國立政治大學國際經營與貿易學系研究所

碩士學位論文

論數位身分制度於銀行業之應用與管理法制

A Study on Application and Regulatory Framework of Digital Identity System in Banking Industry

指導教授：楊培侃　博士

研究生：陳俐伶　撰

中 華 民 國 一 〇 九 年 七 月

DOI:10.6814/NCCU202001680

謝辭

能夠走到這一步內心真的感慨萬千，從進入法組，到從波蘭交換回來，再到休學進入職場，一邊上班一邊寫論文，最後拿到學位，一路走來要感謝許多人。首先一定要感謝的絕對是指導教授楊培侃老師，除了在學期間課業上的指導之外，老師不厭其煩叮嚀我的論文進度，甚至是關心我的心理狀況，在我最低潮的時候作為燈塔指引著我，就連自己可能都無法相信自己的時候，是老師給予支持讓我覺得自己能夠做得到。各個方面都要謝謝楊培侃老師，如果沒有老師，這篇論文絕對不可能完成。感謝論文口試委員郭土木老師以及臧正運老師，兩位老師在口試當天給予的寶貴建議帶給我許多啟發，讓我能夠更完善地修改內容。

謝謝楊光華老師、施文真老師以及蔡孟佳老師在校期間的指導，在法組的兩年時光絕對是我目前人生密度最緊實的兩年，法組課程、電子報和研究計畫撰寫，以及籌辦大大小小的研討會，這些學習與歷練對我來說都是非常珍貴的經驗，謝謝老師們。

另外絕對不能不提法組的夥伴們，茹穗、虹妤、郁珊、潔如、元閔以及柏霆，謝謝有你們一起在研究所期間擔任戰友，離開學校後還不時互相關心鼓勵，若是沒有你們也不會有現在的我，尤其要感謝茹穗，除了一直回答我各種行政流程的問題，口試當天還特地請假來幫我，非常謝謝你。

要能邊工作邊寫論文，若是沒有職場上主管和同事的支持作為後盾，這件事情也是不可能實現，我很幸運能夠擁有這樣好的主管和同事，謝謝。還要感謝幫忙找資料以及發想各種靈感的學長，現在我完成了，也期許你能夠順利完成自己的論文。最後要感謝我的家人，即使在我最迷茫的時候，不知道我為何而煩、為何苦惱，你們仍然默默包容關心著我，謝謝你們！

DOI:10.6814/NCCU202001680

摘要

在網際網路時代下，數位身分的概念隨之而生，其係運用電子化方式擷取、儲存可指涉到特定個人的信物或是身分屬性。而當身分資料與身分提供者所核發之信物結合，再運用有效方式去驗證身分時，就可確認一個人是否具備他所聲稱之身分。

數位身分之管理國際上分別有歐盟、美國、ISO 以及 FATF 訂出相關規範或指引，原則是根據風險基礎方法，根據識別及驗證身分之嚴謹程度訂出不同的保證等級，再依行為之風險決定應採行之保證等級，行為風險越大則應採行之保證等級越大，反之，行為風險越小，則採行較低水準之保證等級。

根據國際規範及標準分析我國銀行實務上識別及驗證客戶身分之做法，得出有根據相應之風險選擇適當保證等級之結論，且符合 FATF 客戶盡職調查之建議。但筆者根據自身在第一線工作之觀察，認為現行做法實際上仍有改善之空間，惟為了達成普惠金融的目標，做法應在監理與彈性之間取得平衡。

此外，本文透過比較分析歐盟、美國及 ISO 之規範和國際標準，認為我國可以借鑑國際之做法，直接規範保證等級，在實務上比較具有彈性；同時建議我國參照 FATF 之數位身分指引做出相應之修正，透過法律正式授權，讓銀行業者在進行客戶盡職調查時較無後顧之憂。

關鍵字：數位身分、身分驗證、數位身分指引、客戶盡職調查

DOI:10.6814/NCCU202001680

Abstract

In digital age, the concept of digital identity comes into being. That is a set of electronically captured and stored attributes and credentials that can uniquely identify a person. When the identity data is combined with credentials issued by identity providers and further authenticate an individual through effective methods, it can decide whether a person is who he claims.

European Union, the United States, ISO and FATF provide relevant regulations or guidance for managing digital identity. Based on risk-based approach, these regulations or guidance set different levels of assurance in accordance with the rigor of identification and authentication of identity, and then determine the levels of assurance that should be adopted according to the risk of the behavior. The greater the behavioral risk, the higher level of assurance that should be adopted. On the contrary, the lower the behavioral risk, the lower the level of assurance.

After analyzing the practice of identifying and authenticating customer identities in selected banks of Taiwan, we find that the appropriate level of assurance is determined based on the corresponding risks, and it complies with the FATF's recommendations of customer due diligence. However, there is still room for improvement. In order to achieve the goal of financial inclusion, the practice should strike a balance between supervision and flexibility. At last, our government can learn from international practices and directly regulate the level of assurance, which is more flexible. At the same time, it is recommended that our government refer to the FATF's guidance on digital identity to make corresponding amendments. Through legal authorization, banks are entitled to operate digital identity system without the fear of running afoul of rules when conducting customer due diligence.

Keywords: Digital Identity, Authentication, Guidance on Digital Identity, Customer Due Diligence

DOI:10.6814/NCCU202001680

目次

DOI:10.6814/NCCU202001680

第一章 緒論

第一節 研究動機與目的

隨著金融科技的不斷進步以及 Bank 3.0 等概念的問世，加上監管機關對於業務項目的逐步開放，臨櫃交易逐步轉為線上交易的潮流越來越大，數位存款帳戶從 2019 年下半年開始成為兵家必爭之地，根據金管會統計，截至去 (2019) 年底數位存款帳戶戶數高達 338.4 萬戶，較 2018 年底 150.8 萬戶一年內大增 1.24 倍[1]。尤其在中央銀行以及各家銀行紛紛降息的情況下，數位存款帳戶依然維持 1%以上不等的利率來吸引客戶，就可得知此種帳戶的重要性。

筆者在金融業服務，目前任職於某家銀行，身為第一線工作人員，在實務上見過不少光怪陸離的案件，以上述提到之數位存款帳戶為例，在臨櫃協助客戶開戶時，就不乏見到一些持自己手機替他人開戶，而實際上使用者為自己的情形，雖然多數為家人之間，但就銀行而言，此種情況將不利於防制洗錢以及打擊資恐等犯罪。更何況光就筆者所見的案例就不少，更遑論若是真有犯罪集團利用人頭開立數位帳戶，那數量會有多驚人。

因此筆者對於「數位身分」的概念產生了極大的興趣，更進一步想要研究銀行業如何應用數位身分以及了解背後的相關規範，進而分析我國銀行業目前之做法是否有遵循國際標準。

第二節 研究方法與範圍

我國目前並無針對數位身分建立管理專法，因此本文採用文獻分析法，整理學者文獻、國際組織研究報告、以及相關領域之專書及論文，介紹目前數位身分

[1] 郭幸宜，「數位帳戶兩大優勢 至去年底開戶數 338.4 萬戶 年增 1.24 倍」，鉅亨新聞網，2020 年 2 月 6 日，網址：https://news.cnyes.com/news/id/4439485（最後瀏覽日：2020 年 7 月 23 日）

DOI:10.6814/NCCU202001680

之制度，又鑑於數位身分是較新之議題，故輔以網路資源之蒐集歸納現行之技術與應用。

再透過比較研究法，比較不同國家或是國際組織對於此領域的規範或是指引，作為分析銀行實際做法之依據，對於實務做法進行分析及評論。

第三節 研究限制

數位身分之概念除了自然人，也包含法人，但是我國針對企業戶線上開戶尚有困難仍需解決，像是實質受益人查核以及身分驗證等問題，尤其我國經濟以中小企業為中流砥柱，若是無法解決此一問題，會阻礙社會經濟的活絡。

然而，我國於去（2019）年下半年已開放一人獨資公司能夠線上開戶，惟筆者研究期間國內尚無銀行正式開放獨資企業開立數位帳戶，且 FATF 的數位身分指引亦只談及自然人，因此本文就暫不討論法人的數位身分問題。

DOI:10.6814/NCCU202001680

第二章 數位身分之意義與制度內涵

「在網際網路上，沒人知道你是一隻狗[2]。」這是自網際網路發明以來流行已久的一句話，透過網路和電腦，無法得知另一端的操作者究竟是何人，就算對方聲稱自己是誰，也無法輕易確認他就是他所主張的那位人士。因此，在網際網路時代下，數位身分(Digital Identity)的概念隨之而生。

數位身分的概念相對於物理身分，在日常生活中我們會出示政府所給予的法定文件表示身分，像是身分證、健保卡、駕照或護照等政府記錄在案的證件；而數位身分是指使用者在電腦網路世界使用各種服務時所彰顯的身分，尤其隨著科技與網路的發展，在經濟活動自實體轉為數位環境的時代，若無法在網路上提示身分證件等信物，要如何在茫茫網海中識別或證明身分，便成為新的課題[3]。本章節將介紹何謂數位身分以及辨識數位身分之技術，最後再闡述數位身分於現今社會之主要應用。

第一節 數位身分之定義

數位身分是運用電子化方式擷取、儲存可指涉到特定個人的信物（Credential）或是身分屬性（identity attributes）[4]。一個人的身分可能由許多不同身分屬性所組成，可能包含傳記性資料（biographical data，如：姓名、生日、性別）、生物資料（biometric data）及其他資料[5]。關於我們的各種資料（像是我們喜歡什麼、

[2] Peter Steiner, WIKIPEDIA, https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog (last visited July. 23, 2020).

[3] 協合國際法律事務所，變革中的金融科技法制，頁 71（2019 年）。

[4] WORLD BANK GROUP, GSMA & SIA, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, p.8, http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf (last visited July. 23, 2020);
陳奕甫，數位身分（Digital Identity），網址：https://medium.com/@yfc/%E6%95%B8%E4%BD%8D%E8%BA%AB%E5%88%86-digital-identity-414a1cc5cba6

[5] WORLD BANK GROUP, GSMA & SIA, *supra* note 4, at 11.

DOI:10.6814/NCCU202001680

做什麼、我們是誰）分散在數位環境中，它分佈在不同的系統、不同的儲存設備、社群網絡、公司伺服器及政府資料庫裡，無論位於何處，這些資料都具有一個重要特徵：可以追溯到特定個人[6]。

而當身分資料與身分提供者（Identity Provider）所核發之信物（如：數位身分證、Mobile ID 等）結合，再運用有效方式去驗證身分時，就可確認一個人是否具備他所聲稱之身分[7]。

一般而言，數位身分是透過三個步驟建立[8]：

壹、註冊（Registration）：註冊包含登錄（enrollment）及查驗（validation）兩階段，是建立數位身分最重要的步驟。當一個人宣稱其為某個人，也就是身分登錄時，身分提供者會存取並記錄該使用者之關鍵身分屬性資料，其中可能包括傳記性資料（例如：姓名、出生日期、性別、地址、電子郵件等）、生物資料（例如：指紋、虹膜掃描）和越來越多的其他屬性資料。在此階段所存取的身分屬性種類及存取之方式會影響之後數位身分的確信等級（level of assurance, LoA）。登錄後，身分提供者會以該屬性與其他既有的身分屬性比對查驗，以確保該身分存在且僅屬於一人，不會指涉到其他人。

貳、核發（Issuance）：使用者經註冊後，身分提供者會核發信物（Credential）予使用者，以表彰使用者的身分。依傳統的形式而言，身分提供者會提供文件（例如出生證明）或某種憑證（例如身分證或護照）；就數位身分而言，信物須為數位形式，例如：晶片卡（Smart Card）、二維條碼（QR Code）、行動身分（Mobile Identity）等。

---

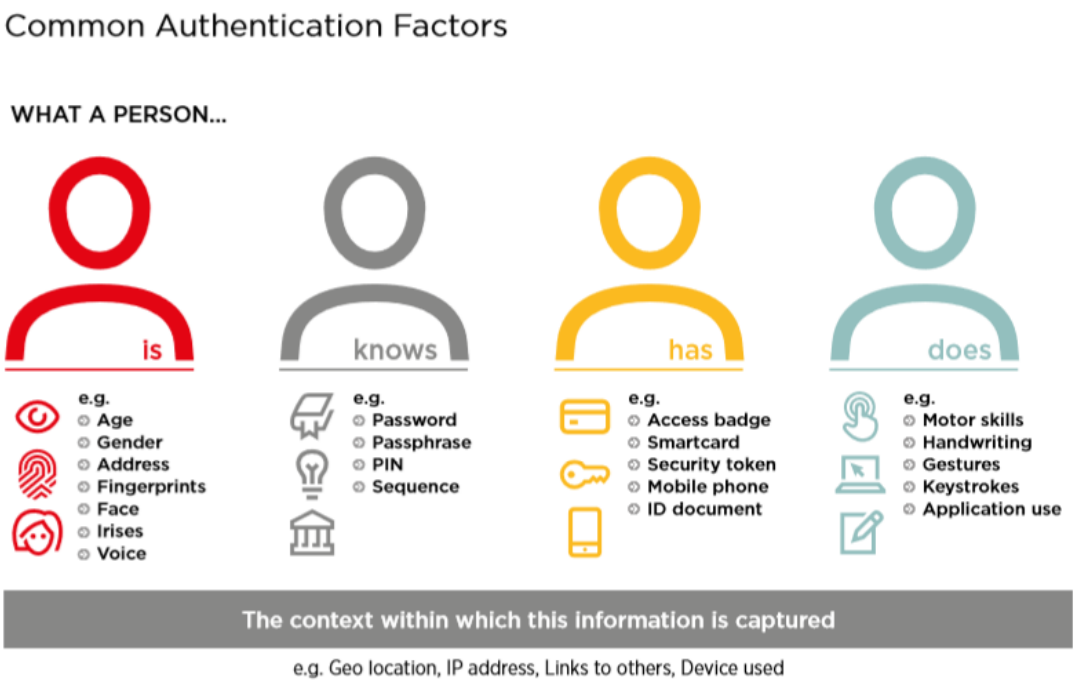
[6] THE BOSTON CONSULTING GROUP, *The Value of Our Digital Identity*, p. 35-36, https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf (last visited July. 23, 2020).

[7] 協合國際法律事務所，前揭註 3，頁 72-73。

[8] WORLD BANK GROUP, GSMA & SIA, *supra* note 4, at 16-19; 同上註，頁 73-74。

DOI:10.6814/NCCU202001680

參、驗證（Authentication）：使用者經註冊、核發後，就可以運用數位身分證明自己的身分進而取得服務。這個過程中，使用者將透過數位信物的一個或多個驗證因素（Authentication Factor）驗證身分。以晶片卡而言，數位信物及生物辨識資料儲存於卡片的晶片內，使用者得依照交易的性質與風險，運用存放於晶片卡內的資料進行不同確信程度的驗證。



來源：World Bank Group, GSMA & SIA, p. 20

數位身分系統能夠對各種功能和服務的最終用戶進行識別和認證，而政府和私部門公司在推廣此系統方面有著共同利益，因為公私部門可以相互依賴來建構和管理身分系統，例如，政府可以將其身份架構的各個方面外包給私營公司（例如系統開發），也可以與私營公司合作以確保官方 ID 與私有服務的交互操作可能性(interoperability)。同樣地，私營公司通常依靠官方形式的證明（例如出生證明、身分證）來驗證其用戶身分[9]。舉例來說，在銀行開戶時必須出示身分證即是一例。在這個應用中，銀行之所以會信賴身分證，是因為身分證係由內政部核發，

[9] WORLD BANK GROUP, GSMA & SIA, *supra* note 4, at 25.

DOI:10.6814/NCCU202001680

而內政部在台灣是被社會大眾、銀行信賴的單位。

而國際打造數位身分與身分驗證，體系上多是透過政府或權威機構在一定準則框架下建構。但無論是由政府、受政府行政委託的機構，或是金融機構本身主導，均仰賴權威機構做為「信賴起源（Trust Anchor）」，因而數位身分的生態系統（digital identity ecosystem）大致可分為以下型態[10]：

一、植基於政府所核發的數位身分「中心化身分」（Centralized Identity Framework based on an official eID as a root）：由政府主導的中心化身分，身分屬性儲存於政府的資料庫，並運用國家所核發的數位身分做為所有公、私部門數位交易的基礎。

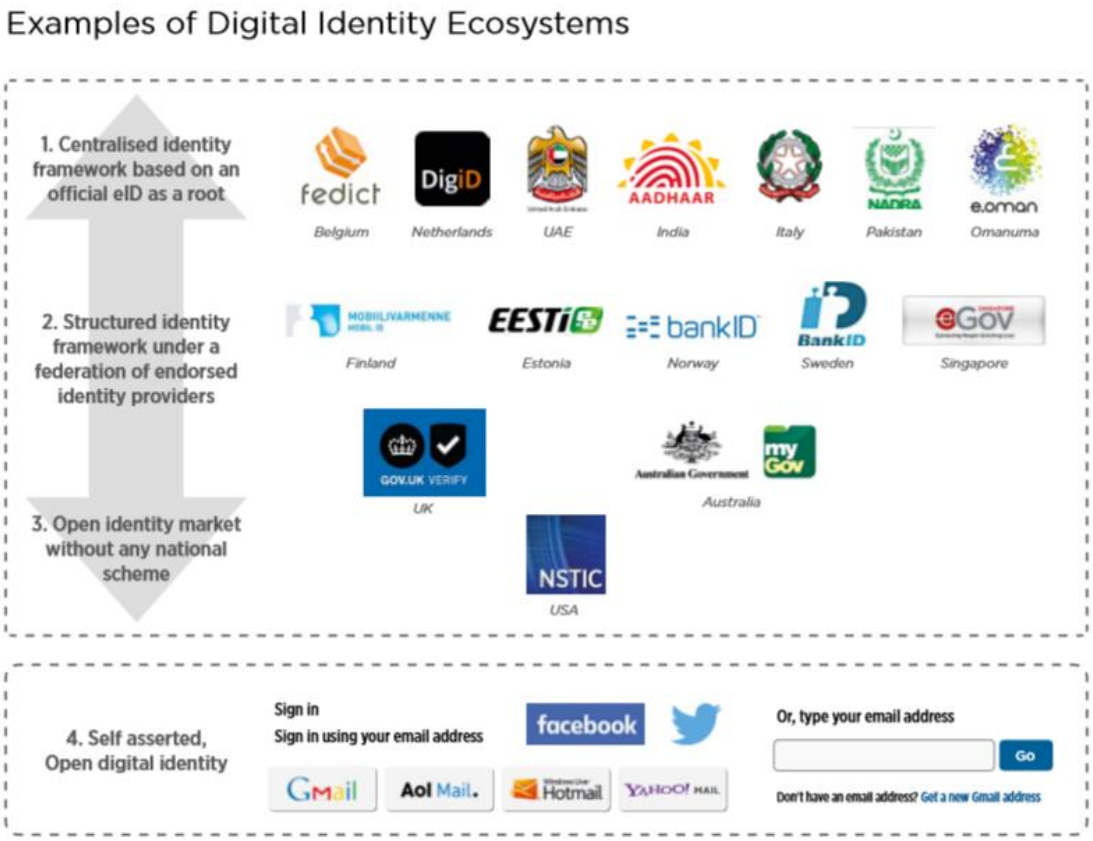
二、經認可的身分提供者「結構型身分」（Structured Identity Framework, under a federation of endorsed identity providers）：由一個或多個的單位，經政府認可後可向民眾提供數位身分。通常此種模式會在政府核發官方身分文件（如出生證明）後，就將數位身分的產製交由私人企業或非營利事業提供。

三、無國家層級「開放身分市場」（Open Identity market without any National Scheme）：公、私部門各自創造、管理及使用各自的數位身分。

四、自行驗證的開放數位身分（Self-asserted, "Open" Digital Identity）：數位身分主要是由大型網路服務提供者（如：Facebook、Google）所提供。使用者可以自己選擇所要存取的身分屬性，且由於未與官方身分資料進行驗證，故其確信程度較低。

[10] WORLD BANK GROUP, GSMA & SIA, *supra* note 4, at 26; 協合國際法律事務所，前揭註 3，頁 74。

DOI:10.6814/NCCU202001680



來源：World Bank Group, GSMA & SIA, p. 25

第二節 數位身分之識別與驗證

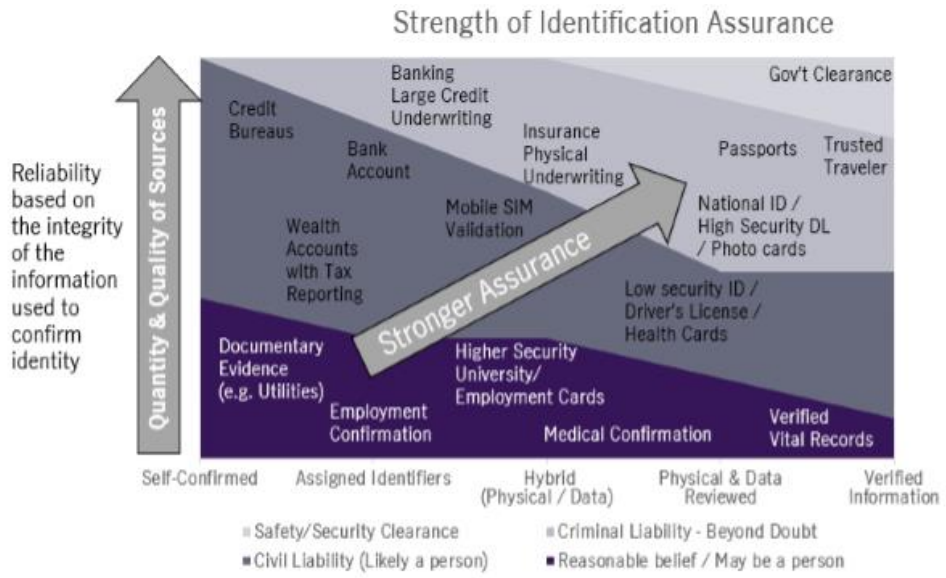
身分驗證技術是為了在網路世界中確認操作者的身分，網路世界中的一切資訊，包括使用者的身分資訊，都是用一組特定的數據來表示，電腦只能識別使用者的數位身分，如何保證以數位身分進行操作的操作者就是這個數位身分的合法擁有者，亦即確保操作者的物理身分與數位身分相對應，身分驗證技術就是為了解決這個問題[11]。

在本節開始之初，必須先區分「身分識別（identification）」和「驗證（authentication）」之差異，如此在接下來的章節中才不會混淆兩者之意義[12]。身

[11] 洪杰文、歸偉夏，新媒體技術，頁 378（2016 年）。
[12] 根據聯合國國際貿易法委員會（UNCITRAL）有關身分管理之最新條文草案，「身分識別（identification）」這個用語已被「身分核實（identity proofing）」取代，而「驗證（authentication）」

DOI:10.6814/NCCU202001680

分識別是為了判斷使用者是誰，識別的內容必須獨一無二，如此才能正確地分辨出每個人[13]，通常係通過使用可靠來源（例：受信任的記錄或機構）提供的屬性，來確立一個獨特的人（個人或實體），並確認上該屬性皆與此一特定人相符的過程，亦即身分核實（identity proofing）[14]。



來源: CAMS – Audit Advanced Certification –Digital Identification Methods and Testing for AML Programs[15]

驗證則是在嘗試登入帳戶或設備時驗證自己的行為，例如通過輸入密碼登入自己的電子信箱帳戶就是一種數位身分驗證。此外，利用生物辨識（像是指紋或虹膜掃描）亦被視為數位身分驗證。綜上所述，數位身分識別是在回答「你是誰？」，

則被「電子身分識別（electronic identification）」所取代，綜上，身分管理過程現在由兩個階段（或步驟） 組成，即「身分核實」和「電子身分識別」；UNCITRAL Working Group, https://undocs.org/en/A/CN.9/WG.IV/WP.162.

[13] 黃鈺書，身分辨識於保險科技之應用相關法律問題研究，私立東吳大學法律學系碩士論文，2018，頁 54。

[14] CAMS, – *Audit Advanced Certification –Digital Identification Methods and Testing for AML Programs*, at 8.

[15] *Id.* at 10.

DOI:10.6814/NCCU202001680

而數位身分驗證則是回答「那是你嗎？」[16]。

所謂身分驗證，就是針對使用者「所知道或所持有的事物」、或「所具備的特徵」進行比對，以確認其身分如其所聲稱。身分驗證技術依其所運用的驗證因子 (Authentication factor)，可概分為三類[17]：

1.知識(Knowledge)因子：使用者所知之事 (Something the user knows)， 如：使用者帳號及密碼、通行密碼片語、安全問題等。

2.持有(Ownership)因子：使用者所持之物(Something the user has)，如：智慧卡、晶片卡、憑證、動態密碼產生器等。

3.固有(Inherence)因子：使用者所具之形徵(Something the user is or does)，如：使用者的臉型、指紋、DNA、虹膜、掌紋等生物特徵。

以下針對前述驗證因子，介紹當前幾種常見的身分驗證技術及應用[18]：

1. 使用者帳號密碼或安全問題

使用者帳號密碼及安全問題係最容易使用的驗證方式。由使用者設定的密碼或安全問題之答案，只有使用者自己知道。驗證時，只須比對輸入的密碼或答案是否正確，即可確認其身分。大多數電腦系統係使用此種方式，進行使用者之身分驗證作業。

2.智慧卡

法國人羅蘭‧莫雷諾 (Roland Moreno) 於1974 年發明智慧卡（Smart Card），

[16] ACAMS, *Digital Identity and Financial Crimes*, https://www.acamstoday.org/digital-identity-and-financial-crimes-2/ (last visited July. 23, 2020).
[17] 李中仁，財金資訊季刊，92 期，2018 年 5 月，https://www.fisc.com.tw/Upload/a19a130b-bb71-43e5-aaec-4c94a3765907/TC/9206.pdf
[18] 同上註。

DOI:10.6814/NCCU202001680

將具有加密儲存及資料處理能力的 IC 晶片置於塑膠卡片上，透過讀卡設備即可讀取或處理資料。儲存於智慧卡晶片內的資料不易被破解或複製，因此，可視為使用者所持有之獨特信物，進而確認其身分。目前智慧卡已廣泛應用於日常生活，如：提款卡、信用卡、門禁卡等。

3. 憑證

憑證（Certificate）是由具公信力的單位（如：憑證中心、政府機關等）所發放的身分證明文件，依型式可分為實體憑證與數位憑證。政府機關所發放的身分證、駕駛執照等，均屬實體憑證；而數位憑證則是利用公開金鑰基礎架構 (Public Key Infrastructure , PKI) 技術所簽發的身分驗證電子檔案，可應用於網路環境，藉以確認持有者身分。

數位憑證須儲存於某一種載具中，如：磁碟、光碟、隨身碟或晶片卡等，通常具有時效性，過期即失效無法使用，須重新申請簽發或展延效期。我國內政部推廣使用的「自然人憑證」，亦為數位憑證之一例。

4. 動態密碼

動態密碼又稱「一次性密碼」(One Time Password , OTP)，係利用特定數學演算法計算所產生的密碼，具備「有效期間短」及「不可預測」之特性，通常須搭配密碼產生載具(Token) 方可使用。

載具型式可分為軟體及硬體兩種，軟體載具如：行動簡訊、電子郵件、電腦軟體或手機 APP 等；而硬體載具則須配備螢幕以顯示動態密碼，並可依實際使用需求，製作成卡片、鑰匙圈等不同的樣式。為供螢幕顯示及密碼計算所需之電力，硬體載具尚須配置電池，因此有其使用期限，一旦電池耗盡，就須重新配發。相對於軟體載具，硬體載具比較安全，但成本也較高。

DOI:10.6814/NCCU202001680

5.生物辨識

生物辨識 (Biometric) 技術係利用生物與生俱來、且獨一無二的生理(Physiological)或行為 (Behavioral) 特徵，經由測量、比對、識別等方式進行身分驗證。常見的生理特徵如： 指紋、虹膜、視網膜、臉型、掌紋、DNA 等，而聲紋、簽名、筆跡等則是常見的行為特徵。

運用生物辨識技術，使用者可「隨身攜帶」獨一無二的特徵，不怕遺失，不易複製，也不必擔心遭人盜用。不過，此類驗證機制須事先收集生物特徵並建檔，且需使用特定的驗證設備。目前實務應用以指紋辨識技術最為成熟，大多數智慧型手機皆配備有指紋辨識系統。臉型辨識亦是發展迅速的一項技術，只需搭配小型攝影機，即可進行身分驗證。

然而僅使用一種驗證方式，安全性上顯然不足，以最常見的帳號密碼驗證方式為例，由於使用者設定的密碼太過簡單遭致他人破解，進而被詐騙的案例屢見不鮮，因此後來產生了多因子驗證機制，利用不同驗證因子與驗證技術之特性，截長補短，以期提升身分驗證之安全性，並兼顧使用者之便利性。

茲列舉幾種常見的多因子驗證機制與使用情境：

1. 使用者帳號密碼及動態密碼

大多數電腦系統皆設有使用者帳號密碼的驗證機制，如能搭配動態密碼「有效期間短」及「不可預測」之特性，將可大幅提升驗證之安全性。採用動態密碼機制須配備密碼產生載具，基於成本及作業考量，硬體載具較適用於注重系統安全強度之企業組織；至於一般企業較傾向採用軟體載具。為提升使用者驗證之安全性，目前多數雲端服務供應商皆有提供動態密碼相關服務。

2. 智慧卡及密碼

DOI:10.6814/NCCU202001680

智慧卡具有難以複製之特性，但為防範卡片遺失或被竊而遭盜用，通常會輔以密碼作為第二道驗證方式，並設定密碼輸入錯誤次數之上限，若密碼輸入錯誤次數超過上限，即無法繼續使用卡片。各金融機構製發之晶片金融卡，即採用此種驗證方式。

3. 憑證或智慧卡及人臉辨識

近年來，人臉辨識技術發展日趨成熟，其具有不易偽造之特性，很適合搭配憑證或智慧卡，提供多因子驗證機制。採用此種驗證方式，須搭配特定的驗證設備，且須先申請憑證或智慧卡，並註冊個人臉部特徵，比較適合門禁管制相關應用。內政部移民署於機場、港口所設置的入出國自動查驗通關系統 e-Gate，即採用電腦自動化方式，結合生物辨識科技，以護照搭配人臉辨識，實施多因子身分驗證機制。

目前國際上對於數位身分管理以及身分驗證等技術頒布了不同的管理規章或是國際標準，像是歐盟的電子身分認證與信賴服務規章（eIDAS）、美國國家標準技術局（NIST）數位身分指引或是 ISO/IEC 29115 國際標準等（詳細內容將於本文後述），綜上可知國際間將身分驗證視為一種風險基礎方法，其邏輯為：「身分驗證方法」、「首次註冊程序」均影響「身分確信程度」，或者又稱「保證等級」（Level of Assurance，LOA），越高強度的驗證方法，搭配越嚴謹的首次註冊程序，所得出的確信程度越高，風險則越低[19]。對於「身分證明」，LOA 取決於驗證方法，包括在註冊過程中所蒐集的個人資料和身分屬性的範圍，以及確定這些身分屬性的精準性。例如在註冊過程中蒐集了個人資料，但沒有對重複數據進行刪除或對現有資料庫進行準確性檢查，則將導致 LOA 降低，因為並沒有對身分資訊進行驗證。

[19] 協合國際法律事務所，前揭註 3，頁 76。

DOI:10.6814/NCCU202001680

隨不同交易對身分真實性的要求程度，將影響所需的驗證過程。例如於線上購物對身分真實性要求較低，採用超商貨到付款，實際上可以採用假名或假電話進行[20]。

來源：World Bank Group, GSMA & SIA, p21; 協合國際法律事務所，《變革中的金融科技法制（2019）》，頁 76

第三節 數位身分之應用與風險

聯合國為了解決全球發展失衡的問題，於 2015 年提出「永續發展目標」（Sustainable Development Goals，簡稱 SDGs），旨在呼籲所有國家（包含已開發國家與開發中國家），能夠在全球夥伴關係中採取行動，畢竟每個問題都是息息相關的，有賴於各國攜手合作才有扭轉當前局勢，進而達到永續發展的可能[21]。

其中聯合國永續發展目標第 16.9 點：「在西元 2030 年以前，為所有人提供合法的身分，包括出生登記[22]。」，大多數人認為數位身分的建構能夠有效達成此一目標之實踐，尤其根據聯合國難民署的說法，數位身分可以促進基本服務的

[20] 協合國際法律事務所，前揭註 3，頁 76。
[21] 倡議編輯室，「聯合國永續發展目標 SDGs 你我都不能缺席」，網址：https://ubrand.udn.com/ubrand/story/12117/3783886（最後瀏覽日：2020 年 7 月 23 日）。
[22] United Nations, https://sustainabledevelopment.un.org/sdg16 (last visited July. 23, 2020).

DOI:10.6814/NCCU202001680

獲取，幫助各國分配社會福利，並讓全球 20 億並未開立銀行帳戶的人擁抱正式的金融工具[23]。

因此，本節將概述數位身分目前最廣泛之應用，也就是數位身分證（eID）以及行動身分（Mobile ID）。

壹、數位身分證

電子晶片身分證（electronic identification, eID）又稱數位身分證，為目前各國發展的趨勢，許多國家透過 eID 作為開啟數位國家與便捷政府的關鍵。2002 年首見於愛沙尼亞，並陸續獲得比利時（2003）、義大利（2006）、西班牙（2006）、德國（2010）等其他歐盟成員之採用，隨後擴及包含香港（2003）、以色列（2013）、日本（2016）等[24]。

以愛沙尼亞為例，該國可以說是推行數位身分證最成功的國家，在 2002 年即推行晶片身分證政策，在政策實施的第一年僅有 10 萬人持有，但是在推動多年後，目前卡片持有率已經高達 98%，除 15 歲以下的愛沙尼亞公民不強制持有外，其餘國民都必須持有晶片身分證[25]。愛沙尼亞政府結合公私部門，研發數位化服務，例如電子健保、電子處方籤、線上開辦銀行帳戶，試圖讓 eID 融入民眾日常生活，目前為止線上進行身分驗證次數已經突破 5.6 億次，數位簽章使用次數則是達到 6.5 億次[26]。

---

[23] Blockchain for the SDG, https://blockchain4sdg.com/digital-identity-sdg-16-9-providing-legal-identity-for-all/ (last visited July. 23, 2020).

[24] 李啟榮，「數位身分證技術探討（一）：數位身分證的多元服務和個資安全保障」，網址：https://www.find.org.tw/index/wind/browse/ed504f626f4cf18dc3fa58f273a6e8d3/（最後瀏覽日：2020 年 7 月 23 日）。

[25] 王立恒，「【國外 eID 實例：愛沙尼亞】技術、法源、開源三管齊下，2 千項數位服務才能安心用 eID」，網址：https://www.ithome.com.tw/news/117367（最後瀏覽日：2020 年 7 月 23 日）。

[26] 蔣宜婷，「eID 模範生的建議：信任比技術更重要」，網址：https://www.businesstoday.com.tw/article/category/80398/post/202002190015/eID%E6%A8%A1%E7%AF%84%E7%94%9F%E7%9A%84%E5%BB%BA%E8%AD%B0%EF%BC%9A%E4%BF%A1%E4%BB%BB%E6%AF%94%E6%8A%80%E8%A1%93%E6%9B%B4%E9%87%8D%E8%A6%81

DOI:10.6814/NCCU202001680

而我國預計 2020 年 10 月起全面換發數位身分識別證（New eID），藉由 New eID 提供民眾一證多用、免排隊等便利服務，並採用國際標準、安全密碼、防偽機制、身分最小化來提升民眾個資安全保障[27]。

貳、行動身分

行動身分指的是一種數位身分，可以使用於智慧手機、平板電腦、穿戴式裝置與物聯網或與其相關的系統中，進行身分識別管理之技術。概念上可以包含指紋、聲紋或臉部辨識等生物辨識方式，或者是某些裝置上利用使用者所擁有的資料的驗證方式等[28]。eID 仍需要實體卡，而行動身分只需要行動裝置，它可用於存取安全的電子服務，也可對文件進行數位簽章，具有不需要讀卡機之特性，不過此服務僅限於載有特殊 sim 卡的行動裝置[29]。

數位身分固然帶給人們便利與方便，但也不得不去思考背後可能的隱憂，由於數位身分通常需要建立集中資料庫來保存敏感的個人資料，因此容易受到惡意行為者的破壞或受到公共機構的濫用等[30]，是故當我們在享受數位身分所帶來的科技紅利時，同時也必須關注是否對於隱私權造成危害，以及資訊安全的保障是否足夠等問題。

[27] 前揭註 24。
[28] 蘇柏毓，「淺談 Mobile ID 安全之法令要求與應用案例」，網址：https://nccnews.com.tw/202002/ch2c.html（最後瀏覽日：2020 年 7 月 23 日）。
[29] Access Now, NATIONAL DIGITAL IDENTITY PROGRAMMES: WHAT'S NEXT?, p. 9, https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf (last visited July. 23, 2020).
[30] *Id*. at 2.

DOI:10.6814/NCCU202001680

第三章 國際間數位身分制度之管理規範

隨著科技的進步以及數位化的發展，數位身分之應用越來越多元，不論是在公部門的電子化政府服務，或是在私部門的商業電子交易等，對於身分之驗證需求越來越多，為了保障資訊以及交易之安全，各國或國際組織制定相關規範或國際標準予以因應，以其能夠防止身分之偽造與冒用等問題。

承第二章所述，目前國際上對於數位身分之管理以及身分驗證頒布了不同的管理規章或是國際標準，以下將概述歐盟、美國與 ISO 有關數位身分驗證之相關規範，並且再進一步闡明 FATF 數位身分指引之內容以及目前貿易協定裡有關數位身分內容之最新發展。

第一節 歐盟 eIDAS

壹、立法目的及背景

歐盟為了符合 2010 年歐洲數位議程(A Digital Agenda for Europe)中數位單一市場(digital single market)之目標，並建立消費者對於線上電子交易環境之信賴，於 2014 年通過「電子身分認證與信任服務規章（The Regulation(EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market，以下簡稱 eIDAS）」，希望能提供歐盟公民、企業與公部門安心使用電子交易的基礎環境[31]；此規章主要針對身分識別機制（electronic identification schemes, eIDs）、認證（authentication）和信賴服務提供者（trust service providers, TSP）等通盤規範，主要想解決歐盟既有電子簽章指令僅就電子簽章定義和提供憑證服務應具備條

[31] European Commission, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid (last visited July. 23, 2020).

DOI:10.6814/NCCU202001680

件規範之不足，以及個人身分認證無法於全歐盟一體適用之窘境等問題[32]。

貳、規範

eIDAS 之立法形式為規章（Regulation），與指令（Directive）不同，係具有強制力之法律，無須經過歐盟成員國轉換成內國法，直接適用於所有會員國。eIDAS 有關電子身分認證之規定在第二章第 6 條至第 12 條，規範電子身分認證之相互承認、電子身分認證通知資格、保障等級、通知、安全漏洞、責任及合作等內容。本章將以保證等級（Level of Assurance）為主軸，分述在不同的等級下，應有何種程度之驗證規範。

有關電子身分認證之相關要求，重點如下[33]：

一、電子身分認證方案應具備保證水準

第 8 條規定，電子身分識別方案應保證該方案中所發布的電子身分識別方式，應具備所保證的低、中、高各種水準。而該保證之低、中、高水準應分別符合下列標準：

（一）具備保證之低水準指的是電子身分識別方案中所採用的電子身分識別方式僅提供有限程度的保密性，且採用的技術規格、標準與程序僅能減低識別資料被濫用的風險。

（二）具備保證之中等水準指的是電子身分識別方案中所採用的電子身分識別方式提供充分程度的保密性，且採用的技術規格、標準與程序能大幅降低識別資料被濫用的風險。

[32] 李姿瑩，「歐盟 eIDAS 對國內電子簽章和身分認證規範之可能借鏡」，科技法律透析，2019 年 11 月，第 31 卷第 11 期，頁 25-26。
[33] 前揭註 28。

DOI:10.6814/NCCU202001680

（三）具備保證之高水準指的是電子身分識別方案中所採用的電子身分識別方式提供較中等程度更高的保密性，且採用的技術規格、標準與程序能避免識別資料被濫用。

二、技術細節另由施行細則決定

第 8 條亦要求歐盟執委會對於保證等級另為規定，亦即應透過本規則之施行細則(implementing acts)，訂定上述符合高中低水準所必要之技術規格、標準與程序，訂定相關技術規格、標準與程序時，應考量下列要素之可靠性與品質[34]：

（一）能證明與確認申請使用電子身分識別方式的自然人或法人身分的程序。

（二）電子身分識別方式的發行程序。

（三）使接受電子身分識別方式的信任方(relying party)可認證使用電子身分識別方式的自然人或法人身分的認證機制。

（四）發行電子身分識別方式之組織(entity)。

（五）電子身分識別方式申請與發行過程之參與者。

（六）已發行電子身分識別方式之科技與安全規格。

三、保證等級

施行細則規定要求之項目中，與使用方式之要求與管理相關之例示如下：

[34] 根據 eIDAS 第 8 條規定之要求，歐盟執委會於 2015 年 9 月通過歐盟電子交易身分識別與信任服務規則的施行細則(COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market)，其目的在於訂定保證水準中所必要之技術規格、標準與程序。也是為了確保不同電子交易身分識別方案中的保證水準得以互通。

DOI:10.6814/NCCU202001680

（一）電子身分識別方式的類別與設計

電子身分識別方式的類別與設計之保證水準與要求事項	
保證水準	要求事項
低	1.使用至少一種驗證因子 2.使發行者能透過合理步驟確認該電子身分識別方式在本人所控制或保有下使用
中	1.使用至少兩種驗證因子 2.能被推定電子身分識別方式僅在本人所控制或保有下才能使用
高	在中度保證水準的要求外再增加： 1.電子身分識別方式可避免遭到複製、竄改或其他潛在高風險之攻擊 2.可使本人在可信賴的保護下避免他人使用其電子身分認證方式

（二）暫停使用、撤銷使用與再啟用

暫停使用、撤銷使用與再啟用之保證水準與要求事項	
保證水準	要求事項
低	1.能即時有效地暫停或撤銷電子身分識別方式之使用 2.具備措施防止未經授權之電子身分識別方式暫停、撤銷或再啟用 3.僅在回復暫停或撤銷前之保證水準要求後，才能在啟用電子身分識別方式
中	與低度保證水準要求相同
高	與低度保證水準要求相同

（三）認證機制

DOI:10.6814/NCCU202001680

認證機制之保證水準與要求事項	
保證水準	要求事項
低	1.在釋出個人識別資料之前電子身分識別方式與其有效性經過可靠地驗證 2.當個人識別資料儲存為認證機制的一部分時，必須保護資料以避免資料被竊取或侵害 3.認證機制採用安全控制措施驗證電子識別方式，大幅降低攻擊者以猜測、竊聽、重播或操縱通信等方式進行基本攻擊，破壞認證機制之風險
中	除低度保證水準的要求外再增加： 1. 在釋出個人識別資料之前，電子身分識別方式與其有效性經過動態認證機制可靠地驗證 2.認證機制採用安全控制措施驗證電子識別方式，大幅降低攻擊者以猜測、竊聽、重播或操縱通信等方式進行中度攻擊，破壞認證機制之風險
高	除中度保證水準的要求外再增加： 認證機制採用安全控制措施驗證電子識別方式，大幅降低攻擊者以猜測、竊聽、重播或操縱通信等方式進行高度攻擊，破壞認證機制之風險

第二節 美國 NIST 數位身分指引

壹、訂定目的及背景

隸屬於美國商務部的國家標準技術局（National Institute of Standards and Technology, NIST）負責制定資訊安全的相關標準與規範，在 2004 年首度公布名為「電子身分驗證指引」(Electronic Authentication Guideline)的 SP 800-63 系列文件，旨在依聯邦資訊安全管理法 (Federal Information Security Modernization Act,

DOI:10.6814/NCCU202001680

FISMA) 進一步界定其法定責任[35]，並陸續更新及增訂其內容。

然而隨著科技與技術的進步，包含信用卡及簽帳卡等支付方式的身分詐欺犯罪嚴重威脅美國的經濟活動，為了加強金融交易市場裡的資訊安全，美國總統歐巴馬於 2014 年 10 月 17 日簽署「改善消費者金融交易之安全性」行政命令（Executive Order 13681 - Improving the Security of Consumer Financial Transactions），指示相關單位做出因應[36]。因此 NIST 在 2017 年推出最新版本並更名為「數位身分指引」（Digital Identity Guideline），共由主要文件《數位身分指引》及轄下三個子文件《註冊與身分證明》、《驗證與生命週期管理》及《聯合與斷言》所組成[37]。

數位身分指引主要是為了實施數位身分服務的機構提供技術層面的要求，該指引涵蓋的範圍包含身分證明、註冊、身分驗證、管理過程、驗證協議等，並根據風險的不同來訂定保證水準（Level of assurance），這些機構可以使用此指引作為其風險評估的一部份，靈活地選擇適合其需求的保證級別[38]。

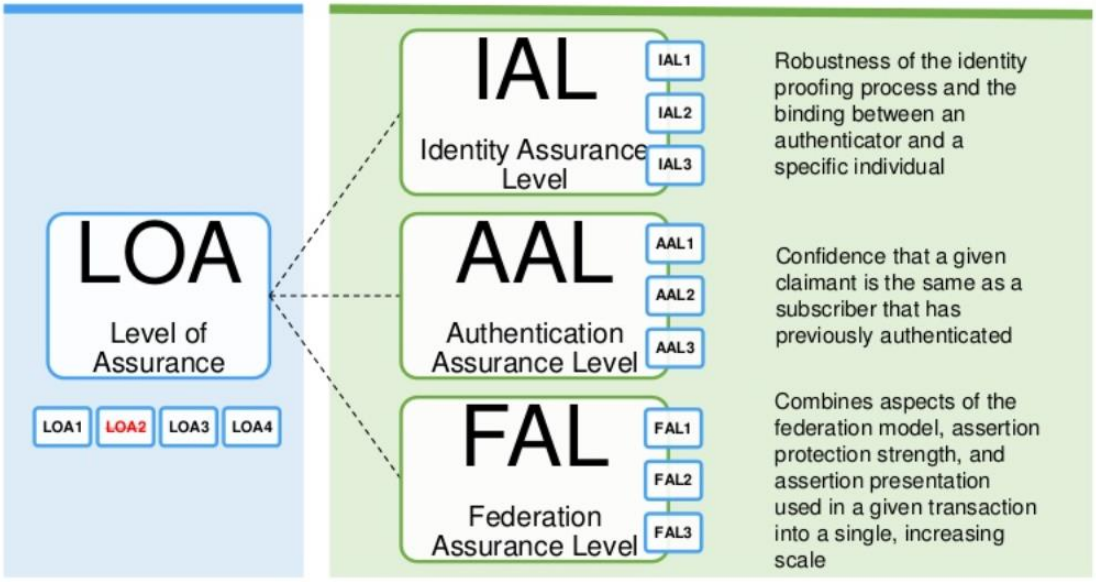
貳、內容

最新版本的數位身分指引刪除了原先四種保證等級的概念（LoA1、LoA2、LoA3、LoA4），而改為身分保證等級（Identity Assurance Level, IAL）、驗證保證等級（Autheticator Assurance Level, AAL）以及聯盟保證等級（Federation Assurance Level, FAL）。

[35] NIST, Special Publication(SP)800-63-3, P. i, https://www.nist.gov/itl/tig/projects/special-publication-800-63 (last visited July. 23, 2020).
[36] 3 CFR 13681 - Executive Order 13681 of October 17, 2014. Improving the Security of Consumer Financial Transactions, https://www.govinfo.gov/content/pkg/CFR-2015-title3-vol1/pdf/CFR-2015-title3-vol1-eo13681.pdf
[37] NIST 於 2017 年公布的版本為 SP 800-63-3，轄下三個子文件分別為 SP 800-63A《註冊與身分證明》（Entrollment & Identify proofing）、SP 800-63B《驗證與生命週期管理》（Authetication & Lifecycle Management）及 SP 800-63C《聯合與斷言》（Federation & Assertion）。
[38] *Supra* note 35.

DOI:10.6814/NCCU202001680

IAL 是指身分證明過程中識別個人身分的可靠性；AAL 是指身分驗證過程中驗證個人身分的可靠性，以及身分憑證（authenticator）與個人身分屬性之間聯繫的緊密性；FAL 是指聯盟身分管理模式[39]中，身分提供方（Identity Provider, IdP）提供給身分接受方（Relying Party, RP）有關使用者身分資訊的可靠性[40]。



來源：FIDO Alliance[41]

這些類別區分為機構提供了選擇身分解決方案的靈活性，並增強了在任何保證級別將隱私增強技術作為身分系統基本要素的能力。舉例來說，此指引支持在使用多因素驗證的情況下，也允許匿名。除此之外，此指引還要求聯盟身分提供者在探詢資料時能夠支持範圍較大的選項，例如回答一個人是否比特定年齡大，而不是直接給定整個出生日期，從而鼓勵最大限度地減少身分資訊的傳播。儘管

[39] 聯盟身分管理模式（Federated Identity Management）：不僅能實現跨多個服務提供者間的互通性需求，還可實現跨多個身分管理系統的互通性需求。這類模式的特點是聯盟內的服務提供方將協定認可一套技術標準，使用者使用其中一個服務提供方 A 所頒發的身分憑證驗證身份後，該服務提供方 A 對身分的驗證結果將在聯盟內進行共用，其他服務提供方可直接獲取用戶在 A 中的特定公開資訊及 A 對用戶的身分驗證結果（Open ID），或直接獲取來自用戶的授權，允許其擁有對 A 身分管理系統中有關使用者資訊的使用權限；陳徽，歐盟與美國電子身份管理立法比較研究，暨南大學碩士學位論文，2018 年，頁 25。

[40] *Id.*

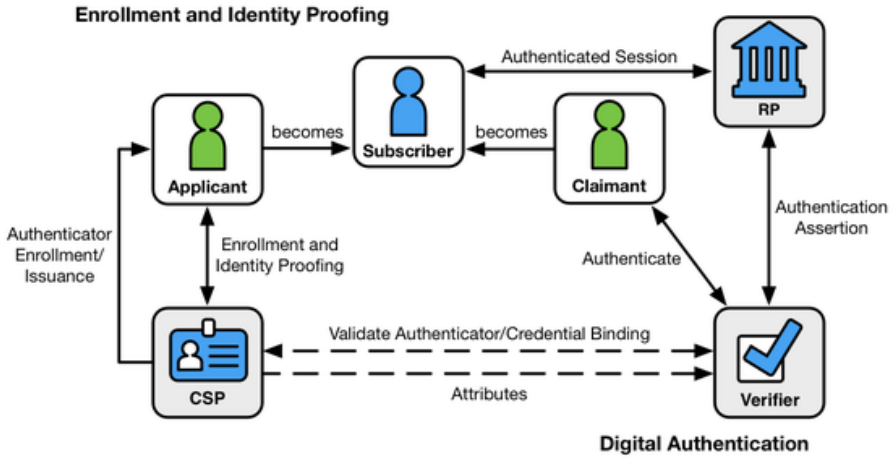
[41] FIDO Alliance, https://www.slideshare.net/FIDOAlliance/nist-80063-guidance-fido-authentication (last visited July. 23, 2020).

DOI:10.6814/NCCU202001680

許多機構要求對個人進行完全識別，但此指引鼓勵在可能的情況下，甚至在需要完全識別的情況下，都應以假名的方式存取政府數位服務，從而盡可能地限制蒐集個資[42]。

一、身分保證等級（IAL）

身分保證等級	
1	僅僅是自我聲稱（Self-asserted）的身分，或被視為是自我聲稱的。
2	需要以遠程（remote）或面對面（in-person）的方式進行身分證明；此層級要求身分屬性之驗證（verified）程序，已至少符合 SP 800-63A 之規定。
3	需要以面對面的方式進行身分證明;身分屬性必須由經授權的身分提供方透過檢查物理文件（如 SP 800-63A 中所述）的方式進行驗證。



來源：NIST[43]

二、驗證保證等級（AAL）

驗證保證等級	
1	對於身分主張者（claimant）控制著一個經註冊的身分憑證有一定程度的確信。此層級需要使用單因素驗證。成功的驗證需要身分主張者透過安全的身分驗證協議來證明持有與控制身分憑證。
2	對於身分主張者控制著一個或多個經註冊的身分憑證有高度確信。需要身分主張者透過安全的身分驗證協議來證明持有與控制兩種不同的驗證因素。層級 2 及更高層級需要使用被認可的加密技術。

[42] *Supra* note 35, at v.
[43] *Id*. at 10.

DOI:10.6814/NCCU202001680

3	對於身分主張者控制著一個或多個經註冊的身分憑證有極高的確信。層級 3 的驗證是基於身分主張者通過加密協議來證明持有密鑰。層級 3 與層級 2 一樣需要使用被認可的加密技術，但層級 3 要求更高，使用的須是更安全的密碼學身分憑證以使身分驗證足以對抗偽裝攻擊（provides verifier impersonation resistance）。

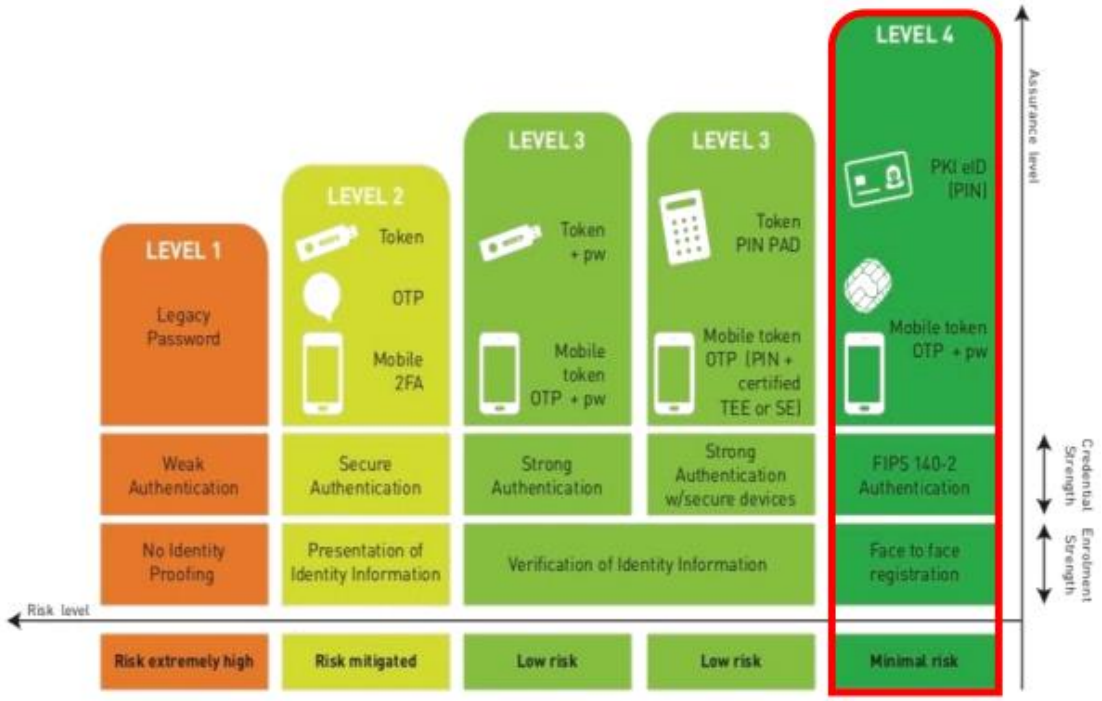
三、聯盟保證等級（FAL）

聯盟保證等級	
1	允許身分接受方（RP）從身分提供方（IdP）獲取用戶的身分斷言（bearer assertion）。身分提供方必須使用被認可的加密方式簽署該身分斷言。
2	附加要求身分提供方所使用的被認可的加密方式，應確保加密的身分斷言僅能為身分接受方所解密。
3	要求請求身分斷言的用戶（subscriber）出示證據證明其擁有與所請求之身分斷言本身相關聯的加密密鑰。該身分斷言同樣應經身分提供方使用被認可的加密方式所簽署，並僅由身分接受方所解密。

第三節 ISO /IEC 29115

國際標準化組織（International Organization for Standardization, ISO）制定了 ISO/IEC 29115 個體驗證信賴框架（Entity authentication assurance framework），提供管理用戶身分驗證的框架，將信賴保證依強弱分為四個等級，為每個定義的級別規定了標準和準則。

DOI:10.6814/NCCU202001680



來源：ISO/IEC 29115

ISO/IEC 29115 將身分驗證分為三個部分，分別是登錄（Enrollment）、信物管理（Credential management）以及驗證機制（Entity authentication），依各應用之特性、失敗後帶來之風險、影響，選擇所適合對應之信賴保證等級。

保證等級	敘述	目的	控制
1 –低	對所宣稱的身分沒有多大的信心或沒有信心	身分在上下文中是唯一的	自我主張（Self-asserted）
2 -中	對所宣稱的身分有些許信心	身分在上下文中是唯一的；以及身分所屬的實體屬於客觀存在	通過使用來自權威來源的身分資訊來證明身分
3 –高	對所宣稱的身分有高度信心	身分在上下文中是唯一的，與該身分相關的實體是客觀存在的，身分經過驗證，並且在其他上下文中使用了身分	通過使用來自權威來源的身分資訊+驗證來證明身分
4 -非常高	對所宣稱的身分有非常高度信心	身分在上下文中是唯一的，與該身分相關的實體是客觀	通過使用來自權威來源的身分資訊+驗證+親自現身

DOI:10.6814/NCCU202001680

		存在的，身分經過驗證，並且在其他上下文中使用了身分	來證明身分

第四節 FATF 客戶盡職調查與數位身分指引

防制洗錢金融行動工作組織(Financial Action Task Force on Money Laundering, FATF)成立於 1989 年，為七大工業國組織成員組成的政府間國際組織，為世界上最重要打擊洗錢的國際組織之一，旨在樹立標準並促進國際防制洗錢及打擊恐怖分子行動，於 1990 年提出「關於洗錢犯罪問題之 40 項建議」，作為國際反洗錢犯罪之基礎原則，該建議對於反洗錢之各國國內立法、金融機構規範與國際間相互合作等事項提出建議與行為準則，其後於 2012 年 2 月將原 40 項建議整合了 9 項打擊資恐特別建議，整併為新的 40 項建議[44]。

隨著新型態金融資產與服務的出現，FATF 不斷修改其建議內容。而數位支付以每年約 12.7%的速度增長，預計在 2020 年將達到每年 7,260 億筆交易[45]，到了 2022 年，預估全世界 GDP 的 60%將會數位化[46]。對於 FATF 而言，如何在數位金融服務領域裡識別和驗證個人是一個新的挑戰。數位身分的技術正在迅速發展，從而衍伸出各種數位身分系統，因此 FATF 在 2020 年 3 月推出了數位身分指引（Guidance on Digital Identity），旨在協助政府、受監理實體（regulated entities）[47]和其他利害關係人於利用數位身分驗證機制下，滿足 FATF 之客戶盡職調查

[44] CAMS 第六版，頁 88-89。
[45] Capgemini & BNP Paribas (2018), World Payments Report 2018, https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/WorldPayments-Report-2018.pdf (last visited July. 23, 2020).
[46] International Data Corporation (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predictions
[47] 在此指引中「受監理實體」是指金融機構、虛擬資產服務提供者（virtual asset service providers, VASPs）以及 FATF 標準中所定義的指定之非金融事業或人員（designated non-financial businesses and professions, DNFBPs）。

DOI:10.6814/NCCU202001680

（customer due diligence, CDD）要求[48]。

所謂受監理實體，最主要的規範對象就是金融機構，因此本節將以金融機構為主體，介紹 FATF 為了防制洗錢及打擊資恐所要求的客戶盡職調查內容為何，再進一步講述 FATF 因應數位化發展，此次所推出的數位身分指引之主要內容。

壹、FATF 第 10 項建議－客戶盡職調查[49]

一、通則

根據 FATF 的建議，所有具防制洗錢及打擊資恐義務的金融機構都必須執行 CDD 措施，包括辨識和驗證客戶的身分，當：

（一）建立業務關係時[50]；

（二）超過美元／歐元 15,000 之臨時性交易，或是第 16 項建議註釋所涵蓋之電匯交易；

（三）發現疑似洗錢或資恐；或

（四）金融機構對於其過去取得客戶身分資料之真實性或妥適性有所懷疑。

此外，金融機構必須使用風險基礎方法以：

（一）確定客戶身分，並利用可靠、獨立來源之文件、資料或資訊以識別客戶及驗證客戶身分。禁止匿名或使用明顯的假名開立帳戶。

---

[48] FATF, Guidance on Digital Identity, p. 5, ttp://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf (last visited July. 23, 2020).

[49] FATF, The FATF Recommendations, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (last visited July. 23, 2020).

[50] FATF 的建議並不定義這個概念，而是留給各國決定業務關係是否成立。

DOI:10.6814/NCCU202001680

（二）辨識實質受益人及採取合理措施確認實質受益人身分，藉此知悉誰是實質受益人。對於法人及法律協議，應涵蓋金融機構採取合理措施瞭解該客戶之所有權及控制權結構；

（三）瞭解並在適當情形下取得有關業務往來關係之目的及性質之資訊；

（四）對客戶業務往來關係進行持續性審查及對其所從事交易之全部過程進行詳細的審視，以確保所進行之交易符合該機構對客戶、業務往來及風險之認知，必要時包括其資金來源。

金融機構在進行 CDD 時，區分「客戶識別」和「驗證客戶身分」是必須的。客戶識別，在於蒐集（未來的）客戶資訊以辨識他／她，在這個階段，無需徵提身分證明文件。相反的，驗證客戶身分需要使用可靠、獨立來源的文件、資料或資訊以印證在辨識過程中所獲得的資料的真實性[51]。

二、客戶身分識別[52]

FATF 的建議並未詳細說明企業在防制洗錢及打擊資恐的義務下，於建立標準的業務關係或 15,000 美元／歐元以上的臨時性交易時，所應蒐集用以妥適執行身分識別的具體客戶資訊。各國立法各不相同，但共同的客戶資料往往包括姓名、出生日期、地址和辨識號碼（例：身分證字號）。其他類型的資料（如客戶的職業、收入、電話和電子郵件地址等）一般都是為了商業或防制詐欺需求，並非是客戶審查時所要求的核心客戶資訊，雖然這些資訊可以適當地增強高風險情況的客戶審查。

FATF 的建議允許國家的法律或規範將風險基礎方法運用於建立業務關係

[51] FATF, Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, ¶ 66, http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf (last visited July. 23, 2020).
[52] *Id*, ¶¶ 75-76.

DOI:10.6814/NCCU202001680

時必須蒐集到的客戶資料，但必須權衡其標準，因為如果識別過程過於精簡，監控僅能有限的減輕風險，且人工或電子過濾交易可能無法有效地辨識個別可疑活動。

三、客戶身分驗證[53]

FATF 的建議要求金融機構使用可靠、獨立來源的文件、資料或資訊來驗證客戶的身分。在決定可靠性和文件的獨立程度時，各國應考慮到在特定國家詐欺和偽造的潛在風險，確認哪些可以構成其防制洗錢及打擊資恐制度下的「可靠、獨立來源的文件、資料或資訊」是每個國家的責任。在身分驗證方式和時點上，運用風險基礎方法可以引入一定程度的靈活性。

業界指出，在所有情況下客戶身分驗證階段是最困難和繁重的一部分。嚴格的驗證要求可能戕害普惠金融。世界銀行指出，最近的調查顯示缺少身分文件是受訪者對未開立銀行帳戶最常提到的主要原因之一，尤其是在需要大量或正式的政府發行文件的國家。

為了解決這樣的挑戰，多數國家已經擴大了可接受用以身分驗證程序的證件範圍，這些文件包括過期的外國證件、領事文件或其他無證人員通常可於居住國取得的紀錄（帳單、稅務證明、醫療文件等）。使用風險基礎方法，當地主管機關通常對於事先定義的業務類型，以及具有低餘額的特定（普惠金融）產品及帳戶，允許更廣泛的文件。各國應採取風險基礎方法的優勢，施以相稱的可接受證件的要求，以支持提供相關服務給這些次級銀行用戶（underbanked）的族群。

四、非面對面進行之身分識別[54]

運用創新科技對提供金融服務給次級銀行用戶和偏遠人口是一種具發展潛

[53] *Id*, ¶¶ 77-79.
[54] *Id*, ¶¶ 86, 89.

DOI:10.6814/NCCU202001680

力的管道。在這方面，行動銀行和行動支付在過去幾年已顯著發展，尤其在開發中國家，具有重大的潛力以方便沒有銀行帳戶人士獲取基本服務。根據世界銀行，四分之三的全球居民有使用手機，而行動電話用戶（50 億）絕大多數是在開發中國家。在非洲撒哈拉以南的地區，蓋洛普全球民調的調查表示，16%成年人在過去 12 個月中曾使用手機支付帳單或匯款。雖然行動銀行提供普惠金融的可能性，目前，它主要是支付和轉帳服務。這雖已提供正規金融服務有效的第一步，但還不能提供全面的銀行或其他金融服務。

對金融機構而言，非面對面的業務關係或交易潛藏較高風險，應權衡身分詐欺風險與洗錢資恐風險，以個案評估新開戶客戶是否應採用強化的 CDD 措施。就開戶階段辨識低風險客戶而言，金融機構必須對其客戶同樣採用有效的程序。在許多情況下，雖然沒有直接與金融機構面對面，第三方或代理人仍參與了開戶手續。在這種情況下，與代理人及第三方有關的原則仍適用之。部分國家的情況下，金融機構仍要求客戶寄回身分證明文件的數位影本，一旦驗證完成，該帳戶才會啟用。

貳、數位身分指引

此指引旨在幫助政府機構更加了解數位身分制度是如何運作的，並闡明如何在全球反洗錢及打擊資恐的標準下使用它們。主要聚焦於 FATF 第十項建議（客戶盡職調查），亦即開戶時使用數位身分進行身分識別與驗證，是否有依照 FATF 第十項建議(a)點「金融機構必須使用風險基礎方法以確定客戶身分，並利用可靠、獨立來源之文件、資料或資訊以識別客戶及驗證客戶身分」之要求[55]。另外必須合先敘明的一點在於，此指引只談到自然人之身分識別與驗證[56]。

[55] FATF, Guidance on Digital Identity, ¶ 42, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (last visited July. 23, 2020).
[56] *Id*, ¶ 44.

DOI:10.6814/NCCU202001680

一、FATF 第十項建議(a)點及(d)點

（一）身分證明文件不拘形式，包含物理以及數位形式[57]

（二）「可靠、獨立來源的」身分證明[58]

對於反洗錢及打擊資恐的目的而言，決定現有的數位身分證明文件是否可靠且來源獨立，保證水準就派上用場了。在數位身分的脈絡下，數位形式的「文件、資料或資訊」必須「可靠、獨立」的要求意味著，用來執行客戶盡職調查的數位身分依靠技術、適當的治理、流程和程序，對於結果的準確程度有適當程度的信心。

（三）使用風險基礎方法進行客戶盡職調查[59]

根據 FATF 第十項建議及其註釋，受監理實體被要求辨識及評估洗錢及資恐風險，並採取適當措施以控管或降低風險，亦即在高風險的情況下，必須加強客戶盡職調查，反之在低風險的情況下，應簡化客戶盡職調查。

在評估風險時，受監理實體應在確定總風險和應採取的適當緩解措施之前，考慮所有相關風險因素，並根據各種風險因素的風險類型和級別來區分執行客戶盡職調查的程度（例如，在特定情況下，與客戶建立業務關係時使用一般的客戶盡職調查措施，而在持續監控交易的情形下採行加強的客戶盡職調查，反之亦然）。

此外，雖然註釋中提及非面對面的業務關係或交易潛藏較高風險，但不代表非面對面的業務關係或交易就一定被視為高風險[60]。有鑑於數位身分技術之進步，必須釐清一點，非面對面的客戶識別以及交易若是依據可靠且獨立來源的數位身

[57] *Id*, ¶ 79.
[58] *Id*, ¶ 84.
[59] *Id*, ¶¶ 85-86.
[60] *Id*, ¶ 88.

DOI:10.6814/NCCU202001680

分，並同時採取適當的措施以控管或降低風險，此種情形可能會是一般風險等級，又或是若實施更高的保證水準和/或適當的洗錢及資恐風險控制措施，甚至可能會降低風險[61]。

（四）就業務關係進行持續的盡職調查

對於受監理實體，對既有客戶進行持續的身分驗證可提供合理的確信，即今天主張該身分的人與之前開設帳戶或其他金融服務的人相同，也就是與開戶時進行可靠且獨立來源之身分識別和驗證的人實際上是同一位。

二、使用風險基礎方法進行客戶盡職調查時，評估數位身分是否足夠可靠且獨立

在決定數位身分的使用是否符合 FATF 第十項建議(a)點及(d)點時，政府、金融機構以及其他利害關係人必須進行以下評估[62]：

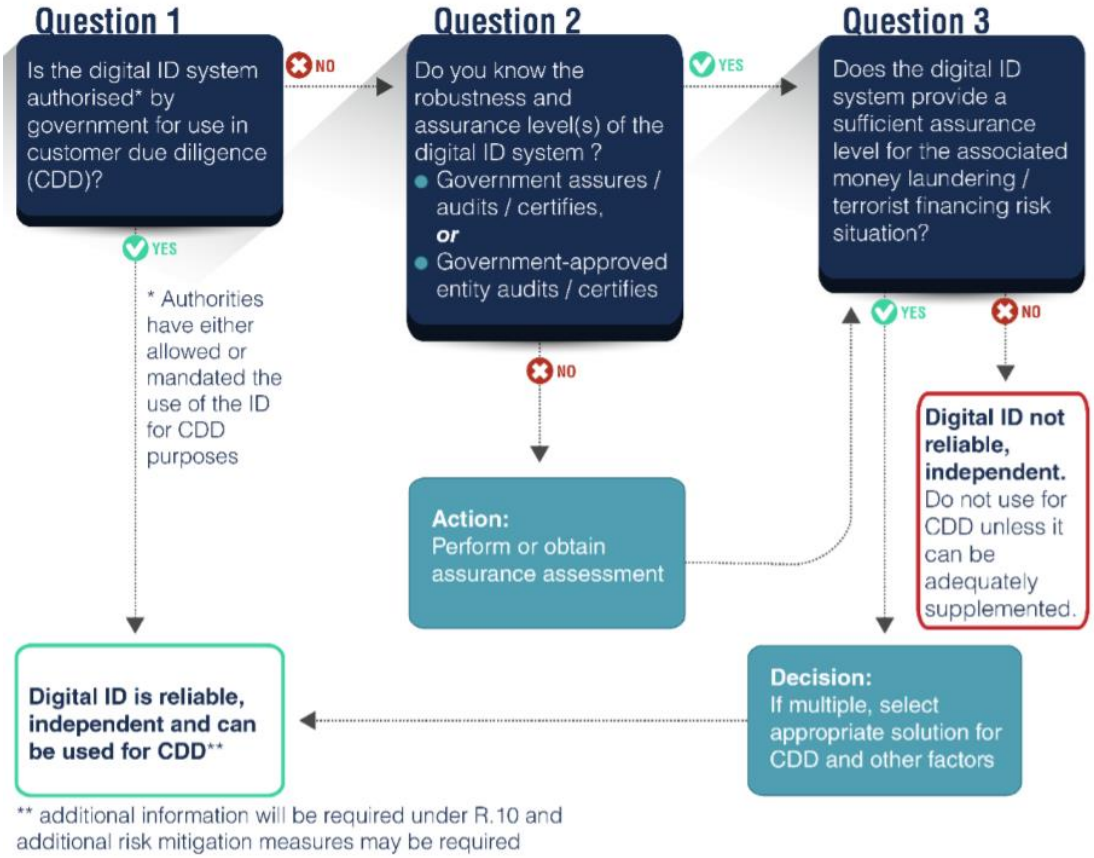
（一）根據數位身分系統之技術、體系結構和治理，了解其保證等級，以確定其可靠性/獨立性；

（二）根據數位身分之保證等級，基於潛在的洗錢、資恐、詐欺或其他非法融資風險來決定數位身分系統是否適當的可靠以及獨立。

在特定的司法管轄範圍裡，根據數位身分系統和規範框架，政府和受監理實體在評估身分系統的保證等級及所採行的 CDD 措施適當性時，可能具有不同的角色和責任，受監理實體的決策流程圖如下圖所示：

[61] *Id*, ¶ 89.
[62] *Id*, ¶ 139.

DOI:10.6814/NCCU202001680



1.問題一：政府是否允許或透過法律強制使用數位身分系統來進行客戶盡職調查[63]？

若是政府「支持」數位身分系統，並認為它適合在客戶盡職調查中使用，受監理實體可以使用數位身分系統，而無需執行問題二和問題三中的評估。

各國政府可以通過發布法規或向受監理實體提供指引之方式，來明確指出其允許或要求受監理實體在客戶盡職調查中使用數位身分系統。各國政府應對其數位身分系統的運作方式及其相關保證等級保持透明公開。

2.問題二：數位身分系統的相關保證等級[64]？

如果政府未明確或暗中授權使用數位身分系統來進行客戶盡職調查，則受監

[63] *Id*, ¶¶ 144-146.
[64] *Id*, ¶¶ 147-151.

DOI:10.6814/NCCU202001680

理實體必須先為正在考慮採用的數位身分系統確定其保證等級，亦即決定數位身分的每一個階段流程的可靠性或確信程度。

如果政府直接或透過指定相關組織來保證、稽核或認證（assures, audits or certifies）數位身分系統，則受監理實體可以依靠政府或該組織之評估來回答決策過程中的問題二。政府也可以同意國內外的專家機構[65]測試/稽核並認證受監理實體可能採用的數位身分系統之保證等級。

如果政府既未授權在客戶盡職調查中使用數位身分系統，也未提供來自於官方對於數位身分系統保證等級的資訊，則受監理實體必須通過以下任一項來確定系統本身的可靠性和獨立性：1.自己進行保證評估；或 2.使用專家機構稽核或任證過保證等級的資訊（儘管未經政府正式核准）。

3.問題三：數位身分系統是否適合洗錢及資恐風險的情況[66]？

若受監理實體透過問題二中所述的過程，得到數位身分系統的保證等級，就應根據相關非法金融風險，分析數位身分系統是否足夠以 FATF 所要求之風險基礎方法來進行客戶盡職調查。

換句話說，鑑於潛在的洗錢及資恐風險，根據採取的保證等級，數位身分系統是否適合用來確認客戶身分以及進行持續的盡職調查？受監理實體應在相關非法金融風險的背景下，分析數位身分系統（基於其保證等級）是否適當。

根據國家的防制洗錢及打擊資恐要求和可用的數位身分系統，受監理實體可以選擇不同保證等級以進行身分證明和身分驗證。在這種情況下，受監理實體應根據潛在非法活動類型和洗錢及資恐風險，來相應決定身分證明和身分驗證的可靠性程度。

[65] ISO, ITU, W3C, FIDO, OIDF, GSMA 等機構，詳細請參考指引附錄 D。
[66] *Id*, ¶¶ 152-153.

DOI:10.6814/NCCU202001680

第五節 數位經濟夥伴協定

新加坡貿工部長陳振聲於 2020 年 6 月 12 日透過視訊會議，與紐西蘭貿易及出口增長部長派克（David Parker）和智利外交部長特奧多羅·里貝拉（Teodoro Ribera Neumann），以電子方式簽署了數位經濟夥伴協定（Digital Economy Partnership Agreement, DEPA）[67]。

壹、背景

DEPA 係全球首個聚焦於促進數位經濟發展的國際合作協定，目的係改善現有貿易規則無法完全因應數位化時代，並解決數位貿易所帶來新問題；該協定將能提高效率和節省成本，有利相關經濟體和業者取得競爭優勢，並與新加坡現有自由貿易協定相輔相成。其重要主題及內容包括： 數位貿易之便捷化：數位身分認證(Digital Identity)、無紙化貿易(Paperless Trade)、電子發票(E-Invoicing)、金融科技與電子支付(Fintech and E-payment)、 資料之跨境流通與創新：個資保護(Personal Information Protection)、跨境資料流通(Cross-border Data Flows)、政府公開資料(Open Government Data)、資料創新與法規沙盒機制(Data Innovation and Regulatory Sandboxes)、 建構值得信賴的數位環境，促進中小企業及民眾之數位參與程度：人工智慧(AI)、線上商業活動之消費者保護(Online Consumer Protection)、中小企業合作(SME Cooperation)及擴大數位涵蓋範圍(Digital Inclusivity)等[68]。

貳、內容

[67] 駐新加坡台北代表處，「新加坡、紐西蘭和智利簽訂數位經濟夥伴關係協議(DEPA)」，https://www.taiwanembassy.org/sg/post/29695.html（最後瀏覽日：2020 年 7 月 23 日）。

[68] 經濟部國際貿易局，「新加坡、紐西蘭及智利宣布完成數位經濟夥伴協定（Digital Economy Partnership Agreement, DEPA）談判，並預計於 2020 年 4 月簽署」，https://www.gov.tw/News_Content.aspx?n=872E51DB9B88306C&sms=53E09032BF601A56&s=6966B4C8347F7285（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

第 2.7 條第 2 項(d)：締約國應努力實現使用數位身分進行個人和企業的跨境身分驗證以及電子 KYC。

第 7 條就數位身分做進一步的規範，第 7.1 條：認識到締約國在個人或公司數位身分方面的合作將增加區域和全球的聯繫，並認識到每個締約國對數位身分可能有不同的實現方式和法律方法，每一締約國應努力促進各自數位身分制度之間的交互操作可能性。包含：

一、建立或維護適當的框架，以促進締約國間數位身分之技術交互操作可能性或通用標準；

二、在每個締約國各自的法律框架下，提供相應的數位身分保護，或者承認數位身分的法律和規範效果，無論是自主還是通過彼此同意；

三、建立或維持更廣泛的國際框架；及

四、就數位身分之政策和法規進行技術實施、安全標準以及使用者採用之最佳實踐及知識交流。

參、特性

DEPA 的協定設計非常特別，透過模組化的設計將不同主題區分成一個個模組（Module），締約國可以選擇直接適用 DEPA，或是自行決定在何種環境中全部或部分適用模組。其中包括直接將 DEPA 納入其他貿易協定中，或選擇使國內政策與 DEPA 保持一致[69]。

[69] Asian Trade Centre, *Unpacking the Digital Economy Partnership Agreement (DEPA)*, http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa (last visited July. 23, 2020).

DOI:10.6814/NCCU202001680

第四章 數位身分於我國銀行業之法規與應用

我國金管會自 2015 年起推動「打造數位化金融環境 3.0」，已開放銀行既有客戶得於線上辦理存款、授信、信用卡、財富管理、共同行銷等多項服務[70]，為因應金融科技快速發展，銀行金融服務有再以數位化方式增進效率及便捷之空間，因此在風險可控管、消費者權益受保障之前提下，利用科技、結合創新，發展多元線上金融服務，並依銀行業務需要，陸續新增相關開放項目，舉例來說自 2019 年起開放新戶線上申貸等業務，並且開放「7 歲領有身分證的未成年人」、「持有居留證且年滿 20 歲的外國人、一人獨資公司的法人」都可線上開立數位帳戶[71]。

隨著科技的進步，消費者得以數位方式使用越來越多的金融服務，我國法規亦相應規範之，因此本章將概述我國銀行業應用數位身分之相關法規。

第一節 數位身分於我國銀行業之相關法規

目前我國對數位身分之管理並沒有相關專法之規範，也沒有任何辦法、注意事項、作業規範或是作業範本可茲參考，但是針對不同的業務仍有相應的規範及安控基準可以遵循，像是本文所探討之數位身分在銀行業之應用，則有若干法規規範之，以下則以開立數位帳戶為中心，介紹可能涉及之規範。

壹、銀行受理客戶以網路方式開立數位存款帳戶作業範本

我國自 2015 年即開放銀行業受理客戶線上開戶，依「銀行受理客戶以網路

[70] 金融監督管理委員會，「銀行線上服務全面升級」，網址：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201905140002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News（最後瀏覽日：2020 年 7 月 23 日）。

[71] 金融監督管理委員會銀行局，「未來獨資組織、本國未成年人及外國成年人符合一定條件將可直接透過網路開立存款帳戶」，網址：ps://www.banking.gov.tw/ch/home.jsp?id=169&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201911280002&toolsflag=Y&dtable=News（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

方式開立數位存款帳戶作業範本」，數位存款帳戶依身分認證強弱與不同使用範圍分為三類，功能最全面的「第一類帳戶」需使用自然人憑證完成驗證後，才能完成開戶，少數銀行再依有無透過視訊驗證進而區分帳戶的交易限制[72]；而「第二類帳戶」是透過既有之自行銀行帳戶或金融支付工具完成驗證，「第三類帳戶」則是他行存款客戶、或既有之自行信用卡客戶於線上開立之帳戶，後兩類帳戶雖有驗證流程較簡便的優點，但使用範圍及交易額度亦大幅受限[73]。

除了就帳戶類型做分類之外，此作業範本尚針對客戶審查作業、帳戶管理、帳戶使用原則、結清銷戶作業以及持續監控措施等等做出了細部規範。

貳、金融機構辦理電子銀行業務安全控管作業基準

根據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[74]與非電子轉帳及交易指示類[75]，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[76]，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，以下表格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[77]：

[72] 彰化商業銀行將第一類數位帳戶依有無透過視訊驗證之差別，區分交易限制：若有，則非約定轉帳無交易限制，且此類型客戶可使用電子憑證作為網路銀行轉帳安控機制；若無，則每筆非約定轉帳交易最高限額為新臺幣 5 萬元、每日累計最高限額為新臺幣 10 萬元、每月累計最高限額為新臺幣 20 萬元。

[73] 第二類數位帳戶之每筆非約定轉帳交易最高限額為新臺幣 5 萬元、每日累計最高限額為新臺幣 10 萬元、每月累計最高限額為新臺幣 20 萬元；第三類數位帳戶之每筆非約定轉帳交易最高限額為新臺幣 1 萬元、每日累計最高限額為新臺幣 3 萬元、每月累計最高限額為新臺幣 5 萬元。

[74] 電子轉帳及交易指示類係指該交易指示直接涉及資金轉移或直接影響客戶權益者。

[75] 非電子轉帳及交易指示類係指與資金轉移無關或不直接影響客戶權益之服務項目。

[76] 高風險交易係指該訊息執行結果對客戶權益有重大影響；低風險交易則係指該訊息執行結果對客戶權益無重大影響。

[77] 表格說明：必要（Mandatory）係指金融機構必須具備該項防護措施；非必要（Conditional）係指金融機構得視情況自行決定是否需要具備該項防護措施。

DOI:10.6814/NCCU202001680

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，安控基準針對金融機構就通訊傳輸時應達到之安全防護措施之設計方法做出規範，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，整理如下：

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

DOI:10.6814/NCCU202001680

參、金融機構運用新興科技作業規範

銀行公會為協助銀行適當管理運用新興科技之風險，以促進銀行業務健全經營，特定訂「金融機構運用新興科技作業規範」。此規範主要分為四大類，分別是雲端服務安全控管、社群媒體控管程序、自攜裝置安全控管以及生物特徵資料安全控管。就數位身分而言，「生物特徵資料安全控管」即為本節之重點。

第二章曾提及生物特徵可作為識別及驗證身分之因素，此規範則進一步規定銀行業使用此類資料時，應盡之義務。像是運用生物特徵資料作為識別客戶身分時，其蒐集、處理及利用之行為，應納入個資管理機制；蒐集生物特徵資料時，應取得客戶同意，並讓客戶充份了解所蒐集之目的及方式；生物特徵資料儲存於銀行內部系統時，應將原始生物特徵資料去識別化使其難以還原、將原始生物特徵資料及假名標識符進行加密儲存、將生物特徵資料分別儲存於不同之儲存媒體（如資料庫）；以及應確保生物特徵資料於傳輸過程中之訊息隱密性、完整性、不可重複性及來源辨識性，相關控管應符合「金融機構辦理電子銀行業務安全控管作業基準」等等。

第二節 數位身分於我國銀行業之應用

「普惠金融全球合作夥伴組織」（Global Partnership for Financial Inclusion，GPFI）指出，數位身分自首次開戶（Onboarding）」、客戶盡職調查（Customer due diligence，CDD），乃至個別交易確認放行均有應用空間[78]。

本節將簡單介紹目前我國銀行業實務上應用數位身分之時機，大致區分為開戶、客戶盡職調查、驗證身分等。

[78] THE GLOBAL PARTNERSHIP FOR FINANCIAL INCLUSION-GPFI, *G20 Digital Identity Onboarding*, https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf (last visited July. 23, 2020).

DOI:10.6814/NCCU202001680

壹、開戶

「銀行受理客戶以網路方式開立數位存款帳戶作業範本」規範了不同種類之數位帳戶得採用之驗證方式，各家銀行得再依據自身風險評估後自行決定開放哪些種類的數位帳戶或是哪些種類之驗證方式，舉例而言，某些銀行並無開放第一類數位帳戶之開立，或是未採用以既有之自行信用卡驗證之方式開立第三類數位帳戶。

貳、客戶盡職調查

金融機構為有效防制洗錢，應執行客戶盡職調查，至少包括取得客戶資訊、評估客戶風險及辨識、驗證客戶之實質受益人等合理措施。依我國《金融機構防制洗錢辦法》第三條之要求，銀行與客戶建立業務關係時，徵提客戶身分證明文件，並進行客戶資料之審查，就客戶身分作確認，一般稱為「認識你的客戶（Know Your Customer, KYC）」。

以開立數位帳戶為例，銀行於確認客戶身分時，應以可靠、獨立來源之文件、資料或資訊，辨識及驗證客戶身分，並保存該身分證明文件影本或予以記錄。(《金融機構防制洗錢辦法》第三條第四項第一款）因此，要求客戶提供國民身分證正反面影像檔及具辨識力之第二身分證明文件（如健保卡等）影像檔以供備查。

參、身分驗證

我國銀行在確認客戶身分時，可以透過很多不同的方式驗證客戶身分，例如客戶臨櫃辦理業務時，可以透過面對面互動的方式向客戶取得基本資訊，並以紫光燈查驗客戶提供之國民身分證以確認證件之真偽，再至內政部戶政司網站檢核身分證換補發時間地點，核驗該證件是否為最新版本之身分證。

若客戶非臨櫃，而是透過網路與銀行進行業務往來，則此時便是銀行應用數

DOI:10.6814/NCCU202001680

位身分驗證客戶身分的時候，銀行業實務上最常利用的幾個方式茲分述如下。

一、自然人憑證

自然人憑證是由我國內政部憑證管理中心所簽發的數位憑證，「憑證」包含了「數位簽章」跟「公開金鑰」。這個公開金鑰是智慧型的 IC 卡自己演算出來的一組金鑰對中的一半，另一半稱為「私密金鑰」，則永遠儲存在 IC 晶片當中。經由憑證使用人和憑證管理中心約定，使用此憑證即可辨認身分，啟用了加解密的功能，不管在網路上傳什麼資料，資料都被加密，即使駭客攔截了資料也無法輕易的解開[79]。本文的第二章第二節曾提過「數位憑證」，自然人憑證即為一例。

自然人憑證作為台灣官方的網路身分識別機制，讓使用者在網路上作資料交換時，如同網路身分證般辨識身分，因此我國銀行業在驗證客戶身分時，透過官方機構內政部所簽發的自然人憑證，自是最基本的一種驗證方式。

二、生物辨識

我國金融監督管理委員會於 2016 年提出的「金融科技發展策略白皮書」將生物辨識列為金融科技的重大基礎建設之一，銀行應瞭解相關技術如何運作並與相關服務整合，以提供客戶更好的服務。

中華民國銀行公會「金融機構辦理電子銀行業務安全控管作業基準」（以下稱安控基準）第七條交易面之介面安全設計規定，使用憑證簽章得應用於高風險交易，而高風險交易之安全設計可應用於低風險交易；應用於低風險交易之安全設計可應用於身分確認（如簽入作業）。使用晶片金融卡及使用一次性密碼（One Time Password, OTP）則僅限應用於低風險交易；至於使用前述三項之任「兩項以上技術」，也僅限應用於低風險交易，明確闡述了生物辨識技術在金融機構的

[79] 內政部憑證管理中心，「什麼是自然人憑證」，網址：https://moica.nat.gov.tw/what.html（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

使用，即在適當的「兩項以上技術」搭配下，生物辨識技術可以運用在低風險交易及身分確認（簽入作業）上。

2017 年修訂之安控基準更將生物辨識技術增訂「間接」驗證機制，使金融機構可選擇「直接」或「間接」驗證生物特徵。依據安控基準規定：「間接驗證」係指由客戶端設備（如行動裝置）驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。此為我國已經開放金融機構可透過一定的安控機制而信任類似 Apple iPhone 手機指紋、臉部辨識或 Samsung Galaxy S8 虹膜辨識的驗證結果，進而進行低風險交易或簽入作業。反之，「直接驗證」即指自行驗證生物特徵，因此金融機構辦理生物特徵「直接驗證」需從事前述生物辨識技術的感測、擷取、註冊、儲存、比對及決策等程序[80]。

「間接驗證」相較於「直接驗證」具備執行流程簡單、操作簡易及快速完成特性，因此目前我國銀行業主要是利用「間接驗證」生物辨識技術，搭配第 2 項身分認證技術於行動銀行進行客戶身分驗證[81]。

三、透過第三方業者進行身分確認

（一）財團法人金融聯合徵信中心

財團法人金融聯合徵信中心（以下簡稱聯徵中心）是國內唯一的金融信用資訊中心，負責金融機構間信用資料的建置，並對會員機構提供信用資訊查詢服務，以協助促進金融機構間信用交易的健全發展[82]。聯徵中心為了協助會員機構驗證當事人之身分證與內政部戶政司提供予聯徵中心之六項驗證值是否相符，並加強身分確認，開發 Z21「國民身分證領補換資料查詢驗證」及 Z22「通報案件紀錄

[80] 黃世欽，「生物辨識技術與我國金融機構之運用」，銀行公會會訊第 103 期，頁 8-9。
[81] 同上註。
[82] 財團法人金融聯合徵信中心編輯部，紙上談信「當事人信用報告」13 項資訊讓信用一覽無餘，金融聯合徵信雜誌，民國 97 年 1 月號。

DOI:10.6814/NCCU202001680

及補充註記資訊」此兩種產品以防止偽冒開戶等不法情事。

依據銀行公會制定之「銀行受理客戶以網路方式開立數位存款帳戶作業範本」，銀行於客戶申請開立數位帳戶時，必須查詢聯徵中心 Z21「國民身分證領補換資料查詢驗證」及 Z22「通報案件紀錄及補充註記資訊」，藉以檢視當事人有無警示通報在案及防範偽冒開戶情形。

（二）財金資訊股份有限公司

財金資訊股份有限公司（以下簡稱財金公司）是由我國財政部及公、民營金融機構共同出資所籌設，為全國金融資訊與跨行交易處理之樞紐，提供金融帳戶資訊核驗服務[83]。

當客戶於銀行線上申請服務，使用「他行存款帳戶」進行身分驗證時，只要是與財金公司配合「跨行金融帳戶資訊核驗」之機構[84]，皆可透過此方式進行驗證，惟其驗證之存款帳戶需為臨櫃開立（非數位存款帳戶），且開通手機簡訊密碼功能。

（三）財團法人聯合信用卡處理中心

財團法人聯合信用卡處理中心（以下簡稱聯卡中心）是由財政部及公、民營金融機構捐助基金所成立，配合「電子化支付比率五年倍增計畫」政府政策，依據法令規範，以提升金融服務作業效率前提，新增建置「信用卡輔助持卡人身分驗證」平臺，提供電子支付機構及金融機構可接受民眾於線上以「信用卡」進行輔助持卡人身分驗證之機制[85]。

[83] 財金資訊股份有限公司，公司介紹，網址：https://www.fisc.com.tw/tc/profile/index.aspx（最後瀏覽日：2020 年 7 月 23 日）。
[84] 參與之機構名單請參考財金公司：
https://www.fisc.com.tw/tc/business/Detail.aspx?caid=b38613b7-e55d-4841-bba7-25643821fe1f
[85] 財團法人聯合信用卡處理中心，信用卡輔助持卡人身分驗證平臺，網址：

DOI:10.6814/NCCU202001680

當民眾於電子支付機構網站線上註冊及開立第二類或第三類電子支付帳戶時，或於銀行線上開立數位帳戶、申辦信用卡時，將透由送驗機構傳送信用卡資訊至聯卡中心認證平臺，再由發卡機構驗證是否為使用者本人之信用卡支付工具。

來源：財團法人聯合信用卡處理中心[86]

四、行動身分

行動身分亦即 Mobile ID，是新興起的一種數位身分驗證方式，透過載有 SIM 卡的行動裝置，與電信事業連線並驗證過去申辦該行動門號的個人資料[87]。

台灣證券交易所旗下公司台灣網路認證股份有限公司所成立的「TWID 身分識別中心」推出 Mobile ID 行動身分識別服務，透過手機就可以進行實名認證，可以拿來當作網路上的身分證。而 Mobile ID 行動身分識別服務主要是由利用用戶當初向各電信公司申請門號的資料做基礎，透過載有 SIM 卡的行動裝置連線

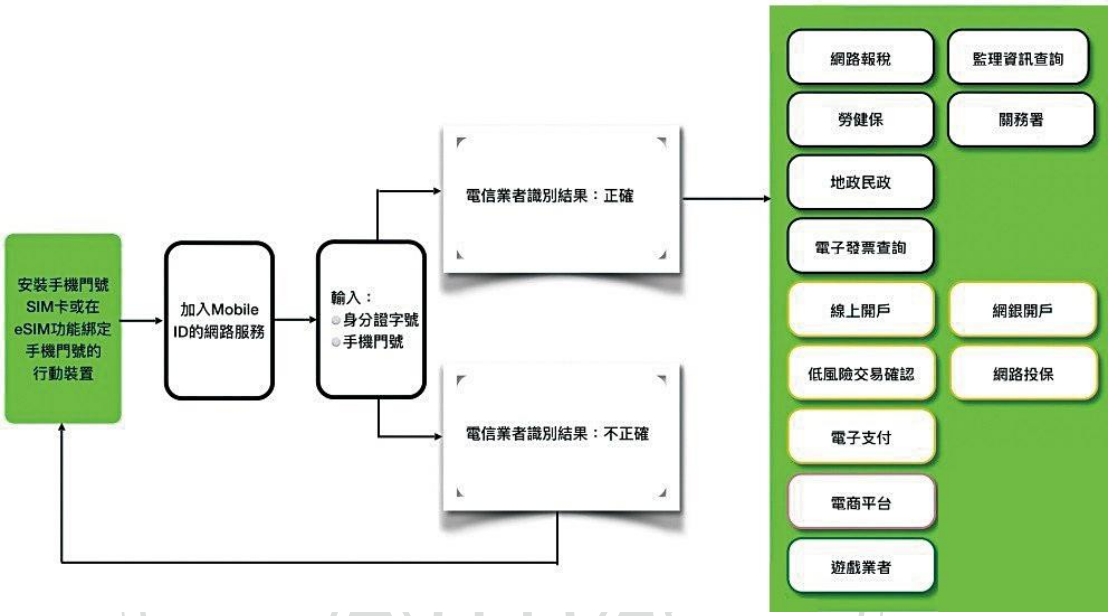
ps://www.nccc.com.tw/wps/wcm/connect/zh/home/BusinessOperations/CardBusiness/CardVerificationPlatform（最後瀏覽日：2020 年 7 月 23 日）。

[86] 同上註。

[87] 協合國際法律事務所，前揭註 3，頁 74。

DOI:10.6814/NCCU202001680

至 Mobile ID 平台發出確認請求，並由「TWID 身分識別中心」向各電信公司查詢門號用戶的基本資料（手機門號及身分證字號），做為電商、行動支付、遊戲業等應用服務商、網路銀行等業者作為用戶身分識別使用，達到實名認證行動化、交易確認行動化[88]。



來源：NCC NEWS 月刊[89]

目前由玉山銀行與 TWID 身分識別中心共同合作，領先推出 Mobile ID 行動身分識別服務，為首家銀行業者也是第 1 家電子支付機構完成導入，提供電子支付會員在進行玉山跨境 e 指購時，可以藉由行動電話門號加強實名身分認證，具有行動化、免臨櫃辦理及跨業別整合等特點，讓顧客享有更快速、便利、安全的數位服務[90]。

[88] 蘇柏毓，前揭註 28。
[89] 同上註。
[90] 數位時代，「玉山銀行首推 Mobile ID 行動身分識別服務」，網址：https://www.bnext.com.tw/article/54939/mobile-id（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

第五章 銀行應用數位身分之操作準則與國際標準之遵循程度分析

雖然我國銀行林立，各家銀行具體採行之做法不一，原則上仍遵照金管會以及銀行公會所訂定之相關規範，或許做法或是安控機制的選擇有些許不同，但相去不遠，因此筆者將先介紹我國銀行業目前應用數位身分識別及驗證客戶身分之普遍做法，再分析我國銀行業目前做法採用的保證等級為何，進而根據所採用的保證等級，來分析使用數位身分進行客戶盡職調查時，是否有合於 FATF 之相關建議。

第一節 銀行識別及驗證客戶身分之做法

根據我國金融機構防制洗錢辦法，識別及驗證客戶身分統稱為確認客戶身分，而確認客戶身分之時機包含臨櫃交易以及非臨櫃交易，由於本文僅討論應用數位身分之情況，故以下介紹完銀行通用之規定與作業流程後，再聚焦闡述應用數位身分確認客戶身分之做法。

根據我國金融機構防制洗錢辦法，確認客戶身分之時機主要在於與客戶建立業務關係時，即與銀行之任一業務為新往來時。而確認客戶身分之方式則必須以可靠、獨立來源之原始文件、資料或資訊，辨識及驗證客戶身分，並保存該身分證明文件影本或予以記錄，如：以「紫光燈」設備驗證客戶之新式國民身分證後，並拍攝證件與人像，留存資料。又確認客戶身分措施，應包括瞭解業務關係之目的與性質，並視情形取得相關資訊，如：確認客戶的任職公司及職稱、資金主要來源是否合法、開戶目的及性質、預計與個案銀行往來之業務等。

所謂身分證明文件除身分證外，尚指其他可資證明身分之有效文件，如健保

DOI:10.6814/NCCU202001680

卡、護照、駕照或學生證等；外國人士或大陸人士如無其他本國核發之身分證明文件，得以當地核發之身分證明文件佐證。

壹、開戶

上述為通則，若是當客戶於線上申請開立數位存款帳戶時，就是銀行必須應用數位身分識別及驗證客戶身分的時候了。以開立流程為例，客戶必須填寫姓名、身分證字號及出生年月日，銀行先行判斷該客戶是否為既有客戶，若是，再輸入留存於該銀行之手機號碼，下一步即以簡訊發送OTP驗證碼至客戶手機之方式，作為初步確認客戶身分之方式（第二類數位存款帳戶）；若客戶非該銀行之既有客戶，客戶必須再輸入欲驗證銀行之機構、驗證銀行帳號以及留存於該行之手機號碼，一樣透過簡訊發送 OTP 驗證碼至客戶手機（第三類數位存款帳戶），惟後者較前者不同之處在於個案銀行是透過財金公司之金融帳戶資訊核驗服務，透過他行帳戶進行客戶身分確認。

初步確認客戶身分後，客戶除填寫開戶基本資料外，尚須上傳身分證正反面照片，以及第二證件之正面照片，客戶送出完整資料後則由銀行進行審核。根據「銀行受理客戶以網路方式開立數位存款帳戶作業範本」，銀行下一步必須查詢聯徵中心「Z21 國民身分證領補換資料查詢驗證」及 Z22「通報案件紀錄及補充註記資訊」，確認客戶是否有短期間內密集/多次新開戶紀錄、受監護/輔助宣告、警示帳戶或衍生管制帳戶、密集開戶或其他異常態樣。

若經判斷皆無異常，接著透過各家銀行之 AML 系統進行姓名檢核及區分客戶風險等級，再依客戶風險等級進行相應之客戶盡職調查，完成後通過審核即成功開立數位存款帳戶。

從前述流程可以歸納開戶時個案銀行識別及驗證客戶身分之做法，包含透過我國官方機構核發之證件以及透過手機號碼發送 OTP 簡訊驗證碼等方式確認身

DOI:10.6814/NCCU202001680

分。

貳、交易

以我國數位存款帳戶為例，經歸納整理後，可透過以下幾種方式進行交易：1.以晶片金融卡搭配晶片密碼透過 ATM/網路銀行/網路 ATM 交易；2.使用 OTP 動態密碼或憑證（e-token）透過網路銀行交易；3.裝置綁定後，透過行動銀行交易。

當客戶進行交易時，銀行如何驗證客戶身分，從上述幾種交易方式歸納分析如下：

1.以晶片金融卡搭配晶片密碼透過 ATM/網路銀行/網路 ATM 交易：當客戶透過 ATM 及網路 ATM 交易時，不需要網路銀行的帳號及密碼，因此使用晶片金融卡以及晶片密碼交易，則是使用兩種驗證因素；而透過網路銀行交易時，登入需要輸入帳號密碼，則是使用三種驗證因素。

2.使用實體OTP 動態密碼或憑證透過網路銀行交易:透過網路銀行交易時，登入需要輸入帳號密碼，使用實體 OTP 動態密碼是會發送一組密碼至實體 OTP 設備，此種方式是使用兩種驗證因素；憑證本身即是一種驗證因素，因此透過此種交易方式也是兩種驗證因素。

3.裝置綁定後，透過行動銀行交易：透過行動銀行交易時，登入需要輸入帳號密碼或是部分手機可以使用生物辨識（如指紋、臉部）登入，再輔以綁定過的裝置也就是手機，因此透過此種方式交易是使用兩種驗證因素。

第二節 銀行採用之保證等級

壹、身分識別

DOI:10.6814/NCCU202001680

就開立數位存款帳戶而言，客戶必須上傳由政府所發行之國民身分證正反面影像以及附有本人照片之第二證件（如健保卡、駕照等）正面影像，銀行再至聯徵中心查詢 Z21 及 Z22，核驗客戶提供之證件資訊是否與內政部資訊相符。

根據 eIDAS、NIST 及 ISO 的規定，依是否出示身分資訊，再依核驗的方式決定保證等級，就銀行之做法，透過遠程以肉眼的方式查看證件影像，再至聯徵中心查詢換補發紀錄，而非透過紫光燈照射物理證件的方式核驗，依 eIDAS 標準對客戶身分有大致（substantial）確信，依 NIST 標準則有 IAL2 之保證等級。

進一步分析客戶必須提供由官方機構所發行之身分證明文件的做法，表示不能使用假名或是匿名開戶，又代表客戶身分必須與現實世界之身分連結，且我國之國民身分證對應每一個國民皆有專屬之編號，因此就官方證件所對應到之客戶會是獨一無二的，因此依 ISO 標準則有 Level 3 之保證等級強度。

在身分識別的階段，僅能由客戶提供之影像核驗，雖然影像有可能被後製或是造假，但是透過查詢換補發紀錄，可以初步排除舊證件遺失或是被不肖之人竊取利用之情形。

貳、身分驗證

一、開戶

在開立數位存款帳戶的情況下，銀行透過客戶留存於本行或他行之行動電話號碼使用 OTP 簡訊驗證碼驗證身分。以筆者服務的銀行為例，目前會檢核客戶留存之行動電話號碼，不同客戶不能留存同一支號碼，此驗證方式得確認當初留存電話之人，與目前收到簡訊者為同一人。此外，客戶變更行動電話號碼必須透過雙因素驗證，例如透過晶片金融卡使用網路 ATM，再輸入晶片密碼，確認無誤後始能變更行動電話號碼，此安控機制是為了加強確認變更行動電話號碼的人

DOI:10.6814/NCCU202001680

為本人，避免詐騙集團輕易使用旗下人頭之行動電話號碼進行變更。

值得留意的是，依據驗證強度的不同區分帳戶類型及相應之交易限額，本行既有客戶為第二類數位帳戶，而透過第三方業者財金公司「金融帳戶資訊核驗服務」以他行臨櫃開立之存款帳戶驗證，則為第三類數位帳戶。

若以 eIDAS 之保證等級分類標準，我國銀行業目前的驗證機制可以對客戶身分有大致（substantial）確信，因 OTP 簡訊驗證碼係採動態方式產生之一次性密碼，亦即當客戶回傳驗證碼給個案銀行時，其身分經過「動態」認證機制可靠地驗證。

若以 ISO 之標準，我國銀行業目前的驗證機制有 Level 3 之保證等級強度，因為銀行是使用曾經留存於本行或他行之行動電話號碼驗證身分，表示客戶過去留存行動電話號碼時已驗證過身分，此次再透過 OTP 簡訊驗證碼確認客戶為同一人。

若以 NIST 之保證等級分類標準，我國銀行業有 AAL2 之保證等級，因為依現行留存行動電話號碼之規定，不同客戶不能留存同一支號碼，行動電話號碼是以客戶之身分證字號歸戶，因此銀行透過客戶留存在自行或他行之行動電話進行驗證，是透過雙因素驗證。惟根據 NIST 最新版本之指引，其認為透過手機簡訊取得 OTP 驗證碼不夠安全，主要原因有 2 個：一是行動裝置的作業系統容易遭受木馬程式的中間人攻擊，進行控制；另一點則是在電信通訊基礎上，傳送簡訊的安全性受到挑戰[91]。

二、交易

我國銀行業之網路銀行及行動銀行業務設計與安全控管均參照主管機關訂

[91] 周峻佑，「透過簡訊執行二次驗證不再安全，美國國家標準技術研究所建議別再使用」，2017 年 3 月 17 日，網址：https://www.ithome.com.tw/news/112845（最後瀏覽日：2020 年 7 月 23 日）

DOI:10.6814/NCCU202001680

定之「金融機構辦理電子銀行業務安全控管作業基準」（以下簡稱安控基準）與「個人網路銀行業務服務定型化契約範本」之規定辦理。

若是在交易的情況下，根據「銀行受理客戶以網路方式開立數位存款帳戶作業範本」，僅有第一類數位存款帳戶得進行高風險交易。由本節前述之歸納可得知，當客戶進行低風險交易時，銀行驗證客戶身分之手段至少採用兩種驗證因素。根據 eIDAS、ISO 及 NIST 有關驗證機制之保證等級分類標準，至少採用兩種驗證因素可被視為有大致確信、Level 3 以及 AAL2 之保證等級，亦即當客戶進行交易時，對於客戶之身分有實質/高度確信。

就 OTP 簡訊碼此種驗證方式做進一步說明，以筆者服務的銀行為例，為了交易安全之考量，已參照 NIST 指引之建議在交易確認方面停用此項服務，而改以裝置綁定的安控機制，然而仍有部分銀行保留此種交易驗證方式。

第三節 銀行操作準則與 FATF 建議之合致性

金融機構被課予防制洗錢及打擊資恐之義務，我國之防制洗錢及打擊資恐相關規範皆參照 FATF 之建議，因此本文主要討論之 FATF 第十項建議客戶盡職調查，亦為我國銀行業所須遵循的，原則上該建議之內容就是我國金融機構防制洗錢辦法第三條之內容。

其實 FATF 數位身分指引之重點就在於應用風險基礎方法使用數位身分進行客戶盡職調查時，必須(1)了解數位身分系統之保證等級及(2)鑑於洗錢及資恐風險，根據採用的保證等級，評估數位身分系統是否可靠及獨立。

雖然 FATF 數位身分指引沒有強制力，僅供大眾參考，但 FATF 作為防制洗錢及打擊資恐的重要組織，針對新科技及新議題所推出之指引，當然需要我們去參考，因此本節將分析我國銀行現行之做法，是否符合 FATF 之建議。

DOI:10.6814/NCCU202001680

就保證等級的部分，前一節已進行初步分析，是以本節將分析第二點，評估數位身分系統是否可靠及獨立。其實筆者不認為目前的台灣有任何完整的數位身分系統，即使內政部有自然人憑證作為網路身分證，但發卡數至今（2020）年 7 月之累計發卡數才 700 多萬張[92]，使用場景仍多為官方導向，如報稅、報關等。即使部分銀行能使用自然人憑證開戶，但限於確認身分，無法從上面取得更多資料，更遑論使用資訊來進行客戶盡職調查。因此本節將僅討論數位身分本身，而不是整個數位身分系統。

根據 FATF 的指引，可用來確認客戶身分之文件、資料或資訊不限於形式，因此銀行使用客戶拍攝之身分證件電子影像檔作為身分證明，並無問題。而數位形式的「文件、資料或資訊」必須「可靠、獨立」的要求意味著，用來執行客戶盡職調查的數位身分依靠技術、適當的治理、流程和程序，對於結果的準確程度有適當程度的信心。

換句話說，係指個案銀行取得客戶之電子文件、資料或資訊時，其過程及驗證身分之機制是否足夠妥適，進而使個案銀行對於客戶身分有適當程度的確信，如此憑藉該數位身分所進行的客戶盡職調查才有意義。至於個案銀行取得客戶之文件、資料或資訊時，其過程及驗證身分之機制經前一節分析後，其保證等級多為中間水準，亦即能夠有實質/高度的確信，因此憑藉此保證等級所取得之客戶文件、資料或資訊用來進行客戶盡職調查，能夠符合 FATF 第十項之建議。

然而，客戶盡職調查之本質不僅僅是確認客戶身分而已，尚包括瞭解欲往來業務關係之目的與性質，並視情形取得相關資訊。但是就開立數位存款帳戶為例，我國銀行業目前僅在客戶填寫開戶申請時，由客戶以勾選的方式回答欲往來業務關係之目的、資金來源以及預計之去向，毋須附上相關佐證之文件。相較之下，

[92] 內政部憑證管理中心，網址：https://moica.nat.gov.tw/faq_in_c_18_3.html#（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

若是臨櫃開戶之情形，當客戶回答開戶是為了薪資存款，銀行可要求客戶提供聘書或是員工識別證等文件以茲證明，但開立數位存款帳戶僅需留存身分證件影像而不必留存其他文件資料。

第四節　小結

雖然透過以上分析，我國銀行業現行之做法似乎形式上皆合於規範或是指引，但根據筆者實際的工作狀況，仍覺得實務上在確認身分時有不足之處。

以簡訊驗證碼為例，該機制是透過使用者行動電話號碼確認身分，能夠得出原留存行動電話號碼之人，與此次提出身分確認之行動電話號碼為同一人，但無法確認當初留存行動電話號碼之人，真的是開戶之人。客戶變更行動電話號碼必須透過雙因素驗證，例如透過晶片金融卡使用網路 ATM，再輸入晶片密碼，確認無誤後始能變更行動電話號碼。但筆者實際碰到的例子是，太太持有先生的晶片金融卡，由太太設定晶片密碼，最後留存太太的行動電話號碼，但帳戶的戶名實際上是先生的。若將此例的當事人轉換為人頭以及詐騙集團，整個驗證過程一樣會成功。

所以若是詐騙集團再透過前述之方式繼續申請開立數位帳戶，銀行其實在開戶階段以及初步的客戶盡職調查都不會發現問題。但銀行針對客戶之交易都會進行持續的交易監控，若經系統判斷交易態樣可疑或是疑似洗錢，會再由 AML 經辦進行下一步的調查，依然能夠在三道防線內防堵洗錢或是資恐之風險。

然而道高一尺、魔高一丈，隨著科技不斷的進步，即便是 OTP 簡訊驗證碼都有可能被不肖分子中途攔截或竄改，因此根據 NIST 最新的指引，已認證這種驗證方式並不安全，建議取消這種 OTP 簡訊驗證碼在交易確認的使用，以筆者服務的銀行為例，目前在交易確認方面已停用簡訊 OTP 服務，但在開戶之身分確認時依然保有此種方式。

DOI:10.6814/NCCU202001680

目前最新的趨勢是希望能夠利用區塊鏈分散式帳本的技術，從資料源頭進行保護，亦即將身分資料加密後並切碎放在區塊鏈上，讓資料變得比較安全，並能透過對應的技術將這些碎片快速組合以驗證。根據相關業者指出，他們是透過上述的技術架構，來做到零信任（Zero Trust），以及去識別化（De-Identification）。因為過去只要帳號密碼相符合，就信任你是使用者，而所謂的零信任，就是即使帳號密碼正確但還是不信任，因為知道密碼可能會被盜用，而去識別化則是能因應歐盟 GDPR 的法規要求[93]。

雖然筆者覺得我國銀行業目前之做法仍有改善空間，但是推動金融科技以及數位身分應用之初衷，是希望能夠達成普惠金融。若是再以更嚴格的方式驗證身分，可能會徒增成本以及造成民怨，反而與普惠金融的目標背道而馳，因此銀行業在推出新產品、新服務甚至是應用新科技時，應該要衡量如何在監理與普惠金融之中取得平衡。

除了分析我國銀行之做法外，透過比較歐盟、美國、ISO 以及 FATF 之規範和指引，以下試著提出對我國做法上的啟發或借鏡。目前我國對數位身分之管理以及識別/驗證身分機制之保證等級並沒有相關專法之規範，也沒有任何辦法、注意事項、作業規範或是作業範本可茲參考，但是針對不同的業務仍有相應的規範及安控基準可以遵循，像是金融機構辦理電子銀行業務安全控管作業基準，根據交易之風險類型，規定在不同風險下，需要使用何種安全設計方法。

我國目前之做法是比較針對性的細部具體規範，規定在什麼情況下可以使用什麼機制，與國際間從上位的角度，直接就確信程度予以分級的規範方式不同，歐盟、美國以及 ISO 皆是以程度劃分，例如達到某種保證等級必須使用至少兩種驗證因素，至於選擇什麼因素則交由當事者自己決定。後者這種規範方式比較

[93] 羅正漢，「基於區塊鏈技術的身分驗證方興起，強調零信任與去識別化」，網址：https://www.ithome.com.tw/news/129143（最後瀏覽日：2020 年 7 月 23 日）。

DOI:10.6814/NCCU202001680

具有彈性，尤其科技日新月異，原先認為安全可控的驗證因素可能過不久就被認為不合適（像是 OTP 簡訊驗證碼）。因此，或許我國可以借鑑國際之做法，直接規範保證等級。

但其實就我國目前的做法而言，就操作上的結果來說，與國外直接規範保證等級的方式相比，差異並不大。保證等級之所以彈性，是因為它的定義較為籠統，歐盟或是美國都有再額外訂定相關指引，進一步說明如何能滿足不同的保證等級要求。因此要選擇哪一種方式其實是立法論的問題，筆者認為目前兩種方式沒有孰好孰壞，端看立法者的選擇。只是目前對於數位身分的討論，不僅僅在於銀行業之應用，我國未來即將換發數位晶片身分證，筆者認為或許應該在最上位的層次制定專法規範數位身分之管理，至於金融業或是其他行業要如何應用，就是下面層次有關如何具體適用的問題，不過數位晶片身分證不是本文主要探討的對象，就點到為止。

至於 FATF 針對利用數位身分進行客戶盡職調查之指引，我國亦可參照其內容作出相關法規之修正，透過法律正式授權，讓銀行業者在進行客戶盡職調查時較無後顧之憂。

DOI:10.6814/NCCU202001680

第六章 結論

數位身分之概念在網際網路問世後就已經有了，其實並不是最近才有的概念，然而隨著科技與技術的進步，盜用身分並且進一步進行詐欺、洗錢等犯罪越來越猖獗，為了管理以及遏止犯罪，識別及驗證身分的技術以及規範勢必與時俱進。

數位身分制度之建立主要以國家為首進行管理，以歐盟為例，旗下 28 個會員國有推行 eID 的國家高達數十國，在此種政治經濟與文化緊密交流的生態圈中，若無法跨境認證其中一國所發行之數位身分，勢必造成適用上之窘境，於是歐盟順勢而為推出電子身分認證與信任服務規章，以期提供歐盟公民、企業與公部門安心使用電子交易的基礎環境。除歐盟之外，美國 NIST、國際組織 ISO 以及 FATF 皆針對數位身分推出國際標準或是指引。

總結這些相關規範及指引，可以得出在管理數位身分時，識別及驗證數位身分原則是根據風險基礎方法分級，若是識別及驗證的過程越嚴謹，則保證等級越高，從事的行為若風險較高，則採取的保證等級亦必須高；若從事的行為風險較低，則採取相應的保證水準即可。

我國雖沒有就數位身分推出專法，但是針對不同的業務仍有相應的規範及安控基準可以參考，以數位存款帳戶為例，以驗證的強度區分帳戶種類以及交易限制，針對不同風險等級之交易，所對應之安控機制也有不同。然而因我國並沒有明確就識別及驗證身分之機制規定保證等級，本文隨即參照國際規範以及標準，分析我國銀行業之現行實務做法，得出目前識別及驗證機制原則上可被定調為中級，亦即有實質/高度的確信。

而 FATF 數位身分指引對金融機構如何利用數位身分滿足客戶盡職調查要求，提供進一步的指導。其核心意義在於銀行取得客戶之電子文件、資料或資訊時，其過程及驗證身分之機制是否足夠妥適，進而使銀行對於客戶身分有適當程度的

DOI:10.6814/NCCU202001680

確信，如此憑藉該數位身分所進行的客戶盡職調查才有意義。經本文分析，我國銀行業於驗證機制採行的保證等級，能夠使銀行利用數位身分進行客戶盡職調查時，符合 FATF 之建議。

盡管本文分析後得出銀行現行做法能夠滿足 FATF 建議之結果，但根據筆者在業界的第一線觀察，現行識別及驗證身分機制甚至是防制洗錢及打擊資恐之做法，仍有改善之空間。但是推動金融科技以及數位身分應用之初衷，其目的是希望能夠達成普惠金融，若是以更嚴格的方式驗證身分，可能會徒增成本，將客戶拒之門外，反而與普惠金融的目標背道而馳，因此不論是以管理機關或是以銀行的角度，新產品、新服務甚至是新科技問世時，在管理面及業務面要衡量如何在監理與普惠金融之中取得平衡。

此外，本文透過比較分析歐盟、美國及 ISO 之規範和國際標準，認為我國或許可以借鑑國際之做法，直接規範保證等級，在實務上比較具有彈性；同時建議我國參照 FATF 之數位身分指引做出相應之修正，透過法律正式授權，讓銀行業者在進行客戶盡職調查時較無後顧之憂。

DOI:10.6814/NCCU202001680

參考文獻

壹、中文

一、專書

1. 協合國際法律事務所，2019 年，《變革中的金融科技法制》
2. 洪杰文、歸偉夏，2016 年，《新媒體技術》

二、期刊論文

1. 李中仁，2018 年，以多因子驗證機制強化身分驗證之安全性，財金資訊季刊，92 期
2. 財團法人金融聯合徵信中心編輯部，2008 年，紙上談信「當事人信用報告」13 項資訊讓信用一覽無餘，金融聯合徵信雜誌， 1 月號
3. 黃世欽，2018 年，生物辨識技術與我國金融機構之運用，銀行公會會訊第 103 期
4. 蘇柏毓，2020 年，淺談 Mobile ID 安全之法令要求與應用案例，NCC News，第 14 卷

三、學位論文

1. 陳徽，2018 年，歐盟與美國電子身份管理立法比較研究，暨南大學碩士學位論文
2. 黃鈺書，身分辨識於保險科技之應用相關法律問題研究，東吳大學法律學系碩士論文（2019 年）

四、研究資料

DOI:10.6814/NCCU202001680

1. CAMS 第六版

五、網路資料

1. 內政部憑證管理中心，https://moica.nat.gov.tw/faq_in_c_18_3.html#
2. 內政部憑證管理中心，什麼是自然人憑證，https://moica.nat.gov.tw/what.html
3. 王立恒，【國外 eID 實例：愛沙尼亞】技術、法源、開源三管齊下，2 千項數位服務才能安心用 eID，https://www.ithome.com.tw/news/117367
4. 李啟榮，數位身分證技術探討（一）：數位身分證的多元服務和個資安全保障，https://www.find.org.tw/index/wind/browse/ed504f626f4cf18dc3fa58f273a6e8d3/
5. 周峻佑，透過簡訊執行二次驗證不再安全，美國國家標準技術研究所建議別再使用，https://www.ithome.com.tw/news/112845
6. 金融監督管理委員會，銀行線上服務全面升級，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201905140002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News
7. 金融監督管理委員會銀行局，未來獨資組織、本國未成年人及外國成年人符合一定條件將可直接透過網路開立存款帳戶，https://www.banking.gov.tw/ch/home.jsp?id=169&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201911280002&toolsflag=Y&dtable=News
8. 倡議編輯室，聯合國永續發展目標 SDGs 你我都不能缺席，https://ubrand.udn.com/ubrand/story/12117/3783886
9. 財金資訊股份有限公司，公司介紹，https://www.fisc.com.tw/tc/profile/index.aspx

DOI:10.6814/NCCU202001680

10. 財團法人聯合信用卡處理中心，信用卡輔助持卡人身分驗證平臺，https://www.nccc.com.tw/wps/wcm/connect/zh/home/BusinessOperations/CardBusiness/CardVerificationPlatform
11. 郭幸宜，數位帳戶兩大優勢 至去年底開戶數 338.4 萬戶 年增 1.24 倍，https://news.cnyes.com/news/id/4439485
12. 陳奕甫，數位身分（Digital Identity），https://medium.com/@yfc/%E6%95%B8%E4%BD%8D%E8%BA%AB%E5%88%86-digital-identity-414a1cc5cba6
13. 經濟部國際貿易局，新加坡、紐西蘭及智利宣布完成「數位經濟夥伴協定（Digital Economy Partnership Agreement, DEPA）」談判，並預計於 2020 年 4 月簽署，https://www.gov.tw/News_Content.aspx?n=872E51DB9B88306C&sms=53E09032BF601A56&s=6966B4C8347F7285
14. 蔣宜婷，eID 模範生的建議：信任比技術更重要，https://www.businesstoday.com.tw/article/category/80398/post/202002190015/eID%E6%A8%A1%E7%AF%84%E7%94%9F%E7%9A%84%E5%BB%BA%E8%AD%B0%EF%BC%9A%E4%BF%A1%E4%BB%BB%E6%AF%94%E6%8A%80%E8%A1%93%E6%9B%B4%E9%87%8D%E8%A6%81
15. 駐新加坡台北代表處，新加坡、紐西蘭和智利簽訂數位經濟夥伴關係協議(DEPA)，https://www.taiwanembassy.org/sg/post/29695.html
16. 羅正漢，基於區塊鏈技術的身分驗證方興起，強調零信任與去識別化，https://www.ithome.com.tw/news/129143

貳、英文

一、研究資料

DOI:10.6814/NCCU202001680

1. CAMS, *Audit Advanced Certification –Digital Identification Methods and Testing for AML Programs*
2. Capgemini & BNP Paribas (2018), World Payments Report 2018, accessed online at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/WorldPayments-Report-2018.pdf
3. International Data Corporation (IDC), IDC Future Scape: Worldwide IT Industry 2019 Predictions
4. The Boston Consulting Group, *The Value of Our Digital Identity*, https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf
5. The Global Partnership for Financial Inclusion-GPFI(2018), *G20 Digital Identity Onboarding*, https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

二、國際組織資料

1. FATF, Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion
2. FATF, Guidance on Digital Identity
3. FATF, The FATF Recommendations
4. World Bank Group, GSMA & SIA, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

DOI:10.6814/NCCU202001680

三、官方資訊

1. 3 CFR 13681 - Executive Order 13681 of October 17, 2014. Improving the Security of Consumer Financial Transactions, https://www.govinfo.gov/content/pkg/CFR-2015-title3-vol1/pdf/CFR-2015-title3-vol1-eo13681.pdf
2. NIST, Digital Identity Guideline, Special Publication(SP)800-63-3
3. UNCITRAL Working Group, https://undocs.org/en/A/CN.9/WG.IV/WP.162
4. United Nations, https://sustainabledevelopment.un.org/sdg16

四、網路資料

1. ACAMS, *Digital Identity and Financial Crimes*, https://www.acamstoday.org/digital-identity-and-financial-crimes-2/
2. Asian Trade Centre, UNPACKING THE DIGITAL ECONOMY PARTNERSHIP AGREEMENT (DEPA), http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa
3. Blockchain for the SDG, https://blockchain4sdg.com/digital-identity-sdg-16-9-providing-legal-identity-for-all/
4. FIDO Alliance, https://www.slideshare.net/FIDOAlliance/nist-80063-guidance-fido-authentication

DOI:10.6814/NCCU202001680