多元之數位身分驗證機制含電子簽章研究案
期末研究成果說明會

政治大學金融科技研究中心
勤業眾信聯合會計師事務所
臺灣網路認證股份有限公司
達文西個資暨高科技法律事務所

2022/07/14

多元之數位身分驗證機制(含電子簽章)研究案簡介

為金管會推動《金融科技發展路徑圖》中3-2法規調適及3-6倫理規範的推動項目。本研究案之研究目的：

- ✓ **建立多元之數位身分驗證與簽章機制**

  為建立金融市場通用之身份驗證與簽章機制，本研究將整理市場上相關技術，針對適法性、可行性、技術性以及資安等面向進行分析比較，並提出可行之方案。

- ✓ **訂定數位金融服務管理規範**

  為改善我國金融產業於數位金融服務法令或自律規範不一致或缺漏處，本研究將盤點數位金融服務相關法令，彙整檢視應調整之處，並蒐集市場參與者建議，進行管理規範之調整與修訂。

委託研究為期一年(2021/09~2022/08)，共有五項工作項目

1. 整理及蒐集銀、保、證、期等領域國內外與研究議題相關之規範及技術。
2. 視研究進度或委託單位需求，於執行期間內規劃召開公聽會或研討會，瞭解國內金融機構及新創業者之實際需求。
3. 自金融機構、消費者及監理機關角度，分別就各項機制之適法、可行性、技術方法及資安等面向統合應注意之事項。
4. 於執行期間內分別提出期中與期末報告，並就金融機構及新創業者之提問為說明。
5. 訂定數位金融服務管理規範（主管機關視研究結果決定）。
   - 法規、規章、各公會自律規範及證券期貨周邊單位相關規範之修正及建議。
   - 強度不須至法規、規章或自律規範位階之建議內容，訂定最佳實務守則。

多元之數位身分驗證機制(含電子簽章)研究案研究範疇

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

11項場景應用需求與6項多元身分驗證機制

應用場景（11項）

～由銀行公會、壽險公會、證券公會、投信投顧公會、金融科技創新園區提供～

- 銀行帳戶約定核驗
- 身分驗證多元化
- OpenID Connect驗證方式
- 監理資料共用
- 基金平台串接電支
- Face OTP
- 行動投保簽名
- 視訊投保
- 電子文件簽章
- 法人開戶
- 線上申辦金融服務

- 生物辨識機制
- 電信認證機制
- 委由第三方進行身分驗證
- 身分驗證機制優化
- 電子簽章搭配影像／視訊機制
- 監理機制

～由委託單位集保公司整理提供～

多元身分驗證機制 (6項)

需求訪談

- 5 個公會訪談
  銀行、壽險、證券、投信投顧、金融科技創新園區
- 6 場訪談座談會
- 72 個場景需求被提出

研究分析

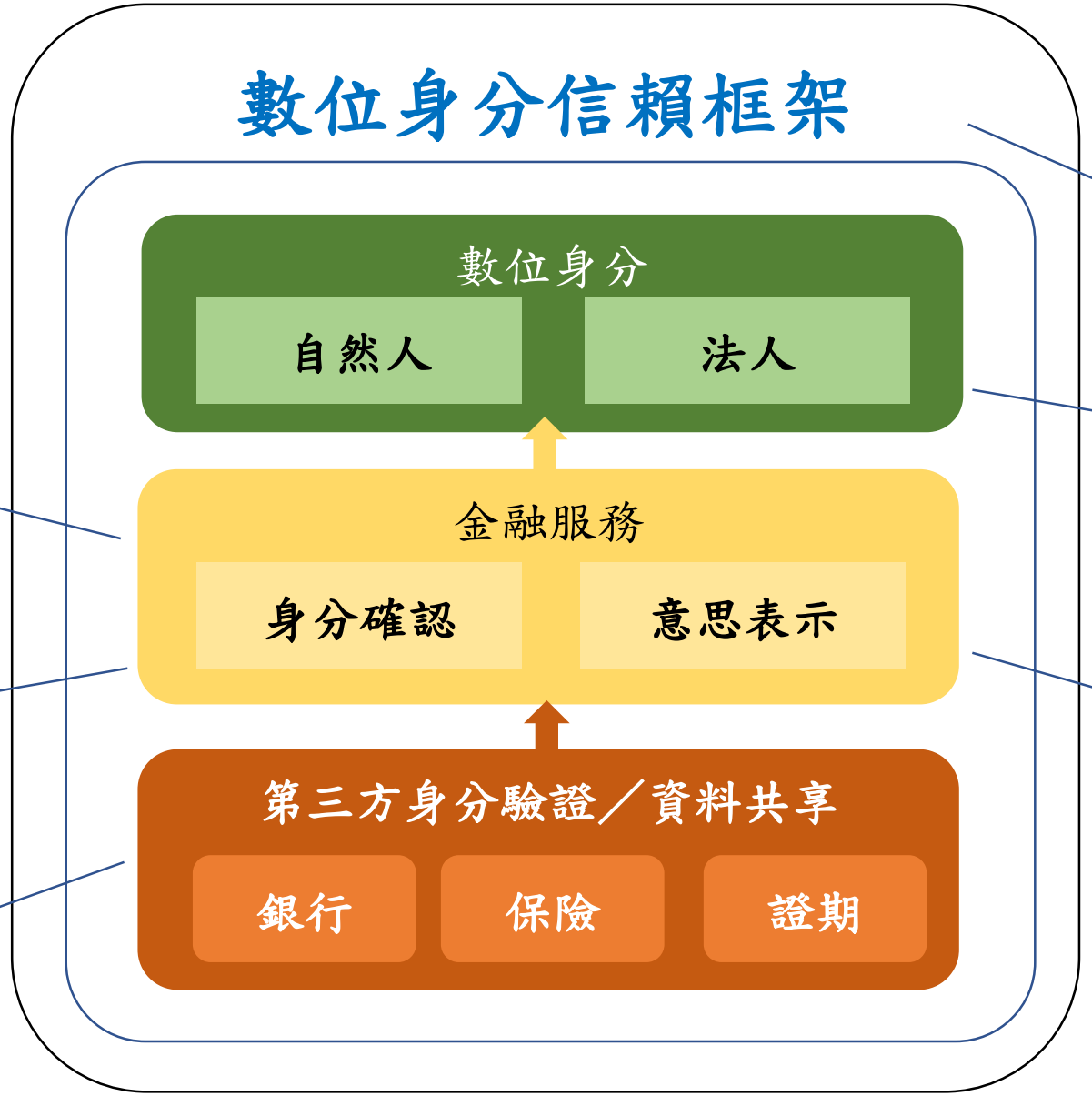
- 3 個國際數位身分趨勢研究
  世界經濟論壇、世界銀行、防制洗錢金融行動工作組織
- 5 個國家數位身分研究
  歐盟、澳洲、英國、瑞典、新加坡
- 4 個數位身分主題研究
  信賴機制、數位身分政策、法人數位身分、電子簽章應用
- 10+ 種身分辨別技術分析
  晶片金融卡、FIDO、生物辨識..等
- 15+ 金融相關法令分析

期中產出

- 1 個流程與分析框架
- 6 個研究議題
- 1 份期中報告
- 1 場研討會

我國金融產業對於多元數位身分的議題與痛點

1. 身分信賴框架
2. 第三方身分驗證
3. 生物辨識
4. 電子文件簽章
5. 法人數位身分
6. 資料共享



2. 第三方身分確認的規範

3-1. 身分核驗採生物辨識的人體辨識的適法性

6. 如何在使用者授權下，進行共享資料的交換

1. 沒有銀/保/證一體適用的數位身分信賴框架

5. 目前法人數位身分驗證與授權的困難

4. 電子簽章法未能與時俱進

3-2. 意思表示採生物辨識的錄影佐證方法的效力性

* 政治大學金融科技研究中心　繪製

數位金融服務管理規範及相關法規調適之建議

臧正運 老師
研究案協同主持人
政大金融科技研究中心監理科技創新實驗室執行長
政大法學院副教授

2022/7/14

數位身分的框架思考

- ✓ **跳脫產業疆界**來思考數位身分制度
- ✓ 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識別、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**
- ✓ 數位身分的本質是**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）
- ✓ 數位身分制度首重**信任框架的建構**，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
- ✓ 勿忘妥適數位身分制度的設計**有助於提升普惠金融**

一、數位金融服務管理規範之建議與方向

數位金融服務管理規範之目的－1

我國是否有訂定數位金融服務管理規範之必要，從目的觀之，有以下考量：

- 數位金融服務管理規範的頒布或有助於金融機構加速推動創新業務，如此方能避免法規不明的模糊空間。
- 我國監理模式係「機構型監理」，有別於「功能型監理」，而機構型監理之法規條文體例分散，因此主管機關應審視散見於各金融服務業別的法令，統一訂定數位金融服務管理規範，與時俱進、符合實務需求。

然數位金融服務管理之所以需要系統性及一致性的規範，其實亦植基於：

- 金融服務虛擬化與遠距化的發展浪潮，以及使用者對於金融服務便利性日益攀升的需求。
- 當金融機構提供數位服務的情形越普遍，甚至在跨金融機構的服務串接場景時，民眾更希望享受安全、便利以及效率的服務，而非重複驗證及標準不一，各金融業各行其道而讓使用者困惑。

上述的發展浪潮與客戶需求映射到數位金融服務的提供以及對金融機構身為服務提供者的影響而言，主要在金融服務的兩個重要環節帶來挑戰：獲取客戶及服務客戶。

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

數位金融服務管理規範之目的－2

獲取客戶

過去金融機構透過近距離與客戶進行實際接觸的方式查驗客戶的身分，並對客戶的背景及所提出的文件進行實體的盡職調查，進而與客戶建立契約關係，以提供長期的服務。

遠距化使得金融機構必須遠端為客戶開戶，並在虛擬化的脈絡下以非實體的方式查驗客戶遠端所提示的電子文件。

服務客戶

過去金融機構協助客戶執行特定交易，可以近距離與客戶實體互動，以驗證是否為客戶本人，進而確認客戶所為之意思表示真實無誤。

- 遠距化與虛擬化使金融機構在客戶身分驗證（Authentication）及意思表示確認（亦稱授權或簽章，英文以Authorization統稱）的環節承擔一定的風險，因未能實體與客戶互動，有可能在客戶身分遭他人偽冒情況下執行未經客戶授權並造成客戶與金融機構損失的交易。

訂定數位金融服務管理規範之主要目的

在虛擬化與遠距化的浪潮中，勢必需要一套管理機制，協助金融機構有效控管在獲取客戶及服務客戶流程中的風險，並保障客戶權益以及相關個資隱私資料；而這樣的管理機制，便需要一套管理規範加以實現。

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

數位金融服務管理規範之功能

數位金融服務管理規範要處理的議題，主要在確保於「身分識別」、「客戶盡職調查」、「身分驗證」及「交易授權」四大環節中，消費者遭偽冒以及個資外洩的風險能降到最低，並達到維持金融機構健全業務經營與金融穩定的效果。

- 風險的管控會帶來成本，然金融機構拉高遠距服務與虛擬通路的使用門檻，或許有助於降低風險，但可能導致客戶接近使用金融服務的不便利與遭排拒，而不利於金融普惠。**數位金融服務管理規範也必須帶有普惠金融的關懷**。
- 從功能面來說，數位金融服務管理規範必須**在風險控管與金融普惠間取得平衡**：
  - ✓**確保消費者有便於行使的數位身分**（Digital Identity）
  - ✓**兼顧資訊安全與個資隱私保護的要求**，降低市場上的詐欺風險以及消費者無謂的權益損失。

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

我國訂定數位金融服務管理規範之必要性－1

國際發展之盤點

世界銀行（World Bank）提出數位時代下的永續發展身分識別原則（Principles on Identification for Sustainable Development toward the Digital Age）

防制洗錢金融行動工作組織（Financial Action Task Force, FATF）針對其40項建議中的第10項建議客戶盡職調查（Customer Due Diligence）發布數位身分指引（Guidance on Digital Identity）

數位身分制度的健全是數位金融服務發展的關鍵，其發展應體現普惠金融的價值，並兼顧風險管理。

政府機關立法與制定法規範的重點在於以下幾個方面：

- 保護客戶身分資料的隱私及安全
- 建構全面的監理與信任框架，釐清不同參與者的權責
- 匯集各方利害關係人的共識，釐清數位身分發展的機會與挑戰
- 協助市場參與者落實風險基礎方法在數位身分系統中各個環節的實現

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

我國訂定數位金融服務管理規範之必要性－2

除現有的個人資料保護法制外，我國金融業與數位身分相關法規大多散見在不同業別（如銀行業、保險業及證券業等）的自律規範與法規命令中，欠缺全面性的監理框架，亦未針對不同角色（如數位身分的倚賴方、身分服務提供者、信物服務提供者等）釐清相關的權責義務。

我國現行監理法制亦未能匯集各方利害關係人（如金融業者、金融科技業者等）之共識，系統性地檢視數位身分制度在金融服務領域之應用可以帶來怎樣的機會，又應該以何種機制體現風險為基礎之方法。

除上述國際組織頒布的原則與指引外，自2021年中旬以來，包含英國、歐盟及澳洲等數位金融服務發展較為成熟的國家，都已經開始針對數位身分推展相關立法與修法的工作：

英國
在2021年2月提出的政策文件 - 英國數位身分與屬性信任框架（The UK Digital Identity and Attributes Trust Framework）

歐盟
在2021年6月提出的歐盟數位身分規則草案 (European Digital Identity Proposal)

澳洲
在2021年10月1日提出的受信任數位身分法案（Trusted Digital Identity Bill）

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

可資參採之典範－澳洲數位身分制度

經過本研究的詳細評估，其中以澳洲的制度最值得我國參採。其主要理由有二：

澳洲制度已有相關在法律層級以及法規命令層次的細節性規範之規劃，雖然尚未正式成為法律，但制度規劃完整，具實用性的參考價值。

澳洲制度之規劃雖以所有產業作為規範對象，而不限於金融業，但其特別梳理分數位身分制度中的不同角色，並針對不同角色應該具備的功能要件，以及應該履行的義務提出規範，特別適合我國借鏡。

- 在澳洲，原本澳洲公民已經可以透過既有的數位身分機制（如myGovID）接近使用至少80項的政府服務。然而這樣的數位服務僅止與C2G（Citizen to Government）的層次。澳洲政府希望透過上述法案的制定，擴大數位身分認證系統的涵蓋範圍至私部門，實現C2B（Consumer to Business）甚至是B2B（Business to Business）。

- 受信任數位身分法案（Trusted Digital Identity Bill）也希望在法律層級上明確規範在該國原有之數位身分信任框架（The Trusted Digital Identity Framework）中之不同參與者的角色，並設計嚴謹的認證規則（Accreditation Rules），明定這些參與者應履行的義務（Obligations）與應滿足之功能性要求（Functional Requirements）。

- 該法案希望在落實隱私與消費者保護的基礎上，建立永久性的治理安排與明確之監理架構。

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

可資參採之典範－澳洲數位身分制度

根據澳洲法案的設計：

數位身分系統係指可以促進與管理下列兩大功能之系統：

1. 個人身分的核驗（Verification）
2. 個人數位身分或資訊的驗證（Authentication）

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（Accredited Participants）：
   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。

澳洲數位身分法案

- 將數位身分系統的運作拉高至法律授權的層次
- 明定不同參與者的功能、義務與認證程序，讓各個有志從事數位身分服務的業者有明確的規則可循，也能同時確保消費者的個資隱私與資訊安全保護。

這種以明確法規提出清晰監理框架（Regulatory Framework）的制度設計模式，正是我國所欠缺，也是未來我國訂定數位金融服務管理規範可資參採的模式

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

我國訂定數位金融服務管理規範之必要性－3

檢視我國的現狀

我國現行法規範的紊亂複雜，不利於數位身分制度的發展。相關規定散見於不同業別的規範之中。

- 客戶盡責調查部分通常與洗錢防制法、金融機構洗錢防制辦法，以及各業別的防制洗錢及打擊資恐注意事項範本的規範攸關
- 身分識別、身分驗證及交易授權的環節，所設法規則多元複雜（如右表所示）
  - ✓ 有些與身分確認及身分驗證相關，但分屬於自律規範及法規命令等不同層次，如金融機構辦理電子銀行業務安全控管作業基準及電子支付機構資訊系統標準及安全控管作業基準。
  - ✓ 有的則是與交易確認直接相關，其中有些規定以書面進行交易授權時，所稱之書面，依電子簽章法之規定，得以電子文件為之，如銀行辦理高資產客戶適用之金融商品及服務管理辦法及銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法；但有些卻又經主管機關於不同交易情境中加以排除適用，如金管會依據電子簽章法公告排除電子簽章法適用之項目（如保險部分)等。

	銀行業	電支業	證券業	投信投顧業	保險業
法規命令或行政規則		電子支付機構身分確認機制及交易限額管理辦法 電子支付機構資訊系統標準及安全控管作業基準辦法			保險業務員管理規則 保險業辦理遠距投保及保險服務業務應注意事項
自律規範	金融機構辦理電子銀行業務安全控管作業基準 銀行受理客戶以網路方式開立數位存款帳戶作業範本 金融機構運用新興科技作業規範 金融機構提供自動櫃員機系統安全作業規範 金融機構提供行動裝置應用程式作業規範		臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分確認及額度分級管理標準	中華民國證券投資信託暨顧問商業同業公會國內證券投資信託基金電子交易作業準則 中華民國證券投資信託暨顧問商業同業公會受益憑證事務處理規則 中華民國證券投資信託暨顧問商業同業公會境外基金電子交易作業準則	保險業招攬及核保作業控管自律規範 壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則 保險業經營電子商務自律規範

與數位身分識別與驗證相關之金融法規範

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

我國訂定數位金融服務管理規範之必要性－3

檢視我國現狀造成的痛點

上述這些龐雜紊亂的規定，至少造成以下幾個實務運作上的痛點：

以身分確認與身分識別環節為例，究竟何種機制可以在何種類型的業態中被法規所允許？在新興科技發展下，哪些信物可以被使用？（如電信認證或特定生物識別技術下的設計是否可以作為身分確認與識別之方式？）

法人究竟應如何在數位情境下進行身分確認與身分識別？

在交易授權與意思表示確認的環節中，某些新興技術與方案的運用，如生物識別及視訊錄影等，是否符合電子簽章法的要求？又是否必然須受到電子簽章法之拘束，而沒有其他探求當事人真意，並確認意思表示真實性與不可否認性之機制存在的空間？

在客戶盡職調查的環節中，金融機構是否可以倚賴金融同業甚或其他第三方業者所提供之客戶資料來進行自身的認識客戶程序？又或者可以直接委由第三方業者代為調查？

上述這些痛點，有的係因現行法規未有明確規定所致，有的則是因為不同業別規範密度寬嚴不一所致，有的則是在不同規範實際適用時所可能產生的疑義所致，形成我國深化數位金融服務發展的重大挑戰。

Source：臧正運，數位金融服務管理規範的制度框架思考，台灣法律人，4月號，2022年4月，頁128-139。

我國訂定數位金融服務管理規範之規範模式

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

我國的數位金融服務管理規範該建立在何種層級？

1

理想中，**法律的層級**較高，也有助於跨越不同業別的鴻溝，甚而提供未來金融產業與其他產業間數位身分驗證的法源基礎及強制性規範，並可在必要時建立適當罰則。然而立法的成本甚高，需要長時間社會共識的累積，且涉及到不同主管機關間的分權與互動，難度頗高。

2

將數位金融服務管理規範置於**法規命令層級**，優點在於主管機關將享有訂定規範內涵的裁量與彈性，但主要問題在於，我國現行法律似乎不存在可以直接授權主管機關訂定此等跨業別（如跨銀行、保險、證券、支付等業別）法規命令的法源依據，在實踐上可能需搭配各業別業法的同步修正，或在不同業法中找到針對該業種之營運範圍進行授權的法源依據，並透過這些授權來訂定單一的法規命令。

3

透過**指引**的模式，由主管機關以行政指導之方式針對數位金融服務管理頒布跨業別均一體適用的指引，並責請各公會同步將現行相關之自律規範進行修正甚至廢止。此一模式在2021年12月已有先例，即金管會所訂定之「金融機構間資料共享指引」。此模式的優點在於對主管機關而言便利可行，但缺點是指引的法律層級較低，在與其他現行之法律或法規命令有所衝突時，將無法適用，而仍有可能徒增爭議。

本研究雖認為，**釜底抽薪之道乃是針對所有產業制定一套不分產業得以一體適用的基準規範**，但囿於該作法茲事體大，除涉及跨部會的機關協調，且超出本研究案的範疇，亦未能有效率地直接協助解決當下之痛點與挑戰，**故建議方案限縮在主管機關金管會權限所及之處**。

我國訂定數位金融服務管理規範之法律依據選擇－1

本研究建議以下兩種實現我國數位金融服務管理規範之方案：

方案一：提案修改金融科技發展與創新實驗條例（下簡稱「沙盒條例」），修正現行之第1條及第18條，或另增訂第18條之1，直接透過法律層級的授權，讓金管會取得訂定數位金融服務管理規範之權源，進而訂定數位金融服務管理規則。

此方案之優點與好處：

一. 沙盒條例之立法目的本就及於「促進普惠金融及金融科技發展」，而數位金融服務以及相關數位身分機制乃係金融科技發展之骨幹，亦是國際清算銀行轄下之金融穩定研究所（Financial Stability Institute）於2020年1月所提出之「金融科技樹（FinTech Tree）概念中，位於樹根 -「政策賦能」(Policy enablers)五大因子之一的Digital ID（數位身分）。因此透過在沙盒條例中增修相關授權條款，符合法律規範目的之一致性，在規範體制上亦屬合宜。然論者或許主張，沙盒條列乃是針對創新實驗所設計之規範，並非針對一般性的金融服務。

- 配套作法，是直接由主管機關檢討目前沙盒條列的執行成效，並評估是否對該條列進行較為全盤性的修正，將此修改為「金融科技發展與創新條例」，做為促進我國金融機構科技持續深化發展的根基。

- 另一較為簡便作法，乃同時修改沙盒條例第1條之立法目的，將其由原本的「為建立安全之金融科技創新實驗（以下簡稱創新實驗）環境，以科技發展創新金融商品或服務，促進普惠金融及金融科技發展，並落實對參與創新實驗者（以下簡稱參與者）及金融消費者之保護，特制定本條例。」，修改為「**為促進金融科技之發展，**並建立安全之金融科技創新實驗（以下簡稱創新實驗）環境，以科技發展創新金融商品或服務，**進而達到促進普惠金融及落實對參與創新實驗者（以下簡稱參與者）及金融消費者之保護**，特制定本條例。」

我國訂定數位金融服務管理規範之法律依據選擇－2

二. 修改沙盒條例的另一個好處，乃是沙盒條例具有同時拘束金融機構與辦理創新實驗之非金融機構的效力，倘若未來該條例進一步進行如上所述更為全面之修法，將可直接產生拘束金融科技業者之效果，而讓非屬金融業之金融科技業者得以在法律有明文規定的情形下進入數位身分體系、扮演相關角色的可能。**法律授權若能賦予金管會直接規範這些在數位身分體系中扮演角色之非金融業者，將使我國數位金融服務管理規範更有力道，而能達到促進產業發展與消費者保護之效果**。

三. 選擇修改沙盒條例第18條或增訂第18條之1的原因，乃在於現行條例之第18條第2項，本就有「主管機關應制定並定期檢討金融科技發展之政策，積極提供金融科技業必要之協助、輔導與諮詢服務，並應定期邀集金融科技業代表與政府相關部會代表，研議、協調與金融科技發展相關之事項。關於金融科技發展之輔導及協助機制，其辦法由主管機關定之。」之規定，申言之，該條文之立法目的，即在於促使主管機關積極輔導與協助金融科技產業之發展，故若將有助於金融科技產業發展的數位身分制度授權條文置於其中或其後之條文，應尚屬符合立法體例之安排。

四. 透過此一法律明文之授權，將給予主管機關未來進行相應裁罰的權限，在數位身分制度之參與者未能履行責任的情況下予以裁處，將更能收保護消費者之成效。

我國訂定數位金融服務管理規範之法律依據選擇－3

方案二：倘若方案一因涉及修改現行法律，需經過立法院審議通過而較為曠日廢時，則本研究認為另一折衷之作法，乃是將數位身分制度的落實，視為金融業內部控制與內部稽核制度之一環，而透過複數法律的授權，訂定一個「金融業辦理數位金融服務管理規則」。此作法在規範模式上需確保兩個面向均屬可行：亦即我國確有「複數法律共同授權主管機關訂定單一法規命令」及「單一法律授權主管機關訂定複數法規命令」之前例可循。

- 雖學說上對於不同之法規命令訂定之合法性時有爭論，但實務上只要符合「制定法規命令時有有效法律之授權」、「法規命令之內容與授權制定之法律規範一致」、「形式上法規命令由經授權之行政機關依法定方式及程序制定」之要件，即為合法之法規命令。

- 經盤點金融業相關法規，可知實務上確實有複數法律同時授權主管機關訂定單一法規命令之立法模式。舉例而言，境外結構型商品管理規則、金融控股公司及銀行業內部控制及稽核制度實施辦法、銀行辦理高資產客戶適用之金融商品及服務管理辦法等均屬之。故在立法模式上，若能找出現行金融法律中適合用來授權金管會頒布數位金融服務管理規範的授權條文，則可循前開幾個法規命令的作法與體列，訂定數位金融服務管理規範。

我國訂定數位金融服務管理規範之法律依據選擇－4

- 即便釐清了「複數法律共同授權主管機關訂定單一法規命令」確實可行，仍需在現行金融法律中找到合適且可被合法解讀為立法者確有授權金管會因應時勢需要，而訂定數位金融服務管理規範之相關條款，以符合法律保留及授權明確性之原則。本研究基於上述論述認為，數位金融服務管理規範要處理的議題，主要在確保於「身分識別」、「客戶盡職調查」、「身分驗證」及「交易授權」四大環節中，消費者遭偽冒以及個資外洩的風險能降到最低，並達到維持金融機構健全業務經營與金融穩定的效果，而此一目的與「確保金融業建立合宜之內部控制制度，並確保該制度得以持續有效執行，以促進金融機構健全經營」之規範目的相同。因此，可以**將金融機構從事數位金融服務時所應遵循之規定，視為其履行內部控制制度之一環，而透過金融業內部控制之法規命令加以規範**。

- 惟採取此一立法模式的主要問題在於，我國現行已有諸多金融業內部控制制度之法規命令，如金融控股公司及銀行業內部控制及稽核制度實施辦法、證券暨期貨市場各服務事業建立內部控制制度處理準則，以及保險業內部控制及稽核制度實施辦法等規定，若要修改這些各業別的現行規定而納入數位金融服務的管理規章，恐將使法規更形紊亂，除了有同時修改眾多法規命令之困難外，亦有因修法不慎而使各業別未來在適用上產生落差或疑慮的可能。

我國訂定數位金融服務管理規範之法律依據選擇－5

為解決上開疑慮，本研究思考另一可行性，**便是在不影響現行各業別內控內稽辦法的前提下，由金管會直接訂定一套獨立於這些內控內稽辦法的法規命令來規範數位金融服務**。

基此，本研究進一步探討我國是否有「單一法律授權主管機關訂定複數法規命令」之前例。經查，實務上確有以單一法律授權主管機關訂定複數法規命令之立法模式（如證交法第44條第4項，即同時授權訂定境外結構型商品管理規則、證券商受託買賣外國有價證券管理規則、證券商設置標準及證券商管理規則。）換言之，**縱使主管機關已依據特定法律條文制定法規命令，行政機關仍得基於該條法律之授權制定其他法規命令**。因此金管會作為主管機關，仍然得以藉由右表所列法條之授權，以複數法律之授權訂定另一全新之法規命令，如本委託研究案所指之數位金融服務管理規範。

訂定我國數位金融服務管理規則之法律授權依據

法規名稱	法律依據	法條內容
金融控股公司法	第51條	金融控股公司應建立內部控制及稽核制度；其辦法，由主管機關定之
銀行法	第45條之1	銀行應建立內部控制及稽核制度；其目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵行事項之辦法，由主管機關定之。
證券交易法	第14條之1第1及第2項	公開發行公司、證券交易所、證券商及第十八條所定之事業應建立財務、業務之內部控制制度。 主管機關得訂定前項公司或事業內部控制制度之準則。
期貨交易法	第97條之1第1及第2項	期貨交易所、期貨結算機構及期貨業，應建立財務、業務之內部控制制度。 主管機關得訂定前項公司或機構內部控制制度之準則。
證券投資信託及顧問法	第93條	證券投資信託事業及經營接受客戶全權委託投資業務之證券投資顧問事業，應建立內部控制制度；其準則，由主管機關定之。
保險法	第148條之3	保險業應建立內部控制及稽核制度；其辦法，由主管機關定之。

我國訂定數位金融服務管理規範之法律依據選擇－6

綜上所述，**方案二的建議便是由前頁表列法律，**由金管會另行訂定「**金融業辦理數位金融服務管理規則**」。

之所以不稱為「數位金融服務管理規範」，係因中央法規標準法第3條之規定，「各機關發布之命令，得依其性質，稱規程、規則、細則、辦法、綱要、標準或準則。」故**本研究參酌相類似之立法例如結構型商品管理規則，建議將此一規範命名為「金融業辦理數位金融服務管理規則」（下簡稱「數位金融服務管理規則」）。**

方案二的優點在於主管機關立即可行，毋需經過立法院審議的漫長程序，且同樣能有效管理金融機構從事數位金融服務時應遵循之事項。**然此方案之缺點在於除了仍可能有法律授權明確性的爭論外，主要還在於此一規範無法直接拘束非金融業者。按數位身分系統的參與角色眾多，未來將不乏非金融機構，因此方案二的模式是否有助於我國數位金融服務的長遠發展，恐不無疑問。因此，本研究仍強烈建議以方案一為首選，方為釜底抽薪之道。**

數位金融服務管理規則應實現之精神及目標－1

未來無論採取方案一或方案二的規範模式，此一數位金融服務管理規則，應要能實現以下之精神及目標 ：

- 接軌國際規範：
  從制度設計的觀點，協助金融市場建構合宜的數位身分系統，該系統應包含數位身分建構的重要流程、數位身分系統中不同參與者的角色功能與責任義務，以及數位身分使用的不同信賴風險等級（Level of Assurance）。

- 梳理數位身分建構的流程：
  如依據ISO-29115的標準，基本上可以分成三大流程：
  1. 登錄階段(Enrolment)旨在核驗與確認個體所提示之身分資料與個體之關聯性（主要在回答「確認個體究竟是誰？」此一問題）
  2. 信物管理階段(Credential Management)旨在以核發信物的方式，建立並維護個體與身分資料之關聯性(主要在回答：「個體可以持何種信物向服務提供者主張自己便是該個體本人？」此一問題)
  3. 驗證階段(Authentication)旨在驗證個體與身分資料的關聯性(主要在回答：「個體是否確實就是之前所登錄的個體？」此一問題)。

上述流程的釐清是數位金融服務管理規範訂定的根基，透過梳理這些流程，將有助於所有利害關係人使用同一語彙與觀念架構，思考數位身分在金融領域的應用問題。此外，流程的解構也可以協助不同業者認識自己擬扮演的角色，進而協助主管機關針對不同角色的功能加以規範。

數位金融服務管理規則應實現之精神及目標－2

未來無論採取方案一或方案二的規範模式，此一數位金融服務管理規則應該要能實現以下之精神及目標：

- 應要能針對數位身分系統中不同參與者的角色功能與責任義務進行原則性的規範。而不同參與者應賦予相應之以原則為基礎（Principle-based）的功能要求與責任。

- 數位金融服務與實體金融服務相同，基本上都存有一定程度的交易風險，惟數位金融服務因虛擬化與遠距化的特性，相較於實體交易可能存有較高之客戶遭偽冒及交易未經授權的風險。
  - ✓ 風險的管控與消費者的便利使用存在一定的抵換關係，強度越高的風險管控措施，通常也意味著交易上更多的不便利性，因此國際組織也提醒各國仍要存有提升普惠金融的關懷，採取風險基礎方法的身分驗證模式，不必然將所有的交易均視為高風險的交易。
  - ✓ 金融機構也應依照不同業態的特性、交易的類型、客戶遭偽冒所可能造成的損失、對金融體系的影響等因子，訂定彈性且容許個別差異的風險信賴等級。而風險信賴等級的決定，其實涉及到一國社會對數位交易的信任程度，以及個別金融機構與該國消費者對風險的容忍程度，不必然僅僅由特定技術或驗證機制之安全等級高低加以決定。
  - ✓ 應要提供合宜的授權空間，將風險信賴等級之決定，交各產業公會、技術業者與消費者等利害關係人之代表共同研商與訂定，以利於數位金融服務的廣泛推展及風險與便利間的衡平。
  - ✓ 為了確保各方參與者確實依照所商定之風險信賴等級數位金融服務，在此數位金融服務管理規則中，應有相應的條款，要求金融機構等各參與訂定內規，說明自身評估信賴風險等級之邏輯與如何確保其內控制度落實上開邏輯之作法，並賦予金管會日後針對該等內規加以檢查的權限。

數位金融服務管理規則的實質內容建議－1

數位金融服務管理該規則之未來需要涵蓋的面向與重點，參酌本研究進行的場景與痛點分析，並借鑑澳洲法案的制度設計，提出建議如下：

一. **法源依據**：建議採取方案一。然若考量修法不易，可改採方案二之作法，尋求相關授權規定。

二. 名詞定義：須針對「數位金融服務」、「數位身分系統」、數位身分系統之參與者即「身分服務提供者」、「屬性服務提供者」、「信物服務提供者」、「身分交換平台」、「倚賴方」，以及「信賴風險等級」、「數位意思表示」等詞彙明確加以定義。其中「數位身分系統」係指下述之「數位身分的建構流程」及「數位金融服務的四大環節」。

三. **數位身分的建構流程**：參考ISO29115，明示三大作業流程，說明「身分登錄」、「信物管理」及「身分驗證」的內涵並提出相關參與者應遵循的主要流程。

四. **數位金融服務的四大環節**：針對「身分識別」、「客戶盡職調查」、「身分驗證」及「交易授權」四大環節提出基本定義，並分別以四大環節作為規則中各章節的標題，撰寫具體內容。

五. **數位身分系統之參與者的功能要求與責任義務**：針對數位身分系統中不同參與者的角色功能與責任義務進行原則性的規範。在功能要求部分，主要著重在「詐欺控管」、「個人資料保護」、「安全維護措施」、「使用者體驗」及「技術測試與功能評估」等面向進行稍微細緻但以原則為基礎之規定，詳參下列附件一的例示說明。而在責任義務方面，則可以參考附件二的例示說明，由金管會訂定相關規定。

(續)

數位金融服務管理規則的實質內容建議－2

數位金融服務管理該規則之未來需要涵蓋的面向與重點，參酌本研究進行的場景與痛點分析，並借鑑澳洲法案的制度設計，提出建議如下：

(續)

六. **數位身分系統之參與者的認證制度**：明訂擬參與數位金融身分管理系統之參與者，應依相關條件向主管機關（或主管機關指定之專責機構）申請之認證審查程序與退出程序。

七. **信賴風險等級的決定**：責由各產業公會，並要求其與技術業者與消費者等利害關係人之代表共同研商與訂定屬於各自產業之信賴風險等級。這些信賴風險等級應以原則為基礎，讓個別金融機構可以針對各產業公會所訂出之信賴風險等級，依照自身風險承受度與技術水平，自行訂定滿足不同風險等級的作業流程與技術運用。未來這些金融機構對客戶從事數位金融服務時，應制定自身機構就上開作業流程與技術運用之應遵循辦法，並依照辦理。未來金管會可定期進行該金融機構是否遵循其自身應遵循辦法辦理金融檢查，必要時限期令其改善或予以裁罰。

八. **數位意思表示**：藉由本規則的訂定，釐清數位金融服務與電子簽章法過去經常混淆、盤根錯節的關係。在規則中明定金融機構之客戶與消費者依照本規則所進行的數位意思表示，係屬金管會依照電子簽章法第4條第4項以及第9條第2項，將客戶以電子文件為意思表示及電子簽章之情境，就其應用技術與程序另為規定之情形，而不受電子簽章法其他規定之限制。

九. **罰則**：明定主管機關對數位金融身分系統參與者之監理手段與違規效果。

二、相關法規調適之建議

現行法令盤點分析-銀行業

規範名稱	應用場景	主要內容	盤點分析
金融機構辦理電子銀行業務安全控管作業基準	身分確認	針對電子銀行交易面及管理面，分別規定安全需求及安全設計之準則。	銀行業身分確認相關規範已具有完整之架構及內容，以《金融機構辦理電子銀行業務安全控管作業基準》為例，其中關於「介面安全設計」之內容較為詳盡，其內容與澳洲《Trusted Digital Identity Framework Accreditation Rule》中對於系統安全性之要求類似，且細節也相當完善《金融機構辦理電子銀行業務安全控管作業基準》之規範範圍涵括電子銀行業，其範圍較大，相較之下其餘規範，則係針對較為細節之事項。如《金融機構運用新興科技作業規範》中關於生物特徵資料之安全要求，亦有於澳洲《Trusted Digital Identity Framework Accreditation Rule》中提及。整體而言，於身分確認相關規範上，銀行業相較於其餘金融產業，已建立較為完整之規範。未來可依照本研究所提出關於訂定數位金融服務管理規則之相關建議，不分銀行業等金融業別，要求金融業從事數位金融服務時應遵循數位金融服務管理規則之辦理。
銀行受理客戶以網路方式開立數位存款帳戶作業範本		使銀行建立明確之「認識客戶政策」作業程序，包括接受客戶開立存款帳戶之標準、對客戶之辨識、存款帳戶及交易監控等重要事項。	
金融機構運用新興科技作業規範		促進銀行業務之健全經營，並針對生物特徵資料之安全訂定相關要求。	
金融機構提供自動櫃員機系統安全作業規範		確保金融機構提供之自動櫃員機（即ATM），其系統之資訊安全。	
銀行防制洗錢及打擊資恐注意事項範本	KYC/CDD	依據集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求分公司（或子公司）提供有關客戶、帳戶及交易資訊，並應包括異常交易或活動之資訊及所為之分析；必要時，亦得透過集團管理功能使分公司（或子公司）取得上述資訊。	金融產業KYC/CDD相關規範，均源於《洗錢防制法》要求各行業訂定之防制洗錢及《打擊資恐注意事項範本》，關於上開範本之不足，可於後續統一歸納。
信用卡業務機構管理辦法	意思表示確認	將原先有關信用卡申請書之申請人聲明及同意事項中，重要事項之確認機制，由「簽名確認」修正為「以『簽名』或『其他得以辨識申請人同一性及確定申請人意思表示之方式』確認」	相較於對意思表示確認有急迫需求之壽險業而言，銀行業之規範較為滯後，當壽險業已經能以視訊方式進行意思表示確認時，銀行業僅得透過錄音取得，且僅限於高資產客戶始能採用錄音方式進行意思表示確認，故銀行業於意思表示確認之相關規範應得適度放寬。未來可依照本研究針對數位金融服務管理規則之建議，在規則中明定金融機構之客戶與消費者依照本規則所進行的數位意思表示，係屬金管會依照電子簽章法第4條第4項以及第9條第2項，將客戶以電子文件為意思表示及電子簽章之情境，就其應用技術與程序另為規定之情形，而不受電子簽章法其他規定之限制。
銀行辦理高資產客戶適用之金融商品及服務管理辦法		銀行於執行高資產客戶之通知及說明程序時，應進行錄音，惟若客戶不同意錄音，銀行應作成書面紀錄並請客戶簽名確認	
銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法		銀行依據商品適合度制度對客戶做成之屬性評估及分析結果，需要經客戶以本辦法規定之方式確認意思表示。	

法規調適建議-銀行業

《金融機構辦理電子銀行業務安全控管作業基準》已經具備完善之規範架構，然其中各項標準如加解密系統之技術要求及安全設計應遵循之標準等，仍過於繁瑣。未來可依照本研究所提出數位金融服務管理規則之實質內容建議辦理，並適時參酌國外先進規範之標準，調整本作業基準之內容。建議意思表示作法：

問題解析	建議
紙本作業, 意思表示以書面簽名或蓋章行使意思表示，但是如是以非紙本作業： 例如，保險遠距投保試辦計畫及行動投保或銀行電子銀行安控基準法及銀行辦理高資產客戶適用之金融商品及服務管理辦法有納入電子簽名、錄音、錄影、視訊等作法。但都未從法理與技術準則之角度梳理及同時慮及實務的作法。 例如，如以視訊、錄音、錄影等技術表達數位意思，其依附於其同意之電子文件，與不可篡改性之技術準則為何？又如行動投保使用之電子簽名，目前條款只有電子文件而無電子簽章，而是使用紙本簽名授權電子簽名，但是紙本簽名實務上與電子簽名無法勾稽。而電子簽名本身又無法驗證簽署本人之電子簽名?	相關議題建議如涉有數位意思（Digital Intention ）之表示及電子文件，為使電子文件具法律效力，建議法源上需溯回電子簽章法須依電子簽章法，電子簽章依附於電子文件、可以確認辨識簽署人、及電子文件真偽。 數位意思表示 ，建議從Best Practice 的角度審視數位意思表示之實務做法，考慮包含法源依據、技術標準及實務實作。如屬數位意思表示內容涉及生物性數位意思授權（如電子簽名、錄音、錄影、視訊等）及電子文件與建議則可參考 eIDAS 分級之作法，分為BES (Basic Electronic Signture, AES (Advanced electronic signature) 之分級作法，及技術評核準則。同時顧及法源（電子簽章法）、技術準則（ETSI EN）以及實務實作。

現行法令盤點分析-保險業

規範名稱	應用場景	主要內容	盤點分析
保險業務員管理規則	身分確認	建立保險業務員之資格取得、登錄、撤銷、教育訓練及懲處等其他應遵循事項之管理規則。	壽險業於新冠肺炎疫情前仍需遵循「親晤親簽」之要求，然因為疫情之嚴峻，進而推行壽險業數位身分確認之進展，依據《保險業辦理遠距投保及保險服務業務應注意事項》及《壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則》等規定，讓壽險業得透過視訊錄音錄影方式代替親晤。惟相關規範之詳細程度較低，也未允許生物特徵識別之方式。未來可依照本研究所提出關於訂定數位金融服務管理規則之實質建議辦理。
保險業辦理遠距投保及保險服務業務應注意事項		因應金融科技及新冠肺炎疫情發展，提供消費者便利安全之非面對面接觸投保及保險服務，建立保險業辦理遠距投保及保險服務業務之共通性適用標準。	
人身保險業辦理行動投保身分確認程序業務應遵循事項規範		就人身保險業辦理行動投保之業務，訂有多元之身分確認程序。	
保險業招攬及核保作業控管自律規範		為規範人身保險商品之招攬及核保作業風險控管，並進一步保障客戶權益及避免道德風險。	
壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則		因應疫情，在客戶同意之情形下，提供以視訊錄音錄影之方式代替親晤。	
人壽保險業防制洗錢及打擊資恐注意事項範本	KYC/CDD	依集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求國外分公司(或子公司)提供有關客戶及交易資訊，包括異常交易或活動之資訊及所為之分析；必要時，並得透過集團管理功能使國外分公司(或子公司)取得上述資訊。	金融產業KYC/CDD相關規範，均源於《洗錢防制法》要求各行業訂定之防制洗錢及《打擊資恐注意事項範本》，關於上開範本之不足可於後續統一歸納。
壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則	意思表示確認	原本之親晤親簽方式，可在確認客戶身分及客戶同意之前提下，改採視訊錄音錄影方式取代。	意思表示之確認向來為壽險業最注重之議題，也因此壽險業向來均遵循親簽之原則，然因為疫情之阻礙，改變原先以親簽確認客戶意思表示之方式，現今也得以透過錄音及錄影方式確認。
保險業經營行動服務自律規範		保險業於經營行動服務時，應確認業務員或服務人員提供之行動裝置，其介面和尺寸得清楚顯示電子文件之內容，以供客戶知悉相關資訊。 又客戶於辦理行動服務時，應於應簽名處「逐一」簽名，或逐一於主管機關核准之方式表達意思表示，可知在現行實務規範下，仍需「逐一」表達意思表示同意。	

法規調適建議-保險業

- 壽險業相較於其餘金融業者，具有較新穎之意思表示確認規範，以明文規定可以採取視訊錄音錄影之方式確認客戶之意思表示，然觀察《壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則》及《保險業經營行動服務自律規範》等規範，亦可知道其係為因應疫情而在急迫下發布之規範，所以容許之意思表示確認方式僅限於視訊錄音錄影，故建議可以逐步增加意思表示確認之方式，並依照本研究所提出關於訂定數位金融服務管理規則之實質建議辦理。

現行法令盤點分析-證券業

規範名稱	應用場景	主要內容	盤點分析
臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分確認及額度分級管理標準	身分確認	證券商辦理線上開戶作業時，應透過出具本人證件，或是經由本標準規定之第三方認證方式確認客戶身分。	證券業身分確認相關規範相較於銀行業發展較緩慢，目前規範層面僅推進至線上開戶作業之應用，且提供之身分確認方式亦未開放生物特徵識別，就此部分之架構及內容亦有不夠詳盡之虞，未來可依照本研究所提出關於訂定數位金融服務管理規則之實質辦理。
臺灣期貨交易所股份有限公司「期貨經紀商受理期貨交易人存入保證金、權利金應行注意事項」		依集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求分公司（或子公司）提供有關客戶、帳戶及交易資訊，並應包括異常交易或活動之資訊及所為之分析；必要時，亦得透過集團管理功能使分公司（或子公司）取得上述資訊	
證券商防制洗錢及打擊資恐注意事項範本	KYC/CDD	依集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求分公司（或子公司）提供有關客戶、帳戶及交易資訊，並應包括異常交易或活動之資訊及所為之分析；必要時，亦得透過集團管理功能使分公司（或子公司）取得上述資訊。	金融產業KYC/CDD相關規範，均源於《洗錢防制法》要求各行業訂定之防制洗錢及《打擊資恐注意事項範本》，關於上開範本之不足將於後續統一歸納。

法規調適建議

- 證券業者亦有確認客戶意思表示之需求，然卻沒有相關之規範，雖然實務上證券業者早有以OTP等方式確認客戶意思表示之作法，然漏未規範之情形可能導致業者難以遵循。故建議證券業在短期得參酌《保險業經營行動服務自律規範》等意思表示確認相關規範，訂定完整之意思表示確認方式及流程，中長期則依照本研究所提出數位金融服務管理規則之實質內容建議辦理。

現行法令盤點分析-投信投顧業

規範名稱	應用場景	主要內容	盤點分析
中華民國證券投資信託暨顧問商業同業公會國內證券投資信託基金電子交易作業準則	身分確認	使投資人便於採用電子工具申購、買回及轉申購共同基金、確保交易公平暨保障投資人權益，並做為證券投資信託事業經營本項業務之作業準據。	投信投顧業相較於其餘金融產業，其身分確認之相關規範意旨均係為便利投資人進行投資，然其確認客戶身分之方式較少，且規範亦不詳盡，未來可依照本研究所提出關於訂定數位金融服務管理規則之實質建議辦理。
中華民國證券投資信託暨顧問商業同業公會境外基金電子交易作業準則		使投資人便於採用電子工具申購、買回及轉換境外基金、確保交易公平暨保障投資人權益。	
證券投資信託事業證券投資顧問事業防制洗錢及打擊資恐注意事項範本	KYC/CDD	依集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求分公司（或子公司）提供有關客戶、帳戶及交易資訊，並應包括異常交易或活動之資訊及所為之分析；必要時，亦得透過集團管理功能使分公司（或子公司）取得上述資訊。	金融產業KYC/CDD相關規範，均源於《洗錢防制法》要求各行業訂定之防制洗錢及《打擊資恐注意事項範本》，關於上開範本之不足可於後續統一歸納。
臺灣集中保管結算所股份有限公司防制洗錢及打擊資恐查詢作業要點		協助證券業、票券業、證券金融事業、證券投資信託事業、期貨信託事業及證券投資顧問事業等業者，辦理客戶資料查詢比對，以落實防制洗錢之客戶審查作業，並設置防制洗錢及打擊資恐查詢系統。	

法規調適建議-投信投顧業

- 投信投顧業者亦有確認客戶意思表示之需求，然卻沒有相關之現行規範，雖然實務上投信投顧業者早有以OTP等方式確認客戶意思表示之作法，然漏未規範之情形可能導致業者難以遵循。故建議在短期內投信投顧業得參酌《保險業經營行動服務自律規範》等意思表示確認相關規範，訂定完整之意思表示確認方式及流程；中長期則可依照本研究所提出關於訂定數位金融服務管理規則之實質建議辦理。

法規調適建議–跨機構議題

資料交換	法人身分確認	自然人憑證	Mobile ID	第三方驗證
目前僅在KYC/CDD有較多著墨。而現行各金融業《防制洗錢及打擊資恐注意事項範本》中關於KYC及CDD之規定，幾乎只開放集團內部之資料交換。 但《金融機構間資料共享指引》訂定後，已規定在符合條件下得適度跨業進行資料交換，且因有臺灣集中保管結算所股份有限公司設置之「防制洗錢及打擊資恐查詢系統」可供金融業者進行KYC及CDD。	依據《銀行受理客戶以網路方式開立數位存款帳戶作業範本》規定，僅有自然人及股東三人以下之公司得採用視訊等其他方式進行身分確認，且限於以網路方式開立數位存款帳戶時得應用，得應用之場景極為限縮，建議得參照澳洲RAM之作法，發展適合臺灣的在地化方案。	依據自然人憑證核發及管理作業要點規定，目前我國自然人憑證仍需親自辦理申請事宜，且核發之自然人憑證需為IC卡，我國雖已有行動自然人憑證的規劃，但後續應用範圍及便利性仍值得觀察。	現行銀行業仍無法採用Mobile ID平台作為電信認證之基礎，然得透過以用戶身分模組連結至電信業者之方式確認客戶身分，後續建議得開放以Mobile ID平台加上TWID身分識別中心之機制進行客戶身分認證。	現行規範對於第三方認證屬於規範缺漏之情形，金融機構應參酌數位金融服務管理規則，利用第三方認證機構，提升身分確認之便利性。

法規調適建議-電子簽章

目前最大挑戰

- 在於各界對電子簽章法的詮釋莫衷一是，且該規定未能與時俱進。二十年前立法考量是數位簽章技術為主、也有明確的技術規範與遵循標準。惟當時未有如今科技技術之蓬勃發展，致使如其他生物特徵技術類電子簽名、錄音、錄影、視訊、生物識別等技術之應用缺乏法源依據、技術準則、及實務實行標準，以至造成今日種種亂象及諸多討論。
- 應用其他生物特徵技術類電子簽名、錄音、錄影、視訊、生物識別等數位意思表示技術，製作具法律效力之電子文件，建議仍須從法源、技術準則、以及實務實行等面向訂立標準。

建議

- 未來金融管理規範建立納入以我國現行電子簽章法、 ISO 29115、歐盟eIDAS 、以及其他國家如澳洲《Trusted Digital Identity Framework Accreditation Rule》為框架，同時考慮新興科技技術及資安為藍本。
- 主要範疇應包括數位身份驗證及電子簽章，而電子簽章包括既有之《數位簽章 》及《其他生物科技類》即新興科技類技術之電子簽章。

數位金融服務管理規則與相關法規調適之建議小結

1. 建立各界對數位身分框架思考的共識，中長程以推動各產業一體適用的數位身分制度為目標，短程內聚焦於金融服務產業之發展。
2. 我國確實有訂定數位金融服務管理規則之必要。建議直接針對沙盒條例進行修法，將其修正為「金融科技發展與創新條例」，並賦予主管機關針對數位金融服務加以監理的明確法律授權依據。
3. 以明確法制推動多元的數位身分生態體系，將非金融機構之參與者納管，以確保於「身分識別」、「客戶盡職調查」、「身分驗證」及「交易授權」四大環節中，消費者遭偽冒以及個資外洩的風險能降到最低，並達到維持金融機構健全業務經營與金融穩定的效果。
4. 信賴風險等級的決定應要求各產業公會與技術業者與消費者等利害關係人之代表共同研商與訂定屬於各自產業之信賴風險等級。並且在各產業公會中所訂定之信賴風險等級應留由相當空間的授權條款，允許個別金融機構可以自行訂定內部之數位金融服務信賴風險等級之應遵循辦法，該金融機構對客戶從事數位金融服務時，應依照自身機構之應遵循辦法所揭示的信賴風險等級之相關程序辦理，主管機關僅須定期進行該金融機構是否遵循其自身應遵循辦法的金融檢查，必要時再限期令其改善或予以裁罰。
5. 釐清金融服務場景中不同類型之金融交易所涉及的不同風險，以風險為基礎架構信賴風險等級，並依風險等級規範「數位意思表示」（確認及授權）行使的具體方式。
6. 短程由目的事業主管機關對電子簽章法的相關規定明確且積極進行除外解釋，中長程則依照科技發展的現況與趨勢進行電子簽章法的翻修。
7. 法人數位身分制度之要素有四：建立法人之數位身份（如數位工商登記）、建立法人代表人之數位身分（如自然人憑證）、建立法人代表人之授權機制（如法人授權其特定員工辦理數位金融服務），以及數位意思表示行使的方式（如是否揚棄公司大小章的慣習，或建置數位大小章等設計）。由法人在數位情境所進行之金融交易應該在流程設計上具備可追蹤性（Traceability)，以確保日後若發生爭議時能加以釐清與處理。

數位身分驗證技術應用分享

謝明華 老師
研究案協同主持人
政大金融科技研究中心副主任
政大風險與保險研究中心主任
2022/7/14

Agenda

- 身分驗證信賴框架
  - ISO/IEC 29115
  - NIST 800-63 Digital Identity Guidelines
- 身分驗證類別
  - 對稱/非對稱
  - 精準/非精準
  - 自行驗證/第三方驗證
- 生物特徵驗證
- 電子簽章國際規範指引參考：
  - 歐盟 eIDAS (electronic IDentification, Authentication and trust Services)

一、身分驗證信賴框架

個體身分驗證信賴架構 (ISO/IEC 29115)

登錄階段
Enrolment Phase

- Application and initiation
- Identity proofing
- Identity verification
- Record-keeping recording
- Registration

信物管理階段
Credential Management Phase

- Credential creation
- Credential pre-processing
- Credential initialization
- Credential binding
- Credential issuance
- Credential activation
- Credential storage
- Credential suspension, revocation, and/or destruction
- Credential renewal and/or replacement
- Record-keeping

個體驗證階段
Entity Authentication Phase

- Authentication
- Record-keeping

- **每個階段都分為 4 個信賴等級 (LoA: Level of Assurance)**
- **整體信賴等級取三個階段中最低的 LoA**

參考資料：
- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

身分識別機制的六個角色

參與角色(單位)	工作職掌
個體 Entity	身分識別的標的。 可以是自然人、法人，甚至於是伺服器，或是一個系統。
註冊權責單位 Registration Authority， RA	負責申請者登錄相關作業的權責單位。
公正第三方 Trusted Third Party， 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，如：身分核驗。
信物服務提供單位 Credential Service Provider， 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。
信賴單位 Relying Party， RP	信賴並使用身分識別機制所得結果的單位。 (常常為提供應用服務單位Server Provider， SP)
驗證單位 Validation Authority， VA	提供身分驗證服務的單位。

參考資料：
- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

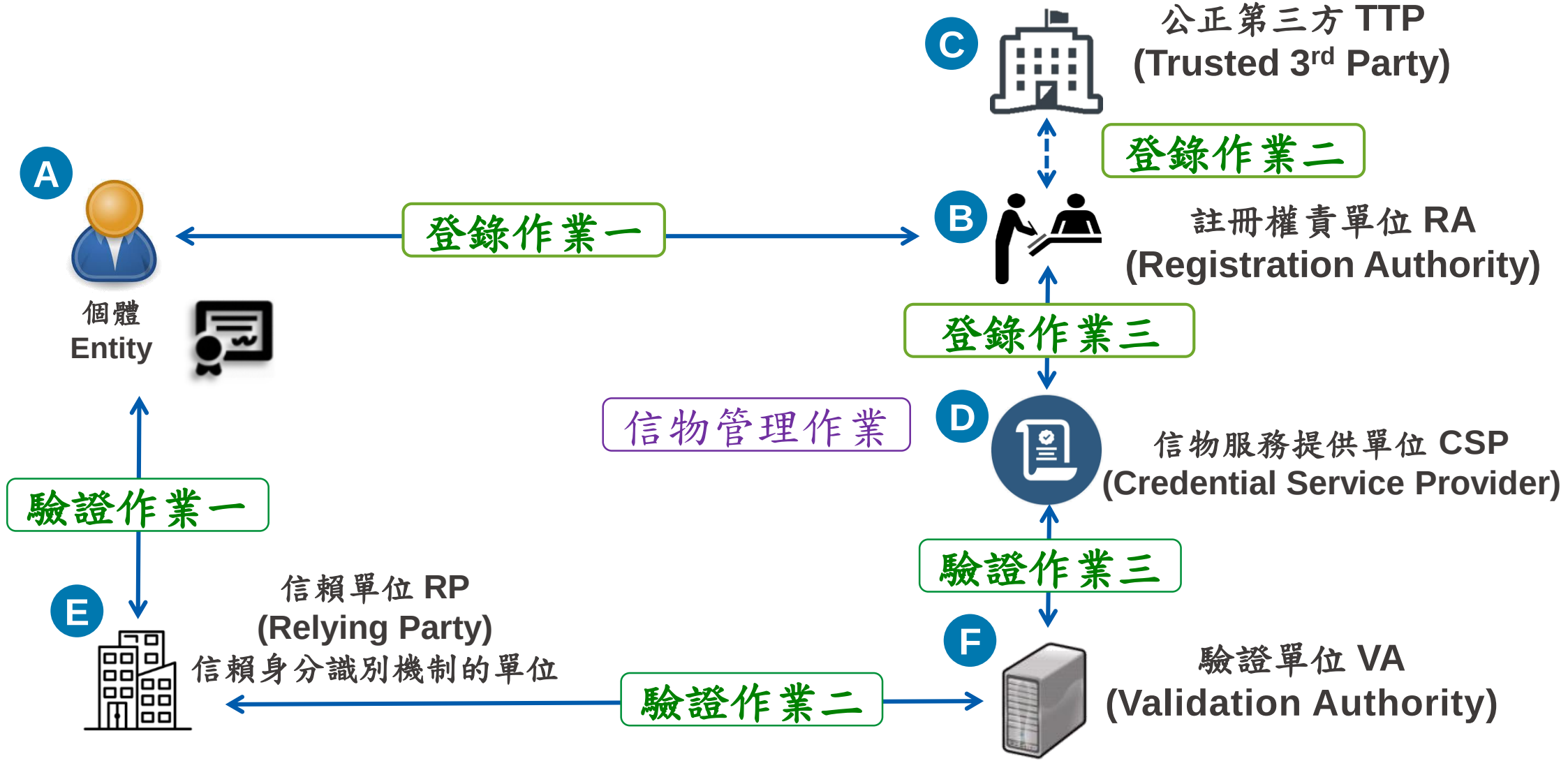
身分識別機制的三個階段

階段	簡稱	主要作業內容
登錄階段 Enrolment Phase	登錄 Enrolment	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。
信物管理階段 Credential Management Phases	管理 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」。
個體驗證階段 Entity Authentication Phase	驗證 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」。

參考資料：

- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

六個角色與三階段主要關係及流程



參考資料：

- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

登錄 Enrolment (以晶片金融卡為例)

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

登錄作業一

客戶持身分證及第二證件親臨銀行櫃台申請：

1. 人工確認人臉與身分證照片之**關聯性(Authentication)**。
2. 人工確認身分證之**真偽(Verification)**。
3. 透過與內政部之系統確認身分證之**有效性(Validation)**。

A 個體 自然人

＋ 第二證件

C 公正第三方 TTP
內政部

登錄作業二

B 註冊權責單位 RA
銀行櫃檯

登錄作業三

D 信物服務提供單位 CSP
銀行發卡系統

F 驗證單位 VA
銀行驗證系統

E 信賴單位 RP
銀行AP或其他應用系統

參考資料：

- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

信物管理 Credential Management

(以晶片金融卡為例)

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

身分資料核驗暨信物管理
完成身分資料核驗後，妥善核發信物及其管理。

C 公正第三方 TTP
內政部

A 個體
自然人

信物管理作業

信物
晶片金融卡 + 首次密碼

B 註冊權責單位 RA
銀行櫃檯

信物管理作業

D 信物服務提供單位 CSP
銀行發卡系統

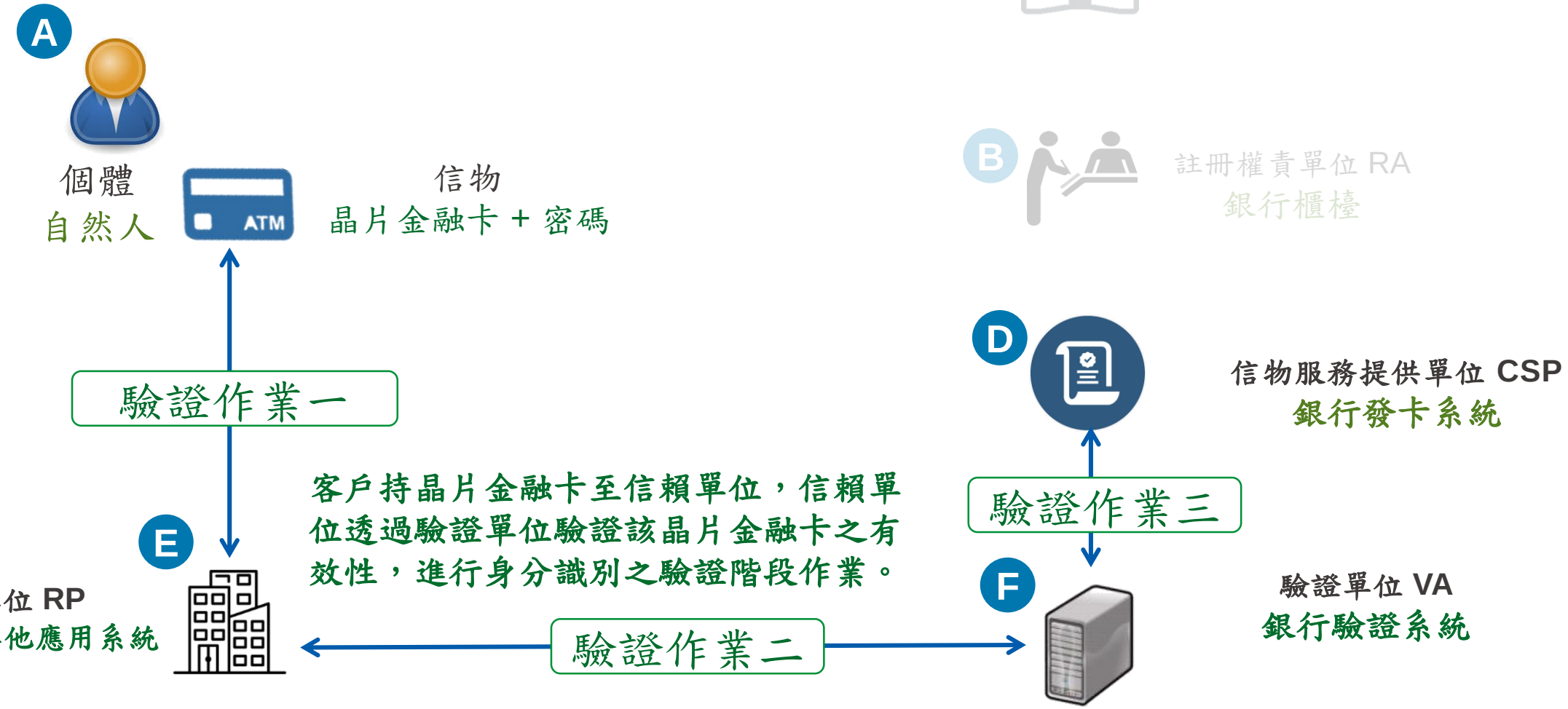
F 驗證單位 VA
銀行驗證系統

E 信賴單位 RP
銀行AP或其他應用系統

參考資料：
- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

驗證 Authentication

(以晶片金融卡為例)



參考資料：

- 連子清與杜宏毅 (2022)。身分識別之書。臺灣網路認證股份有限公司，台北市，台灣。
- International Organization for Standardization (2013).ISO/IEC 29115:2013 Information technology – Security techniques - Entity authentication assurance framework.

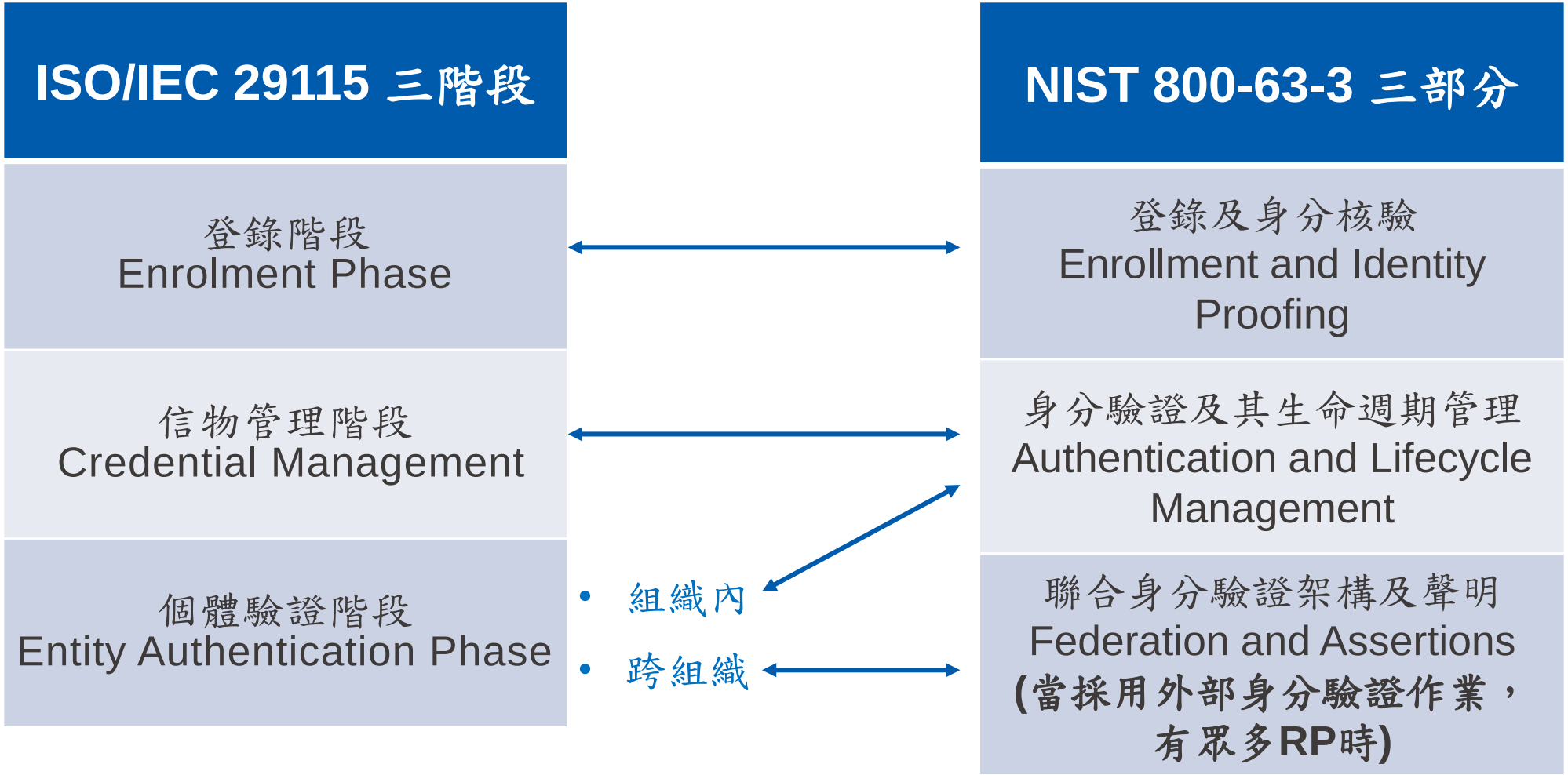
NIST《數位身分指引 Digital Identity Guidelines》(NIST SP 800-63-3)

- NIST (The National Institute of Standards and Technology)
- NIST SP 800-63-3 報告，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。
- NIST 800-63-3 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
   Enrollment and Identity Proofing (NIST SP 800-63A)
2. 身分驗證及其生命週期管理
   Authentication and Lifecycle Management (NIST SP 800-63B)
3. 聯合身分驗證架構及聲明
   Federation and Assertions (NIST SP 800-63C)

參考資料：
- 鄭婷方(2017)。NIST 關於數位身分之研究報告。(報告編號：TWCA-TR-010)臺灣網路認證股份有限公司。
- NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

ISO/IEC 29115 與 NIST 800-63-3 之對應比較



臺灣網路認證股份有限公司 內部整理

登錄及身分核驗
Enrollment and Identity Proofing

對應到 ISO/IEC 29115「登錄」階段

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

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, IAL) 等級**。

嚴謹度	IAL 等級	說明
低	IAL 1	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。 例如：部分數位社群帳號、Email申請，無須提供身分證明資料，即可進行申請。
中	IAL 2	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。 例如：提供相關證身分證明文件予金融機構，經金融機構驗證無誤後，方可申請相關數位金融服務。
高	IAL 3	除了 IAL 1 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，為身份核驗最嚴格的等級。 例如：民眾至戶政事務所臨櫃申請自然人憑證。

參考資料：
- 鄭婷方(2017)。NIST 關於數位身分之研究報告。(報告編號：TWCA-TR-010)臺灣網路認證股份有限公司。
- NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

身分驗證及其生命週期管理
Authentication and Lifecycle Management

對應到 ISO/IEC 29115 「管理」、「組織內驗證」 階段

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

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 (Authenticator Assurance Level, AAL) 等級**：
(最常見的驗證方式，即為密碼 Password)

嚴謹度	AAL 等級	說明
低	AAL 1	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，或者是 OTP 認證方式。
中	AAL 2	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，例如符合 FIPS 140 level 1 之設備。
高	AAL 3	需使用「多因子」的身分驗證方式外，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」。

參考資料：
- 鄭婷方(2017)。NIST 關於數位身分之研究報告。(報告編號：TWCA-TR-010)臺灣網路認證股份有限公司。
- NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

聯合身分驗證架構及聲明
Federation and Assertions

對應到 ISO/IEC 29115
「跨組織驗證」 階段

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 上述 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給多個 RP 單位使用時，則會出現聯合身分驗證架構**，此時則可以參考**三個 FAL (Federation Assurance Level, FAL) 等級**：

嚴謹度	AAL 等級	說明
低	FAL 1	RP 單位獲得一經 IdP 簽署的身分聲明。
中	FAL 2	除 FAL 1 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	FAL 3	除了 FAL 1 及 2 要求外，使用者須證明對該「私密金鑰」的所有權。

參考資料：
- 鄭婷方(2017)。NIST 關於數位身分之研究報告。(報告編號：TWCA-TR-010)臺灣網路認證股份有限公司。
- NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

二、身分驗證類別

身分驗證種類 (對稱/非對稱)

身分識別機制	對稱式	非對稱
定義	被驗證單位所保存的信物與註冊登錄至驗證單位的資料相同。	被驗證單位所保存的信物不等同於註冊登錄至驗證單位的資料。

類別	身分識別項目	Entity所示	CSP所驗
對稱式	網路銀行帳號密碼	帳號、密碼	帳號、密碼
	Mobile ID 門號身分識別	個資、SIM卡資料	個資、SIM卡資料
	晶片金融卡	晶片金融卡及PIN碼	晶片金融卡TAC押碼值及相關個資
	臨櫃驗證國民身分證	身分證正本	身分證正本
非對稱式	FIDO	私鑰	以私鑰簽章之資訊
	PKI 電子憑證	憑證私鑰	以私鑰簽章之資訊
	書面用印	印章	用印結果
	手寫簽名	簽名行為習慣	簽名結果
	生物辨識(以人臉為例)	臉部	當下臉部特徵擷取結果
	翻拍或國民身分證影本	身分證正本	身分證影本

參考資料：葉人瑋與黃湘凌 (2021)。身分識別機制之分類比較研究報告。(報告編號：TWCA-TR-009)臺灣網路認證股份有限公司。

身分驗證種類 (精準/非精準)

身分識別機制	精準型	非精準型
定義	驗證單位與使用者所約定的知識在呈現、儲存、處理或傳輸的形式上，或是在於驗證信物的方法上，是不帶有不確定性存在	驗證單位與使用者所約定的知識，可能是一個數值區間、一個集合，因而在驗證時也可能存在含糊不清(vagueness)的部分。

類別	身分識別項目	正常運作情境中的不確定性
精準型	網路銀行帳號密碼、Mobile ID 門號身分識別、晶片金融卡、FIDO、PKI電子憑證	現行機制中無不確定性
非精準型	書面用印	用印時的印泥量、技術將影響成像的品質辨識者主觀判斷的歧異或含糊不清
	書面簽名	簽名者的每次簽名或有不同辨識者主觀判斷的歧異或含糊不清
	生物辨識(以人臉為例)	影像/訊號擷取技術受限，每次擷取或有不同。

參考資料：葉人瑋與黃湘凌 (2021)。身分識別機制之分類比較研究報告。(報告編號：TWCA-TR-009)臺灣網路認證股份有限公司。

身分驗證種類 (自行驗證/第三方驗證)

身分識別機制	自行驗證	第三方驗證
定義	驗證單位和註冊單位係同一單位。	驗證單位和註冊單位不是同一單位。

類別	身分識別項目	RP單位	RA/CSP/ Verifier單位
自行驗證	自行網路銀行帳號密碼	RP單位同時為RA、CSP及Verifier單位	
	自行晶片金融卡		
	直接驗證的生物辨識機制		
第三方驗證	自然人憑證	金融機構(SP單位)	內政部MOICA憑證管理中心
	Mobile ID門號身分識別		電信業者
	跨行網路銀行帳號密碼		帳戶管理銀行
	跨行晶片金融卡		帳戶管理銀行
	跨行存款帳戶驗證		帳戶管理銀行
	TW FidO	政府機構 (SP單位)	內政部FIDO中心

參考資料：葉人瑋與黃湘凌 (2021)。身分識別機制之分類比較研究報告。(報告編號：TWCA-TR-009)臺灣網路認證股份有限公司。

三、生物特徵驗證

Gartner 生物特徵驗證技術產業概況

- 裝置本身(如手機)的生物特徵驗證機制已經被廣泛使用，並被整合進許多應用程式。
- 生物特徵驗證機制可單獨提供無密碼驗證方式, 也可以跟其他驗證方式整合. Phone-as-a-token 的驗證方式將會在多數工作環境中扮演主導的地位.
- 在金融跟零售業，生物特徵驗證可提供高安全性的客戶驗證。 過去行動通路 (Mobile channels) 已被廣泛使用, 最近因全通路行銷 (Omnichannel) 的普及更提高了生物特徵驗證的關注度。
- 隱私權不會對生物特徵驗證的採用造成不可逾越的障礙
- SRM 主管和供應商往往過於關注資料安全而忽視其他監管需求
- FIDO 已成為生物特徵驗證實作的主流做法。

生物特徵驗證機制特點

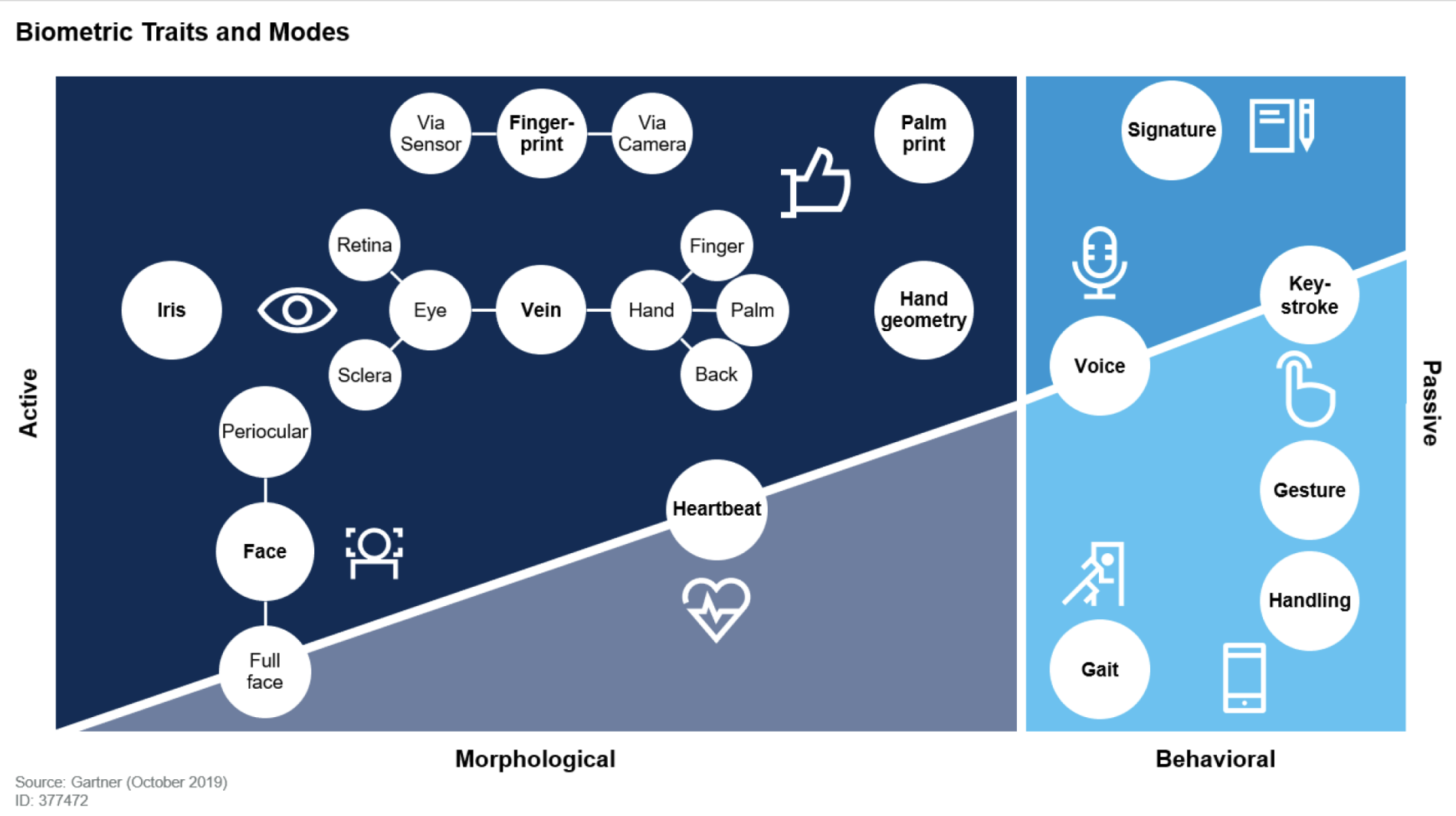
- 主要作為無密碼的驗證方式
- 加強UX/CX
- 提升信用跟問責
- 跟非生物方式的差異 (passwords 跟 cryptographic keys)
  - Stochastic variation: 每次生物特徵的樣本均會有些微差異，探測資料永遠不會跟參考資料完全相同
  - No dependence on shared secrets: 生物特徵驗證不依賴於生物特徵的保密性，而是依賴於模仿活人向傳感器 (sensor) 呈現特徵的困難度。

生物特徵跟模式

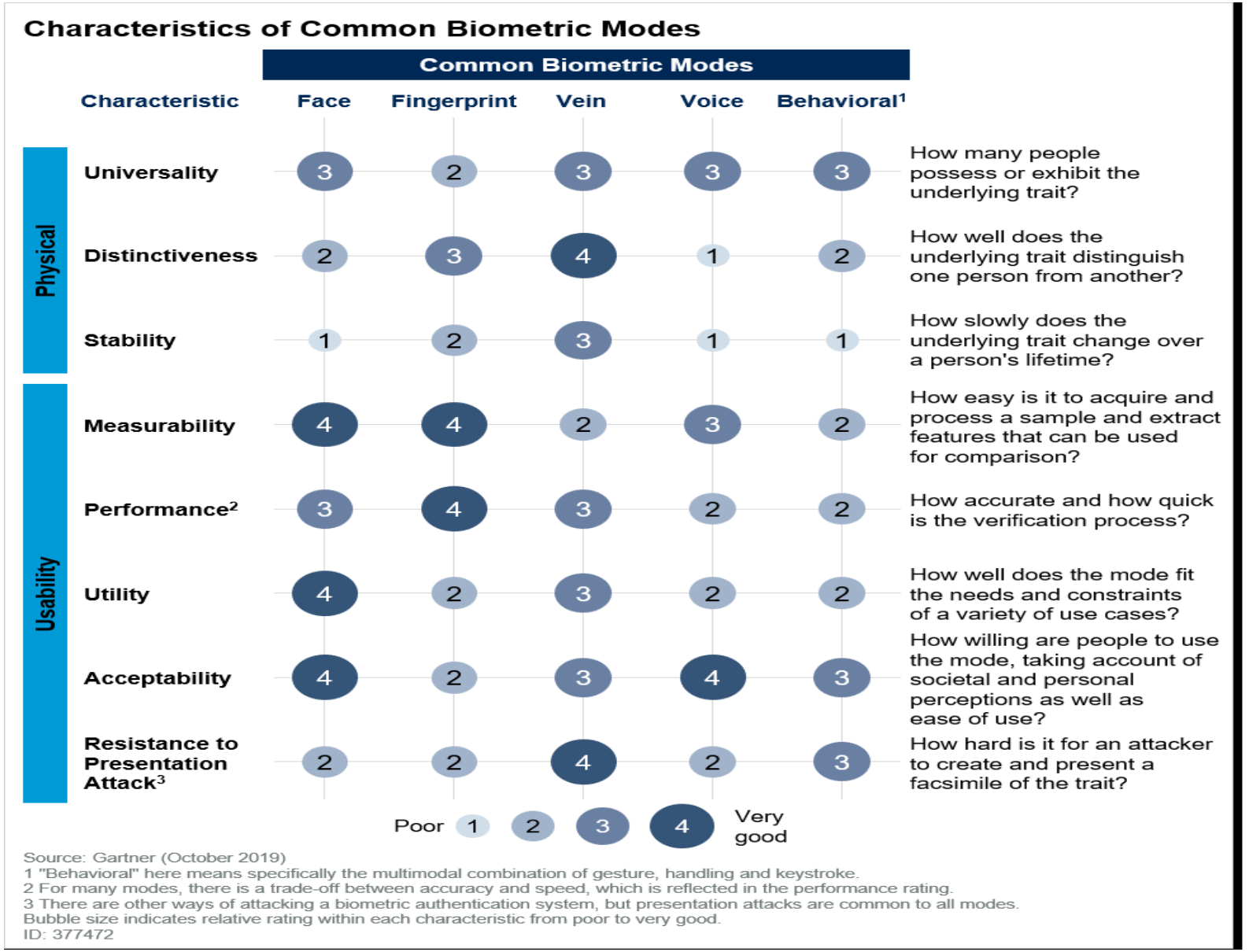
- 主動模式 (Active Modes)
  - 透過分離的註冊流程
  - 獨特的驗證步驟
  - 需要使用者確認意圖跟行為
- 被動模式 (Passive Modes)
  - 透過平常的使用習慣持續收集跟註冊，無須主動註冊
  - 使用者多半不知道資料採集跟分析在進行中

生物特徵跟模式

Figure 1. Biometric Traits and Modes



生物特徵認證技術比較



採用生物辨識技術時的五大特性

特性	說明	範例 (以人臉)
獨特性 (Distinctiveness)	• 主體的生物特徵具備獨特性,足以辨識出主體	人臉足以辨識出主體
可重複性 (Repeatability)	• 又可稱為持久性 (permanence) • 在很長一段時間（如：幾年）內，每一個主體的生物特徵都不會有太大的變化	在一定時間內人臉不會有太大變化
可存取性 (Accessibility)	• 能具體呈現給感測器（例如：相機或指紋掃描器，或是手指幾何測量設備）讀取並轉化為可衡量的指標	透過感測器能將人臉轉化為特徵值並予以量化
普遍性 (Universality)	• 所需特徵對主體來說都是顯而易見，最好是大部分主題都擁有的	所有主體都有人臉
可接受性 (Acceptability)	• 普遍民眾可接受的生物特徵，或者是易於操作、不具侵入性之生物特徵	大部分民眾可接受人臉辨識

參考資料：鄭婷方 (2021)。生物識別技術研究報告(報告編號：TWCA-TR-003)。臺灣網路認證股份有限公司。

生物辨識的分類

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

參考《金融機構運用新興科技作業規範》定義

直接驗證 生物特徵技術

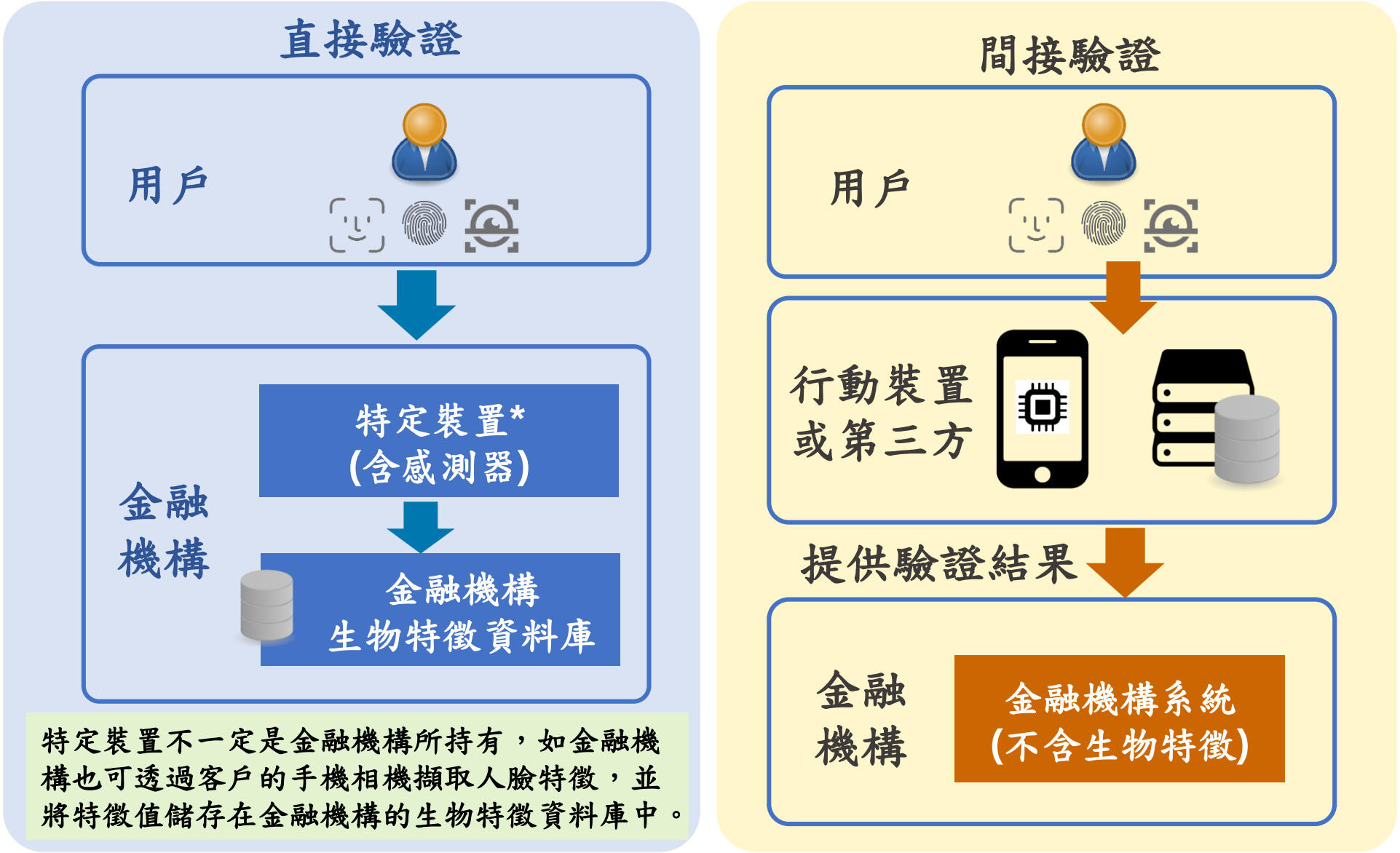
是指由金融機構驗證客戶之生物特徵，以確認其身分。

間接驗證 生物特徵技術

是指由第三方驗證客戶之生物特徵，再將驗證結果傳送至金融機構，以確認其身分。

臺灣網路認證股份有限公司 內部整理

直接驗證與間接驗證



直接驗證與間接驗證

差異點 / 驗證方式	直接驗證	間接驗證
特徵擷取	應用單位臨櫃 / 設置於指定地點的特定設備	第三方裝置
對環境的掌控度	高	低
比對驗證	應用單位系統端比對	裝置端比對
儲存與管理	應用單位系統	第三方裝置
隱私暴露風險	相對較高 （透過網路傳遞資訊） （擷取設備至後端比較子系統）	相對較低 （裝置內傳遞資訊）
成本	需特定裝置 成本較高	裝置為個體自備 成本較低
應用	高風險交易應用	行動裝置解鎖

參考資料：鄭婷方 (2021)。生物識別技術研究報告(報告編號：TWCA-TR-003)。臺灣網路認證股份有限公司。

直接驗證與間接驗證 (套用ISO/IEC 29115架構)

	直接驗證	間接驗證
登錄	1. 客戶需到金融機構指定的特定設備(ATM或臨櫃等)進行生物特徵登錄作業 2. 登錄前須**依金融機構規定進行身分核驗流程**	客戶**依自己手上所持有的裝置自行進行登錄動作**。 (開啟裝置的生物辨識功能)
信物	約定的生物特徵	約定的生物特徵
管理	登錄後的生物特徵 **保管在金融機構系統中**	登錄後的生物特徵 **保管在客戶持有的裝置上**
驗證	金融機構須自特定設備(感測器)上擷取生物特徵後，與系統中的客戶資料及生物特徵自行進行比對。	金融機構相信第三方(客戶持有的裝置)驗證結果
應用舉例	中信 ATM 指靜脈服務	金融機構 APP 生物辨識快速登入方案

參考資料：鄭婷方（2021）。生物識別技術研究報告(報告編號：TWCA-TR-003)。臺灣網路認證股份有限公司。

四、電子簽章國際規範指引參考：歐盟 eIDAS (electronic IDentification, Authentication and trust Services)

歐盟eIDAS對電子簽章的要求

	合格型 QES (Qualified Electronic Signature)	進階型 AES (Advanced Electronic Signature)	一般型 ES (Electronic Signature)
完整性	簽章後內容無法變更	簽章後內容無法變更	簽章後內容無法變更
簽署者身分	必須100%確認簽署者身分，須做到面對面確認或同等效力做法	有很高比例可確認即可	不須確認
真實性	須確認簽名和簽署者的關連性	須確認簽名和簽署者的關連性	不須確認簽名是否關連到簽署者
驗證性	須確認簽名是否在簽署者本身控制下完成。 • 可搭配多因子認證(選用)	須確認簽名是否在簽署者本身控制下完成。 • 可搭配多因子認證(選用)	不須確認簽名是否在簽署者本身控制下完成。
硬體	須使用安全的簽名設備	須使用安全的簽名設備	不須要
法律效力	具法律效力，不承認簽名的一方須舉證	具法律效力，簽名人須自行舉證	具法律效力，簽名人須自行舉證

參考資料：連子清 (2021)。歐盟eIDAS 研究報告(報告編號：TWCA-TR-007)。臺灣網路認證股份有限公司。

期末研究小結

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

身分驗證信賴框架與類別：

- 對稱／非對稱、精準／非精準、自行驗證／第三方驗證
- 以 ISO/IEC 29115 拆解其身分驗證之架構 (三個作業階段、六個角色、一信物)
- 美國 NIST 800-63-3 可呼應 ISO/IEC 29115 的三個作業階段 (登錄、管理、驗證)

生物特徵驗證技術：

- FIDO 已成為實作的主流做法
- 分為直接驗證、間接驗證 (參考《金融機構運用新興科技作業規範》)
- 可以 ISO/IEC 29115 拆解其身分驗證之架構進行系統化的分析

國際電子簽章標準：

- 歐盟 eIDAS → 依據不同簽章方式、身分驗證方式，定義不同等級的簽署標準

臺灣網路認證股份有限公司 內部整理

數位身分驗證場景最佳實務指引分享

陳恭 老師
研究案協同主持人
政大金融科技研究中心副主任
政大區塊鏈創新實驗室執行長
政大資管系教授
2022/07/14

期中研究總結
我國金融產業對於多元數位身分的痛點與議題

痛點	議題
1. 沒有銀/保/證一體適用的數位身分信賴框架	1. 身分信賴框架
2. 第三方身分識別服務的議題	2. 第三方身分驗證
3. 身分核驗採生物辨識的議題	3. 生物辨識
4. 電子簽章法未能與時俱進	4. 電子文件簽章
5. 目前法人數位身分驗證與授權的困難	5. 法人數位身分
6. 如何在使用者授權下，進行共享資料的交換	6. 資料共享

1. 身分識別信賴框架最佳實務指引

A

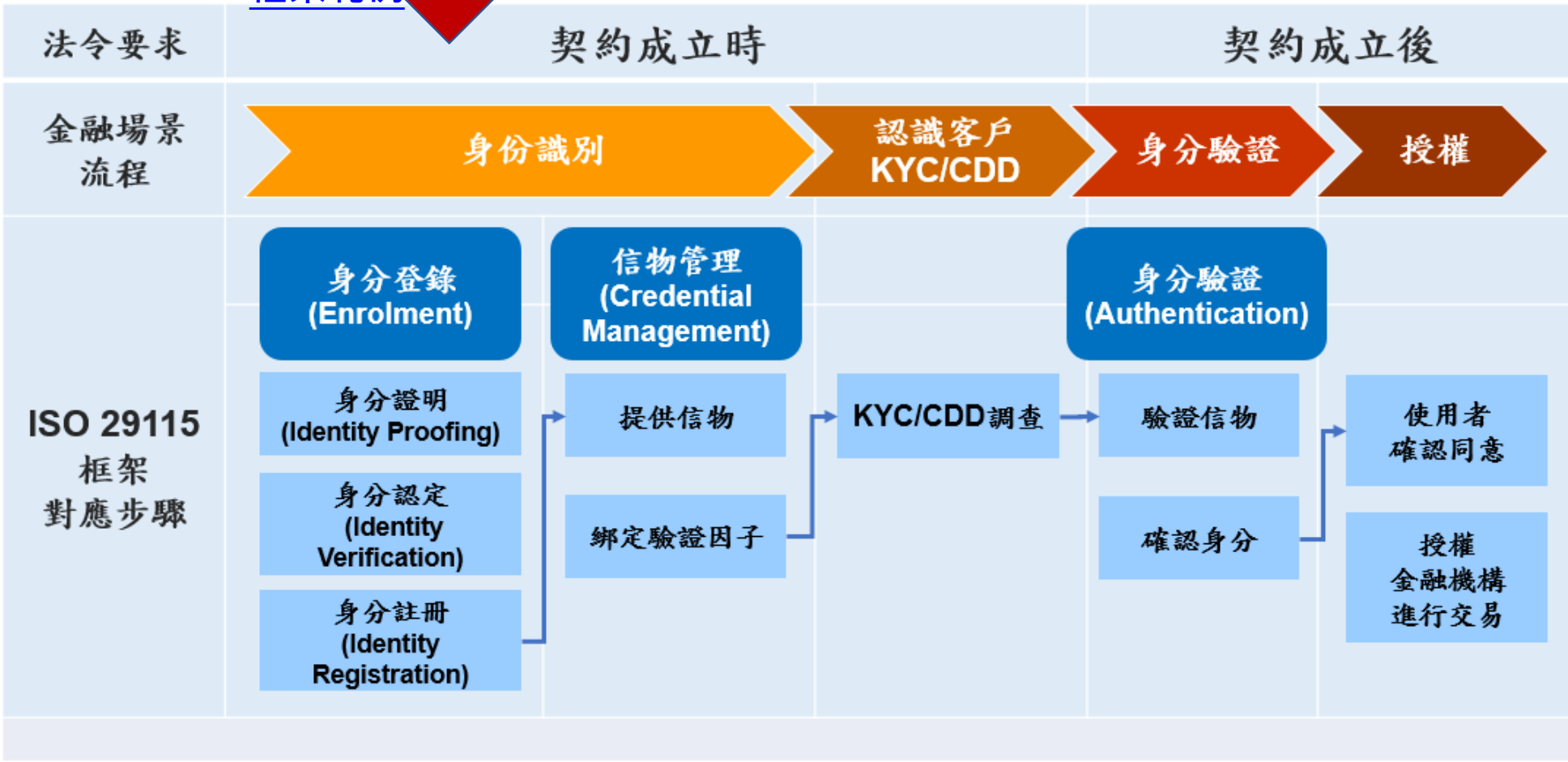
- 參考國際標準，[發展身分識別信賴框架]，包含實務作業基準與信賴風險等級(LoA)。 標竿範例：ISO 29115，NIST 800-63

[框架範例]

B 界定業務風險等級

C 評估機制信賴等級

D 選定合適驗證機制



1. 身分識別信賴框架最佳實務指引

A

- 參考國際標準，發展身分識別信賴框架，包含實務作業基準與信賴風險等級(LoA)
- 標竿範例：ISO 29115，NIST 800-63

		作業	範例
B	界定業務風險等級	• 依選定身分識別信賴框架，建立「業務的身分識別風險評估框架」 • 對選定業務進行身分識別作業之風險評估，訂定所需之信賴等級	• 提供線上開戶服務，擬透過第三方驗證機制進行新戶身分識別與證明作業(enrollment) • 評估該業務之風險等級為LoA3

C	評估機制信賴等級	• 對各項可能採用的身分驗證機制，進行信賴等級評估	• 選取第三方身分識別服務，進行LoA評估
			  • 晶片金融卡
			  • 網銀帳戶+手機簡訊驗證
			  • 電信認證等

D	選定合適驗證機制	• 權衡身分驗證信賴等級需求與其他需求，挑選適合之身分驗證機制	• 兼顧信任等級與其他需求，挑選網銀帳戶+手機簡訊驗證

A. 發展身分識別信賴框架

參考國際標準，發展身分識別信賴框架，建立識別與驗證機制實務作業基準與信賴風險等級(LoA)評估框架

- 範例：以ISO29115為基礎
- 以登錄作業為例
  - 控制點範例
  - 實務作業說明
  - LoA評估

登錄作業

項次	控制點範例	自評結果 LoA 1	2	3	4	實務作業說明
16.	【自然人 (非臨櫃)】 必須提供 2 個 (含) 以上具權威性且不同單位核發之身分資訊。其中，第 2 個 (含) 以後之身分資訊至少要完成其與「個體」或「第 1 個身分資訊」之關聯性驗證 (例如：確認帶有與「個體」外觀匹配的持有人照片，或帶有與「第 1 個身分資訊」相匹配之資訊)					
17.	【自然人 (非臨櫃)】 必須提供證據證明其擁有具權威性單位核發之身分資訊 (如駕照)					
18.	【自然人 (非臨櫃)】 必須檢核證明文件當下有效且客觀存在					
19.	【自然人 (非臨櫃)】 確保由受信任之第三方(TPP)，透過權威資訊來源，檢查個體對當前擁有的高可信度信賴等級 (LoA3) (含) 以上信物的主張 (訊息驗證&確認唯一)；或， 驗證僅能由該個體提供或可能只有該個體所知的資訊					

Source: 臺灣網路認證股份有限公司

B. 界定業務風險等級

B 界定業務風險等級

C 評估機制信賴等級

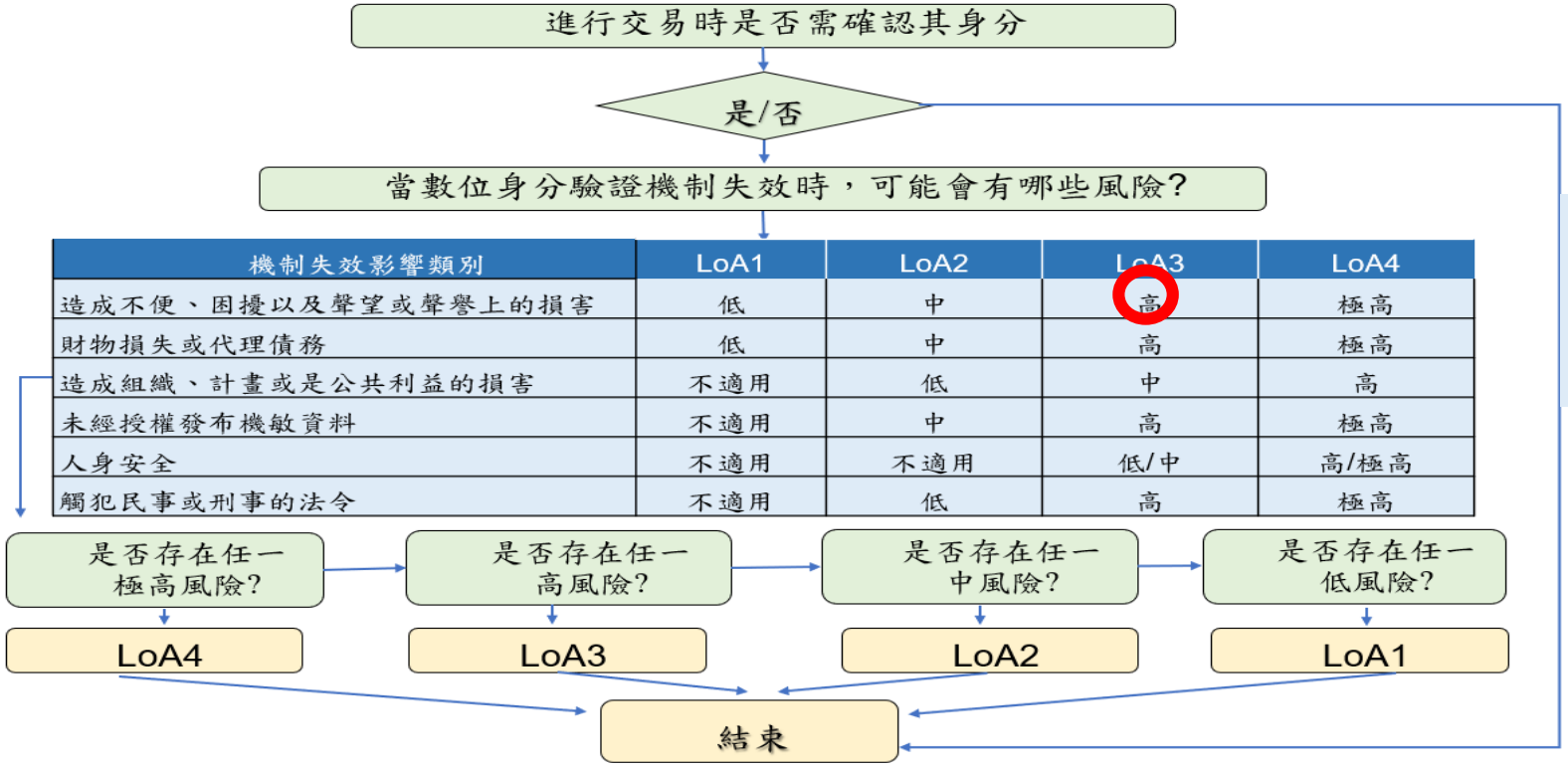
D 選定合適驗證機制

作業

- 依選定身分識別信賴框架，建立業務的「身分識別風險評估框架」
- 對選定業務進行身分識別作業之風險評估，訂定所需之信賴等級(成本與複雜度一併考量)

範例

- 某業務將提供線上開戶服務，擬透過第三方驗證機制進行新戶身分識別與證明作業(enrollment)



機制失效影響類別	LoA1	LoA2	LoA3	LoA4
造成不便、困擾以及聲望或聲譽上的損害	低	中	高	極高
財物損失或代理債務	低	中	高	極高
造成組織、計畫或是公共利益的損害	不適用	低	中	高
未經授權發布機敏資料	不適用	中	高	極高
人身安全	不適用	不適用	低/中	高/極高
觸犯民事或刑事的法令	不適用	低	高	極高

身分識別失效會大幅影響商譽將風險等級設為LoA3

C. 評估機制的信賴等級(LoA)

B 界定業務風險等級

C 評估機制信賴等級

D 選定合適驗證機制

作業

- 對業務可能採用的各種身分驗證機制進行信賴等級評估(LoA)

範例

- 晶片金融卡跨行帳戶驗證服務：LoA4，但需讀卡機
- 網銀帳戶驗證服務：LoA2，但使用者體驗佳
- 電支帳戶驗證服務(假設有)：LoA2
- 電信驗證(Mobile ID)：LoA3？因部分通訊行，未能落實雙證件查驗，影響LoA等級

信物管理階段 (Credential Management)

可參考【eKYC 自評說明 與 參考範例(進階)】填寫

項次	控制點範例	自評結果 LoA 1	2	3	4	實務作業說明
1.	制定並遵行信物產製作業流程					
2.	在最終的信物與個體的綁定之前，提供信物服務的單位(CSP)必須充分保證信物已綁定並保持綁定到正確的個體					
3.	信物完成綁定後，必須提供信物不被竄改的保護措施，建議的措施如： (a) 以數位簽章；或 (b) 針對保存於硬體裝置上之信物，初始設定為鎖定狀態					
4.	信物產製時之資訊傳遞過程，需透過受保護的渠道進行 (如 SSL/TLS 網路傳輸數位資訊、親臨或彌封傳遞紙本文件)					
5.	信物必須儲存於符合 ISO/IEC 19790:2012 規範的硬體安全模組 (Hardware Security Module，HSM) 中。(例如：符合 Common Criteria ISO/IEC 15408 v2.3 EAL 4+ (含增項 AVA_VLA.4 及 ADV_IMP.2)、FIPS 140-2/140-3 Level 3 (含) 以上，或其他相同安全強度之認證)					
6.	為防止信物交付至個體前遭盜用，保存於硬體裝置上之信物，於產製作業完畢時必須設定為鎖定狀態					
7.	如果信物或產生信物的方式是保存在硬體裝置上，則這些空白的硬					

D. 選定合適驗證機制

B 界定業務風險等級

C 評估機制信賴等級

D 選定合適驗證機制

作業

- **權衡身分驗證信賴等級需求與其他需求，挑選適合之身分驗證機制**

- **新戶身分識別風險信賴等級需求為LoA3**
- 客戶體驗考量
- 服務提供成本
- 其他因素

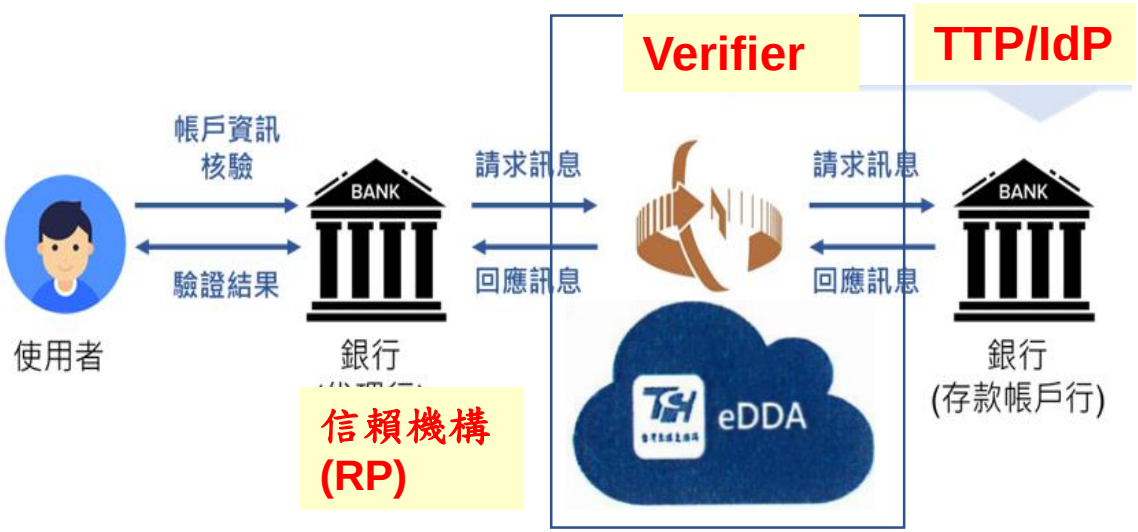
範例

- 晶片金融卡跨行帳戶驗證服務：LoA4，但需讀卡機
- 網銀帳戶驗證服務：LoA2，但使用者體驗佳
- 電支帳戶驗證服務(假設有)：LoA2
- 電信驗證(Mobile ID)：LoA3？因部分通訊行，未能落實雙證件查驗，影響LoA等級

- 網銀帳戶驗證LoA不足，透過用戶留存銀行的手機行簡訊驗證，以提升LoA等級
- **選擇：網銀帳戶驗證+用戶手機簡訊驗證**

2.第三方身分識別服務的議題

- ”電子銀行業務安控作業基準”第七條列舉：
  - ✓ 「跨行金融帳戶資訊核驗」機制
  - ✓ 「信用卡輔助持卡人身分驗證平 臺」
  - ✓ 電信認證
- 實務上，類似的還有票交所的eDDA服務
- 可用於
  - ✓ 新開戶身分識別：一次性
  - ✓ 交易前驗證：多次性



- NIST 800-63標準包含**聯合身分驗證架構**(federated authentication)，規範跨機構驗證
  - ✓ IdP：身分識別服務商；RP：信賴機構
  - ✓ 3種FAL：聯合信賴等級
- **代理型聯合驗證**(proxied federation)

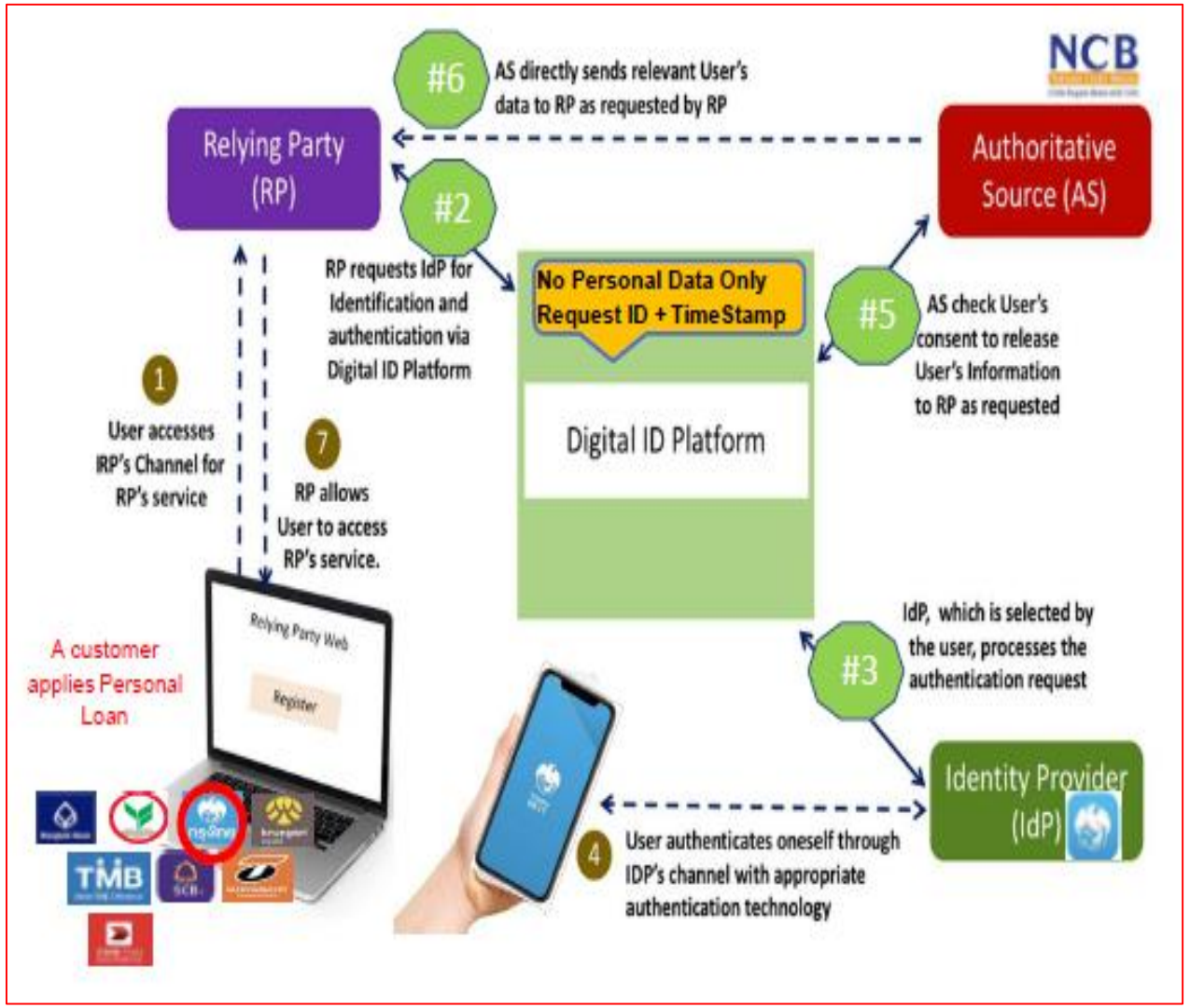
建議：透過框架，界定

- 各角色的資格限制
- 權利義務
- 認證與稽核作業
- …

2.跨機構第三方身分識別服務國際範例

1. 期中報告已介紹 瑞典BankID案例

2. 近年泰國政府也發展了NDID平台
   - National Digital ID (eKYC)
   - 以NIST 800-63為參考框架，初期由銀行擔任IdP(身分識別服務商)與RP，互驗
   - 未來公私協力跨大參與：RP的範圍也會逐步跨大，跨產業合作
   - 從eKYC邁向eConsent，機構間共享客戶資料



圖片來源：NDID官網

3.生物辨識技術應用於身分驗證之實務與建議 (1/2)

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

現況：

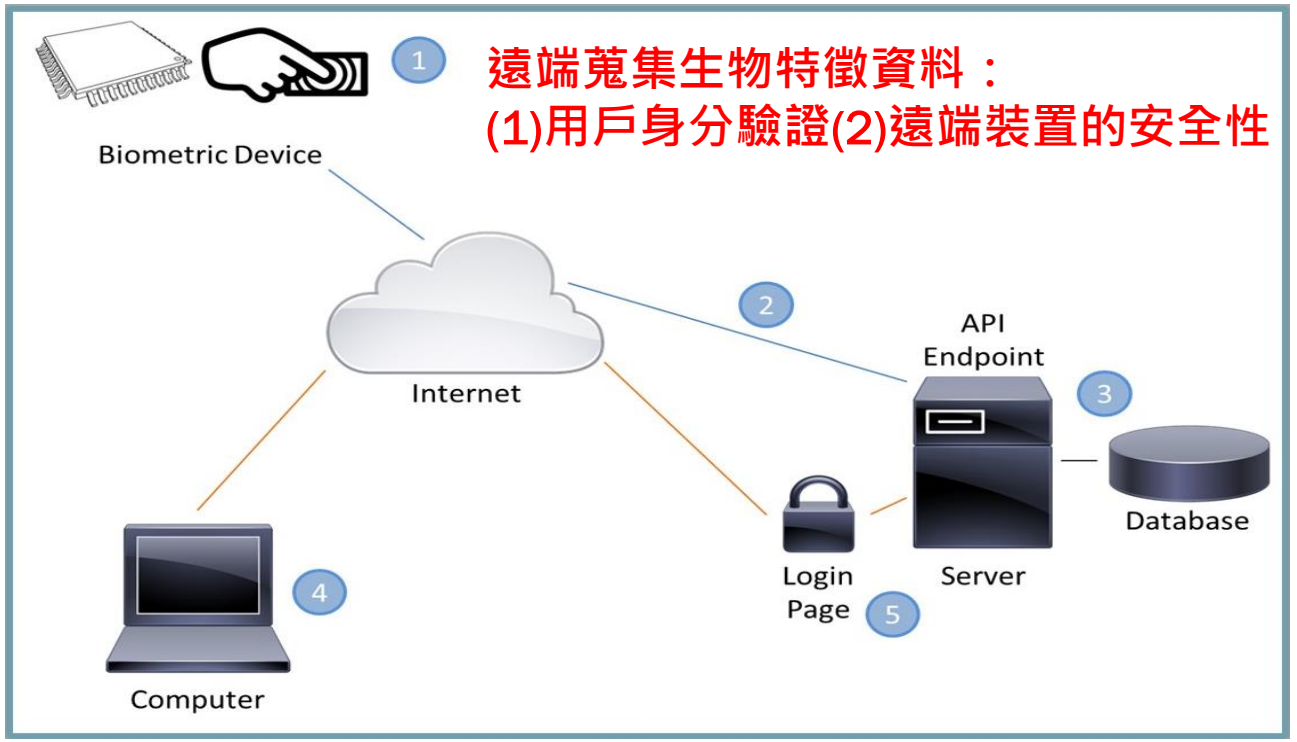
銀行業相關規定散見於銀行公會制定之
- "電子銀行業務安控作業基準"
- "金融機構運用新興科技作業規範"

新興科技作業規範之第五條原則性提示
- 生物特徵資料之蒐集、傳輸與保管
- 建立錯誤接受率與錯誤拒絕率標準
- 內部作業控管

驗證方式區分為
- **間接驗證**：用戶裝置保管與驗證生物特徵(兩項以上技術)
- **直接驗證**：後台保管與驗證生物特徵

電子銀行業務安控作業基準本年**5月修訂版**，第八條第二款第五目之四
- ✓ 新增辦理非約定轉帳若採憑證簽章、…直接人臉辨識軌跡等技術…

- **建議：須注意 所蒐集得生物特徵(直接驗證用) 或 裝置註冊的生物特徵(間接驗證)為非本人之風險**



「金融機構提供自動櫃員機系統安全作業規範」中第六條第3款第3目，"採用兩項技術進行身分確認"中，有一些相關安全規範，**建議：增加更明確的安全要求**。

3. 生物辨識技術應用於身分驗證之實務與建議 (2/2)

美國國家技術標準局，數位身分識別指引(NIST 800-63)，針對運用生物特徵進行身分驗證的指引重點[Sec. 5.2.3]：

- **生物特徵資料有其獨特性，運用於身分驗證要謹慎處理**。
- 生物特徵資料可列為”驗證因子(factor, something you are)”，但不應該單獨視為信物(authenticator)
- 生物特徵資料運用於身分驗證應結合安全儲存裝置一起使用，並視為”多因子信物”(multi-factor authenticator) [63B, Sec. 4.2.1]， something you are+ something you have
- 蒐集與驗證生物特徵資料的裝置必須經過安全認證。
- 生物特徵資料的傳輸與保管必須有嚴謹的資訊安全措施。
- 生物特徵資料的處理必須具備偵測”偽冒攻擊 (PAD)”能力(>90%)。
- 生物特徵資料運用於身分驗證必須制定最小可接受的”錯誤接受率”(FMR or FAR)，例如千分之一。
- 為避免集中(直接)驗證的大風險，建議採用本地(間接)驗證。
- …

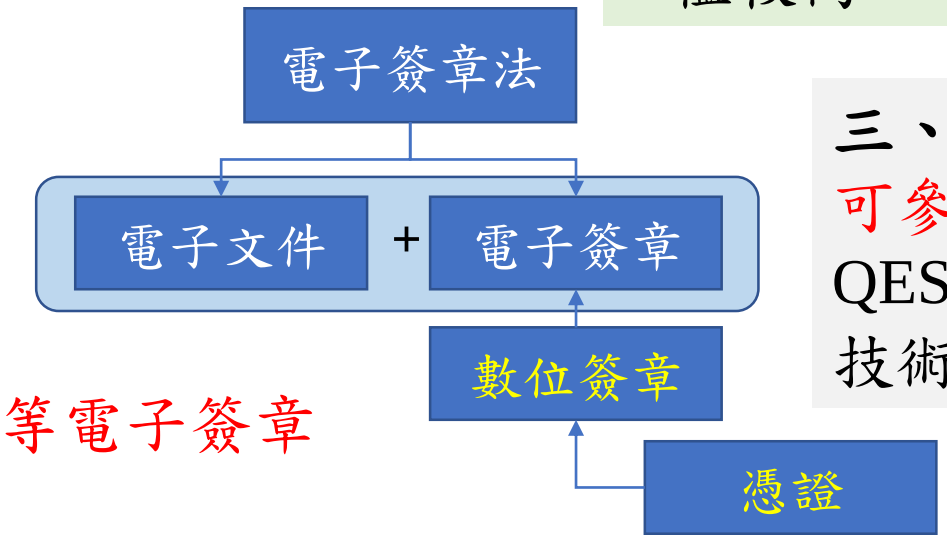
p.s. 保險業辦理遠距投保及保險服務業務應注意事項，第七條要求錯誤率不得高於萬分之一。

4. 電子簽章法議題與實務建議(1/2)

一、**法規**：電子簽章法規範兩大項目
- 電子文件(第4, 6條)
- 電子簽章(第5條)

- 故"依電子簽章法"辦理，可分
  - 需書面者：可採電子文件
  - 依法令規定應簽名或蓋章者需採電子簽章

二、**現況**
- 法令已20年
- 非強制性，有排除性條款
- 技術中立，只針對**數位簽章**有細部規範
  - ✓目前沒有技術被明確認可為"電子簽章"
- 數位簽章需使用合規憑證，使用門檻較高



三、**未來修法建議**

可參考歐盟eIDAS，分ES, QES, AES三等級，分級制定技術規範與法律效力。

＊電子簽名不等同等電子簽章

4.電子簽章法議題與實務建議 (2/2)

建議：法規未要求簽名蓋章，可考慮依第4、6條，以符合電子文件的要式實現

第 4 條

1. 經相對人同意者，得以電子文件為表示方法。
2. **依法令規定應以書面為之者**，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。

法務部案例

- 法務部就**個資法**中要求的書面同意，改以電子文件執行的函釋

  法務部(法律決字第10303508040號)案例:
  同意書雖係以**電子方式**為之，倘足以確認當事人意思表示，並有可為證明方式，即具有個人資料保護法『書面同意』效力。

另一路徑：中央事業主管機關另訂規定

第 9 條

1.依法令規定應簽名或蓋章者，經相對人同意，得以電子簽章為之。
2. 前項規定得依法令或行政機關之公告，排除其適用**或就其應用技術與程序另為規定。**但就應用技術與程序所為之規定，應公平、合理，並不得為無正當理由之差別待遇。

勞動部案例

二、就應用技術與程序另為規定

法規名稱	條次(項次、款次)	法規文字內容	另為規定事項
勞工保險條例	第十一條	符合第六條規定之勞工，各投保單位應於其所屬勞工到職、入會、到訓、離職、退會、結訓之當日，列表通知保險人；其保險效力之開始或停止，均自應為通知之當日起算。但投保單位非於勞工到職、入會、到訓之當日列表通知保險人者，除依本條例第七十二條規定處罰外，其保險效力之開始，均自通知之翌日起算。	應使用合於電子簽章法第十條規定之憑證並經政府機關（構）提供之線上申請系統執行申報者。
	第十四條第二項	被保險人之薪資，如在當年二月至七月調整時，投保單位應於當年八月底前將調整後之月投保薪資通知保險人；如在當年八月至次年一月調整時，應於次年二月底前通知保險人。其調整均自通知之次月一日	應使用政府機關（構）提供之線上申請系統辦理投保手續者。

5. 法人數位身分驗證與授權的議題與建議 (1/4)

- 銀行業者主要反映(1)新開戶作業；(2)線上辦理貸款業務，對保作業中的困難。
- 新版電子銀行業務安控作業基準已針對近來主管機關的開放做出一些修訂：

1. （修正第四條）授信業務新增既有法人客戶、法人新戶及法人戶之負責人得申辦無涉及抵押權或質權設定之貸款、同意金融機構查詢聯徵中心信用資料、線上成立貸款契約。

2. (修正第八條第三款第六目) 新增法人授信業務有關同意金融機構查詢聯徵中心信用資料、簽約對保之安全設計。

第八條 交易類別之安全設計

三、「電子轉帳及交易指示類」之申請指示

(三)辦理法人授信業務應遵循下列要求：

１、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制：

(１)採用第七條第一款硬體憑證簽章之安全設計。

(２)法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。

２、辦理本行既有法人客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：

(１)採用第七條第一款硬體憑證簽章之安全設計。

(２)透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依第八條第三款第二目第一子目個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照第九條第七款規定辦理。

３、辦理3位以下本國籍自然人股東之法人新戶(不包括有法人股東之公司)之貸款契約成立，簽約對保方式應採用第七條第一款硬體憑證簽章之安全設計。

４、辦理法人戶之負責人或保證人契約成立之簽約對保方式，應採用下列任一方式之安全設計：

(１)採用第七條第一款硬體憑證簽章之安全設計。

(２)採用第七條第五款視訊會議，並搭配第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」。

５、法人戶徵授信相關文件之上傳，應採用法人戶及其負責人貸款契約成立之安全設計機制。

5. 法人數位身分驗證與授權的議題與建議 (2/4)

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

第八條 交易類別之安全設計
三、「電子轉帳及交易指示類」之申請指示

(三)辦理法人授信業務應遵循下列要求：
1、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制：
(1)採用第七條第一款硬體憑證簽章之安全設計。
(2)法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。
2、辦理本行既有法人客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計：
(1)採用第七條第一款硬體憑證簽章之安全設計。
(2)透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依第八條第三款第二目第一子目個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照第九條第七款規定辦理。
3、辦理3位以下本國籍自然人股東之法人新戶(不包括有法人股東之公司)之貸款契約成立，簽約對保方式應採用第七條第一款硬體憑證簽章之安全設計。
4、辦理法人戶之負責人或保證人契約成立之簽約對保方式，應採用下列任一方式之安全設計：
(1)採用第七條第一款硬體憑證簽章之安全設計。
(2)採用第七條第五款視訊會議，並搭配第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」。
5、法人戶徵授信相關文件之上傳，應採用法人戶及其負責人貸款契約成立之安全設計機制。

修改重點：

- 對3位股東以下之法人特別處理：
  新開戶可用硬體憑證驗證身分
- 銀行可查詢申貸案相關人士的聯徵中心信用資料
- 原本紙本留存印鑑的對保流程可採電子傳送，且在傳送前要進行線上身份驗證
- 對保作業可透過視訊會議進行

本案建議：
朝法人數位身分制度之四要素持續精進：

1. 建立法人之數位身份（如數位工商登記）
2. 建立法人代表人之數位身分（如自然人憑證）
3. **建立法人代表人之授權機制（如法人授權其特定員工辦理數位金融服務），**
4. 數位意思表示行使的方式（如是否揚棄公司大小章的慣習，或建置數位大小章等設計）。

由法人在數位情境所進行之金融交易應該在流程設計上具備可追蹤性（Traceability)，以確保日後若發生爭議時能加以釐清與處理。

5. 法人數位身分驗證與授權的議題與建議 (3/4)
法人戶業務可用資源：線上查詢公司基本資料

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

國發會 MyData 平台

資料集名稱	資料提供單位
公司負責人、董監事與經理人之公司登記資料	經濟部商業司
商業負責人、合夥人、經理人及法定代理人之商業登記資料	經濟部商業司
工廠及其事業主體負責人之工廠登記資料	經濟部商業司
有限合夥代表人、合夥人及經理人之有限合夥登記資料	經濟部商業司

國發會 MyData 平台

財稅金融	企業土地財產資料	財政部財政資訊中心	工商憑證
財稅金融	營業稅籍登記	財政部財政資訊中心	工商憑證
財稅金融	發票驗證(紙本發票)	財政部財政資訊中心	工商憑證
財稅金融	前廿大交易對象進銷項憑證資料	財政部財政資訊中心	工商憑證
財稅金融	營業人銷售額與稅額申報書	財政部財政資訊中心	工商憑證

個人化資料自主運用(MyData) | 資料下載(商工) (nat.gov.tw)

5. 法人數位身分驗證與授權的議題與建議 (4/4)
法人戶業務可用資源：線上查詢公司基本資料

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

集保：公司負責人及主要股東資訊申報平臺

資料內容為董事、監察人、經理人及持有已發行股份總數(或資本總額)超過10%之股東姓名或法人名稱、國籍、出生年月日或設立登記之年月日、身分證明文件號碼或統一編號及持股數(或出資額)。另無限公司或兩合公司沒有董事、監察人制度，只要申報出資超過10%之股東即可。

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

版本：20220401

以 API 介接公司負責人及主要股東資訊查詢平臺申請/變更/停用申請書

申請類別：□新申請 □變更 □停用　　填表日期：　年　月　日

申請單位基本資料			
申請單位代號 （首次申請由集保結算所填寫）		營利事業/扣繳單位 統一編號	
申請單位名稱（全銜） （限總公司申請）			
申請單位登記地址	郵遞區號：＿＿＿＿地址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿		
申請單位本國公司戶總數 （截至填表日止）	家		

常見問題 (tdcc.com.tw)

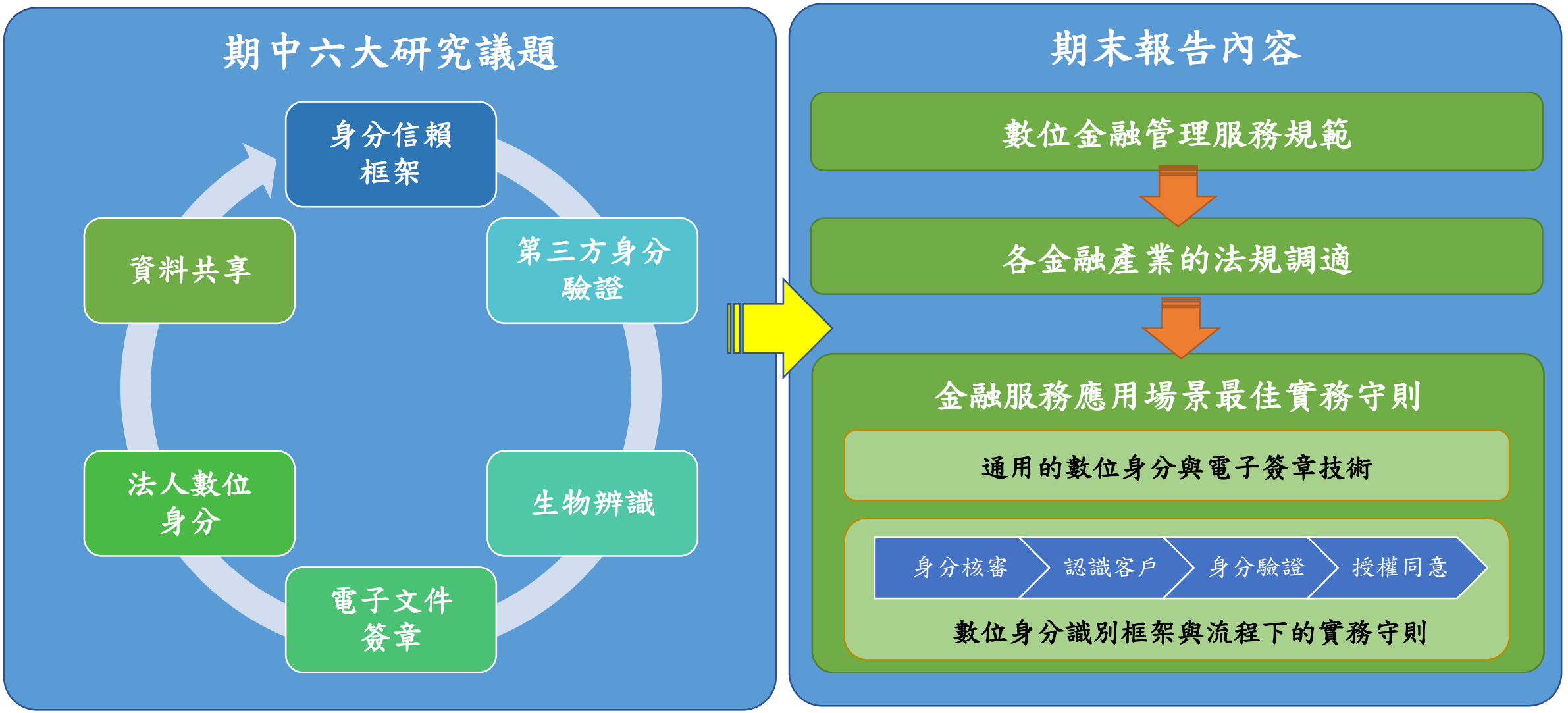
期末研究小結

1. 參考國際標準，發展數位身分信賴框架
   - 實務作業基準
   - 信賴等級評估框架(LoA)
   - 風險信賴等級評估框架
2. 第三方身分識別服務的相關規範
3. 生物特徵識別技術運用規範的深化
4. 電子簽章法限制下的因應措施與調整方案
5. 法人業務數位化的持續擴展

期末研究結論與建言

王儷玲 教授
研究案主持人
政大金融科技研究中心主任
2022/7/14

期末研究成果



研究議題:信賴框架

痛點與需求說明

1. 我國目前沒有一個銀行/保險/證期共用的數位金融服務規範，身分確認以及意思表示的方式，目前規範都散落在各個行業的作業辦法之中。
2. 金融業目前沒有統一針對與第三方業者對於身分介接與資料交換的規範與技術標準。
3. 借鏡國際修法經驗，起草「數位身分與屬性信賴框架」，明確規範數位身分生態系中的互信角色與功能。

建議作法

1. 制訂我國「數位金融服務管理規範」明確規範數位身分應用與管理，以及適用的數位意思表示方式。
2. 針對跨機構或跨產業的數位身分相互確認資料交換，制訂相關規範與作法。
3. 在信賴框架下採以風險為基準的管理方式，搭配差異化、分級化的監督機制。

金融數位服務管理規範設計方向

法源層級方案

法律層級

✓方案一：提案修改「金融科技發展與創新實驗條例」，修正現行第18條或是增訂第18條之1，透過法律層級的授權，讓金管會取得訂定數位金融服務管理規範之權源，進而訂定數位金融服務管理規則。

法規命令層級

方案二：將數位身分制度的落實，視為金融業內部控制與內部稽核制度之一環，而透過複數法律的授權，訂定一個「金融業辦理數位金融服務管理規則」

制度設計與推動方式

目的

- 可以依金融服務的二項重點來設計：獲取客戶及服務客戶
- 協助金融機構有效控管獲取客戶及服務客戶流程中的風險，並保障客戶權益以及相關個資隱私資料

精神

- 借鏡與接軌國際規範與標準：例如：澳洲法案、ISO 29115…
- 參與者應賦予相應之以原則為基礎（Principle-based）的功能要求與責任

功能

- 確保於「身分識別」、「客戶盡職調查」、「身分驗證」及「交易授權」四大環節
- 確保消費者有便行使數位身分與資訊安全/個資隱私保護的要求

推動

- 以風險管理為基礎，建構全面的監理與信任框架，釐清不同市場參與者的權責
- 可以依澳洲系統為案例，將數位身分系統運作拉高至法律授權私級，並建立監理框架的制度

架構

- 可以依(1).法源、(2).名詞定義、(3).數位身分建構流程、(4).數位金融服務作業、(5).參與者功能與責任義務、(6).認證制度、(7).風險等級、(8).數位意思表示、(9).罰則等章節規劃設計。

金融法規盤點與調適

產業	銀行業	保險業	證期業	投信投顧業
主要法令	• 金融機構辦理電子銀行業務安全控管作業基準 • 銀行受理客戶以網路方式開立數位存款帳戶作業範本 • 金融機構運用新興科技作業規範 • 金融機構提供自動櫃員機系統安全作業規範 • 銀行防制洗錢及打擊資恐注意事項範本 • 信用卡業務機構管理辦法	• 保險業務員管理規則 • 保險業招攬及核保作業控管自律規範 • 保險業經營行動服務自律規範 • 人身保險業辦理行動投保身分確認程序業務應遵循事項規範 • 保險業辦理遠距投保及保險服務業務應注意事項 • 壽險業因應新冠肺炎疫情服務涉親晤親簽與紙本作業之暫行原則 • 人壽保險業防制洗錢及打擊資恐注意事項範本	• 臺灣證券交易所股份有限公司證券商受理線上開戶委託人身分確認及額度分級管理標準 • 臺灣期貨交易所股份有限公司「期貨經紀商受理期貨交易人存入保證金、權利金應行注意事項」 • 證券商防制洗錢及打擊資恐注意事項範本	• 中華民國證券投資信託暨顧問商業同業公會國內證券投資信託基金電子交易作業準則 • 中華民國證券投資信託暨顧問商業同業公會境外基金電子交易作業準則 • 證券投資信託事業證券投資顧問事業防制洗錢及打擊資恐注意事項範本 • 臺灣集中保管結算所股份有限公司防制洗錢及打擊資恐查詢作業要點
盤點建議	• 《電子銀行安控作業基準》已有相對完善之規範架構，建議針對數位意思表示可參酌國外作法進行調整。 • 相關修正建議如涉有數位意思表示及電子文件，為使電子文件具法律效力，並評估其使用其他技術（如電子簽名、錄音、錄影、視訊等）。	• 意思表示部份為保險業最注重，所以此部份的規範較完善。 • 壽險業相較於其他金融業者，具有較新意思表示確認規範，但目前法源為因應疫情之作法，建議可以逐步增加意思表示確認之方式。	• 證券業身分確認，目前規範層面僅推進至線上開戶作業之應用，亦未開放生物特徵識別之身分確認方式。 • 證券業者亦有確認客戶意思表示之需求然卻沒有相關之規範，建議可以進行調整。	• 投信投顧業相較於其餘金融產業，其身分確認之相關規範意旨均係為便利投資人進行投資，然其確認客戶身分之方式較少，且規範亦不詳盡，應可明確定義第三方認證方式。 • 投信投顧業者亦有確認客戶意思表示之需求然卻沒有相關之規範，建議可以進行調整。

身分確認

各產業都有明確規範，但欠缺生物辨識與第三方驗證的規範。

KYC/CDD

各產業都依洗錢防制法，有明確的規範相關的作法。

意思表示

各產業對於意思表示，有相對應作法；但對於數位身分的數位意思表示的規範則不足。

研究議題：第三方身份驗證

痛點與需求說明

第三方驗證在不同場景下對應之解決方案沒有明確的信賴等級規範，且無法確認何種解決方案應如何適用

1. 外部身分驗證：金融機構在身分審核時透過外部確認消費者身分；如：內政部自然人憑證、MobileID
2. 帳戶代驗：金融機構必須確認消費者帳戶資訊；如：票交所eDDA、財金公司Pcode 2566
3. 金控互驗：金控下各機構透過共通平台進行身分驗證；如：金融FIDO
4. 銀行代驗：非金融業者透過現有的銀行網銀/行銀帳戶驗證；如：開放銀行的Oauth

建言作法

建議未來應規劃不同角色、風險等級與信賴等級的機制。不同場景未來可改善作法如下：

1. 外部身分驗證：(1).建議未來可以整合行動(無卡)自然人憑證的身分審核功能。(2).MobileID：後續建議得開放以Mobile ID平台，加上不同身分識別機制，進行客戶身分的多因子認證。
2. 帳戶代驗：可擴大eDDA與Pcode的銀行介接家數，提供便民的跨行的身分驗證。
3. 金控互驗：金融FIDO具備高度互通性，應可逐步應用在整個金融產業數位身分的相互驗證機制中。
4. 銀行代驗：有鑑於金融業者（特別是銀行業）並不信任風險高、信賴度低的外部業者的身分確認作法，建議可以把開放銀行TSP角色納入在「金融數位金融管理規範」，確認彼此可以接受的風險等級與信賴等級。
5. 涉及多方聯合身分驗證時可參考NIST 800-63標準之聯合身分驗證架構。

研究議題：生物辨識

痛點與需求說明

身分審核確認：利用AI進行生物驗證確認是否為本人(如：活體辨識)

1. 電子簽名使用：在意思表示時，透過綁定的生物特徵或透過生物識別的錄影，進行交易確認的意思表示(如：APP簽名、錄影簽名、金融FIDO)。
2. 身分驗證使用：消費者事先註冊生物特徵，爾後在金融服務時用來身分驗證使用(如：ATM虹膜辨識)
3. 生物辨識技術有精準度問題，在金融服務場景也會有不同信賴等級的狀況，且現行規範允許壽險業採生物辨識進行身分確認，但僅允許採用人臉辨識及活體辨識。

建言作法

未來建議可參照《金融機構運用新興科技作業規範》新增其餘生物辨識技術。在不同場景應用，則建議：

1. 身分審核確認：採多因子身分驗證，生物識別的錄影資料目前可為法律承認的電子證據，建議搭配其它的身分識別機制確認本人身分。
2. 電子簽名使用：在數位意示表示，建議應納入錄影加生物辨識的作法。
3. 身分驗證使用：目前僅在「新興科技管理辦法」中有制訂生物特徵資料庫的使用管理原則；建議在未來在「金融數位金融管理規範」中規範生物特徵的風險信賴等級（LoA），作為身分確認與意思表示的適用範圍以及相關的應用場景。

研究議題：電子簽章

需求與痛點說明

1. 電子簽章法僅規範電子憑證作法，在舊有電子憑證必須存在卡中的作法，金融產業推廣不易，維護成本高。
2. 保險業法規仍以親晤親簽原則為主，不易以電子憑證方式進行。
3. 電子簽章法太老舊，未能納入新興科技，如生物特徵或錄影作為電子簽章的方式。
4. 客戶最常用服務是表單式的填寫（如修改地址、帳戶等），此類作業大多仍為紙本加蓋章（簽章）作業。

建言作法

1. 建立電子簽章應用的法定基礎。未來金融管理規範建議納入ISO 29115、歐盟eIDAS 、以及澳洲《Trusted Digital Identity Framework Accreditation Rule》為框架，同時考慮新興科技技術及資安為藍本。
2. 新的電子簽章應包括既有《數位簽章》及《其他生物科技類》新興科技類技術之新興電子簽章技術。
3. 探討利用行動自然人憑證作為消費者簽署線上文件時的可能性與適法性。
4. 可以參考歐盟eIDAS規範，評做利用電子憑證做為eID、eSignature和eSeal作法。

研究議題：法人數位身分

痛點與需求說明

相對自然人，法人金融服務的場景複雜許多，行使時會有下列幾個狀況：

1. 電子化印章：在法人開戶時必須具備大小章；如：內政部自然人憑證、經濟部工商憑證為法定電子憑證信物
2. 法人網銀服務：在法人進行資金調度時，通常會使用銀行提供之憑證，作為在法人網銀時使用；如：FXML
3. 多人意思表示：在法人進行申請貸款，通常必須具備徵信資料、董事會資料...等佐證文件、以及相關關係人簽名必要文件行使意思表示的申辦文件。
4. 非接觸式開戶：在疫情的影響下，如何協助法人客戶進行非接觸式開戶服務也成為另一個需求。

建言作法

建議參照澳洲RAM之作法，發展臺灣的法人數位身分方案，並納入「金融數位金融管理規範」。

在法人數位身分議題有以下建議：

1. 電子化印章：評估利用自然人憑證與工商憑證作為線上開戶的可行性。
2. 法人網銀服務：可參照澳洲RAM之作法，評估由金融FIDO取代FXML的可能性。
3. 多人意思表示：可參照澳洲RAM之作法，整合金融FIDO，發展法人金融服務方案。
4. 非接觸式開戶：可參考生物辨識作法，提供錄影加生物辨識的解決方案。

研究議題：資料共享

痛點與需求說明

資料共享因對象不同時，共享資料類型而有差異：

1. 客戶金融資料：目前《金融機構間資料共享指引》，規範了三類資料共享對象，(1).金融控股公司、(2).非屬金融控股公司的金融集團、(3).非屬上述二類之金融機構間，資料共享對象是以金融機構為主。
2. 客戶非金融資料：在實際的金融場景應用，客戶在使用金融服務時，則需提供許多非金融產業的外部資料，包含政府或民間資來源；如：myData、醫院電子病歷與費用收據、國稅局資料、財務報告。

建言作法

依資料共享類型，提供相關建言：

1. 客戶金融資料：目前在《金融機構間資料共享指引》已開放可適度跨業進行資料交換，且因有集保結算所設置之「防制洗錢及打擊資恐查詢系統」可供金融業者進行KYC及CDD，故此部分只需再擴大適用對象與範圍、簡化客戶授權模式、開放金控建置資料庫等(可參考2022政大與勤業眾信數位金融脈動展望報告)。
2. 客戶非金融資料：未來可考量使用外部資料源(例如：myData)時，可依第三方身份驗證議題中的相關建言，整合金融機與非金融機構的身分驗證機制，透過風險等級的分類進行資料交換。
3. 未來利用API交換資料時，建議在開放銀行把TSP或跨產業合作公司角色在「金融數位金融管理規範」，確認彼此可以接受的風險等級與信賴等級，讓茲瞭可以雙向交換。
4. 未來資料共享指引能持續進行法規調整，並期待有更多跨機構、跨產業的資料共享指引頒布。

最佳實務作法：身分識別機制評估作法

金融機構在評估身分識別機制時，可以透過三個框架以及四個流程，來評估身分識別機制是否合適所需的風險等級(risk level)與信賴等級(LoA)。

- 實務作業基準框架
- 風險等級評估框架
- 信賴等級評估框架

選擇框架

✓可由主管暨監理單位召集相關單協力訂定“共同作業指引”

➢建立實務作業基準框架、風險等級評估框架以及信賴等級評估框架

界定風險

✓利用框架評估應用/服務在身分識別機制失效時之風險

➢產出應用/服務風險評估報告

評估信賴

✓利用框架盤點既有或擬新建置之分識別機制

➢產出信賴等級評估報告

確認機制

✓透過比對風險等級與信賴等級，確認身分識別機制是否適當

➢確認身分識別技術機制

- 實務作業基準(EAPS) - Entity Authentication Practice Statement
- 本身分識別機制評估方法由本案合作夥伴臺灣網路認證公司提供。

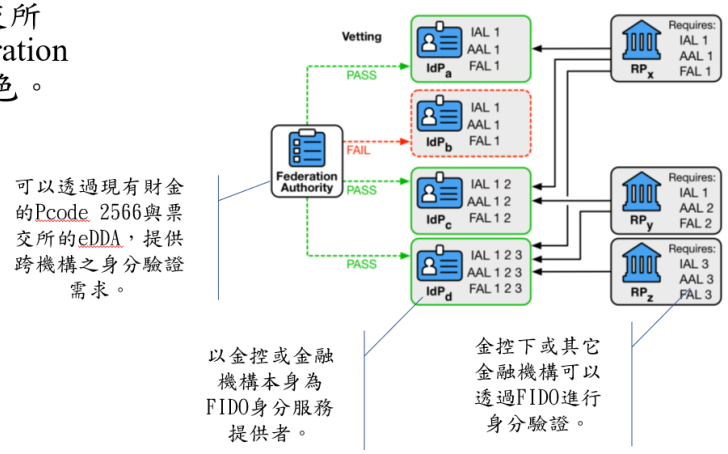
借鏡國外規範建立最佳實務作法

NIST 800-63 (跨機構)

- 說明：NIST 800-63是美國對於身分識別的相關規範。
- 應用：NIST 800-63中有考量到在現實場景中，信賴單位(relaying party)有可能必須與多個身分服業者進行身分驗證作業；因此未來在制定數位金融服務管理規範時，可以參考NIST 800-63C中的不同角色，規劃有跨機構多方參與者角色和制訂必要的責任義務與監理機制。

台灣應用NIST 800-63可能場景

- 由財金/票交所出來做federation authority角色。



eIDAS (電子簽章)

- 說明：eIDAS是歐盟以電子憑證為主的PKI數位身分架構。
- 應用：eIDAS在數位身分以及意思表示上，可以同時作為電子身分及電子簽章使用；未來在制定數位金融服務管理規範時，可參考eIDAS給數位身分與電子簽章必要的法定位階以及相關技術上的應用。

落實未來多元數位身分之行動方案

	短期	中長期
政策法規面	• 進行必要修法作業，賦予主管機關針對金融服務的監理明確法源，制定「數位金融服務管理規範」 • 規範意思表示與確認作法，針對電子簽章法與生物辨識，積極進行明確規定和必要解釋	• 依產業需求推動差異化的監理機制 • 建立金融機構與非金融機構的身分識別共通機制 • 建立跨機構身分識別爭議處理機制
產業推動面	• 各產業公會依「數位金融服務管理規範」，盤點現行法規及自律規範進行調適或廢止不適合規範，**允許個別金融機構可自行訂定內部數位金融服務信賴風險等級之應遵循辦法** • 設計評量基準，評量不同身分識別技術的風險等級與信賴等級 • 規範法人的數位身分的作業方法，建立全面數位化的金融服務	• 規範金融機構與第三方信賴單位(RP)在第三方身分驗證服務角色的權責 • 推動非金融業間跨機構的身分驗證與資料共享 • 制訂金融產業對於身分識別的標準方案(scheme)與資料共享的交換標準(API,資料格式)
業者應用面	• 釐清不同金融服務場景的風險等級，並搭配相同風險等級的身分識別機制 • 加入跨行驗證(eDDA/Pcode)機制 • 推動金融FIDO的跨行驗證，擴大應用場景	• 推動電子簽章與生物辨識的場景應用 • 推動跨產業及跨機構的資料共享場景 • 推動無紙化的線上申請與電子文件簽署應用場景

期末研究總結

1. 提出金融數位服務管理規範的修法，建立金融數位服務的管理與監理制度
2. 由各產業公會重新檢視現有相關規範，進行差異分析與法規調適，允許個別金融機構可自訂內部數位金融服務信賴風險等級之應遵循辦法
3. 盤點現有身分識別技術，界定信賴等級(LoA)，以及可適用的數位金融服務場景(包含自然人與法人應用場景)
4. 針對電子簽章與生物辨識的應用加速不同的創新應用
5. 針對金融生態系中各合作關係人（含新創業者）建立相關作業規劃與風險等級，並建立跨機構的身分驗證機制

願景目標

- 建立金融生態系中一體適用的多元數位身分機制
- 納入非金融機構的參與者
- 建立以風險分級與差異化管理的監理制度

治理/監理制度

謝謝大家
攜手共創台灣金融服務新未來!

感謝本研究團隊所有夥伴們的努力
以及所有提供建言的產業先進之協助!