數位生活—行動裝置身分驗證與安全機制介紹

張皓然/金融聯合徵信中心 研究部

一、前言

金融科技(Fintech)無疑是近年來大家耳熟能詳的專有名詞，在這資訊快速流通的時代，紙本傳遞訊息已無法滿足時代所需，聯徵中心自104年11月1日起已提供個人線上查閱信用報告服務，提供民眾安全及迅速的服務，更在106年1月1日起提供線上加查信用評分的服務，頗受好評。隨著行動網路及智慧型手機普遍化，智慧型手機已經能夠取代電腦部分的功能，因此本中心也非常關注行動裝置上的應用及服務，未來將可透過行動裝置查閱信用報告，持續搭上金融科技的列車，提供更快速、安全及便利的服務。

二、常用之網路身分確認

由於行動裝置發展進步神速，功能也越來越強大，就如隨身攜帶的小型電腦一般，但小而巧的特性使許多電腦週邊的裝置無法在行動裝置上使用，因此可應用於行動裝置上的身分確認便比電腦少。目前實務上常見網路身分確認分成以下幾種：

1. 使用者代號及密碼：

使用者需先向管理者註冊一組使用者代號及密碼，使用服務時必須輸入正確的使用者代號及密碼，伺服器方能提供服務。使用者代號及密碼是相對固定，而有些使用者常貪圖方便，使用簡單易記的密碼保存，很容易遭破解或外洩。為了加強安全維護，管理者通常採取一些措施，例如密碼長度及組合架構、密碼的使用期限、輸入密碼錯誤達一定次數即停止服務等。

2. 晶片卡：

目前常見為自然人憑證、金融卡等實體晶片卡皆為此類，是一種有運算及儲存功能的硬體晶片，通常使用時會搭配密碼使用或限定使用用途，以避免卡片遺失，發卡時系統通常會在卡片上植入一把密鑰，當使用者完成密碼驗證後，卡片端與伺服器端會進行互相傳輸驗

證，而卡片設有保護機制，遺失也不會被盜取卡片內容。由於實體卡不便在行動裝置上使用，後續也衍生出晶片卡應用行動化的技術，例如行動自然人憑證，或是以軟體方式儲存的憑證，例如證券商電子交易憑證。

3. 生物特徵辨識：

運用人體的生物特徵和行為特徵，透過數位運算代碼化，做為身分比對的依據，可分成主動式及被動式採樣，前者需要使用者主動使用採樣設備，例如指紋、虹膜驗證等；後者則利用錄音或錄影射設備採樣，使用者不一定知曉，例如臉型、身型等。

4. 一次性密碼OTP(動態密碼)：

此密碼只能單次使用，當使用過隨即失效，常見分成三種類型，第一類次數型為伺服器產生一組密碼傳送到使用者裝置，使用者輸入此密碼回傳至伺服器進行認證；第二類為時間型，密碼產生裝置會產生一次性有時間限制的密碼，當在此時間內輸入此密碼皆是有效，但超過時間此密碼即失效；第三類為序列型，伺服器及使用者裝置皆產生一序列密碼，每次使用者會輸入其中一組密碼至伺服器比對，當密碼比對正確即可認證成功。

下表為四種驗證機制比較：

表 1

驗證機制	優點	缺點
代號及密碼	使用方便、快速	密碼可能被竊取、無法交換驗證
晶片卡	不易複製、可交換驗證	需搭配讀卡機、需有實體卡片
生物特徵辨識	方便、不容易偽造	成本高、需有特殊裝置、無法交換驗證
一次性密碼OTP	不易複製機制	成本高、裝置有使用年限、無法交換驗證

三、安全管控機制

由於行動裝置有便利與快速獲得資訊，以及存取使用者訊息的特性，類似一台小型電腦，因此在資訊安全方面格外重要，以下為銀行及行動支付的安全設計應遵守的規範：

(一) 電子銀行業務安控機制

依據銀行公會之金融機構辦理電子銀行業務安全控管作業基準，電子銀行業務分成電子轉帳及交易指示類與非電子轉帳及交易指示類，又將前者依據對客戶權益影響之程度分成高風險交易與低風險交易，而後者只包含查詢及通知項目。對於交易面之安全需求分成6種安全防護措施，表2為以非專屬之網際網路作為訊息傳輸途徑，各類別所應達到之安全需求：

表 2

業務類別 / 防護措施	電子轉帳及交易指示類		非電子轉帳及交易指示類
	高風險	低風險	
訊息隱密性	必要	必要	必要
訊息完整性	必要	必要	非必要
訊息來源辨識	必要	非必要	非必要
訊息不可重複性	必要	必要	非必要
無法否認傳送訊息	必要	非必要	非必要
無法否認接受訊息	必要	非必要	非必要

為達到上述之安全需求，實務上發展出幾套方法，表3為通訊傳輸時應達到之安全防護措施之設計方法，應用於高風險交易之設計可用於低風險交易，而應用於低風險交易也可用於身分確認：

表 3

可應用之交易風險等級	安全設計方法
高風險交易	憑證簽章
低風險交易	晶片金融卡
	一次性密碼(OTP)
	兩項(含)以上技術(具有下列三項之任兩項以上技術:1.客戶與金融機構所約定之資訊，例如密碼等。2.確認客戶設備為約定之設備，例如密碼產生器、行動裝置等。3.客戶提供之生物特徵，例如指紋等。)
	視訊會議
	知識詢問
	固定密碼
	委由第三方進行身分確認

(二) NFC行動支付業務安控機制

目前行動支付發展，分成信任服務管理(TSM)平台模式、主機卡模擬(HCE)模式及代碼交易(Token)模式，三種模式所使用之安全控管技術不太相同，應用於手機信用卡身分驗證及資料保護。

依據銀行公會之信用卡業務機構辦理手機信用卡業務安全控管作業基準，辦理手機信用卡業務需要5項安全管控機制，如表4所示：

表 4

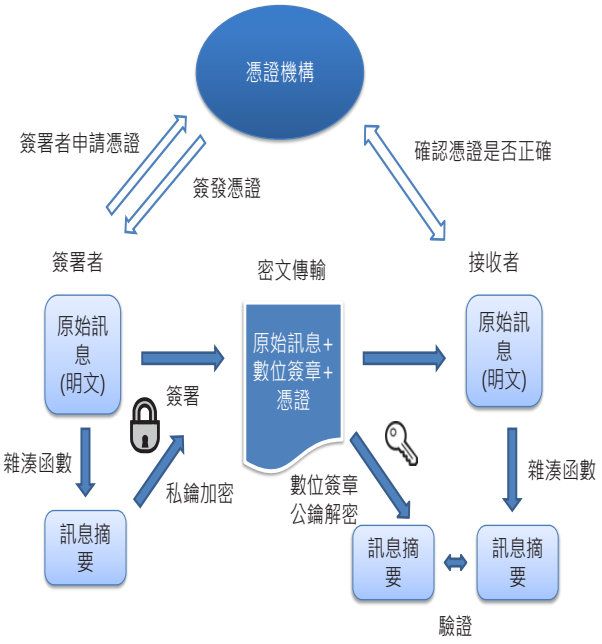
安全設計	說明
訊息隱密性	針對訊息進行全文加密，以防止未經授權者取得訊息之明文
訊息完整性	防止蓄意篡改訊息，可採對稱性加解密系統進行押碼或非對稱性加解密系統產生數位簽章
來源辨識性	應確保持卡人的正確性
不可重覆性	應防止以先前成功之交易訊息完成另一筆交易
金鑰管理	確保金鑰的安全性及品質等

四、數位簽章與憑證

依據電子簽章法，所謂數位簽章指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。而憑證指的是載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

數位簽章中私鑰與公鑰是利用非對稱密碼技術所產製，具有一對一的關係，公鑰可以自由發布，而私鑰必須自行秘密保存，利用密

碼學私鑰可以推算出公鑰，但公鑰要推算出私鑰非常困難，因此具有複雜的邏輯及單向函數的特性。由於公鑰本身無身分識別之方式，因此需要可信賴的第三者或機構來做為公鑰授權單位，證明某一把公鑰確實為某人或某單位所有，以避免偽冒身分，而此第三者或機構將會簽發一張數位憑證，其包含公鑰及基本資料來證明身分，通常簽發憑證之第三者或機構稱為憑證管理中心(Certification Authority，CA)。



五、驗證機制比較

在行動裝置應用方面，由於其使用簡單及便利性高，因此身分認證機制所搭配的硬體只能限縮在行動裝置上，表5-1及表5-2為目前身分驗證機制比較：

表 5-1

身分驗證機制	自然人憑證IC卡	金融憑證IC卡	行動支付TSM平台	行動支付代碼交易(Token)模式
是否需要實體晶片	是	是	是	是
手機可否使用	否	否	可	可
應用之風險等級	高	高	高	高
安全設計	憑證簽章	憑證簽章	憑證簽章	憑證簽章
不可否認性	是	是	是	是
是否有使用期限	是	是	不一定	是
使用便利性	低	低	低	高
發行普及性	低	低	低	低
使用範圍	可橫跨不同單位	可橫跨不同單位	可橫跨不同單位	可橫跨不同單位

表 5-2

身分驗證機制	行動下單憑證	行動自然人憑證	行動網銀	行動支付HCE模式
是否需要實體晶片	否	否	否	否
手機可否使用	可	可	可	可
應用之風險等級	高	高	低	高
安全設計	憑證簽章	憑證簽章	多因子驗證	憑證簽章
不可否認性	是	是	不一定	是
是否有使用期限	是	是	無	是
使用便利性	高	高	高	高
發行普及性	高	低	高	低
使用範圍	企業內部	可橫跨不同單位	企業內部	可橫跨不同單位

六、結論

因應數位化的浪潮，如何在網路上擁有更加安全及便利的身分確認將是未來發展的方向，在安全性方面，使用實體晶片驗證機制相對可承受較高風險，但於行動裝置上無法使用晶片卡，或者必須新增、更換安全元件(可用SD卡、sim卡等)，但使用安全元件需有特定條件將降低使用者的使用意願，為讓使用者有更方便的身分確認方法，便發展出許多行動裝置上可做為身分認證的機制，近年來隨著科技進步，生物辨識設備成本降低，加上操作相較其他認證機制便利，使得許多新推出的行動裝置皆配備生物識別設備，因此越來越多金融機構也開始使用生物辨識作為身分確認的機制，但發展生物特徵識別非常仰賴軟硬體的保密性，一旦資料外洩便可能讓個人特徵被偽冒，故如何有效防止生物辨識資料外洩將是未來的重要課題。

在便利性方面，現行金融業身分認證首要仍是以臨櫃確認，再核發電子交易之密碼函居多，而不同企業間需要各自身分確認之方式，例如某人有兩家銀行帳戶欲申請電子交易服務，在第一家銀行需要臨櫃確認身分，第二家銀行也要重複臨櫃確認身分，且必須記憶各家銀行的帳號密碼，造成相當大的不便，因此設立身分識別中心降低各金融業者之身分確認成本，以及提升民眾在使用電子交易服務的便利性，是未來重要的發展目標。2016年金管會公佈了「金融科技發展策略白皮書」，其中從應用面、管理面、資源面、基礎面四大面向提出11項施政目標，第11項「身分認證:建構整合安全的網路身分認證機制，提供便捷免臨櫃跨業之網路身分認證服務」，即在推行安全、便捷與可跨單位的身分認證方式。

本中心為配合金融科技發展，提升民眾對於查閱信用報告的安全與便利，將與台灣網路認證公司之「TWID投資人行動網」合作，並依照銀行公會之金融機構辦理電子銀行業務安全控管作業基準所訂之安控機制，提供行動裝置線上查閱信用報告的服務，TWID投資人行動網為台灣網路認證公司結合金融業者與金融週邊機構所推出之行動裝置平台，可跨單位使用已上線應用的服務，使用憑證簽章的技術可安全傳遞訊息，減少資訊外洩的風險。未來聯徵中心將持續關注金融科技發展，並參與相關創新的服務。