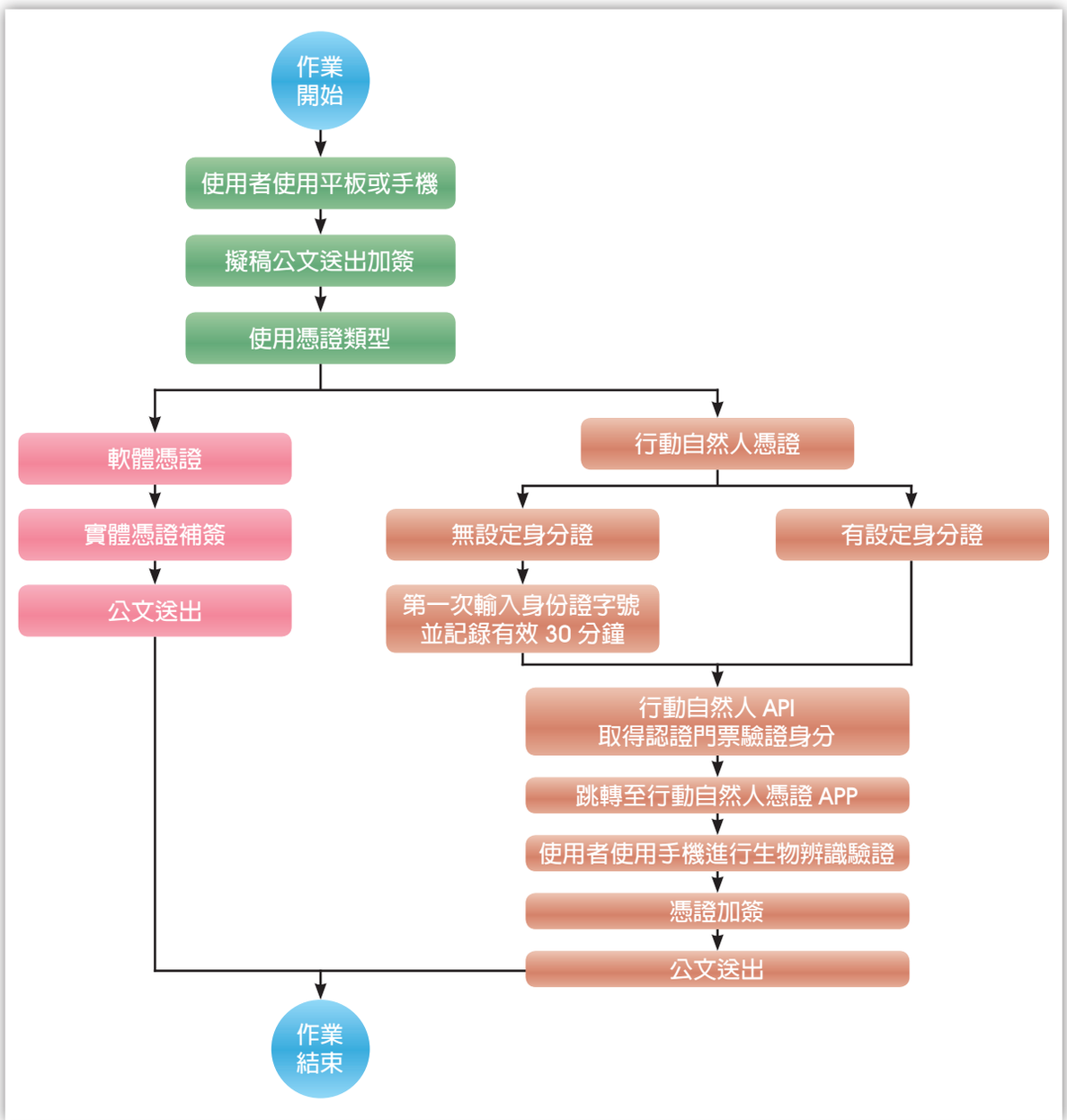

圖 9　系統 A 情境二公文流程加簽案例流程

資料來源：作者整理

（二）系統 B 導入 TW FidO 案例說明：

系統 B 為支援跨瀏覽器使用之公版公文製作系統，僅提供公文製作、線上簽核模組等功能，未整合流程管理、檔案管理等系統，所以本測試案例採未取文號，並繕打公文內容及簽核後送至下一流程點進行測試。

依據情境一公文流程加簽作業，使用者於桌上型電腦之文檔系統擬稿送出加簽，並於手機下載安裝 TW FidO App 後，掃描桌上型電腦桌面顯示 QR Code 認證及簽章（如圖 10）。

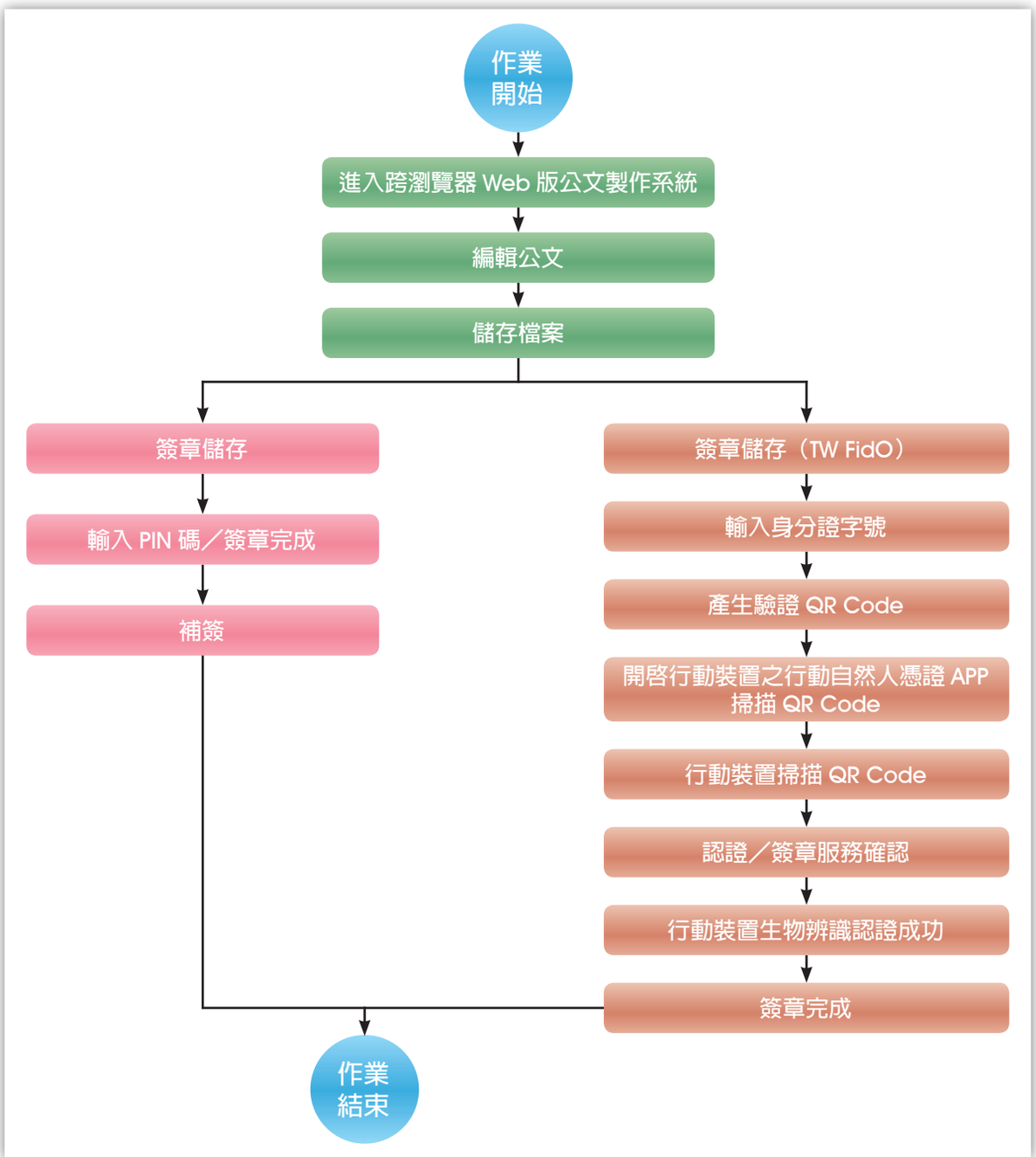

圖 10　系統 B 支援 TW FidO 簽章作業流程

資料來源：作者整理

二、文檔系統導入 TW FidO 實作結果及現行作業差異

（一）實作結果說明

經由技術文件探討，並實際進行系統 A 及系統 B 雛型實作，茲就使用者端及應用系統端實作過程遭遇困難及結果摘述如下：

1. 使用者端

(1) 使用行動憑證進行線上簽核時，基於資通訊安全要求，每件公文簽核均須驗證身分，重新取得系統通行權杖（token）才可簽章，增加操作繁雜度，便利性略顯不足。故仿實體憑證透過公文系統記憶 PIN 碼，使用者於 30 分鐘內無需重複輸入身分證字號。

(2) 每次簽章都要輸入身分證字號驗證身分，相較實體憑證使用密碼之做法，恐有個資保護疑慮，後續建議內政部未來有更好的介接做法。

(3) 原僅發布 Android 版本供廠商實作測試，考量使用 iOS 版本者眾多，經多次與內政部溝通後，俟內政部協助提供 iOS 版本後，始可繼續依時程實作驗證測試。

2. 應用系統端

(1) 現行 TW FidO App 使用者每次簽章均須連結 TW FidO 主機，系統效能須再關注，目前因使用機關不多，尚無具體資訊供評估，已回饋意見予內政部。

(2) 原先提供模式僅能處理 1,300 位元組（bytes）文件大小之簽章，若線上簽核文件大小超出限制，將造成簽章失敗。經多次與內政部反映，並進行內部評估後，始提供支援原始資料簽章功能，由機關線上簽核作業將簽核文件產出雜湊值，將該雜湊值密傳送至行動憑證中心，該中心只要處理簽章功能即可，可有效解決前述文件大小之限制。經內政部協助增修相關 API 功能並提供本研究測試後，確認此方式可正常運作。

(3) 最後實作結果產出電子檔案之格式、憑證及簽章經由電子封裝檔工具箱驗證通過符合文檔規範法遵要求。

（二）導入前後之作業差異說明

1. 導入前

(1) 需使用實體憑證及讀卡機。

(2) 無需使用行動裝置。

(3) 若使用臨時憑證（或軟體憑證）須補簽。

2. 導入後

(1) 無需使用實體憑證及讀卡機。

(2) 需使用行動裝置。

(3) 無需使用臨時憑證（或軟體憑證）進行補簽作業。

伍、結論與建議

文檔系統線上簽核實施範圍之考量因素包括業務屬性、保存年限、公文及其附件大小、決行層級等因素，現行機關線上簽核公文量持續增加，電子檔案長期保存已是備受關注的議題。未來文檔系統發展過程，應在電子檔案管理之安全前提下，善用行動憑證的便利性，使線上簽核功能發揮最大效益。

一、結論

本文提出 2 套文檔系統結合 TW FidO 之線上簽核雛型驗證結果，並經由電子封裝檔工具箱

進行相關檢測均符合通過，顯示導入行動憑證可以順利進行線上簽核作業。

（一）線上簽核導入 TW FidO 行動憑證可行且符合法遵要求

驗證結果顯示行動憑證與線上簽核可順利整合，導入行動憑證可以順利解決實體憑證在遠距辦公的不便利，使線上簽核更具彈性及效率，同時也免除機關使用臨時憑證於歸檔前須以實體憑證補簽程序，符合《電子簽章法》規定及減輕行政作業成本。

（二）擴大運用線上簽核機制的彈性做法

行動憑證使用簽章授權功能均須以身分證字號連線至內政部系統驗證簽章，除有個資保護疑慮外，線上簽核成效也受限於內政部行動憑證系統效能。目前多數機關尚未導入行動憑證進行線上簽核，尚無法確認內政部相關系統穩定性，除使用實體憑證及臨時憑證進行線上簽核外，導入行動憑證進行線上簽核，可作為擴大運用線上簽核機制的彈性做法。

（三）生物辨識可安全且快速取代密碼登入身分驗證功能

本研究主要係驗證行動憑證技術導入線上簽核的概念性實驗研究，研究範圍僅限於電子簽章功能及應用 TW FidO 搭配公文使用情境最適應用模式，目前除於檔案局文檔系統正式導入行動憑證線上簽核外，也在公版公文製作系統完成開發建置，提供各機關（構）整合介接及諮詢參考。未來將持續進行系統優化，以生物辨識達到安全且快速之無密碼身分驗證功能。

二、建議

依前述實作結果，以行動憑證進行電子公文線上簽核於技術面確實可行，惟須有更完整及全面的功能及效能測試，以利後續導入實務作業。根據上述結論，建議未來運用 TW FidO 開發相關系統說明如下：

（一）完善批次補簽功能

本研究受限於內政部提供的行動憑證 API 介接服務功能，目前該部僅提供單次簽核功能，不利於臨時憑證要逐次進行補簽，爰尚待內政部參照實體憑證機制提供批次補簽功能，以便各機關（構）公文及檔案管理系統使用臨時憑證進行批次補簽。

（二）提升系統效能和穩定性

使用行動憑證進行線上簽核時，內政部基於資通訊安全要求，針對每件公文簽核均須驗證身分，重新取得系統通行權杖才可簽章。同時，使用者使用 TW FidO App 時，每次簽章均須連結 TW FidO 主機，當使用量高時，系統效能恐須關注，已回饋內政部評估參考。

（三）優化 API 功能及發布機制

建議內政部提供新版簽章 API 功能時，除於試辦機關先進行功能檢測外，也宜建立發版公告機制。在本次實驗導入期間，發現原先提供介接 API 僅能處理有限文件大小之簽章，若線上簽核文件大小超出限制，將造成簽章失敗，經回饋內政部，請其評估參照實體憑證機制，提供不限長度 API 版本。因無法知悉內政部新版發布時間，相關功能開發測試只能暫停，筆者將持續關注其更版相關訊息，使文檔系統導入行動憑證相關功能增修可按作業期程。

（四）簡化申請流程及延長憑證效期

線上簽核導入 TW FidO 機制，須配合內政部申請程序及線上介接行動憑證主機簽核，與現行實體憑證由機關在本機端處理方式不同。事前

須向內政部提出申請介接行動憑證主機測試環境及正式環境，機關端也需重新開發相關系統功能及介接測試，爰須寬估開發建置及申請介接作業期程。另外需使用實體憑證註冊行動憑證，且行動憑證的簽發效期只有 1 年，需每年更新金鑰，以降低用戶被盜用或破解風險，相較有 5 年效期的實體憑證較不便利，期待內政部未來在系統介接及使用者憑證效期有更彈性及簡便的作業方式。

參考文獻

FIDO Alliance. (n.d.). User Authentication Specifications Overview. Retrieved from https://fidoalliance.org/specifications/ (Jan. 10, 2024)