集保結算所數位身分驗證現況與應用場景評估

召　集　人：許傳昌

研究人員：王秀芬、簡易賜、朱月桂
林欣賢、周　儒、王博玄
劉家亨、丁景麟、李兆文

臺灣集中保管結算所
TDCC Taiwan Depository & Clearing Corporation

中華民國 112 年 12 月

目 錄

第一章　緒論 3

第一節　研究動機與目的 3
第二節　研究方法與範圍 4

第二章　臺灣金融業身分驗證實務 6

第一節　我國數位身分驗證相關規範簡介 6
第二節　我國金融業數位身分驗證應用情形 12

第三章　國際數位身分驗證規範框架 18

第一節　數位身分治理國際規範 18
第二節　國際數位身分發展應用概況 31

第四章　集保結算所數位身分驗證方案探討 52

第五章　結論與建議 53

第一節　結論 53
第二節　建議 55

參考文獻 58

第一章　緒論

第一節　研究動機與目的

全球金融科技蓬勃發展，運用新興科技創新金融業務，借助數位化提供多元服務管道、提升客戶體驗、增強客戶關係，進而開創新興服務模式，已成為金融機構主要策略。隨著數位金融持續創新發展，線上金融服務已成為消費新選擇，從註冊、登入到交易都需要確保安全性，同時兼顧使用方便，而金融機構也需辨識客戶身分、進行認識客戶(KYC)、驗證客戶身分，並確認客戶是否經授權。

考量傳統金融服務場景已由金融機構擴展至「金融生態圈」，金融監督管理委員會（以下稱金管會或主管機關）爰於「金融資安行動方案 2.0」規劃參考數位身分驗證等級國際標準(ISO29115)架構，將網路身分驗證(eKYC)依登錄、信物管理及驗證等階段運作機制，區分信賴等級(Level of Assurance, LoA)，並建立與業務風險對照規範，使金融機構於提供網路金融服務有所遵循，俾利民眾享有安心便利、穩定不中斷的金融服務。

臺灣集中保管結算所股份有限公司（以下稱集保結算所或本公司）作為金融市場的大後台，30 餘年來深耕資本市場，拓展多元服務，也積極推動主管機關「資本市場藍圖」、「金融科技發展路徑圖」與「上市櫃公司永續發展行動方案(2023 年)」等多項政策，在核心服務的基礎上，持續規劃各項數位創新業務，從後台角色逐步推展到中台，提供的各項「線上、數位、免臨櫃」服務，優化金融交易流程，提升投資人數位體驗，並協助金融業永續轉型。

數位身分是推動業務數位轉型之基石，集保結算所近年積極跟上數位金融的進程，建置多項數位業務平台，並配合金融市場與監理的脈動，協助推動各項重要政策，推動多元數位服務，例如集保 e 手掌握 App、股東 e 票通(eVoting)、視訊股東會(eMeeting)、投資人關係整合平台(ESG IR)、證券期貨業 ESG 執行資訊控管系統、大數據監理平台、投資人線上查詢有價證券

資料等數位服務平台，提供 B2C、B2B 及 B2G 等不同類型應用系統，提供證券市場各不同金融產業的參加人(B2B)或民眾(B2B2C)運用。隨著集保結算所業務數位化場景從 B2B 的帳務處理、資訊交換，到 B2B2C 的身分辨識、資料查詢等，在業務數位化趨勢下，為因應各項業務發展需要，實有必要重新逐一檢視現行集保結算所各應用系統之身分驗證機制，並進行全公司適用的數位身分驗證框架之推動與設計，俾利集保結算所數位服務順利發展。

本研究目的，即預為規劃集保結算所各業務系統適用之數位身分驗證框架，以利未來建立一致的數位身分的指引，並導入相關國際規範，以利內外部使用者，及既有系統與新系統共同遵循，提升集保數位服務身分驗證的便利與安全。

第二節　研究方法與範圍

本研究擬蒐集國內金融業實務作法及國際規範框架，包括 ISO29115 與 NIST SP 800-63 等國際標準與規範；針對現行集保結算所各業務系統在數位身分驗證機制的運用上，進行盤點分析，包括技術、資安、流程與法制面向；根據國際標準與規範及參照公司業務特性與發展目標，設計適用集保結算所之數位身分驗證框架，並根據上述框架製作數位身分驗證導入指引與制定內部程序書等行政管理規章，期能順利推動業務數位轉型，提供客戶使用更便利且安全之數位線上服務。

本研究分為五個章節，第一章為緒論；第二章為臺灣金融業身分驗證實務，介紹我國數位身分驗證相關規範及金融業數位身分驗證應用情形；第三章為國際數位身分驗證規範框架，整理包括 ISO29115 與 NIST SP 800-63 等國際標準與規範，並探討國際數位身分發展應用概況；第四章為集保結算所數位身分驗證方案探討，綜整集保結算所數位服務現況，並以集保 e 手掌握為例，分析身分驗證應用實務，就現行各業務系統在數位身分驗證機制的運

用上，進行盤點分析，包括技術、資安、流程與法制面向，探討適用集保結算所之數位身分驗證框架；第五章為結論與建議。茲以圖 1-1 表示本報告之研究方法與研究架構。

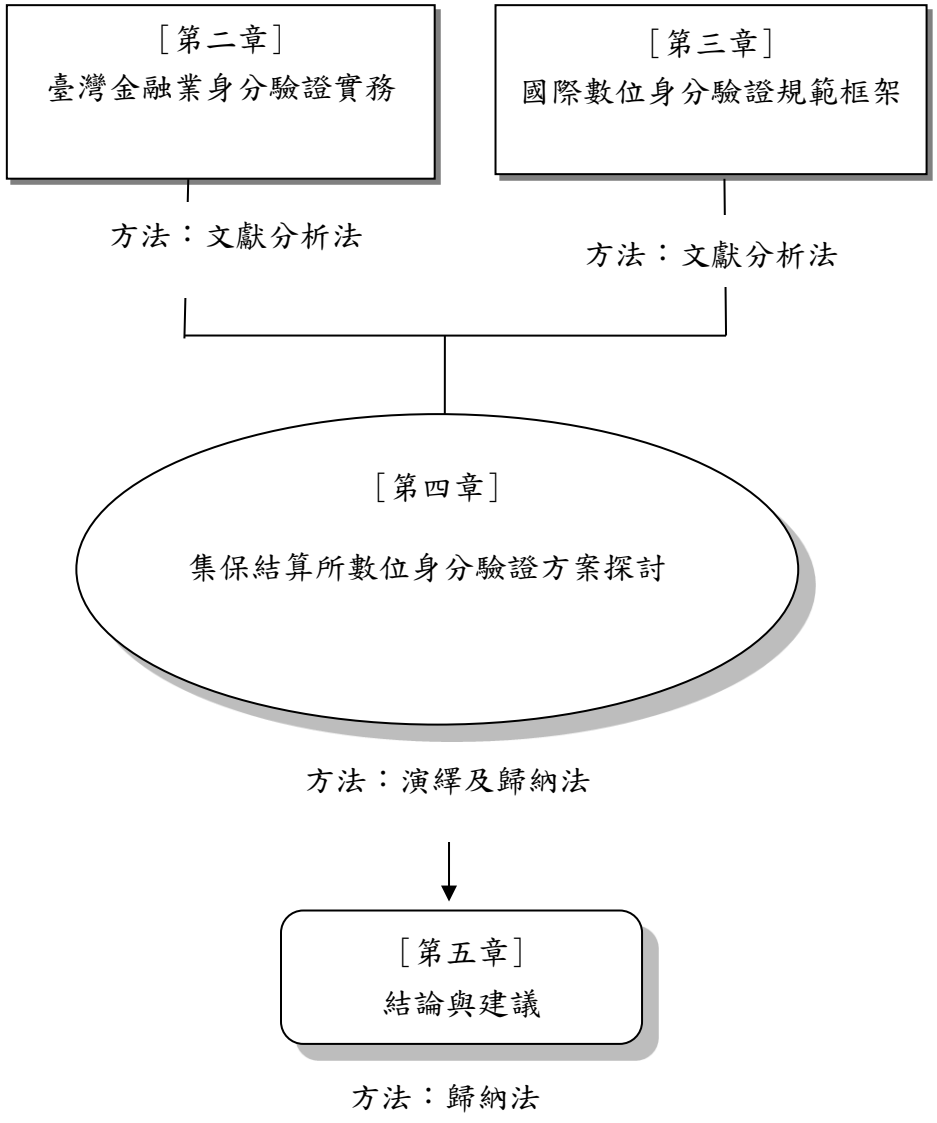


圖 1- 1 研究方法與研究架構

第二章　臺灣金融業身分驗證實務

第一節　我國數位身分驗證相關規範簡介

全球金融科技蓬勃發展，運用新興科技創新金融業務，借助數位化提供多元服務管道、提升客戶體驗、增強客戶關係，進而開創新興服務模式，已成為金融機構主要策略。然而於金融科技快速發展、金融服務創新開放的同時，資通安全也面臨嚴峻的挑戰，駭客的攻擊早已朝向系統化與組織化，除常見之分散式阻斷服務攻擊(Distributed Denial-of-Service, DDoS)、社交工程攻擊、勒索軟體等問題外，更不乏大型金融機構遭駭客跨國盜轉鉅額資金之案例，一旦受駭所帶來的衝擊較之諸往更鉅。

金管會長期關注並督促金融機構資安防護，雖已行之有年也有一定的運作機制，惟鑒於資安威脅日益嚴峻，金融資安防護的思維亦須更快速的調整因應，爰觀察國際金融資安情勢、國際金融資安監理趨勢，並檢討現行資安監理政策，提出「金融資安行動方案」，並於 111 年 12 月 27 日進一步宣布啟動為期三年的「金融資安行動方案 2.0」，以擴大適用、落實與深化、鼓勵前瞻為持續精進方向，訂定 40 項強化金融業資安防護能力措施；另金管會參考當前國際金融科技趨勢，統合我國目前發展金融科技所需專注的領域及實際需要，並於 109 年 8 月 27 日發布「金融科技發展路徑圖」，聚焦強化基礎工程、擴展應用、協調協力 3 大構面，推動數位基礎建設等 8 大主要方向，期能強化金融韌性、建立有效的應變機制，確保整體經濟及金融的穩定；此外，數位發展部並將推動「零信任架構」列為施政重要目標。茲概述如下：

一、金融資安行動方案 2.0

金管會於 111 年 12 月 27 日宣布啟動為期三年的「金融資安行動方案 2.0」，行動方案中針對數位身分執行措施主要規劃分為外部與內部兩個面向，外部面向指金融機構針對外部客戶之數位身分驗證；內部

面向指金融機構對於員工或關係人之內部零信任架構下的身分認證；在內部面向部分，因應數位轉型及網路服務開放，並兼顧洗錢防制需求，規劃參考數位身分驗證等級國際標準（ISO 29115）架構，將網路身分驗證（eKYC）依登錄、信物管理及驗證等階段運作機制，區分信賴等級，並建立與業務風險對照之規範，以利業者於提供網路金融服務遵循，金融行業需建立一致的數位身分驗證，各類業務風險等級與適配之驗證強度規範，此工作應於 113 年完成。在內部面向部分，推動零信任網路資安防護導入金融機構，逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路三大核心機制，並將配合國家資通安全研究院之規劃進行，此工作應於 114 年完成。

集保結算所為國內跨資本市場及貨幣市場唯一的後台機構，為提升使用集保數位服務客戶身分安全，依上述金管會採零信任架構思維重新檢視金融業網路安全防護及資訊系統安全防護基準內容，並依國家發展規劃逐年研議零信任適用範圍，逐步導入三階段零信任核心機制技術，刻正積極研議各內外部作業系統之客戶身分驗證強度。茲將「金融資安行動方案 2.0」有關數位身分執行措施表及集保結算所配合事項臚列如下表：

表 2-1「金融資安行動方案 2.0」數位身分執行措施表

構面	工作項目	工作小項	執行措施	執行期限	說明	集保配合事項
強化資安監理	完備資安規範	建立數位身分驗證等級與業務風險對照規範	因應數位轉型及網路服務開放，建立數位身分驗證等級與業務風險對照規範	113 年	因應數位轉型及網路服務開放，並兼顧洗錢防制需求，可信賴的網路身分識別機制為各業別金融機構共同需求，為提供金融機構明確之執行準據，提升應用金融科技之效率，降低執行風險及減少消費者行政負擔，進而達到保障消費者權益之目的，爰規劃參考數位身分驗證等級國際標準(ISO 29115) 架構，將身分驗證依登錄、信物管理及驗證等階段運作機制，區分信賴等級，並建立與業務風險對照之規範，以利業者遵循。	配合主管機關公布之規範調整公司各類系統數位身分驗證強度

構面	工作項目	工作小項	執行措施	執行期限	說明	集保配合事項
		訂定資通安全防護基準	增修訂資安自律規範，納入網路安全防護及資訊系統安全防護基準內容	持續	為增加防禦縱深，採零信任架構思維重新檢視包含內外部網路之資源存取、網段隔離、邊界防護等議題，檢討修訂網路、資通系統安全等自律規範，使其更臻完整明確。	配合主管機關公布之基準調整公司各類資安程序書
深化資安治理	加強資安管理	鼓勵零信任網路部署	鼓勵金融機構逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路 3 大核心機制。	114 年	因應疫情帶動異地/居家辦公模式，亦隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求。國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國「國家資通安全發展方案(110 年至 113 年)」，亦將發展零信任網路資安防護環境，推動政府機關導入零信任網路，爰規劃鼓勵金融機構採零信任網路部署，逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路三大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。	依國家發展規劃逐年研議零信任適用範圍，逐步導入三階段零信任核心機制技術

資料來源：金管會「金融資安行動方案 2.0」與本研究自行整理

二、金融科技發展路徑圖

為形塑友善之金融科技發展生態系，促進相關服務或商業模式之推出，以提升金融服務之效率、可及性、使用性及品質，金管會於 109 年發佈金融科技發展路徑圖(詳圖 x)，其中「基礎工程」之數位基礎明列「研究發展金融行動身分識別標準化機制」及「開放企業線上開戶作業」2 大推動措施(詳表 x)，包含金融機構共同籌組金融行動身分識別聯盟(F-FIDO)、研議規劃導入國際 FIDO(Fast Identity Online)標準等項目，初期針對中低風險之金融服務，提供通用之行動身分識別(identification)與簽署(authorization)功能，由金融機構向金管會申請業務試辦方式為之，

以驗證低風險業務採用 FIDO 作為身分驗證方式之可行性。

金管會「金融科技發展路徑圖」除了積極推動金融行動識別與資安措施，更力推「行動自然人憑證」及「數位身分認證及授權」主題式監理沙盒與業務試辦，希望能透過「刷臉」、「按指紋」等新興技術完成身分認證，或運用金融科技，提升身分識別的自動化作業，如此不但可減少金融機構 eKYC 成本，未來更可結合資料共享與開放金融發展趨勢，讓數據力發揮更大金融服務綜效。



資料來源:金管會

圖 2-1 金融科技發展路徑圖

表 2-2 金融科技發展路徑圖中身分識別相關措施

推動措施 1	**研究發展金融行動身分識別標準化機制**
(一)始推動臺灣行動身分識別 Taiwan FidO 服務，惟目前僅供政府機關試辦，尚未開放商業應用	
(二)國內金融交易所需身分識別技術的金融憑證（包含身分辨識及交易授權），有由臺灣網路認證公司之身分識別中心(下稱臺網)、亦有由中華電信的金融用戶憑證管理中心提供。	

(三)金融機構共同籌組金融行動身分識別聯 2021.8 盟 F-FIDO，研議規劃導入國際 FIDO 標準，初期針對中低風險之金融服務，提供通用之行動身分識別(identification)與簽署(authorization)功能，由金融機構向金管會申請業務試辦方式，驗證低風險業務採用 FIDO 作為身分驗證方式之可行性。	
推動措施 2	**開放企業線上開戶作業**
(一)參考國外已開放企業線上開戶之作法，評估相關之風險與管理機制，依電子化交易風險程度，由銀行公會研議逐步開放企業線上開戶作業及建置相關管理機制。 (二)鼓勵金融機構介接國發會 MyData，經由民眾或企業授權，取得相關政府機關資料，便利企業線上開戶。 (三)檢視評估數位存款帳戶之相關限制是否合理，及有無科技應用或管理機制可供降低線上開戶之不便性。	

資料來源: 金管會

三、數位發展部「零信任架構」

零信任架構的目的乃是要建立一個對所有資料存取訪問活動採取最小權限的企業資訊架構。零信任架構在美國政府的主推下，已被視為新一代的訪問授權控制措施。由於零信任強調在所有資料訪問活動中，無論來自公司內部或者網際網路外部的訪問請求，無論存取者的身分為員工或者外部客戶，每一個訪問階段都需要持續地驗證和執行授權決策，不再存在過去網路防禦邊界的隱性信任假設的概念。其概念與原則可以參考美國國家標準暨技術研究院 NIST 出版物 SP 800-207：零信任架構(Zero Trust Architecture, ZTA)，而在實作上的導入指引則是可以參考 SP 1800-35 (Draft)：實施零信任架構(Implementing a Zero Trust Architecture)。數位發展部轄下國家資通安全研究院於 111 年 8 月發布「政府零信任網路身分鑑別機制導入建議」，參考美國 NIST 正式頒布標準文件 SP 800-207 文件。在此份文件中明確指出我國零信任三個階段的導入建議，並指出最終階段實現後的零信任參考部署架構，由於我國採取門戶佈署的方式，作為對外門戶的存取閘道會是網路架構中的升級零信任的起點，由此起點界接身分鑑別機制、設備鑑別機制、信任推斷機制與公司既有

之資訊系統(Resource Portal)。

另金管會「金融資安行動方案 2.0」亦鼓勵金融單位逐年部署零信任網路，由於金融單位面臨後疫情時期、數位轉型與極端情境威脅下，當前許多金融業務也已獲得主管機關同意以遠端連線方式辦理，而金融上雲亦是主管機關之推動目標，金融單位的使用者與資訊數據被分散於各地，彼此透過網際網路連結，資安防護需求更甚以往，這使得金融單位須放棄以往保守的資安架構，採用更積極的資安策略，擁抱零信任架構顯得尤為重要。

四、金管會「金融服務業辦理數位身分驗證指引」

為促進金融業發展，提供民眾取得更便利之數位金融服務，金管會訂定一參考性質之指引，就數位身分驗證中具共通性之內容揭示辦理原則，以利各業別數位身分規範具共通性，並作為金融服務業各業別數位身分規範之參考。該指引參考國內外相關文獻，共訂定 10 點條文，臚列如下：

(一)明定指引之訂定目的，以及揭示指引所稱金融服務業係指「金融監督管理委員會組織法」第 2 條第 2 項所稱之金融服務業。

(二)明定金融服務業辦理數位身分驗證除應遵循之相關法規外，依指引辦理，並明確揭示指引僅適用於金融服務業辦理自然人之數位身分驗證。

(三)就數位身分驗證及該驗證機制之參與者予以定義，並簡述數位身分驗證機制於數位金融服務提供過程之運用情形。

(四)說明金融服務業辦理數位身分驗證之三階段作業程序。

(五)明定金融服務業辦理數位身分驗證，其「應用場景之風險等級」與「驗證機制之信賴等級」應依風險基礎原則相互適配。若現行法規、

各業別自律規範及金融周邊單位相關規章未規範之新數位金融服務應用場景或新式數位身分驗證機制，即應依本點規定辦理。

(六)說明數位身分驗證機制失效時可能產生之風險及風險等級評估作業。

(七)對數位身分驗證機制之信賴等級予以定義，並揭示金融服務業依其業務性質得將信賴等級區分為不同級數。並以區分為四個等級為例，分別說明各等級代表之意義。

(八)明定金融服務業辦理數位身分驗證應建立風險管理機制，並納入內部控制及稽核制度，且適時檢討。

(九)明定金融服務業辦理數位身分驗證，應注意與客戶權益有關之事項。

(十)明定金融服務業各產業公會及金融周邊單位於訂定數位身分驗證作業程序及評估作業，宜給予個別業者訂定其內部規範之彈性，俾各該業者依其業務發展情形妥適因應相關風險。

第二節　我國金融業數位身分驗證應用情形

近年來，新冠疫情改變人們的生活，也改變了金融服務的面貌，更加速金融數位轉型的進程。許多金融服務業者爭相提供遠距與無接觸的產品與服務，如網銀開戶、線上證券投資理財、遠距投保等。雖然遠距、免臨櫃、無接觸之創新服務，可以完善客戶體驗及降低資安風險，提升數位金融服務價值並實現普惠金融，但卻面臨建立識別客戶身分最佳驗證機制議題。

身分驗證是所有金融服務的第一道關口，為使民眾更方便、安心使用數位金融服務，許多國家早已發展數位身分驗證相關機制，提升身分驗證的便利性與安全性。茲就我國金融業數位身分驗證應用情形略述如下：

一、金融業通用身分識別技術現況

金融業通用身分識別技術在金融服務領域扮演著關鍵的角色。其目的是為了確定驗證客戶身份，以確保交易和服務的安全性、合規性和可靠性。傳統的身分識別方法如使用密碼和身份證明文件，容易受到詐騙、身份盜竊的攻擊及驗證流程繁瑣耗時，因此金融業需要發展出更高效、安全且便捷的通用身分識別技術。目前，我國金融業廣泛使用的身分識別技術包括以下幾種類別：

（一）身分證驗證：金融機構可以通過比對客戶提供的身分證件與政府數據庫中的信息來驗證身分。這種方法可以提供可靠的身分驗證，但需要與政府數據庫之間的實際連接。

（二）生物特徵識別：這種技術使用個體的生物特徵來識別和驗證身分。常見的生物特徵包括指紋、虹膜和面部識別。生物特徵識別提供了更高的安全性，因為這些特徵是唯一且不易仿冒的。然而，技術上的挑戰包括準確性和隱私保護。

（三）雙因子驗證：這種方法要求客戶提供兩個驗證因素，通常是密碼和額外的驗證碼。這樣可以增加身分驗證的安全性，但仍有可能受到簡訊驗證碼被竊取或社交工程攻擊的風險。

以下彙整我國金融業常用之身分識別種類如下：

表 2-3 我國金融業常用之身分識別種類一覽表

種類	法規	使用裝置	用途
工商憑證	工商憑證管理中心憑證實務作業基準	電腦	工商憑證 IC 卡是公司、分公司、有限合夥或商業用來作為網路上身分驗證用。
證期共用憑證	台灣網路認證股份有限公司憑證實務作業基準	電腦	證券暨期貨相關單位共用憑證，使用此憑證線上辦理相關之業務。

種類	法規	使用裝置	用途
網路下單憑證	1.臺灣證券交易所股份有限公司證券商採用數位簽章注意要點 2.臺灣網路認證股份有限公司憑證實務作業基準 3.中華電信通用憑證管理中心憑證實務作業基準	電腦、平板、手機	數位憑證提供券商辨識交易者身分的功能。
網路銀行憑證	臺灣網路認證股份有限公司憑證實務作業基準	電腦	應用於網路銀行交易作為身分辨識資料，以確保交易資料隱密性、安全性、完整性、辨識性及交易之不可否認性
晶片金融卡	銀行與客戶間之金融卡約定事項	電腦	提供持卡人進行金融交易及消費付款的工具
自然人憑證	1.自然人憑證核發及管理作業要點 2.內政部憑證管理中心憑證實務作業基準	電腦	用於多項政府提供的 E 化服務(例如：線上申辦戶籍登記、申辦報稅、全民健康保險個人健保資料網路服務作業、勞農保應用查詢服務等)，並且降低個人資料外洩的危險。
TW FidO	1.內政部行動自然人憑證核發及管理作業要點 2.內政部憑證管理中心憑證實務作業基準	電腦、平板、手機	讓民眾使用自然人憑證註冊並綁定手機，以儲存在您裝置內的生物特徵（指紋或臉部），進行身分驗證，驗證成功後即可登入並使用多項政府提供的服務。
帳號密碼	約定	電腦、平板、手機	網路服務之身分識別。
生物辨識	金融機構運用新興科技作業規範之第五條原則性提示	電腦、平板、手機	網路服務之身分識別。

種類	法規	使用裝置	用途
電信認證 MID	遵循 GSMA(Groupe Speciale Mobile Association 協會所推行的 Mobile Connect 數位認證標準	手機	經由「TWID 身分識別中心」向各電信業者查詢手機門號用戶的基本資料(手機門號及身分證統一編號)，做為身分識別使用，達到實名認證行動化、交易確認行動化。
健保卡	全民健康保險保險憑證製發及存取資料管理辦法	電腦	下載查詢就醫資訊、用藥狀況、個人未繳保費查詢與繳費以及申辦符合第六類投保身分者加保、轉出、停保、復保等功能
知識詢答	無	電腦、平板、手機	網路服務之身分識別。

資料來源：本研究彙整

二、金融 FIDO

為建立金融 FIDO 標準化機制，依金融科技發展路徑圖規劃由金融科技共創平台數據治理組邀集金融機構共同籌組「金融行動身分識別聯盟」，金管會自 109 年下半年起，即與聯徵中心、財金公司、共創平台數據治理組成員及已導入 FIDO 應用之金融機構、中華民國銀行商業同業公會全國聯合會(下稱銀行公會)等單位共同研商，「金融行動身分識別聯盟」爰於 110 年 5 月 4 日由財團法人金融聯合徵信中心(下稱聯徵中心，擔任聯盟召集人)、財金資訊股份有限公司(下稱財金公司，負責制定技術規格標準)、與金融控股公司、銀行、保險公司、證券商及期貨商等聯盟成員成立，共同規劃研議綁定之信物、生物辨識範圍並共同開發手機身分識別 APP 等，並就不同業別所涉及之交易研議具體應用標準與規範透過產業標準，以多元方式便利客戶進行各項金融服務之身分識別，促進臺灣數位金融服務之發展，為金融消費者提供更有效率、品質的數位金融服務。

FIDO 聯盟是一個非營利產業聯盟，旨在提供開放、互通的標準，解決身分認證技術之間缺乏互通性的問題，並解決使用傳統帳號密碼進行身分辨識可能產生的問題。其認證模式的優點在於將身分的驗證與識別分開，通過在用戶裝置端進行生物特徵驗證，啟動非對稱公鑰私鑰架構，實現線上身分識別的安全性。FIDO 伺服器僅保有公鑰，不儲存密碼、私鑰或個人生物特徵，因此不會洩露隱私權的問題，其驗證架構如圖 2-2 所示。

FIDO 技術的主要組成部分包括以下兩個方面：

(一) FIDO UAF（Universal Authentication Framework）：這個框架旨在通過生物特徵識別、PIN 碼、聲音識別等方法來實現無密碼驗證。使用 FIDO UAF，用戶可以通過指紋、虹膜、臉部識別等生物特徵來驗證身份，取代了傳統的密碼驗證。這樣不僅提高了安全性，還提供了更便捷的用戶體驗。

(二) FIDO U2F（Universal Second Factor）：這個協議旨在提供二次驗證，增加身份驗證的安全性。當用戶輸入密碼進行身份驗證後，FIDO U2F 協議需要使用實體安全金鑰（如 USB 密鑰）來進行第二輪驗證。這樣的二次驗證措施，即使密碼被竊取，駭客仍然需要實體設備才能成功登錄。



資料來源:金管會創新中心

圖 2-2 FIDO 驗證架構圖

另金管會亦臚列自然人客戶適用金融 FIDO 業務範圍，如表 2-4 所示：

表 2-4 自然人客戶適用金融 FIDO 業務範圍

		銀行業	保險業	證券商	期貨商	投信投顧業
申請指示	無加強機制	1. 查詢帳務及個人資料等通知 2. 申辦非約轉 3. 舊戶申辦信用卡 4. 申請補換發晶片金融卡 5. 財富管理業務KYC、風險承受度測驗 6. 申辦信託開戶或終止信託 7. 同意共同行銷		1. 客戶查詢帳務與資料		1. 投信基金及境外基金客戶查詢帳務及個人資料 2. 申辦電子帳戶 3. 簽署基金交易電子約定書 4. 認識客戶作業、風險承受度(KYC、KYP) 5. 風險預告書 6. 變更通訊地址 7. 境外基金開戶業務 8. 申辦電子帳戶 9. 簽署基金交易電子約定書 10. 變更通訊地址 11. 簽訂證券投資顧問契約(含客戶資料表及風險預告書
	加強機制	1. 申辦數位帳戶(數一、數二) 數一、數二帳戶需附加相關強化機制，下階段請銀行公會研議。 2. 申請約定非同一人之約定轉入帳戶 申辦約轉首次不適用、後續應逐筆進行 FIDO 驗證。 3. 新戶申辦信用卡		1. 線上變更資料 2. 線上簽署文件同意書(含風險預告書) 3. 變更交易密碼 4. 憑證申請與展延等 金融 FIDO+電子憑證(含1~4) 5. 線上開戶、銷戶 證券：金融 FIDO+OTP 或電訪 期貨：附加相關強化機制，如：OTP 6. 交易額度調整(採線上開戶者) 需附加相關強化機制，下階段 請證交所研議。		
交易指示	無加強機制	1. ATM無卡提款 2. 協助電支機構確認客戶身分 3. 約轉交易(臨櫃約定) 4. 約轉交易(線上約定) 5. 限定性繳稅費 6. 個資異動	1. 行動投保-業務員登錄 2. 行動保全-業務員或服務人員登錄 3. 行動理賠-業務員或服務人員登錄			1. 受益人申購、買回、轉換等交易 2. 以投資非投資等級債券為訴求之基金風險預告書 3. 基金配息可能涉及本金之風險告知 4. 槓桿型 ETF、反向型 ETF、非投資等級債券 ETF 及經證券交易所或證券櫃檯買賣中心認為有必要簽署風險預告書之 ETF 風險預告書 5. 手續費後收級別費用結構聲明書
	加強機制	1. ATM存提款 金融 FIDO 內的私鑰建議如可放在 CC EAL4+ 認證載具，才會比較安全，較能完全等同現行晶片金融卡，ATM 存提款才能適用金融 FIDO。 2. 非約轉交易 非約轉交易需逐筆FIDO驗證		1. 證券下單登入 金融 FIDO+雙因子認證方 2. 交割專戶客戶分戶帳款項出金 金融 FIDO+雙因子認證方式	1. 期貨下單登入 金融 FIDO+雙因子認證方 2. 客戶保證金專戶出金 金融 FIDO+電子憑證	

資料來源:金管會創新中心

第三章　國際數位身分驗證規範框架

第一節　數位身分治理國際規範

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，亦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，各國與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。

目前國際上對於數位身分之管理以及身分驗證訂定了不同的管理規章及國際標準，如歐盟 eIDAS、美國 NIST800-63-3 及國際標準化組織制定的 ISO/IEC 29115，本章將概述 ISO 與美國有關數位身分驗證之相關規範，並且再進一步分析兩者的差異，以期從中發展適合本公司之身分驗證框架。

一、ISO/IEC 29115

ISO/IEC 29115(International Standard ISO/IEC 29115:2013(E), Information technology – Security techniques – Entity Authentication Assurance Framework，簡稱 EAAF)「個體身分驗證信賴框架」，此框架主要的目的可分為以下六個項目：

(一) 定義參與者：

訂定身分識別機制的六個參與角色，各角色有其工作職掌，依據不同的工作職掌內容各司其職，方能完整提供身分識別機制；

1. 個體[1](entity)
2. 信物提供單位(credential service provide, CSP)
3. 註冊單位(registration authority, RA)
4. 信賴單位(relying party, RP)

[1] 依據 ITUX1252 的規範，個體係指一個可分別、獨立存在、並且在某種環境背景下可被識別出來的東西，可以是「自然人」、「法人」或是「伺服器」、「網站」，甚或是「應用程式」。

5. 驗證單位(validation authority, VA)

6. 公正第三方(trusted third party, TTP)

整理如下表[2]：

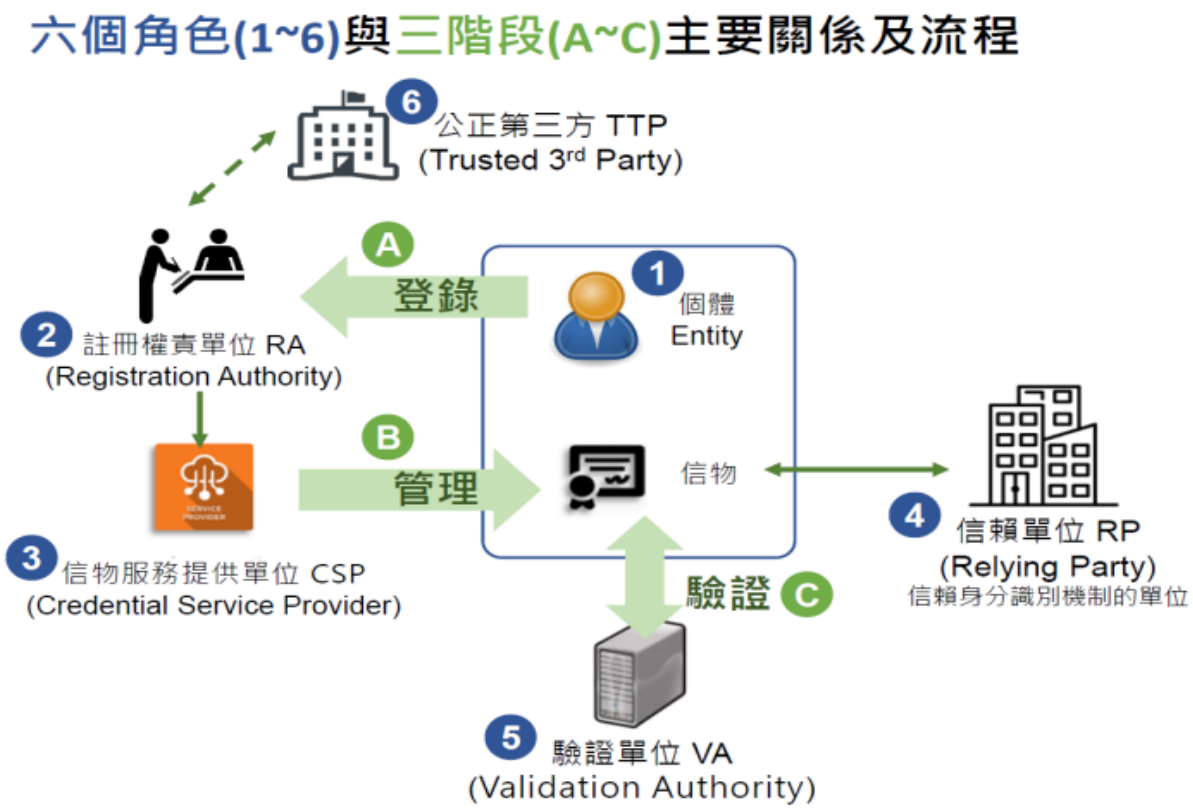
表 3-1 身分識別機制的六個角色

參與角色（單位）	工作職掌
個體	身分識別的標的
信物提供單位(CSP)	負責管理信物生命週期以及個體與身分資料間之關聯性的權責單位
註冊單位(RA)	負責申請者登錄相關作業的權責單位
信賴單位(RP)	信賴並使用身分識別機制所得結果的單位
驗證單位(VA)	提供身分驗證服務的單位
公正第三方(TTP)	除 CSP、RA、VA 所提供之服務項目外，提供身分識別作業所需其他服務的單位

資料來源：連子清、杜宏毅(2022)

(二) 作業程序三階段：一個身分驗證機制，之所以能確認個體與身分資料兩者之間的「關聯性」，建立在「確實的登錄」、「完善的管理」以及「正確的驗證」三項作業基礎之上。因此，在技術方面，ISO/IEC 29115 將身分識別的作業程序分為三個階段；

[2] 資料來源：連子清、杜宏毅(2022)，「身分識別之書-The Book Of Identification」，台灣網路認證股份有限公司



資料來源：政治大學金融科技研究中心(2022)

圖 3-1 身分識別機制六個角色之關係與流程

1. 身分登錄(enrollment)：核驗並確認個體所提示的身分資料與個體之關聯性，包括以下四個步驟：

   (1) 申請

   (2) 身分核驗與身分資料驗證

   (3) 紀錄留存

   (4) 完成註冊

2. 信物管理(credential management)：建立並維護個體與身分資料的關聯性，包括以下項目：

   (1) 產製

   (2) 前置作業

(3) 核發

(4) 啟動

(5) 儲存

(6) 暫禁、撤銷或銷毀

(7) 更新與置換

(8) 紀錄留存

3. 個體身分驗證(entity authentication)：驗證個體與身分資料的關聯性，包括以下兩個步驟：

   (1) 個體與信物之關聯性的驗證：驗證單位(VA)將依照信物服務提供單位(CSP)既定的身分驗證協定，驗證「個體」是否確認「掌控」並「持有」信物。驗證作業的強度，將取決於身分識別機制可信賴程度的要求，即採單因子或多因子的方式進行身分驗證。

   (2) 回覆驗證結果並留存紀錄。

   茲整理如下表：

表 3-2 個體身分驗證步驟

階段	主要作業內容
身分登錄 (enrollment)	核驗並確認個體所提示的身分資料與個體之關聯性。 將完成核驗「實體世界的個體」所對應的「身分資料」進行登錄作業。
信物管理 (credential management)	建立並維護個體與身分資料的關聯性。 除了管理「信物」產製、發放以及維運的整個生命週期外，尚須維護身分資料與信物之間的「連結性」及資料的「正確性」與「即時性」。

階段	主要作業內容
個體身分驗證 (entity authentication)	驗證個體與身分資料的關聯性。 個體提出服務相對應所需之信物，而藉由驗證信物獲得個體身分資料的過程，即為「驗證」。

資料來源：ISO/IEC 29115:2013(E), Figure1

(三) 定義信賴等級：ISO29115 依照信心程度區分成四種數位身分驗證等級(Level of Assurance)，亦可依實際業務需求分級。LoA1 是最低保證級別，LoA4 是標準中規定的最高保證級別，各等級代表定義如下：

1. LoA 1：

   LoA1 是身分驗證機制中信賴度最低的等級，對於使用者「自己宣稱」的身分，基本上只能抱著姑且信之的態度。系統安全要求係數低，當系統失效時並未有任何影響。使用此 LoA1 管控措施時，僅提供最低限度的保證；LoA1 對身分驗證並未有硬性要求，對應的身分驗證方法則建議以密碼保護為最低要求。

2. LoA 2：

   採用 LoA2 等級的身分識別機制時，基本上可以對其身分識別的結果，持有「某些程度」的信心。採用 LoA2 可抵禦中等風險與錯誤的威脅；LoA2 對應的身分驗證應具備單因子驗證技術即可。

3. LoA 3：

   如果對單位而言，在身分識別機制失靈時，會產生「實質性

的風險 (substantial risk)」，建議應用單位採用 LoA3 等級的身分驗證機制，希望對身分驗證系統有高度信任。此 LoA 用於與錯誤身分驗證相關的重大風險；LoA3 對身分驗證具備多因子驗證技術，而且任何「機敏性資料 (sensitive data)」的交換都應加密保護，關於「信物」的產製或儲存，除了必須進行加密保護外，並無特殊要求。

4. LoA 4：

LoA4 屬於最高級別的信賴等級，信賴這套機制的第三方，可以對其所驗證的身分，具「極高的信心」。希望對身分驗證系統有極高高度信任度要求。LoA4 除了必須滿足 LoA3 的規範要求外，在自然人的部分，還必須增加「人為介入 (in-person)」的機制。例如在提示畫面中點選確認鍵，或是回覆特定問題的答案等。在信物管理上，亦要求儲存私密資料以及私鑰的硬體設備必須具備「防篡改 (tamper-resistant)」的功能。此外，在身分驗證過程中，所有經手的「機敏性資料」和其他「個人身分識別資料 (personally identifiable Information, PII)」，都應加密保護。

表 3-3　LoA 等級之信心程度

LoA 等級	對個體宣稱身分之信心程度
LoA1 低(Low) Little or no confidence in the claimed or asserted identity	對主張或斷言的個體身分只有少許的信心或幾乎沒有信心(幾無信心)
LoA2 中(Medium) Some confidence in the claimed or asserted identity	對主張或斷言的個體身分有某種程度上的信心 (有一定信心)
LoA3 高(High)	對主張或斷言的個體身分有高度

LoA 等級	對個體宣稱身分之信心程度
High confidence in the claimed or asserted identity	的信心 (高度信任)
LoA4 最高(Very High) Very high confidence in the claimed or asserted identity	對主張或斷言的個體身分有非常高的信心(非常高度信任)

資料來源：ISO/IEC 29115:2013(E), Table 6-1

(四) 制定評估標準：訂定三個執行階段的「信賴等級」評估標準與方式，即各驗證等級對「身分登錄」、「信物管理」、「身分驗證」有不同要求；

表 3-4 驗證等級評估標準

	LoA1	LoA2	LoA3	LoA4
身分登錄				臨櫃確認
			證件經過驗證	證件經過驗證
		權威單位 核發之證件	權威單位 核發之證件	權威單位 核發之證件
	使用者宣稱	使用者宣稱	使用者宣稱	使用者宣稱
信物管理				硬體安全機制
	授權核發	授權核發	授權核發	授權核發
身分驗證	單因子驗證	單因子驗證	多因子驗證	多因子驗證

資料來源：ISO/IEC 29115:2013(E), 6.1 ~ 6.4

(五) 訂定選用標準：應依照下表身分驗證錯誤時可能造成的風險嚴重性，評估選用信賴等級；

表 3-5 各項信賴等級的潛在衝擊

潛在風險 (對客戶或服務提供者)	LoA1	LoA2	LoA3	LoA4
造成不便、困擾或聲譽受損	低	中	高	極高
造成客戶財務損失	低	中	高	極高
對客戶或公眾利益造成損害	不適用	低	中	極高
機敏個資外洩	不適用	中	高	極高
影響人身安全	不適用	不適用	低/中	高/極高
觸犯民法、刑法	不適用	低	高	極高

資料來源：ISO/IEC 29115:2013(E), Table 6-2

ISO 29115 依登錄、信物管理、身分驗證三個階段來評量不同身分認證工具的信賴等級，將風險評估、信賴等級及作業機制三者適配。

(六) 提供面對威脅之應對方案：提供各作業階段面臨威脅時之應對方案。

表 3-6 各作業階段面臨威脅時之應對方案

階段	常見威脅	評估項目
身分登錄	偽冒	身分核驗：政策遵行(LoA1 以上)
		身分核驗：具權威性的資料(LoA2 以上)
信物管理	信物遭竄改或未經	產信物須經授權，且具適當的產製過程(LoA1 以上)

階段	常見威脅	評估項目
	授權	
	資料外洩或遺失	須安全儲存(LoA1 以上)
身分驗證	猜測攻擊	高強度密碼、信物鎖定(LoA1 以上)
	釣魚評擊	多因子驗證(LoA3 以上)

資料來源：ISO/IEC 29115:2013(E), Table 10-1~10-6

二、NIST800-63-3

(一) NIST800-63-3 概述

在國際標準的前提下，各國可以依自己所要求的信賴等級，再發展各自的數位身分確認框架與標準。舉例來說，美國針對數位身分提出了國家標準暨技術研究院（National Institute of Standards and Technology, NIST）的 NIST 800-63 的數位身分指南（Digital Identity Guidelines）。美國 NIST 800-63 規範的基本架構亦是參考 ISO 29115，旨在說明當服務提供者提供數位服務前，能確認該使用者，確實是「他」所宣稱的「身分」，避免因身分驗證之錯誤或疏忽造成負面影響，共有四份文件；各文件的名稱與用途如下：

表 3-7 NIST 800-63 文件架構

編號	中文名稱	英文名稱	對應流程	對應風險等級
SP 800-63-3	數位身分指引（概述）	Digital Identity Guidelines	第三版數位身分指引	
SP 800-63A	登錄與身分核驗	Enrollment and Identity	身分審查流程 (Identity	IAL (Identity

編號	中文名稱	英文名稱	對應流程	對應風險等級
		Proofing	Proofing)	Assurance Level)
SP 800-63B	身分驗證與生命週期管理	Authentication and Lifecycle Management	身分驗證流程 (Identity Authentication)	AAL (Authenticator Assurance Level)
SP 800-63C	聯邦與身分查驗	Federation and Assertions	身分查驗流程 (Federation Assertion)	FAL (Federation Assurance Level)

資料來源：NIST 800-63-3

NIST800-63-3 將身分驗證分為以下三部分，並根據不同階段定義了不同的保障層級：

1. 登錄及身分核驗：

說明數位身分的登錄及身分核驗，並將此階段定義為三個 IAL(Identity Assurance Level)等級。

表 3-8 NIST 800-63-3 身分登錄及核驗三個等級

嚴謹度	等級	說明
低	IAL1	使用者自行宣稱自己所屬的數位身分，無須與特定真實的身分進行關聯性的證明，該身分不須經第三方驗證
中	IAL2	使用者須提交足以證明自己真實身分的相關身分證明文件，經驗證確認該真實身分

嚴謹度	等級	說明
		真實存在後，方完成身分驗證，此身分核驗的過程可以是臨櫃或線上進行
高	IAL3	除了 IAL1 及 2 的要求外，使用者須臨櫃申請(或受監控的線上申請)，且 CSP 須為經授權或合法培訓之機構，且在申請過程中，須使用生物辨識技術進一步保護該數位身分，為身分核驗最嚴格的等級

資料來源：NIST 800-63-3

2. 身分驗證及其生命週期管理：

說明當使用者重複進行線上作業之「身分驗證」，驗證並確保該使用者與「登錄」時為同一人，並同時將此階段的驗證方式定義為三個 AAL 等級。

表 3-9 NIST 800-63-3 身分驗證三個等級

嚴謹度	等級	說明
低	AAL1	允許至少「單因子」的身分驗證方式，對驗證方式並無特別限制，可以是單一帳號密碼或是 OTP 認證方式
中	AAL2	需使用「多因子」的身分驗證方式，如需更加嚴謹，則需採用經認可的加密方式或設備等
高	AAL3	需使用「多因子」的身分驗證方式，對於身分驗證的方式及設備更加嚴格，需同時足以證明「something you have 所持之物」及「something you are 所具之形」

資料來源：NIST SP 800-63-3 Figure 6-2 Selecting AAL

3. 聯合身分驗證架構及聲明：

在 NIST 文件中數位身分聯合身分驗證(Federation)的定義是「允許在一組網路系統中傳輸身分和認證資訊的過程」。係指將訊息從一個系統發送到另一個系統(第二個系統信任的第一個系統)以「確認」用戶已通過身分驗證的過程，以及與經過身分驗證的用戶所相關的其他資訊對用戶進行身分驗證的系統稱為身分提供者或身分服務提供者，信任身分服務提供者的系統稱為信賴方。

前述 IAL 或 AAL 都是在敘明評估內部身分驗證機制的參考等級，當一個身分驗證須提供予多個 RP 單位使用時，則會出現聯合身分驗證架構，此時可以參考三個 FAL 等級：

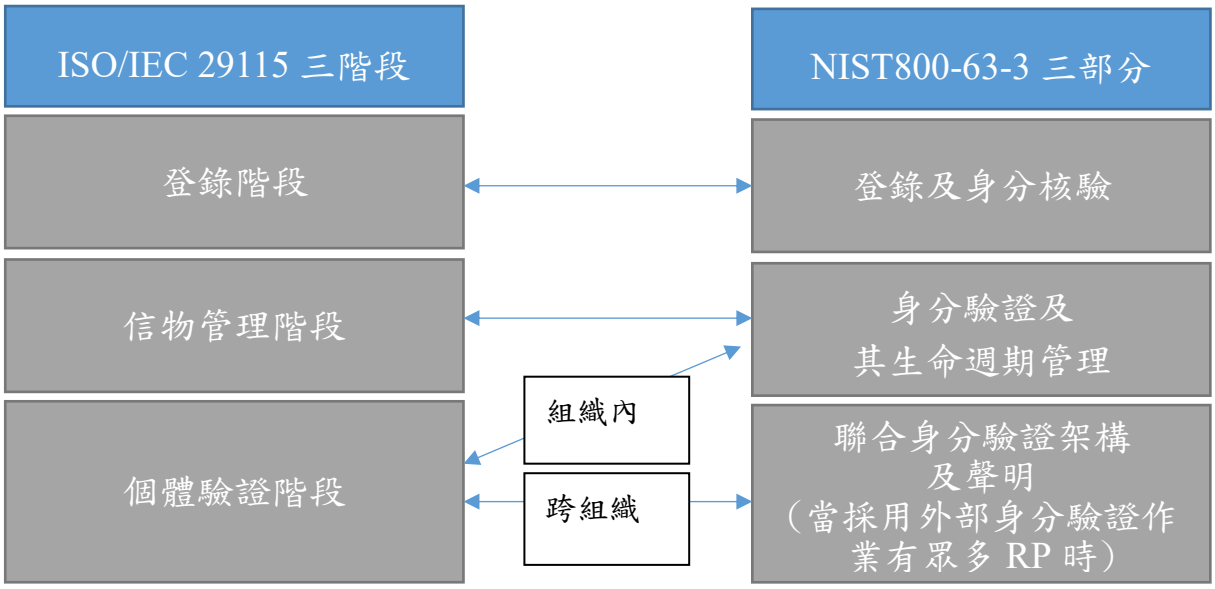
表 3-10 NIST SP 800-63-3 聯合身分驗證三個等級

嚴謹度	等級	說明
低	FAL1	RP 單位獲得一級 IdP 簽署的身分聲明
中	FAL2	除 FAL1 要求外，該身分聲明需進行加密需求，RP 單位是唯一能夠對其解密的一方
高	FAL3	除 FAL1 及 2 要求外，使用者須證明對該「私密金鑰」的所有權

資料來源：NIST SP 800-63-3

(二) ISO/IEC 29115 與 NIST800-63-3 之對應比較

(一) ISO/IEC 29115 身分驗證的三個階段可以與 NIST800-63-3 的三個部分對應，如下圖所示：



資料來源：ISO/IEC 29115、NIST800-63-3

圖 3-2　ISO/IEC 29115 與 NIST800-63-3 之對應比較

(二) ISO 29115 相對 NIST 800-63，更強調管理面與控制點，其 LoA 分三個面向(登錄/辨識、信物管理、信物使用/驗證)，以控制點來界定 LoA。

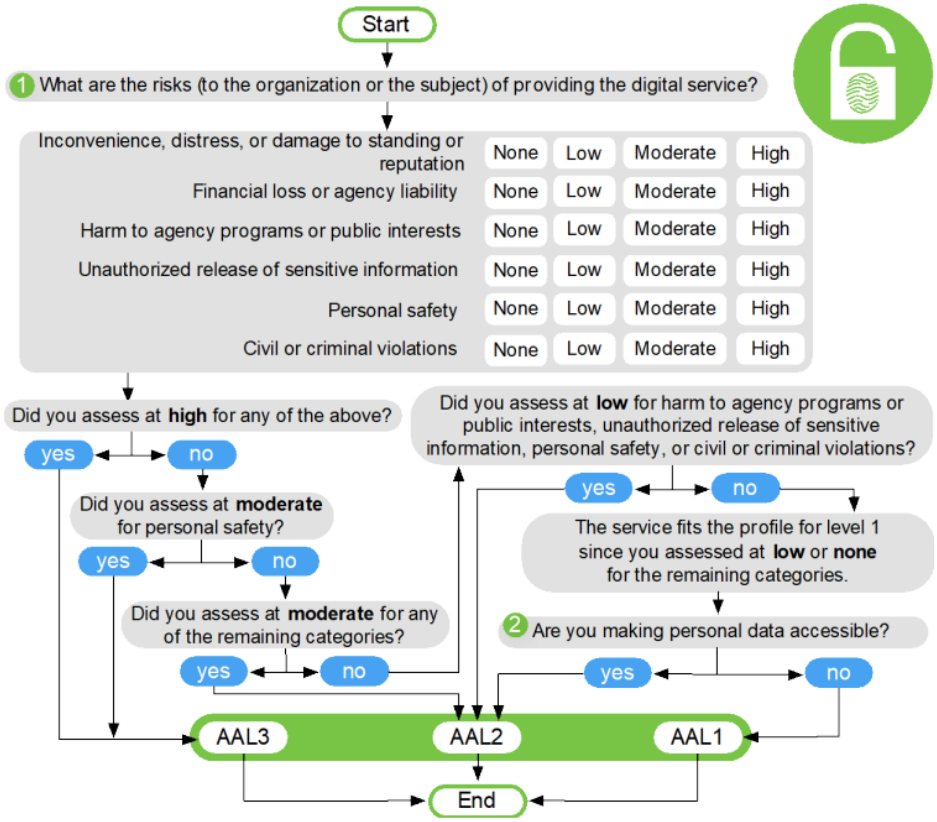
(三) 有關跨機構身分驗證，第三方驗證就是透過外部進行驗證，如實務上有財金公司提供第三方跨機構身分驗證方式，ISO 29115 對此著墨較少，而 NIST 800-63C 有特別針對第三方跨機構身分驗證識別作業規範。

(四) 有關風險信賴等級，不同於 ISO29115，NIST800-63C 把風險信賴等級分為三種：

1. 身分驗證保證級別(Authenticator Assurance Level, AAL)：描述身分驗證過程強度的類別。

2. 聯邦保證級別(Federation Assurance Level, FAL)：描述聯邦式驗證的斷言協議類別，依賴方的身分驗證和特性的資訊(如果適用)。

3. 身分保證級別(Identity Assurance Level, IAL)：傳達申請人聲稱的身分是他們真實身分的信心程度。



資料來源: NIST800-63-3 Figure 6-2 Selecting AAL

圖 3-3 NIST800-63-3 身分驗證信賴等級

第二節　國際數位身分發展應用概況

雖然國際數位身分識別應用的發展有共通的原則與標準，但是各國仍需依國情與當地法規要求，制定相關的身分應用的政策與規範。因此，

本節將研究國際在推動數位身分的先進國家：澳洲、英國、瑞典與新加坡等國家的現行的應用與發展狀況，作為我國的借鏡。

在研究上述各國在數位身分政策的發展時，發現澳洲的 Trust Digital Identity Bill 2021 有提出所謂的信任機制，此機制強調數位身分在跨產業在使用上的相互信賴框架，而澳洲與新加坡在數位身分的應用，也已由自然人發展到法人的應用。由於各國的身分政策與法令內容雜多，因此本章將以數位身分政策與信賴框架為主題介紹澳洲、瑞典、新加坡等國數位身分的應用發展及 2013 年 2 月成立的 FIDO 聯盟。

一、 澳洲

(一) 發展現況：

澳洲政府為了實現澳洲政府數位身分系統（Australian Government DigitalIdentity System）及治理架構，並在法律層級落實人民的隱私保障與消費者保護，於 2021 年 10 月 1 日，由 Minister for Employment, Workforce, Skills, Small and Family Business 提出《the Trusted Digital Identity Bill》，該法案旨在建立安全的可信任數位身份系統，加強網路安全、隱私和個人權利保障，聚焦在擴大澳洲政府數位身分認證系統的涵蓋範圍，私部門的參與、謹守隱私與消費者保護，並建立永久性的治理安排與明確監管架構。

澳洲數位轉型機關（Digital Transformation Agency, DTA；以下簡稱 DTA）依此法案，制定「可信任的數位身分框架（Australian Trusted Digital Identity Framework, TDIF）」，並進一步針對身分服務提供者（Identity Service Providers）、屬性服務提供者（Attribute Service Providers）、信物服務提供者（Credential Service Providers）及身分交換平台（Identity Exchange）等四種合格參與者，提出取得認證所需履行的義務與相應的功能要求。

(二) 澳洲數位身分信任框架（The Trusted Digital Identity Framework, TDIF）

TDIF 是一種信任框架針對屬性服務提供者，信物服務提供者，身份交換和身份服務提供者建立最低要求，以實現並確保 TDIF 認可品質。

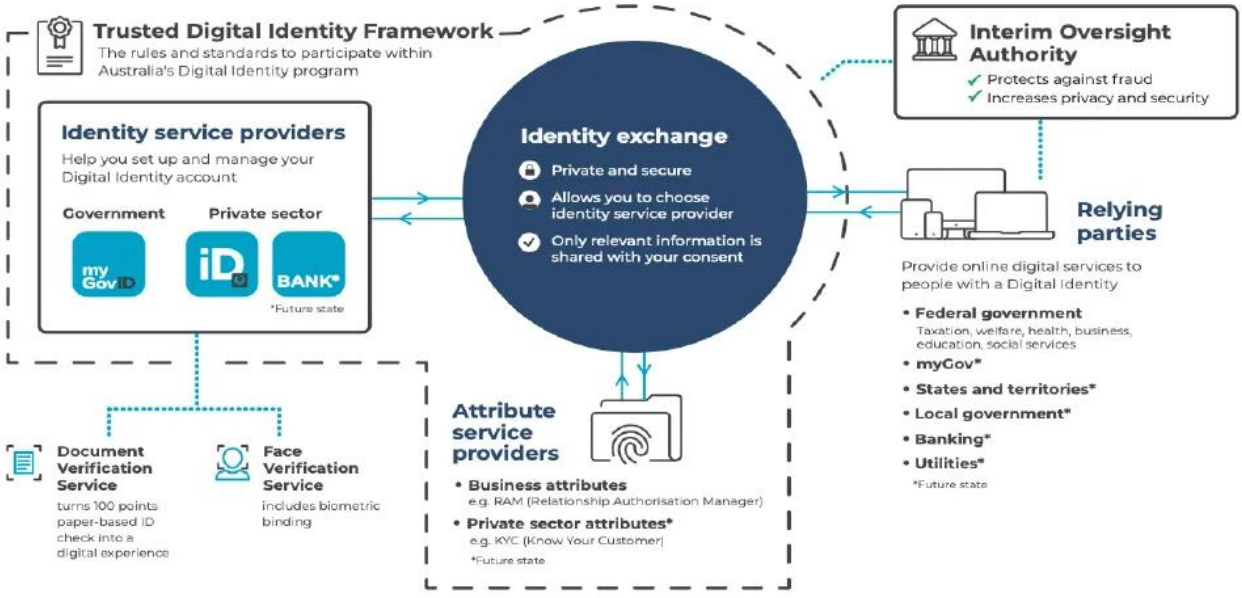


Image source: Australian Government Digital Transformation Agency, DIGITAL IDENTITY LEGISLATION CONSULTATION BACKGROUND PAPER (2020), 9.

資料來源:澳洲 myGovID 研究報告

圖 3-4 澳洲數位身分信任框架

澳洲數位身分系統中大致有五種角色：

1. 倚賴方（Relying Party）：依賴身分服務提供者所提供之身分識別與驗證服務之個體
2. 四種受認證之參與者：
   (1) 身分服務提供者（Identity Providers）：協助使用者建立與管理數位身分之實體。
   (2) 屬性服務提供者（Attribute Service Providers）：協助使用者核驗與管理使用者屬性之實體。

(3) 信物服務提供者（Credential Service Providers）：為使用者管理信物（如密碼及其他權限控制工具）之業者。

(4) 身分交換平台（Identity Exchange）：在使用者同意之下，以安全、注重隱私的方式在倚賴方、身分服務提供者及屬性服務提供者間傳遞資料的業者。

(三) 數位 ID，myGovID：

myGovID 是由澳洲稅務局以及澳洲數位轉型機關(DTA)於 2019 年 10 月共同開發推出，提供 15 歲(含)以上民眾行動化的線上身分證明服務以便安全存取政府相關單位線上服務(如：myGov)來處理個人和商業事務。根據 OpenGov Asia 調查，截至 2021 年 10 月，已有約四百萬人透過 myGovID 註冊數位身分驗證服務，其中約有 82,000 個帳號是運用生物或人臉辨識科技。

(四) 技術應用：

本節參考「澳洲 myGovID 研究報告」簡述澳洲 myGovID 提供之機制。澳洲 myGovID 為澳洲稅務局(Australian Taxation Office, ATO)所發行的行動裝置應用程式與系統，做為澳洲政府的身分服務提供業者，提供 15 歲(含)以上民眾行動化的線上身分證明服務，以便安全存取政府相關單位線上服務 (如 myGov)來處理個人和商業事務。

欲使用此服務的民眾須先進行以下步驟以完成個人設定，取得專屬 myGovID 數位身分：

表 3-11 澳洲 myGovID 機制

強度	基本(Basic)	標準(Standard)	強(Strong)
用途	允許使用有限度(limited)的政府線上服務	允許使用大部分(most)的政府線上服務	允許使用所有(all)的政府線上服務
應具備資料	輸入基本資料並驗證一份身分文件(Your identity strength will still be Basic if you verify one identity document.)	輸入基本資料並驗證至少二分以下的身分文件： 1. 駕照 2. 護照 3. 出生證明 4. 簽證 5. 居留證 6. 難民證 7. 健保卡	輸入基本資料並驗證下料資料： 1. 護照和 2. 下料資料之一 (1) 出生證明 (2) 居留證 (3) 駕照 (4) 健保卡 另外還需要進行照片驗證，將來才能進行臉部辨識(一次性驗證)。

資料來源:澳洲 myGovID 研究報告

myGovID 整體服務在安全上採用密碼學金鑰加密及 PKI 技術，以及行動裝置上既有的安全設定 (例如：指紋、臉部或密碼鎖)，藉以保護用戶的數位身分並避免他人存取相關個人資訊。App 的部份，僅會儲存個人設定所需的核心個人詳細資料：姓名、生日和電子郵件地址。App 設定過程中所拍攝的個人即時臉部照片僅用於一次性檢查，檢查後照片即被刪除且不會傳送出去。

除了自然人應用外，myGovID 也可以作為法人身分使用。法人（Business 身分的申請先由事業的主要負責人(the principal authority of the business) (如下表)要先註冊自己自然人的 myGovID 且身分認

證強度要達「標準」或「強」，再用該自然人 myGovID 連結其事業到關係授權管理平台 (Relationship Authorisation Manager, RAM)。

一旦主要負責人完成上述連結後，就可以在 RAM 上授權其他人成為事業的代表人，進而該被授權人亦可以其自然人 myGovID 就被授權範圍內代表法人進行相關的身分認證。

表 3-12 澳洲主要負責人

類型	說明
獨資機構	獨資商號的負責人(sole trader)
公司機構	已完成澳洲商業登記（擁有商業登記編號）的合格關係人(eligible individual associate)。 例如：受託人(trustee)、董事(director)、稅務專責人員(public officer)、合夥人(partner)、協會或俱樂部負責人(office bearer of a club or association)。
主要個人	主要個人(primary person)，指雖未擁有商業登記編號，但具備以下角色之一者： 1. 事業為公司時，受託公司(corporate trustee)或子公司(subsidiary company)的董事或稅務專責人員。 2. 事業為政府主體(government entity)時，授權聯絡人(authorised contact)屬之。 3. 事業為公益或非營利團體時，受託公司(corporate trustee)或子公司(subsidiary company)的董事或稅務專責人員。 4. 當事業為非法人團體時(unincorporated association)，代表人(office holder)屬之。

資料來源:澳洲 myGovID 研究報告

被授權人(Authorised users and administrators)為主要負責人將事業連結至關係授權管理平台之後，就可以將「代表法人進行身分認證」的權限授權給他人，而他人即此處所稱之「被授權人」。 被授權人類型可以包含：

1. 授權管理人(Authorisation administrator)：當被指派為授權管理人，即可像前述主要負責人，再指定其他人為授權。

2. 被授權的使用者 (Authorised user)：能代表法人進行授權範圍內的身分驗證。

3. 機器信物管理人 (Machine credential administrator, MCA)：被指派後能新增或管理機器信物。

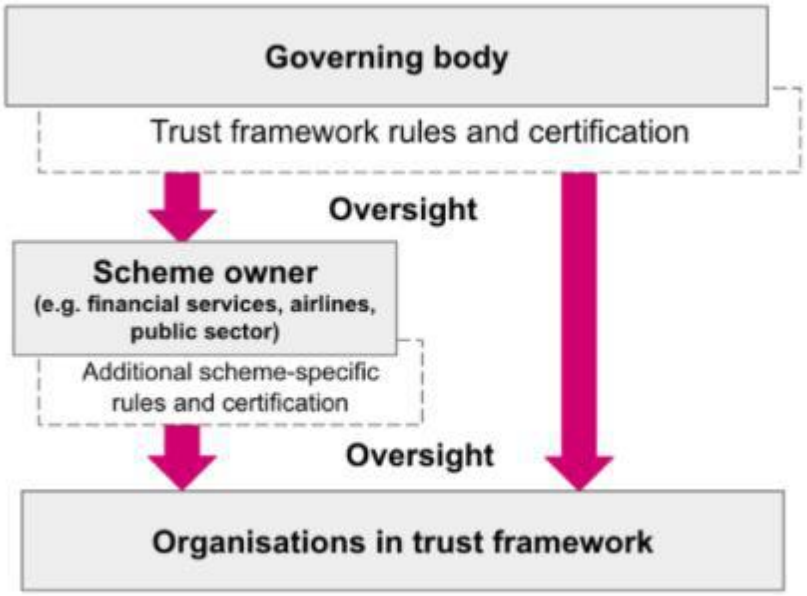
4. 機器信物 (Machine credential)：該信物能使事業在使用標準化商業申報軟體(Standard-Business-Reporting-enable software)時，能直接與政府單位對接與互動。

二、 英國

(一) 發展現況：

英國的數位身分與屬性信賴框架(Digital Identity and Attributres Trust Framework)，是由英國數位、文化、媒體、運動部所提出數位身分證明與屬性交換的信賴框架，目前仍處於草案階段。有別於其他各國以 PKI 的機制建立數位身分的驗證機制，英國則是採用類似聯邦式的機制，建立身分驗證與屬性資料交換的架構。

在這個聯邦當中，各產業可以提出不同的身分證明方案(scheme)，之後會由主管權責單位(govering body)確認技術規範標準以及推動認證(certification)作法，通過認證的機構即可以該產業進行身分驗證與資料交換。



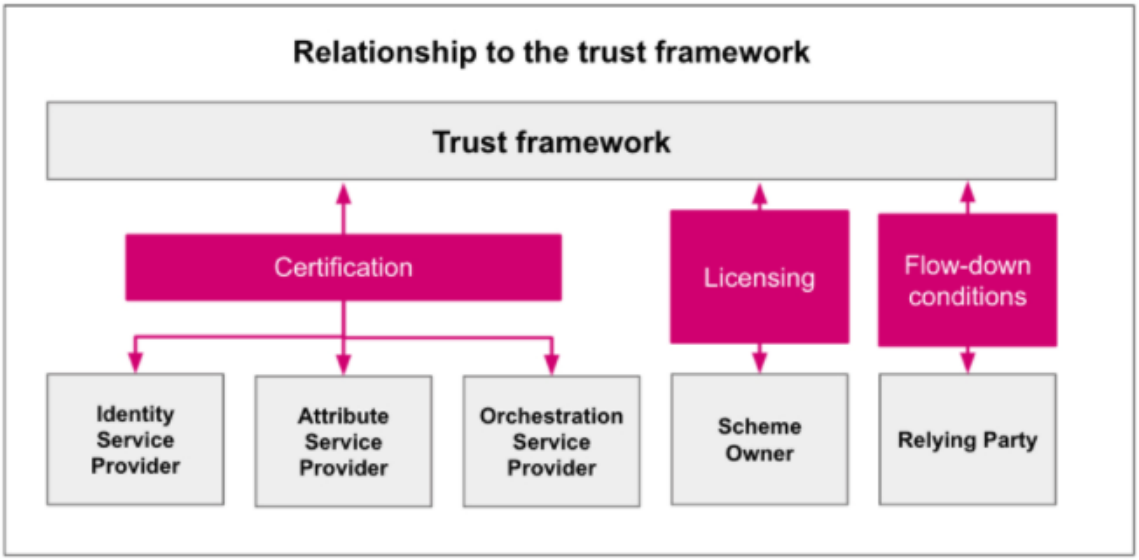
資料來源：政治大學金融科技研究中心(2022)

圖 3-5 英國數位身分與屬性信賴框架運作架構

在這樣的類似的聯邦式機制下，共有五個不同角色（如下圖），分別為：

1. 身分服務提供者(identity service provider)
2. 屬性服務提供者(attribute service provider)
3. 調度服務提供商(orchestration service provider)
4. 依賴方(relying party)

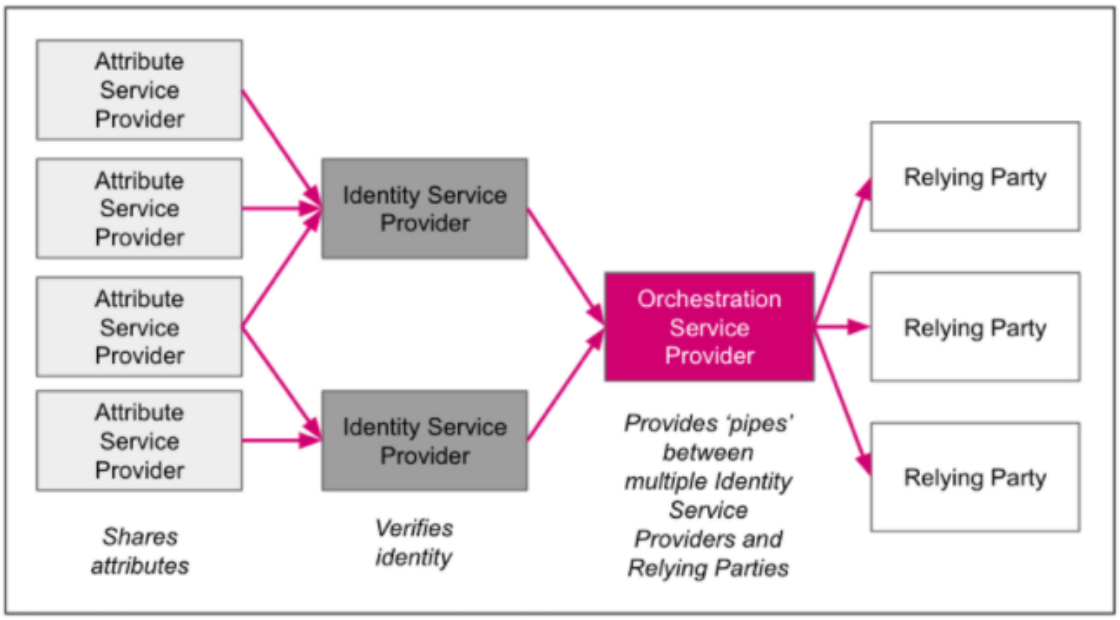
5. 方案所有者(scheme owner)



資料來源：政治大學金融科技研究中心(2022)

圖 3-6 英國數位身分與屬性信賴框架角色架構

在這個信賴框架下，產業業者要進行身分驗證時，身分服務提供者、屬性服務提供者，以及調度服務提供者，都必須要通過技術標準的認證後，才能進行相關的身分驗證與資料交換作業。其中，比較特別的是身分服務提供者的角色功能，身分服務提供者，可以是身分註冊單位(RA)、信物提供單位(CSP)或身分驗證單位(VA)的全部或部份功能。而調度服務提供者則是為對多個身分驗證單位的中介單位。產業可依自己的特性，決定這五個角色如何互動（如下圖）。



資料來源：政治大學金融科技研究中心(2022)

圖 3-7 英國調度服務提供者角色

英國發展現況：

1. 有別於 PKI 機制，英國則是提出聯邦式的機制。
2. 不強調技術，強調產業內身分驗證的參與者角色與功能，再透過標準化過程與認證機制，達到信賴框架之目的。

三、 瑞典

(一)發展現況：

2003 年瑞典集合多間當地銀行進行合資，開發了「Bank ID」。使用 Bank ID 的用戶在拿到一間銀行的憑證後，也可以登入另外一間銀行的帳戶，讓同一組帳號密碼可以通用。Bank ID 的方便性導致使用者急速增加，瑞典政府注意到後，也將 Bank ID 設置為能夠在政府及企業使用的電子憑證系統。

隨著智慧型手機的使用的增加， Bank ID 於 2010 年也相對的推出了行動版的 Mobile Bank ID。它和瑞典最多人使用的行動支付 Swish 綁定，讓非現金支付逐漸流行起來。目前為止，瑞典約一千萬的人口中有超過 800 萬人擁有 Bank ID，而且 96%的使用者有在手機上安裝 Mobile Bank ID，非現金支付的比率因此達到 87%。

瑞典人現在只需使用 Bank ID 一組的認證系統就能進行繳稅、繳水電費、登入網路銀行、或是網路博奕等。根據數據統計公司 Statista 的報告，20 到 50 歲之間的族群平均有高達 98%的使用率，而 70 到 80 歲之間的族群也有近 60%的使用率，顯示出了 Bank ID 的通用性。除此之外，Bank ID 擁有完善的流程，客戶使用它申請車貸的成功率比其他管道還要高 50%。然而 Bank ID 還是有一定的風險。在 2018 年 7 月裡，和 Bank ID 相關的網路詐騙案就在瑞典造成了約 1960 萬瑞典克朗（約新台幣 6,200 萬元）的損失。雖然 Bank ID 的使用方便但仍須針對保護個資安全方面再做加強。

瑞典 Bank ID 兩大特色：

1. 串連行動支付：透過手機版 Bank ID 串連行動支付，讓非現金支付比率提高。
2. 萬用電子憑證：由公私部門合作，讓公司連內部系統都使用 Bank ID 認證，節省企業的後台開發成本。

(二)技術應用：

瑞典 BankID 提供瑞典國民或具有居留權者身分證明(identify)服務，民眾能證明自己的身分以使用企業或機構所提供的電子服務或合約簽屬等，BankID 是一種通用的證明身分方法，在數位應用中，民眾不再需要建立帳號密碼，只需像是傳統環境中拿出身分證件一般的證明自身身分。

使用 BankID 的服務，用戶需透過 BankID 合作銀行，由銀行開啟服務，也就是用戶(end user)選擇啟用這項服務的註冊機構(RA)為 BankID 合作銀行，然而每家銀行的作業流程或有不同。用戶、銀行、BankID 三種角色之外，要實際接受使用 BankID 用戶的依賴方 (RP)，會透過 BankID 服務來對用戶提供驗證與簽章服務。使用 BankID，用戶必須在行動裝置或是個人電腦中安裝 BankID app，同時需要向相對的銀行訂購(order)一個 BankID 依賴方以正確的 SSL 客端憑證(client certificate)透過 BankID 提供的 web service API 識別或進行簽章相關服務，這些服務可能執行在與 BankID 相同的裝置或分別在不同裝置運行，運作上則會有不同的使用流程。

BankID 常見的使用案例有：

1. 數位新戶(digital onboarding): 註冊新戶時，選擇以 BankID 證明身分。
2. 驗證(authentication): 使用銀行服務時，當需要進行身分驗證以證明用戶身分時，使用 BankID 證明用戶身分。
3. 簽章(signing): 透過 BankID 的電子簽章機制可對文件進行簽屬等相關服務，例如用戶需要簽屬合約或是貸款申請書等。

BankID 在技術上，RP 的憑證必須安裝或配置在用戶的金鑰儲存空間(key store)中，由 BankID server 驗證，BankID server 再出示自身憑證以達成雙向驗證，其中資料交換介面上 BankID 採用 JSON 格式，通訊介面透過 HTTP 1.1，且轉址要求透過 HTTPs 傳輸。

在 BankID 核心部分，BankID 技術建立於 Swedish eID 框架之上並滿足信任等級 3 的要求，由身分供應者(Identity Providers)提供 BankID 驗證與簽章的服務。在數位身分的呈現上 BankID 有三種型式：

1. Mobile BankID：用戶透過自身行動裝置中的 BankID app，執行驗證和簽章用戶的憑證儲存於行動裝置中並以個人代碼(personal code)保護。

2. BankID on file：用戶透過電腦上的 BankID Security Application 進行驗證和簽章，用戶憑證儲存在電腦中並以用戶密碼(user password)保護。

3. BankID on card：用戶使用 BankID on file 同樣程式，但憑證儲存於智慧卡(smart card)中，用戶的私鑰是由卡片的 PIN 保護。

為符合瑞典的 eID 框架，採以 SAML2.0 標準，並使用符合 x.509 的憑證於框架中識別各種角色的身分。以上 BankID 之 eID 的應用，皆採用成熟技術，註冊登錄階段透過用戶往來之銀行，且具備核驗用戶是否具有瑞典身分之過程。如此連結政府所管理的身分，運作上透過銀行所發行管理之身分以提供生活應用的簽約與支付所需的身分識別需求。

瑞典 Bank ID 發展重點：

1. 由銀行開始推動的 PKI 憑證系統，進而推動到政府與跨產業的應用。

2. 支援支付與電子文件應用，則遵循歐盟 eIDAS 的規定。

四、 新加坡

(一) 發展現況：

近年來金融產業之技術規格正迅速轉變，支持金融業基礎之資訊技術基礎設施之複雜性逐漸增加，許多金融機構向消費者提供更多元之服務類型，進而提高營運效率。新加玻金融管理局（Monetary

Authority of Singapore）進而於 2021 年 1 月修訂科技風險管理指引（Technology Risk Management Guidelines），訂定金融業技術風險之管理原則以指導金融機構建立健全及穩固之科技管理和監督制度，並保持網路之彈性，加強金融機構網路應變能力。

最早，新加坡的 Singpass 於 2003 年正式在新加坡推出，起初為針對 60 個政府機構進行線上交易之個人存取系統。在新加坡政府推行國民數位身分證計畫後，並歷經於 2017 年 Singpass 系統被發現漏洞，造成部分民眾個資遭竊之事件。新加坡政府為了預防相關資安漏洞再度出現，結合政府技術局於 2018 年推開發以 Singpass 為框架之國民數位身分證，並推出 Singpass Mobile 的 App，要求用戶進行雙重驗證之登錄與設定並且結合人臉辨識、指紋等辨識技術，增加其個資保護及認證之強度。此開發使新加坡成為全球首個將人臉辨識納入國民身分證辨識之國家，並提供其服務更多可行性。並且於 2020 年發表 App 之更新並導入數位身分證（Digital Identify Card, Digital IC），提供用戶做為新的身分驗證方式。於 2021 年 11 月起，除了少數因法律要求實體之情形之外，所有新加坡政府機關已接受將 Singpass 之 數位身分證作為正式的身分證明方式之一。

現 Singpass 以可以提供超過 180 個政府部會的 500 種數位服務（移民署相關程序、納稅、護照更新等服務）給所有公民或持有永久居留權或有工作、親屬、長期簽證等人使用。除了可以用於登入政府服務之外，現在已經陸續開放能用 Singpass 架構至一些私人企業來辨識 民眾或進行相關服務，例如繳納保險費或銀行交易等數位服務。

Singpass Moblie 內也可提供用戶輸入個人資訊（MyInfo）像姓名、身分證字號、地址、聯絡方式、駕照、學歷、就業經歷等個人資訊，並可方便用戶政府服務時，自動輸入相關資訊至表格欄位。日後也可期待新加坡政府開放利用個人資訊（MyInfo）至銀行等金融機構或是私人企業去進行個人資料的存取或利用。

針對 Covid-19，新加坡政府也把疫苗接種證明轉換成電子證書並導入制 Singpass 系統，利於在進行身分驗證的同時也提供因應疫情的相關證明。

(二) 技術應用：

本節參考「新加坡 Singpass 研究報告」，簡述新加坡 Singpass 提供之機制。Singpass 本身是一個行動 APP 為新加坡政府技術局管理的一個可廣泛用於新加坡政府數位服務的 APP，有了 Singpass，用戶可透過此 APP 作為主要的身分識別機制，登入拜訪許多政府單位，甚至是私人企業。Singpass 主要可申請的用戶為「個人戶」，如新加坡公民、永久居民，或者是持有工作簽證、親屬簽證等，都可以透過線上，或於居家附近的 Singpass 櫃台臨櫃申請。完成申請後即會收到一個有效期的密碼函，需在密碼函過期前使用 Singpass APP 完成註冊作業。

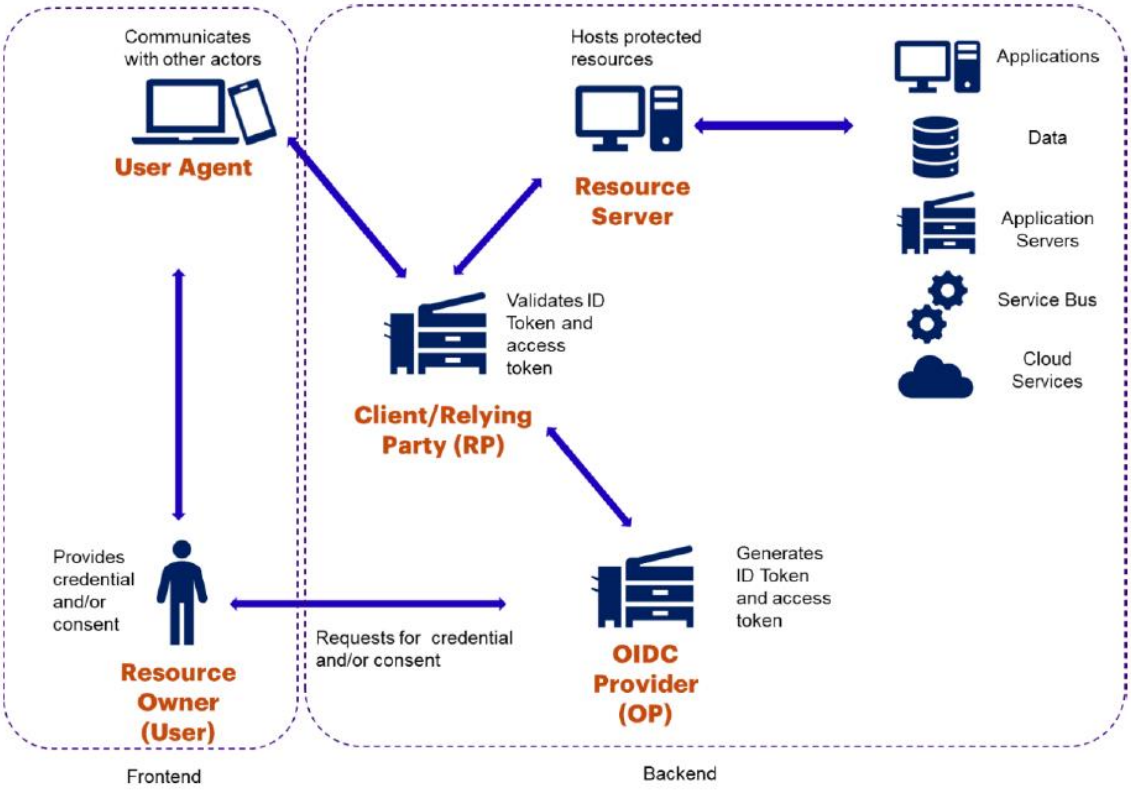
然而 Corppass APP 原本主要提供企業使用，當企業需要申請營業執照、支付公司稅，或進行報帳等作業，則指定的公司員工用戶則可透過 Corppass 登入政府的數位服務進行交易。但 Corppass 官方網站公告於 2021 年 4 月 11 日起，企業也改使用 Singpass APP 於政府數位服務上，因此以下以 Singpass APP 說明該 APP 主要提供的功能及其主要使用的技術。

最大宗的應用，即是用戶可以使用 Singpass APP 註冊並登入數以千計的新加坡政府單位數位服務或者企業，而不需要另外逐一設定帳號密碼，Singpass APP 為政府及企業的數位服務進行身分驗證。政府或企業的數位服務平台或網站上顯示 Singpass Login 的 QR Code，用戶掃描 QR Code 即可使用已註冊的 Singpass APP 登入該數位服務。此功能主要建構在 OpenID Connect (OIDC)及 OAuth 2.0 技術上，其作業程序可參照，以下簡述各職責：

1. OIDC Provider（OP）主要即是擔任 Idp 的角色，用戶於此單位註冊，並管理用戶的身分，並於後續驗證時提供 ID token 及 Access token。

2. Relying Party（RP）則負責驗證 OIDC Provider 所提供的 ID token 及 Access token，並決定是否接續 Resouce server 提供後續的數位服務。

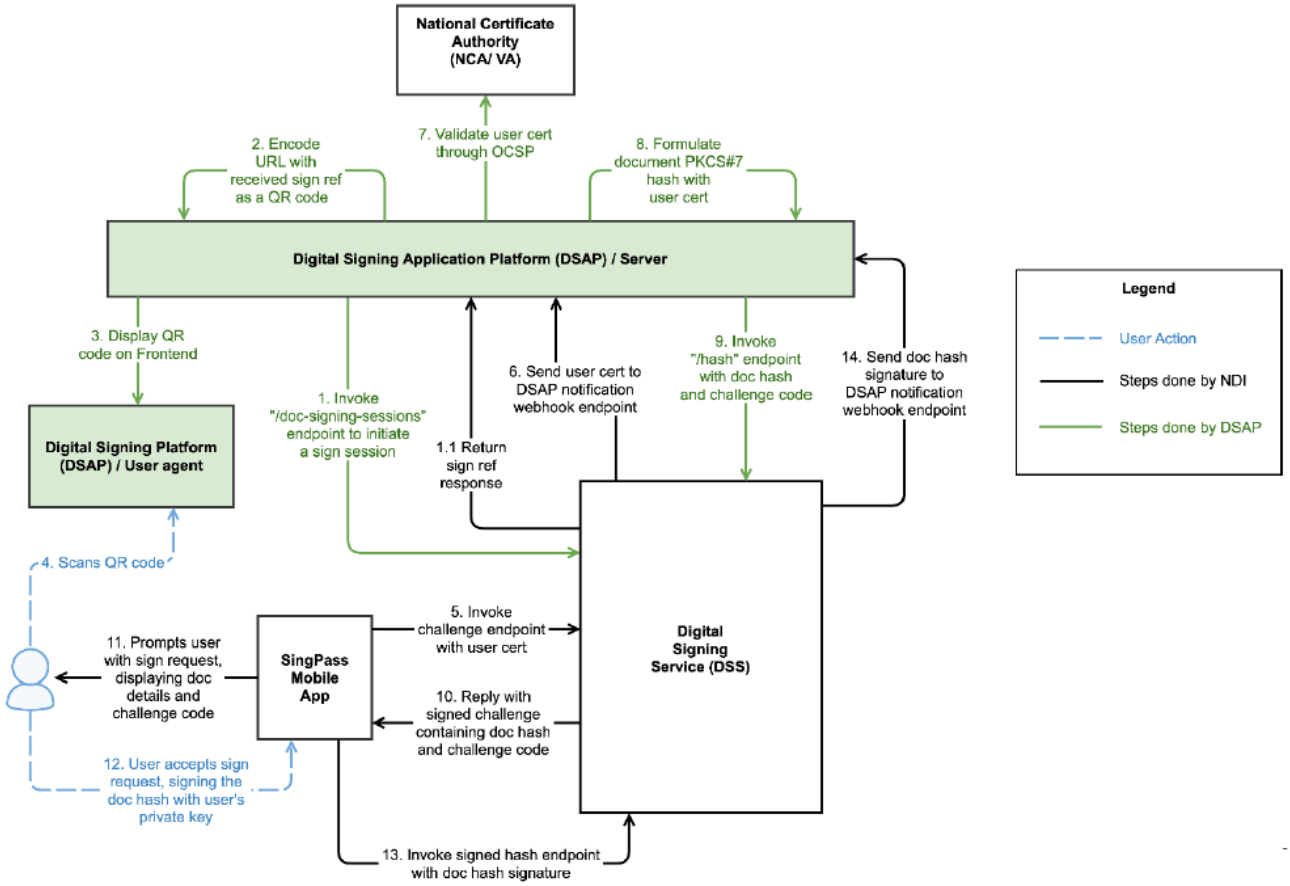
3. Resource Owner（User）則會收到由 OpenID Provider 提出要求驗證的訊息，並在確認提供驗證的 RP 單位後，點選確認同意驗證。



資料來源：新加坡 Singpass 研究報告

圖 3-9 新加坡 Singpass 身分驗證

而除了上述最大宗做為新加坡政或企業的數位服務（平台）的登入機制外，新加坡的企業或民眾亦可以透過 Singpass 進行電子文件的簽署作業，藉由國家認證機構（National Certification Authority）所發行的簽署憑證（signing certificate），對電子文件進行數位簽章作業，以符合新加坡的電子交易法（Singapore's Electronic Transactions Act），簽署的流程可參考下圖。



資料來源：新加坡 Singpass 研究報告

圖 3-10 新加坡 Singpass 電子文件簽署流程

新加坡 Singpass 發展重點：

1. 由政府開始推動的 PKI 憑證系統，推動以 Singpass 的 mobile APP

身分驗證。

2. 不同業者可以透過 OAuth 與 OIDC 技術架構與政府進行跨業的身分識別與資料交換。

3. Singpass 也可以作為電子文件簽章使用。

五、 FIDO 聯盟

(一)FIDO 聯盟簡介：

FIDO 聯盟於 2013 年 2 月成立，是一個具有開放性的非營利產業聯盟，聯盟創始者是 Paypal 跟聯想的創辦人，其他著名的成員還包含 Google、Apple、Microsoft 等各國際科技服務大廠；FIDO 聯盟主要使命為開發和推廣身份驗證標準，藉此幫助全球各個產業、服務應用等減少對密碼的依賴性，並期望透過以下方式來實現：

1. 制定技術標準，確立一套開放，可擴展，可協作的機制，以減少驗證使用者時對密碼的依賴。
2. 實施行業認證計劃，以幫助確保在全球範圍內成功採用該標準。
3. 將成熟的技術標準提交給公認的標準制定組織，使 FIDO 實現標準化。

國際電信聯盟(ITU)於 2018 年也將 FIDO UAF 和 FIDO2 CTAP2/U2F 納入正式標準。因為有了 FIDO 聯盟所制定的標準，才能夠令全球多樣化的無密碼解決方案有統一的標準，讓需求企業挑選符合自己的方案，也讓這些企業的顧客受到更深一層的保障。

(二) FIDO 介紹：

FIDO 全名是 Fast IDentity Online，可將傳統密碼的登錄方式替換為跨網站和應用程式的快速安全登入體驗。FIDO 實際上並不是一款具體的產品，而是一種來自 FIDO 聯盟的開放技術標準，定義

了減少密碼依賴的用戶身份驗證解決方案，只有符合這個標準的方案，才能掛上 FIDO 驗證的名字。

FIDO 的核心主要在於使用者的資料都被保存在硬體裝置端，而非存放於網路伺服器中，驗證資料時並不存在於傳輸過程，因此，能夠最大化的降低資料被竊取的可能性。FIDO 的應用層面廣泛，只要有密碼跟驗證需求，都可以使用 FIDO 解決方案，能夠同時兼顧安全與便利需求，逐漸被要求高度資安的金融界、科技業等廣泛採用。

(三) FIDO 相關規範：

FIDO 是一種方案標準，擁有各式各樣對於網頁端、移動端的不同標準，其主要特徵如下：

1. U2F：實體兩要素(two-factor authentication, 2FA)身份驗證密鑰的標準規格。
2. UAF：無密碼身份驗證技術的標準規格。
3. FIDO 2.0：
   (1) WebAuthn：一組標準的 Web API，允許在瀏覽器中進行無密碼身份驗證。
   (2) CTAP1：FIDO1.0 的 U2F 標準，在 FIDO2 中保留下來並重新更名。
   (3) CTAP2：使用實體密鑰和移動身份驗證器應用程序實現 2FA 和無密碼身份驗證的規範。

六、 小結：

表 3-13 各國身分驗證重點比較

國家	法規/應用	摘要重點
澳洲	TDIF myGovID	1. 澳洲有推動「可信任的數位身分框架(Australian Trusted Digital Identity Framework, TDIF)」作為國家級身分驗證的基礎，並規範身分證明的等級 2. myGovID 是由澳洲國稅局推動的 PKI 身分架構，符合 TDIF 的要求；針對身分註冊時，有區分不同身分證明強度等級 3. myGovID 有擔任驗證單位(VA)角色，提供跨業的業者(RP)使用 myGovID 身分驗證服務
英國	Digital Identity and Attributes Trust Framework	1. 有別於 PKI 機制，英國則是提出聯邦制的機制 2. 不強調技術，強調產業內身分驗證的參與者角色與功能，再透過標準化過程與認證機制，達到信賴機制
瑞典	BankID	1. 由銀行開始推動的 PKI 憑證系統，進而推動到政府與跨產業的應用 2. 對於支付與電子文件應用，則遵循歐盟 eIDAS 的規定。
新加坡	Singpass Corppass	1. 由政府開始推動的 PKI 憑證系統 2. 不同業者可以透過 OAuth 與 OIDC 技術架構與政府進行跨業的身分識別與資料交換 3. Singpass 也可以作為電子文件簽章使用

資料來源：本研究自行整理

整體而言，從各國的發展對我國金融業未來數位身分影響，應跳脫產業疆界來思考數位身分制度。國際間數位身分制度首重信賴框架的建構，該框架的兩大要素是「共商信賴等級」及「釐清不同參與

者的角色功能」，「隱私、詐欺管控、安全保護措施」是各參與者皆須注重的面向，而妥適數位身分制度的設計有助於提升普惠金融。

而以金融產業等級的數位身分系統的主要功能在於：首次開戶時協助客戶之識別與核驗、在整體業務關係中支援持續性及反覆性的身分驗證、落實客戶的盡職調查及交易監管、確保客戶授權與意思表示的真實性及不可否認性。所以，數位身分系統在應用上的本質是信任與風險承受問題，法規跟技術其實是信任與風險承受問題的體現，自然人與法人皆然。

觀諸國際數位身分應用發展，數位身分系統在應用上的本質是信任與風險承受問題，而法規跟技術乃是信任與風險承受問題的體現（自然人與法人皆然）；以金融業來說，數位身分系統的主要功能為協助金融業識別與核驗首次開戶之客戶，在整體業務中支援持續性及反覆性的身分驗證，並可落實對客戶的盡職調查及交易監管，以及確保客戶授權與意思表示的真實性及不可否認性。數位身分驗證制度首重信賴框架的建構，該框架的「共商信賴等級及釐清不同參與者的角色功能」及「隱私、詐欺管控、安全保護措施」等兩大面向，以及設計數位身分制度，將可做為集保結算所構思妥適數位身分驗證制度之重要參考。

第四章　集保結算所數位身分驗證方案探討

(略)

第五章　結論與建議

近年來，隨著金融業的數位化發展，許多金融服務業者爭相提供遠距與無接觸的產品與服務，如網銀開戶、線上證券投資理財、遠距投保等。然而金融業於發展數位創新業務的同時，也面臨不斷變革的資安威脅，促使數位身分驗證議題日益重要。

第一節　結論

本研究經彙整主管機關推動之數位身分驗證機制政策，以及國際數位身分驗證標準與規範，擷取可作為集保結算所建構數位身分驗證框架之參採內容，謹就主要結論說明如下：

一、主管機關高度重視日益嚴重的資安威脅，發布「金融資安行動方案」等重要政策並積極推動

(一)金管會長期關注並督促金融機構資安防護，鑒於資安威脅日益嚴峻，經觀察國際金融資安情勢與資安監理趨勢，於 109 年 8 月發布「金融資安行動方案」，分別從強化主管機關資安監理、深化金融機構資安治理、精實金融機構資安作業韌性、發揮資安聯防功能等四個面向切入；另為加強「金融韌性」，金管會進一步於 111 年 12 月 27 日宣布啟動為期三年的「金融資安行動方案 2.0」，在追求安全、便利、不中斷的金融資訊服務之願景下，以「金融資安行動方案」為基礎，滾動檢討精進措施。

(二)金管會於「金融科技發展路徑圖」，除了積極推動金融行動識別與資安措施，更力推「行動自然人憑證」及「數位身分認證及授權」主題式監理沙盒與業務試辦，希望能透過「刷臉」、「按指紋」等多元新興技術完成身分認證，或運用金融科技，提升身分識別的自動化作業；另金管會近期公布的「金融科技發展路徑圖 2.0」，積極推廣金融科技技術與應用，推出「金融 FIDO V2 計畫」，致力於實現普惠、創新、韌性和永續的金融科技生態環境。

(三)金管會為促進金融業發展，提供民眾取得更便利之數位金融服務，訂定一參考性質之「金融服務業辦理數位身分驗證指引」，就數位身分驗證中具共通性之內容揭示辦理原則，以利各業別數位身分規範具共通性，並作為金融服務業各業別數位身分規範之參考。

二、參考國際推動身分驗證機制做法，規劃建構全公司適用之多元身分驗證框架，將可降低資安風險、有助提升集保結算所數位金融服務的信賴水準

(一)身分驗證是所有金融服務的第一道關口，隨著科技的進步以及數位化的發展，為了保障資訊以及交易之安全，防止身分之偽造與冒用，目前國際上已有對於數位身分之管理以及身分驗證，訂定了不同的管理規章及國際標準，如歐盟 eIDAS、美國 NIST800-63-3 及國際標準化組織制定的 ISO/IEC 29115。

(二)另為使民眾更方便、安心使用數位金融服務，許多國家正積極發展數位身分驗證相關機制，以提升身分認證授權的便利性與安全性，如澳洲推動數位身分信任框架，澳洲及新加坡發展數位 ID 如 myGovID、Singpass，美國提出 NIST 數位身分指南，歐盟則修訂 eIDAS 規範電子簽章，此外，ISO、FIDO 等國際組織也推動各項技術標準。

(三)隨著數位身分驗證在金融服務更為廣泛運用，鑑於數位服務對於身分之驗證需求越來越多，數位身分應用也越來越多元，集保結算所可參考國際 ISO29115 與 NIST SP 800-63 數位身分驗證標準規範，制定及推動身分驗證機制，設計全公司適用之數位身分驗證框架，並制定公司內部適用程序文件，作為釐清各業務應用場景之主體、驗證等級(LoA)、風險評估、信物管理、驗證流程設計等業務應用指引，將可降低資安風險，提升集保結算所數位金融服務的信賴水準。

三、集保結算所 30 多年來業務多元發展，已涵括股票等 5 大核心業務及許多輔助的業務，現行系統的身分驗證機制尚屬嚴謹，惟可再參考建議框架強化提升

(一)集保結算所深耕市場後台服務 30 多年，在集保 4.0「數位與資安」時代，集保結算所業務已涵括股票、期貨、債票券、跨境保管、基金等 5 大核心業務，周圍還有許多輔助業務系統，以及人事管理、財務管理等內部系統，每一個業務都有其專屬的業務系統，對於這些核心及大大小小業務系統的身分驗證，集保結算所都是很嚴謹的進行風險評估與信賴等級，來規劃設計各業務系統之相關身分驗證機制。

(二)集保結算所於規劃各業務系統身分驗證過程中，以攸關 400 多萬用戶的集保 e 手掌握系統最有挑戰性。首先，針對集保 e 手掌握所提供之各項功能服務進行嚴謹的風險評估，並依照身分驗證三個作業階段之措施進行檢視，由於集保 e 手掌握提供服務包含證券、基金及銀行等個人資產資料之查詢，涉及機敏個資及公司商譽，根據風險評估應符合 LoA3 之信賴等級，因此，現行集保 e 手掌握身分驗證機制採裝置碼（UUID）搭配帳號與密碼（或生物辨識），符合專屬之 LoA3 要求。然而若集保 e 手掌握未來新增線上申請或變更基本資料之服務，應用場景之延伸除了會提升風險影響，同時應考量是否須結合電子簽章機制作為相關意思表示之用途，以符合相關規範。

第二節　建議

本研究綜上二項建議如下：

建議一：集保結算所各業務系統依本研究之驗證框架，進行盤點分析及確認未來公司之驗證框架，於評估框架導入的挑戰後，研擬推動順序及時程

未來本公司建立之驗證框架須包含之重點如下：

(一)依集保結算所業務特性，規劃設計數位身分驗證框架，參照 ISO 29115 之身分登錄、信物管理及驗證三個階段，將風險等級與驗證機制分為三級或四級。

(二)依照數位身分驗證評估流程，彙整各項系統之用戶類型、角色、交易類型等基本資料，進行身分驗證錯誤對系統的影響評估，且應用場景之風險等級與驗證機制之信賴等級應依風險基礎原則相互適配。

(三)依集保結算所各系統風險高低及使用對象分類，建議參考下列原則逐步進行系統導入：

1.高風險系統之內部使用者優先：有鑑於內部使用者具有如大量或跨單位資料查詢之權限，且新增第二因子之數量成本較低且使用習慣衝擊較小，建議高風險系統內部使用者，優先採用新式身分驗證。

2.網際網路系統優先：考量網際網路連線使用者為不特定對象，較專線網路之特定對象較為多元，建議網際網路系統優先導入。

3.中高風險系統之 B2C 使用者：參照金管會「金融服務業辦理數位身分驗證指引」之公布期程，本公司如電子投票系統等屬指引規範納入之系統，配合安排系統導入。

4.中高風險系統之 B2B 使用者：考量本公司多項 B2B 系統，係由參加人指定內部人員執行職務，建議未來參考前項指引，研議一致的數位身分驗證規範，作為全公司內外部系統共同遵循，以利系統處理邏輯一致，簡化系統開發人力投入。

建議二：依據未來公司確認之數位身分驗證框架，制定於公司 ISO 程序文件中，以作為各業務應用場景應用參照，同時依「金融服務業辦理數位身分驗證指引」要求，納入內控制度並定期檢視是否合宜

(一)本公司現行系統，應依照數位身分驗證框架及優先順序，依據風險、成本及相關衝擊性，循序漸進逐步導入，並建議制定集保結算所數位身分驗證程序文件；另針對未來新系統上線，建議於程序文件中，明定數位身分驗證相關評估流程，以利新系統開發時遵循，並定期檢視是否合宜。

(二)本研究建議數位身分驗證框架建構後，業務及資訊單位針對新系統需求開發，應共同討論判斷該系統之身分驗證等級與驗證機制；屬提供

自然人客戶之數位服務，須配合金管會「金融服務業辦理數位身分驗證指引」，檢視本公司辦理自然人數位身分驗證的相關服務規章，評估落實指引的方式；另本公司新種數位服務應用場景或新式數位身分驗證方式，其規章應參考該指引之原則，並納入內控制度。

(三)考量本公司多項 B2B 系統，參加人指定自然人執行職務，建議未來研議一致的數位身分驗證規範，提供全公司內外部系統共同遵循，以利邏輯一致，系統簡化。

參考文獻

1. Aleksandr O., Vitaly P., Sergey B., Sergey A., Yevgeni K., and Mario G. (2019). **"Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications,"** IEEE Network, Vol. 33, Issue: 2.
2. Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). **"Electronic Authentication Guideline. National Institute of Standards and Technology".**
3. CEMLA (2019). **"Key Aspects around Financial Technologies and Regulation Policy report,"** Fintech Regulatory Aspects Working Group.
4. Grassi, P.A., Garcia, M. E., & Fenton, J.L.(2017). **"Digital Identity Guidelines. National Institute of Standards and Technology".**
5. ISO/IEC 29115:2013(E). **"Information technology – Security techniques – Entity authentication assurance framework"**.
6. NIST SP 800-63-3.(2017) **"Digital Identity Guidelines: Enrollment and Identity Proofing Requirements"**.
7. Nilesh A.L., Salendra P., Mohammed F.(2016).**"A Review Of Authentication Methods,"** International Journal Of Scientific & Technology Research Vol. 5.
8. World Bank Group. (2018) **"Technical Standards for Digital Identification Systems".**
9. Yin, R. K. (2018). **" Case study research and applications: Design and methods. Sage publications".**
10. 谷湘儀、臧正運(2019)，**「變革中的金融科技法制」**，臺北：五南。
11. 李中仁(2018)，**「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。

12. 政治大學金融科技研究中心(2022)，「**多元之數位身分驗證(含電子簽章)研究案**」，集保結算所專題研究計畫。

13. 連子清、杜宏毅(2022)，「**身分識別之書-The Book Of Identification**」，台灣網路認證股份有限公司。

14. 連忻(2023)，「**試論我國建構數位身分法制之框架—從金融場景出發**」，政治大學法律學系碩士論文。

15. 黃世欽(2018)，「**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。

16. 陳漢榮(2023)，「**數位個體身分驗證的風險與挑戰-以應用於金融業來探討**」，臺北科技大學工業與科技管理 EMBA 專班碩士論文。

17. 國家資通安全研究院(2023)，「**政府零信任架構身分鑑別機制導入建議_V1.1**」，資安院零信任架構專區網頁。

18. ----(2023)，「**政府零信任架構說明_V2.0**」，資安院零信任架構專區網頁。

19. 臧正運(2022)，「**數位金融服務管理規範的制度框架思考**」，臺灣法律人：第 10 期，頁 128-139。

20. 葉丞軒(2023)，「**數位金融發展之挑戰-以數位身分驗證與電子簽章為核心**」，東吳大學法律學系碩士論文。

21. 蘇柏毓(2020)，「**淺談 Mobile ID 安全之法令要求與應用案例**」，NCC News：第 14 卷。