財團法人台北外匯市場發展基金會

專題研究計劃

我國開放銀行發展剖析與政策建言

受託研究單位：國立政治大學產學營運暨創新育成總中心

計畫主持人：王儷玲 (國立政治大學風險管理與保險學系教授)

研 究 員：

謝煦憲 (國立政治大學金融科技中心顧問)

李桓宇 (國立政治大學金融科技中心專案經理)

黃柏堯 (國立政治大學風險管理與保險學系研究所碩士生)

中華民國一一〇年 1 月 3 日

目　錄

第一章　前言 1
第一節 計畫背景 1
第二節 計畫目的 3
第三節 計畫內容說明 5
第四節 研究方法說明 5
第二章 開放銀行發展趨勢 7
第一節 開放銀行全球發展現況 7
一、全球發展概況 7
二、開放銀行的定義與目的 11
三、API 經濟的應用 13
四、消費者賦權意識提升 19
第二節 開放銀行發展的框架 22
一、推動方式 22
二、開放銀行推動五大重點 25
第三節 各國開放銀行發展分析 28
一、英國 28
二、 歐盟 34
三、 澳洲 37
四、 香港 42
五、 新加坡 45
六、 美國 48
七、 加拿大 52
八、 日本 55
九、 中國 58

第四節 國外開放銀行案例 61
一、 帳戶類型情境 64
二、 支付類型情境 66
三、 中小企業相關情境 66
第三章 台灣開放銀行發展剖析 68
第一節 台灣開放銀行發展分析 68
第二節 台灣開放銀行法令基礎 70
第三節 台灣開放銀行業務限制 73
一、銀行篩選 TSP 限制 73
二、篩選條件的不明確 74
三、銀行僅為資料提供角色 74
四、無資料交換的應用情境 74
第四節 台灣開放銀行資安要求與問題 75
一、身份認證 78
二、第三方身份認證 78
第五節 TSP 輔導方案與說明 78
第六節 TSP 輔導問題觀察 81
第四章 國外開放金融之新金融生態系 84
第一節 新金融生態系對未來金融服務的影響 85
第二節 消費者賦權的發展與因應 89
一、國外消費者賦權法令分析 90
二、台灣個資法與開放銀行關係與問題 93
第三節 開放銀行的 TSP 管理與平台 96
一、國際各推動方式作法 96
二、台灣 API 管理平台作法 99

第五章 台灣開放銀行政策建議 101
第一節 金融科技發展路徑圖將促進開放銀行之發展 101
第二節 法令與政策層面建議 104
一、鼓勵 TSP 治理制度的建立 104
二、積極推動公開資料範圍與簡化交易確認作業 106
三、推廣資料共享至資料交換應用 108
第三節 業務推廣層面建議 110
一、成立 API 管理中心 110
二、建立一致性的驗證機制 111
三、建立合規雲端服務平台與設立合規服務提供廠商名單 111
四、推動資安保險 112
五、建立開放銀行生態系 113
第四節 技術層面建議 114
一、第三方身份認證 115
二、強化法遵與監理科技 116
第五節 總結 116
附錄. 參考資料 118

圖目錄

圖 1 全球開放銀行發展 10
圖 2 各國開放銀行發展評估 11
圖 3 Google API 收費標準 16
圖 4 API 商業模型優缺點 17
圖 5 銀行運作體系的轉變 18
圖 6 OBIE Open Banking App Store 條件選取 31
圖 7 OBIE Open Banking App Store 選取結果 32
圖 8 歐盟 TSP 申請流程 37
圖 9 香港對 API 之保護要求.....45
圖 10 香港對 API 之安全標準.....45
圖 11 新加坡 API 開放數量統計.....47
圖 12 美國金融監理架構 50
圖 13 中國開放金融市場現況 60
圖 14 「開放 API」業務推動進程.....69
圖 15 台灣開放銀行推動架構 70
圖 16 業務安全控管作業規範 75
圖 17 第二階段 open API 技術與資安規範 76
圖 18 台灣 TSP 合規範圍 79
圖 19 台灣 TSP 合規項目 80
圖 20 台灣 TSP 技術/資訊驗證 81
圖 21 平台經濟模式 88
圖 22 個資法適法性架構 95
圖 23 金融科技發展路徑圖 102
圖 24 金融科技發展路徑圖推動策略 103

圖 25 基於風險管理基的 TSP 業者分級制度 106
圖 26 TSP 資安保險類別 112
圖 27 開放銀行生態系 TSP 合作與監管示意 114

表目錄

表 1「開放 API 平台」第一階段 TSP 業者.....2
表 2 英國開放銀行法源與做法.....28
表 3 歐盟開放銀行法源與做法.....34
表 4 澳洲開放銀行法源與做法.....39
表 5 澳洲 API 開放種類.....40
表 6 香港開放銀行法源與做法.....43
表 7 新加坡開放銀行法源與做法.....46
表 8 美國開放銀行法源與做法.....48
表 9 加拿大開放銀行法源與做法.....53
表 10 日本開放銀行法源與做法.....56
表 11 中國開放銀行法源與做法.....59
表 12 台灣銀行與 TSP 業者合作之建議審查資料與文件..73
表 13 新金融服務發展進度.....85

第一章 前言

第一節 計畫背景

我國開放銀行在 2019 年正式啟動。台灣開放銀行的起源為金融監督管理委員會(以下稱金管會)促使國內金融產業持續朝數位化趨勢邁進，接軌國際，順應全球金融生態的潮流，推動「開放 API」標準，建構平衡金融創新與客戶保護的「開放銀行」推動框架。為推動此框架，金管會參酌國際經驗與作法責成銀行公會、財金公司以及各家銀行於 2019 年 3 月成立 Open API 委員會，由 Open API 委員會制定相關標準，並規劃相關發展時程。

初期台灣開放銀行的架構是參考英國開放銀行的相關作法，但在實際推動上是採香港與新加坡的漸進模式，分階段推動「開放銀行」。在財金公司的規劃上，第一階段是，銀行自願自律開放「公開資料查詢」，第二階段為「消費者資訊查詢」、第三階段為「交易面資訊」。此外，按照香港模式的邏輯，銀行係與第三方服務業者(Third-Party Service Provider, TSP；以下稱 TSP 業者或 TSP)業者跨業合作，因此發生消費者爭議問題是先找銀行負責，銀行先補償消費者後，銀行再與第三方服務提供業者釐清責任並分擔相關費用。

在實際政策的推動上，金管會指示銀行公會負責研議開放範圍，以及銀行與第三方服務業者合作的自律規範內容。而財金公司則負責制定 Open API 共通標準，包括技術標準與資安標準。另外，政治大學國際產學聯盟也參與負責審閱財金公司提出的技術標準與資安標準，以及彙整 TSP 業者的意見。[1]

1 新聞來源：https：//www.ithome.com.tw/news/133650

財金公司建置的 Open API 平台已於 2019 年 10 月 14 日正式啟用，也代表第一階段的「公開資料查詢 API」正式上線。根據財金公司 API 平台正式啟用新聞稿中指出，第一批上架 API 的銀行多達 23 家[2]，包括大型民營銀行、公股銀行、外商銀行在臺子行，甚至還有規模較小的農業金融機構等都搶先布局。第一批參與的 TSP 業者則有 6 家如下表 1，已開始介接使用。[3]

表 1「開放 API 平台」第一階段 TSP 業者[4]

第三方服務業者	提供服務	合作金融機構
麻布記帳 (MoneyBook)	提供金融商品比較(台外幣存款利率、匯率等)。	台銀、土銀、合庫、一銀、華銀、彰銀、上海、富邦、國泰、高銀、兆豐、全國農金、台中商銀、新光、板信、元大、永豐、玉山、凱基、台新。
實貸比較網 (AlphaLoan)	信貸模擬試算，提供最適銀行信貸方案。	國泰世華
CWMoney	提供金融商品比較(台外幣存款利率、匯率等)、依資產狀況推介金融產品線上數位申辦(貸款商品、信用卡)。	凱基
員工福利整合平台(STAYFUN)	提供即時匯率查詢與換匯操作	富邦
保單管家/ 保險小存摺	提供保單管家 APP 試算保險產品價格、透過保險小存摺 APP 繳交保費，適時推薦適合之繳保費信用卡資訊。	元大
發票存摺	掃描發票時，辨識店家並推介優惠信用卡。	星展

2 「開放 API 平台第一階段『公開資料查詢』」上線金融機構(依銀行代號排序)：台灣銀行、土地銀行、合作金庫銀行、第一銀行、華南銀行、彰化銀行、上海商銀、富邦銀行、國泰世華銀行、高雄銀行、兆豐銀行、全國農業金庫、台中商銀、新光銀行、陽信銀行、板信商銀、聯邦銀行、元大銀行、永豐銀行、玉山銀行、凱基銀行、星展銀行、台新銀行計 23 家。

3 財金公司新聞稿：
https：//www.fisc.com.tw/TC/News/Detail.aspx?PKey=23accc58-b517-42cb-875a-f9891a5526fc

4 財金公司新聞稿：
https：//www.fisc.com.tw/TC/News/Detail.aspx?PKey=23accc58-b517-42cb-875a-f9891a5526fc

然而，邁向第二階段，主管機關將面臨更大壓力，「消費者資訊查詢」功能涉及民眾個資、資安問題，要以什麼標準來挑選 TSP 業者，例如需達到怎樣的資安水平才能取得消費者資訊，如果未來個資保護出問題，該找銀行還是 TSP 業者負責，責任歸屬如何區分，都是相當大的監理挑戰。因此，第二、三階段須面臨五大重點： TSP 業者管理方式、客戶權益保障、爭議處理、損害賠償機制及資訊安全標準。[5]

在第一階段啟動後，第二階段在 Open API 委員會的推動下，也於 2019 年 12 月 26 日完成相關技術標準與資安標準，並於 2020 年 1 月送金管會核備，而黃天牧主委也特別指出開放銀行第二階段將於 2020 年 11 月啟動。[6]

第二節 計畫目的

雖然開放銀行第一階段已經啟動，且第二階段已在 2020 年 6 月通過審查，但政治大學金融科技中心在彙整 TSP 相關意見以及觀察 TSP 與銀行的合作情境後，發現在政策雖有完整的介接與資安相關規劃，但仍欠缺對 TSP 更完善的配套措施情況，因此開放銀行面臨到幾個主要問題。

首先，銀行與 TSP 合作的自律規範法源基礎與銀行委外管理辦法相似，在銀行的高度資安要求下，TSP 的進入門檻與成本相對地高，銀行能合作的 TSP 業者相對少，也就無法達到金融科技的普惠金融目的。其次，在現行已開放的 API 範圍中，銀行與 TSP 的合作情境，僅限於在現有消費者已開戶銀行的相關延伸性服務，對於新申辦業務

5 參見註腳 1

6 新聞來源：https：//www.ithome.com.tw/news/137863

仍需透過銀行端的申辦作業，消費者無法透過 TSP 端使用 API 進行相關申辦業務，欠缺以開放銀行利用 API 的跨業合作情景。最後，國外開放銀行的最終目標都是服務消費者，並期望透過消費者的同意將消費者資料可以公開交換，得到更多更優質的金融服務；但台灣開放銀行在消費者賦權以及資料交換上這塊應用規劃的並不多，消費者感覺不到開放銀行的好處，因此在開放銀行推廣上相對不易。

政治大學金融科技中心認為開放銀行的目的為利用創新科技改善金融服務，並帶來下列幾點的科技創新：

1. 開放銀行可提供整合平台貼近消費者需求
2. 透過開放銀行共享數據有利改善消費者體驗
3. 利用人工智慧增加金融大數據價值

因此，開放銀行可以透過共享數據加速銀行與第三方服務業者的合作，利用共享數據和創新技術提供客戶更加多元的產品和服務。在開放銀行金融數據共享下，銀行與金融科技公司由競爭轉為合作，形成互利共榮的金融生態圈。所以，本專題研究報告期望達成二個目的：

1. 分析台灣開放銀行的現況：

   針對台灣開放銀行現況的探析，第一，先透過國外開放銀行在法令架構、參與業者、開放程度、技術規範等不同構面來探討開放銀行最近發展之因素。第二，透過政治大學金融科技研究中心輔導 TSP 在第二階段進行的相關觀察，將目前台灣開放銀行在推動上碰到的各個問題與狀況進行彙整。

2. 提出台灣未來開放銀行的建言：

   國外目前發展已從開放銀行發展至開放金融，透過國外發展的採討，了解國外對於開放銀行的配套措施，進而比較台灣現行開放銀行發展與國外發展的差異，並找出缺乏的驅動因素以及可以作

為未來政策改善的參考。其次，針對上述問題與發展，針對台灣開放銀行下個階段的政策與作法，提出相關剖析與建言。

第三節 計畫內容說明

本報告共分為五個章節報告，第一章節先介紹台灣開放銀行發展的現況，並針對本報告的研究背景、目的與方法進行說明。其次，本報告的目的雖然是在剖析台灣開放銀行現況，但國外開放銀行也仍在持續發展，因此第二章介紹國際上開放銀行的發展趨勢，並透過開放銀行發展的框架，來分析不同國家在開放銀行的進展，進而進行比較分析。第三章則彙整台灣目前的發展狀況並分析其問題與挑戰，其中介紹台灣開放銀行的發展進程、相關組織、法令以及執行現況。

第四章會針對開放銀行未來的發展與影響進行說明，並分析在第三章所提之台灣開放銀行問題做為案例進行分析。第五章將依據上述分析與國外經驗，提供台灣開放銀行法令、技術、政策上的建言。

第四節 研究方法說明

本報告主要採用的研究方法為質性研究的資料分析法與行動研究法。資料分析法以透過收集初級報告與次級資料進行分析，初級資料為各國開放銀行主管機關所發布之相關規範以及研究報告，如英國金融行為監理總署(Financial Conduct Authority, FCA)、歐洲銀行業管理局(European Banking Authority, EBA)、香港金融管理局(Hong Kong Monetary Authority, HKMA)等各主管機關規範與報告；而次級資料如四大會計師事務所或專業顧問公司如 Accenture 的相關報告。除探討各國的制度以及推動模式，本文也會從 TSP 角度出發，研究國外究竟有哪些類型的 TSP 加入開放銀行，而這些由 TSP 提供的新金融服務

又將如何重塑金融體系，進一步和銀行共同創造新金融生態圈。

行動研究法是研究和行動結合的一種研究方法；即情境的參與者基於解決實際問題的需要，與專家、學者或組織中的成員共同合作，將問題發展成研究主題，進行有系統的研究，講求實際問題之解決的一種研究方法。[7]在本報告中，政治大學金融科技中心為此情境的參與者，負責台灣開放銀行的 TSP 輔導角色，而針對目前台灣開放銀行的研究，則透過政治大學的專家學者進行相關研究如下：

- 彭金隆老師—開放銀行(Open Banking)實施在我國個人資料保護法令之限制與解套研究
- 臧正運老師—開放銀行下的第三方服務提供者治理機制研究— 借鏡澳洲的『消費者資料權(法)』制度
- 宋皇志老師—開放銀行個資保護與侵權責任的研究

透過專家學者的研究，針對台灣銀行的法令與治理進行問題探析與提出相關建議。

[7] 陳伯璋（1998）。教育研究方法新取向：質的研究方法，南宏圖書有限公司。

第二章 開放銀行發展趨勢

第一節 開放銀行全球發展現況

一、全球發展概況

開放銀行是近一兩年各國政府重點發展的金融政策，希望透過資料開放來創造更多金融創新的機會，同時也讓消費者能夠享受到更好的體驗。根據 Allied Market Research 在 2020 年發表的報告，2018 年全球開放銀行市場規模為 72.95 億美元，預計到 2026 年將達到 431.52 億美元，從 2019 年到 2026 年的複合年增長率為 24.4%[8]。目前全球開放銀行發展較成熟的國家包括歐盟、英國、澳洲、香港以及新加坡等等，其中又以美國的發展最為快速，原因在於美國的法規體系過於複雜和分散，因此美國監管機構選擇採用不具約束力的準則來推動開放銀行，例如美國消費者金融保護局(Consumer Financial Protection Bureau, CFPB)於 2017 年頒布的《消費者保護原則：消費者授權的金融數據共享和匯總》，至於實際的運作方式則交由市場上的銀行以及 TSP 自行決定，這樣的運作方式讓美國能夠迅速推動開放銀行[9]。另外，根據 The Financial Brand 的報導分析，也指出 API 在資料交換會取代原有的螢幕截取(screen scraping)功能，因為螢幕截取方式不但不安全，也容易將個資外洩。[10]在 Allied Market Research 研究中認為，2018 年開放銀行的市場商機有超過三分之二來自美國，然而未來成

[8] https ： //www.globenewswire.com/news-release/2020/04/13/2015104/0/en/Open-Banking-Market-Size-to-Reach-43-15-Billion-by-2026-at-24-4-CAGR.html

[9] Developments in Open Banking and APIs： Where Does the U.S. Stand?

[10] https：//thefinancialbrand.com/102918/u-s-financial-institutions-now-lead-in-open-banking-api-token-mobile-app-screen-scrape/

長最快速的地區則是歐洲[11]。

歐洲開放銀行的概念最早出現於歐盟在 2015 年 10 月通過的《支付服務指令修正案》([Revised] Payment Services Directive 2, PSD2)，PSD2 的主要目的在於統合歐盟內部的電子支付市場，透過制定共同規範來讓歐盟內部各國間的支付規格化，提供歐盟範圍內無縫支付服務。PSD2 提出幾項變革，包括強化資安要求、落實消費者保護等等，而其中最重要的一項為：允許第三方支付服務提供者(Third Party Provider， TPP)[12]加入金融市場，同意 TPP 可以使用消費者的銀行帳戶資料，提供帳戶資訊服務，同時也可以進一步發動支付指令，在消費者同意之下直接對消費者銀行帳戶進行扣款支付。在這一條規範之下，銀行必須將資料開放給第三方使用，PSD2 也因此成為開放銀行發展最早的一步，但是在歐盟的 PSD2 中並未使用開放銀行這個詞彙。

受到歐盟 PSD2 政策的影響，英國在 2016 年提出開放銀行的相關規劃，根據英國競爭暨市場管理局(Competition and Markets Authority, CMA)曾針對市場進行調查，發現英國的傳統大型銀行徹底壟斷市場，而且客戶黏著度極高，使得這些大銀行不必做出太多創新與競爭，即可維持現有的市占率，進而導致挑戰者銀行(challenger bank)無法打入市場，而開放銀行即是 CMA 所提出的解決方案之一。根據 CMD 2016 年公布的調查報告[13]中指出，英國四大銀行匯豐(HSBC)、巴克萊(Barclays)、駿懋(Lloyds)及蘇格蘭皇家(RBS)部份業務之市佔率高達 8~9 成，其中個人活存(77%)、企業活存(85%)及企業貸款(90%)；

[11] https：//www.alliedmarketresearch.com/library-access

[12] 根據 PSD 對於「支付服務」定義，第七款「透過電信、數位或 IT 設備接收支付服務使用者的指示執行支付交易，而支付的進行也是透過電信或 IT 系統或網路營運人，而且只是擔任服務使用者與商品或服務提供人的中間媒介。」

[13] CMD - Retail Banking Market Investigation, https ： //www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk.

中小企業對往來銀行之轉換率偏低(約 4%)。

英國開放銀行的目的是期望透過大型銀行與歐盟 PSD2 中的 TPP 業者合作，加速英國銀行的創新能量，進而提昇英國銀行的競爭力。自從 2017 年英國宣布推行開放銀行計畫之後，截至 2020 年 5 月為止，累計共有 175 間 TSP 業者加入開放銀行體系，為市場注入強大的創新能量[14]。

除了上述的美國、歐盟以及英國之外，東亞地區的香港、新加坡也是開放銀行發展的領先族群，皆已建立起完整的開放銀行基礎架構。而台灣、印度、日本、紐西蘭、加拿大、澳洲以及南美洲、非洲等國的發展進程則相對較晚，大多處於研擬規範和建立配套的階段。全球各國開放銀行發展大致如下圖 1 所示。

[14] https：//www.openbanking.org.uk/insights/



圖 1 全球開放銀行發展[15]

而 Capgemini & BNP Paribas《World Payment Report 2018》在 2018 年針對各國市場，依照競爭程度、監理環境、支付系統、銀行和第三方業者之間的資料共享程度等等，來判斷各國是否具備發展開放銀行的市場條件。如下圖 2 所示，該報告將推行開放銀行的國家分為領先者、跟隨者以及保守者，領先者國家包括美國、德國、新加坡，以及目前開放銀行發展最成熟的英國。[16]

[15] Deutsche Bank (2018), Unlocking opportunities in the API economy, p.15.
[16] Capgemini & BNP Paribas,《World Payment Report 2018》.

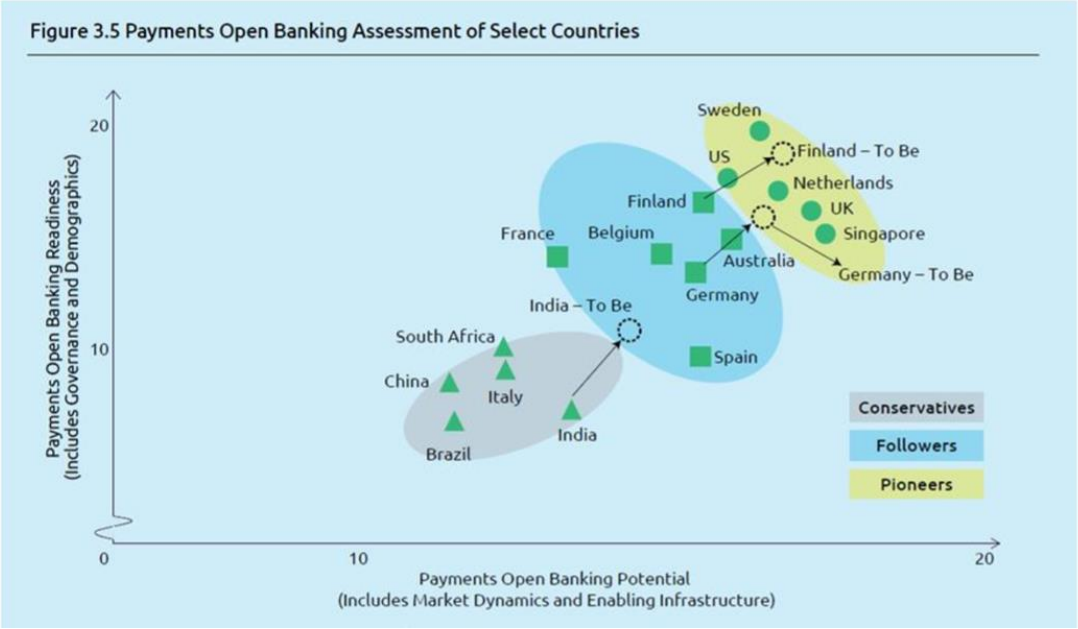


圖 2 各國開放銀行發展評估[17]

開放銀行是一股全球性的變化，各國政府以及專業機構皆積極研究，多數對於未來保有樂觀態度，認為開放銀行可以加速金融創新並建立新形態的生態圈。

二、開放銀行的定義與目的

雖然開放銀行的概念最早出現於歐盟發布的 PSD2，但第一個提出開放銀行(Open Banking)這詞彙的則是英國 CMA，開放銀行在此是作為一種政策般的存在，是為了提升英國銀行競爭力和為英國金融業注入創新能量而存在。而以英國的開放銀行執行組織(Open Banking Implementation Entity, OBIE)官網上對開放銀行的定義是：「開放銀行是一種讓個人與企業利用自身交易資料獲取更優化的金融商品與服務。」[18]開放銀行從原先的單一國家政策，成為世界各國金融創新不能忽視的概念，而台灣也是積極投入的國家之一。

[17] Capgemini & BNP Paribas,《World Payment Report 2018》.
[18] 英國 OBIE 網站：https：//www.openbanking.org.uk/

維基百科則依據英國提出的 Open Banking Standard 和各大顧問公司的報告整理開放銀行定義如下：[19]

開放銀行是一種金融服務詞彙，屬於金融科技的一部分，指的是：

1.使用 Open APIs，使第三方開發者可在金融機構周邊構建應用和服務。

2.為帳戶持有人從開放數據到私有數據提供更多的財務透明度選項。

3.使用開源技術實現以上目的。

開放銀行最初是英國國家金融政策，但作為金融政策，世界各國會因應自身的金融環境而有其變化。比如說資料共享為出發點的澳洲，澳洲政府金融科技諮詢委員會主席 Scott Farrell 在採訪指出，開放銀行指的是銀行的顧客(無論是個人還是企業)都可以請求或同意將其數據安全分享給經過認可的第三方 。

而我國王儷玲指出，開放銀行是指銀行透過與第三方平台合作，以開放應用程式介面 (Application Programming Interface, API)共享金融數據資料，也將金融數據的主導權還給消費者，使消費者可以獲得更多元的金融服務。因此，開放銀行是透過金融數據共享，創造新的商業模式，推動銀行和金融科技公司更深層地合作與競爭，以追求客戶利益極大化。在銀行及第三方的合作下，使金融服務生態系(ecosystem)更多元也更強大。開放銀行的好處，包括改善客戶體驗、利用 API 提供原本銀行無法提供的服務，也讓銀行服務更貼近消費者需求。[20]

由於開放銀行是透過 API 交換資料，也可以說開放銀行是金融業

[19] 維基百科 open banking 定義：https：//en.wikipedia.org/wiki/Open_banking

[20] 王儷玲，台灣發展 Open API 的機會與挑戰：http：//www.ftrc.nccu.edu.tw/wordpresseng/?p=9015

API 經濟的實踐；另外，資料交換必須在消費者同意之下進行，所以消費者賦權也是在開放銀行中必須討論的議題。本章節先就開放銀行中的 API 經濟效應與消費者賦權進行說明，再來透過開放銀行的框架針對各國開放銀行發展狀況進行說明。

三、API 經濟的應用

(一)、API 概念簡介

應用程式介面(API)是系統之間互相交換資料的技術[21]，當今這個全世界都透過網路串連的時代，API 已經成為提供數據和功能訪問的重要工具，在資料共享的應用上扮演著重要角色[22]。那麼究竟甚麼是 API 呢? 企業間又是如何透過 API 創造效益呢? 本研究並不詳細解說 API 背後的技術運作，而是透過大量範例以及模型簡介，將 API 的概念以及實務運作帶給讀者。

首先我們舉一個 ATM 的例子，透過 ATM 來比喻 API 的運作流程以及概念，並將 API 拆解成 Application、Programming 以及 Interface 個別進行說明。在日常生活中，我們會走到 ATM 的原因是希望能夠取得帳戶資訊並完成交易，而 ATM 連接的對象則包括使用者以及銀行，對兩邊資料進行比對篩選後，將我們需要的資訊送到眼前。這就是 Application，負責處理我們的指令輸入以及結果輸出，一旦接收到消費者從網頁、手機 app 發出的指令，下一步就會到背後連接的資料庫中進行搜尋，再將結果輸出。再來針對 Programming 進行說明，Programming 負責的是指令翻譯、確認以及邏輯運算，假設我們對 ATM 輸入提款 10，000 元的指令，Programming 就會將提款的指令翻

[21] Barend, G. (2019), Establishing a Durable Environment for Digital Financial Services.
[22] IBM，API 經濟的演進。英文報告網址：https：//www.ibm.com/downloads/cas/XG8RYO63

譯至銀行的資料庫，並且確認帳戶中是否有足夠餘額可供提領，在交易完成後也負責協助銀行更新帳戶餘額，確保整筆交易能夠順利完成。最後來看 Interface，其實 Interface 就是呈現出我們跟 Application 的互動方式，例如 ATM 中的鍵盤、觸控面板、發鈔口等等都屬於此[23]。

綜合以上，其實 API 的概念並不複雜，然而在技術上卻涉及點到點連接規格的差異，也因此在開放銀行中討論到 API 時，一家銀行可能跟數家 TSP 串接資訊，若每一次串接時都使用不同的規格將導致銀行的建置成本大幅提升，這也是台灣在推動開放銀行時，金管會責成財金公司來建 Open API 平台的原因之一。

(二)、API 商業模型

API 發展至今，已經有越來越多企業透過 API 與合作夥伴串接，匯集出各自的服務生態圈。舉例來說，新加坡線上房產平台 Property Guru，結合銀行房貸試算查詢系統，讓民眾可以確切的掌握貸款資訊，同時讓銀行可提早接觸到潛在客戶；或是日本瑞穗銀行結合日本軟體銀行與兩家電信業者，融合金融與電信大數據，透過 AI 計算出個人信貸分數，只要透過 App 便能輕鬆查詢並取得貸款，有效的運用跨產業數據並打開接觸客群限制。[24]透過上述兩項 API 應用可以發現，其實 API 串接其中一項重要原因在於跨業合作，例如房產平台與銀行房貸，或是銀行信貸與電信業者，都是透過資訊的交換以及服務的互補性來達成雙方獲利，創造出所謂的 API 經濟。

根據 IBM 調查，市場上將近 70%的企業都在尋求外部合作機會來增強實力，而 API 就是企業之間最重要的媒介之一，對成功的企業來說，API 不僅僅是工程師的技術工具，更具備金融科技時代下的策

[23] Upwork, The API Economy, Upwork.
[24] https：//www.gss.com.tw/eis/180-eis93/1992-eis93-7

略價值，代表著創新業務模式的潛力，能夠匯集不同功能來營造全新的客戶體驗。而 IBM 在分析市場環境後，提出三種 API 的商業模型，分別是直接消費(Direct Consumption)、市場創造 (Market Making)以及生態系賦予(Ecosystem Enablement)，以下將透過三種模型來說明企業如何透過 API 來創造經濟價值[25]。

首先介紹直接消費模式，直接消費表示企業將自家的 API 提供給其他業者串接，藉此收取使用費。例如 2020 年 3 月台灣某工程師透過 Google 地圖 API 開發出口罩地圖，然而卻在推出後收到高達兩萬六千美金的帳單，這就是 Google 提供 API 所創造的經濟價值。根據 IBM 統計，Twitter、Netflix 和 Google 等公司推出的公共 API 每天被點擊使用的次數達到 10-50 億次，若以 Google 在「路徑介面集」的收費標準來看(詳見圖 3)，表示 Google 每日可藉由提供 API 來賺取 500 萬至 1 億美元的收入。

直接消費模型的優點包括使用者可以透過低成本獲取現成資料，大幅降低 R&D 費用以及時間成本。但相對來說，該模式的 API 使用者並不會主動推廣該項 API 的服務，也不易透過此模式來吸引或激勵其他業者加入使用。

[25] IBM, Evolution of the API economy.



圖 3 Google API 收費標準[26]

再來看到第二種市場創造模型，表示企業匯集並且整合大量相關的 API，藉此將原 API 提供者的服務加值，創造全新的市場服務。最常見的例子就是 booking.com 訂房網站，透過串接各大飯店的訂房資訊，為消費者創造全新的住宿比價服務。這樣類型的企業通常透過收取佣金或服務費來獲利，類似於經紀人的角色，而開放銀行最醒目的應用之一的記帳軟體也可歸類在此模型底下。市場創造模型能夠增加業者的曝光度，例如知名度較低的飯店可以透過訂房網站推廣出去，但同時也表示加入該模式的門檻較低，市場競爭會更加激烈。

最後一個模型是生態系賦予模型，概念上類似於第一種的直接消費模型，差別在於直接消費是取用 API 後直接套上，在本質上並未改變原本 API 的功能；然而生態系賦予模型在取得 API 後，會更進一步進行包裝和整合，打造出全新的內容後再販售該服務。例如印度的新創銀行 RBL Bank，這間銀行將 API 提供給當地的資產管理公司，

[26] IBM, Evolution of the API economy.

而資產管理公司透過 RBL Bank 的支付 API 以及帳戶 API，打造出屬於該企業的「錢包」，讓客戶在該企業中的金流服務變得更順暢，甚至可以做到共同基金及時贖回的功能。這樣的模式對於 API 使用者來說可以研發出更具創意的服務，而對 RBL Bank 這種 API 提供者而言可以增加通路，然而須注意不能過度依賴合作夥伴，也必須監督合作夥伴是否有損害品牌的行為發生。

	Direct consumption	Market making	Ecosystem enablement
Strengths	Low costs due to direct-to-consumer business model High control over API branding and SLAs	Consumer ecosystem accepts even low-use consumers to achieve a critical mass for effective operations Ability to scale by leveraging multiple producers Ability to provide global footprint by leveraging "local" partners	Access to a wide ecosystem of innovative API mashup offerings Ease of global expansion for producers of digital goods Ability to scale by leveraging multiple producers Ability to provide global footprint by leveraging "local" partners
Challenges	Restricted supply chain and sales channel Lack of incentives for ecosystem partners for promoting adoption	Business viability highly dependent on market liquidity Impact on brand due to third-party SLA dependency Low barrier to entry for competitors leveraging similar capabilities	Revenue dependency on partner sales Possible impact on brand due to third-party SLA dependency Possible impact on consumer offering due to differing versions and upgrade paths of constituent producers

Source: IBM Institute for Business Value analysis.

圖 4　API 商業模型優缺點[27]

以上述三種 API 商業模式，可由例子看出開放銀行下大多數會採用生態系賦予的商業模型，由銀行透過與 TSP 的跨業合作達到建立生態系經營的目的。

(三)、開放銀行下的 API 經濟

在 API 開放之後，如圖 5 呈現，銀行的運作體系會漸漸由垂直鏈型轉為多面向的生態系， TSP 將成為銀行體系中的另一位開發者和行銷通路，而隨著銀行開放的 API 種類不同，各家銀行也將發展出

[27] IBM, Evolution of the API economy.

不同特色。根據資策會報告，全球主要開放銀行開放功能的 API 比重以帳戶資訊(32.9%)以及支付轉帳(28.7%)為最多和次多，接下來的依序是交易(18.2%)、借貸融資(7%)、分行資訊(7%)、投資(6.3%)、外匯交易(4.2%)以及保險(2.8%)。[28]資料顯示除了帳戶資訊以及支付、交易資訊之外，徵信也成為開放銀行中另一個發展的重點應用，而證券、保險等應用則仍待發展。

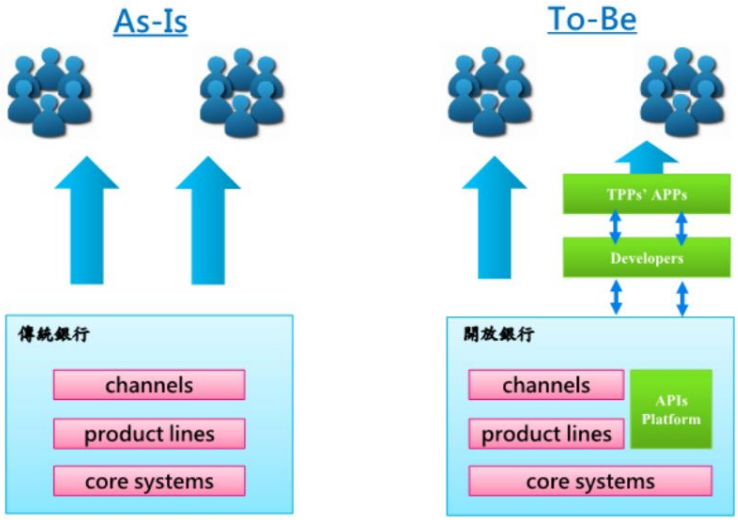


圖 5 銀行運作體系的轉變[29]

除了銀行本身模式會逐漸改變之外，歐洲銀行業管理局(EBA)認為在開放銀行的體系下，市場最終會產生所謂的「平台」模式[30]。平台的概念是從零售業發展而來，表示有許多服務、商品會聚集到一個匯集點，這個匯集點就是平台。在金融科技的時代，平台已不只出現在零售業、電商業的應用，更漸漸在金融業中看到平台的出現，例如 P2P 借貸平台、國際換匯(FXP2P)平台等等，都是金融科技的新產物。平台最主要的任務就是「媒合」，媒合買方與賣方、消費者與提供者，讓交易的雙方能夠在平台上找到彼此，獲取相對應的服務。在開放銀

[28] 資策會產業情報研究所(2019)，開放銀行發展簡報。
[29] 資策會，開放銀行發展趨勢與展望。
[30] EBA, Open Banking： advancing customer-centricity.

行體系下，由於 API 的開放與串接，會使得許多相關服務集中到某一個平台上，如此一來該平台就能夠蒐集更多消費者的資訊，提供更多客製化的金融服務，消費者也能夠享受到一站式的服務網，獲得更佳的消費者體驗。舉例來說，記帳業者最初只是匯集各家銀行帳戶資訊，讓消費者能夠在同一個入口或 APP 管理所有的銀行帳戶資訊，然而記帳業者或許也可以根據帳戶金流來判斷消費者習慣，為消費者提出改善方案；或是根據消費者需求，搭配各家銀行的商品資訊，成為消費者的財富顧問。在這個模式下，所有和帳戶有關的金融服務全部匯集到記帳業者，形成一站式的平台模式，這也是開放銀行下 API 經濟的另一種樣貌。

四、消費者賦權意識提升

歐盟在 2015 年通過的 PSD2 中規定，將過去被銀行視為重要資產的客戶資料分享給非銀行的第三方存取，包括消費者的帳戶資料、歷史交易資料，及銀行產品、服務等資訊。因應 PSD2 規定，歐盟各國必須將 PSD2 納入各國法規中，成為歐盟開放銀行的立法基礎，讓歐盟居民對於自己的資料，享有更大的自主權。由此可見「客戶資料共享」是開放銀行的核心，也是啟動金融創新的引擎，而這中間的主要概念就是消費者賦權。

消費者賦權是一種抽象的概念，通常伴隨著實際的行動而生，表示消費者在市場上和其他對象互動時，能夠依照自己的需求來進行決策，從而實現自己的選擇[31]。消費者賦權的意識在近年來不斷提升，其中一種消費者賦權的權利實踐為資料可攜權，意為消費者可以依照個人的意願來掌握自己的資料，而不必受到其他限制。舉例來說，在

[31] IGI Global, https：//www.igi-global.com/dictionary/consumer-empowerment/40673

台灣就職時常常需要繳交信用報告，現行流程是消費者必須到聯徵中心申請辦理，拿到信用報告後再轉交給公司。但是在資料可攜權的概念下，信用報告的資料應該屬於消費者的個人資料，消費者有權利決定要將自己的資料移轉、交付給誰，在這個狀況下消費者就能夠在授權的情況下，請聯徵中心直接將信用報告轉交給就職公司。這就是資料可攜權的概念，也是消費者賦權的實現，在開放銀行中是非常重要的權利。目前已有部分國家透過立法來保障消費者的資料可攜權，例如歐盟的「一般資料保護規範」(General Data Protection Regulation, GDPR)以及澳洲的「消費者資料權法」(Consumer Data Right, CDR)。

GDPR 是歐盟在 2016 年 5 月 24 日發布的資料保護規則，並在 2018 年 5 月 25 日正式實施。根據 GDPR 第一條，對於資料保護與運用之規定，個人資料保護不應該缺乏彈性，必須考慮到個資在社會上的作用，並且在符合比例原則的前提下，兼顧其他基本權利，在個資保護和基本權利之間取得平衡[32]。接著在第二十條的條文中載明資料主體(通常表示消費者)具有權利，透過有結構的、普遍使用的、機器可讀的形式，接收自己提供給資料控制者(從開放銀行角度出發，此處的資料控制者可想像為銀行)的資料，並且有權利將這些資料移轉給其他對象，而不需經資料控制者同意[33]。在上列的條文當中，可理解 GDPR 賦予消費者所謂的「資料可攜權」，載明消費者具有取得以及移轉個人資料的權利。GDPR 從個人資料權利的角度出發，不只新增了個人的基本權利，更同步解釋 PSD2 中關於銀行必須將資料開放給第三方使用的規定，這也讓 GDPR 以及 PSD2 成為歐盟發展開放銀行

[32] GDPR 第一條第一項，https：//gdpr-info.eu/art-1-gdpr/
[33] GDPR 第二十條，https：//gdpr-info.eu/art-20-gdpr/

的兩大法源依據。

除了歐盟之外，澳洲是另一個透過立法來實現消費者賦權的國家，在 2020 年 2 月 5 日澳洲的 CDR 正式生效[34]。CDR 在本次的內容中制定了三大規則，分別是產品資訊請求、消費者資料請求，以及由他人代表消費者進行的資料請求，其中第二項和第三項規則就是消費者對於資料賦權的實現，規則中寫說消費者能夠直接向資料擁有者索取 CDR 中規定可索取的資料，而且不只是消費者本人具有資料請求的權利，如果是消費者授權的第三人，一樣有資格可以向資料擁有者索取消費者資料[35]。

不論是歐盟的 GDPR 還是澳洲的 CDR，都明文規定消費者的資料可攜權，而在開放銀行下，最根本的概念就是將消費者的資料從銀行透過 API 串接給 TSP，明顯涉及到消費者資料移轉的情境，也因此實施開放銀行其實就是在實現資料可攜權，讓消費者的資料能夠在銀行以及 TSP 之間順暢的移轉。

但可惜的是，目前台灣的法律不能衍生出資料可攜權的權利概念，依照現行的條文，難以辨明個資的所有權人，也無法釐清經整理、分析過的個人資料歸屬於何人，更沒有法源依據來規範資料交換。鑒於以上問題，現階段台灣尚無法達成消費者賦權，未來或許可以研擬修訂個資法、消費者保護法以及其他相關金融法規，開放消費者數據可跨業使用，體現消費者賦權的實質作用。

[34] 評析澳大利亞《消費者數據權利規則》及對我國立法與產業的啟發，http：//pkulaw.cn/fulltext_form.aspx?Db=lawfirmarticles&Gid=801176401a6b24e205b3b43963cb1057bdfb&keyword=&EncodingName=big5&Search_Mode=accurate&Search_IsTitle=0

[35] ACCC, Competition and Consumer (Consumer Data Right) Rules 2020.

第二節 開放銀行發展框架

一、推動方式

開放銀行牽涉到的議題相當廣泛，包括 API 介接、資安標準、監理強度、責任歸屬機制、身分驗證、TSP 權限等等，同時也橫跨多項產業，例如金融業、電信業、信評機構以及各式各樣的 TSP 業者，由此可見開放銀行對於金融體系的影響力之巨大。著眼於開放銀行帶來的強大創新動能，未來或許不只開放銀行，例如英國 FCA 在 2019 年底就發表《Call for Input： Open Finance》，該報告中提出了開放金融的概念，也就是將開放銀行拓展至開放保險、開放證券，將所有和金融服務有關的產業都納入，構築一個新形態的金融生態圈。

由上述可見，開放銀行的潛力、影響力皆非常巨大，綜觀各國的開放銀行發展，僅有少數國家是由市場驅動，透過自由競爭漸漸發展出開放銀行體系，例如美國、中國。其他多數國家則是由主管機關作為發動主體來推動開放銀行發展，其中又可分為政策鼓勵以及法令強制兩種不同的推動方式。以下將分述本段中提到的市場驅動(market driven)、政策鼓勵(regulatory encouraged)以及法令強制(regulatory mandatory)三種不同的推動方式，以及其代表國家。[36]

本研究整理目前各國開放銀行政策推行方式差異之比較表如下表 2，另針對三種政策推動方式的作法差異將於本節後半段進行說明。而目前全球幾大開放銀行代表國家之監理規範、API 開放範圍、產業、參與者、資安標準等細節則會於下一節做更詳細的說明。

[36] BIAN (2020) ,Global Open Banking Initiatives and the added value of the BIAN Open Standards,https：//bian.org/participate/bian-webinars/global-open-banking-initiatives-added-value-bian-open-standards/

表 2 各國開放銀行發展模式比較表

推動模式	法令強制	政策鼓勵	市場驅動
國家	英國 歐盟 澳洲 加拿大 日本	香港 新加坡	美國 中國
優點	● 有相關法令規範可強制推動政策 ● 提供必要註冊機制立認證規範 ● 鼓勵 TSP 業者加入此生態系	● 大多以週邊單位推動，執行較有彈性 ● 規格可以依該地區想推動的場景來設計	● 彈性最大，依市場需求可以設計各種不同情境應用
缺點	● 無法針對市場快速推出必要的 API，僅針對共通項目規範	● 因採自願性質，規模大的金融機構有資源整合，而中小型金融機構較不易，會有市場競爭不平狀況	● 因為市場推動，l初期推動速度會較快；但後期可能會有多家規格競爭，整合不易

(一)、市場驅動

市場驅動表示市場上銀行、科技業者、金融科技業者或是其他產業的 TSP 等參與者互相主動尋求合作，開放 API 給合作夥伴，目的是為了產品以及服務的創新，並塑造與同行之間的差異，以便取得市場上的競爭優勢，代表國家為美國、中國以及奈及利亞。

以美國為例，美國各州之間有獨立運作的州法，再加上高度自由的市場環境，導致由中央統一推動開放銀行政策並不容易。美國最終的做法是 CFPB 在 2017 年頒布《消費者保護原則：消費者授權的金融數據共享和匯總》(Consumer Protection Principles： Consumer-authorized financial data sharing and aggregation)，做為市場上進行開放銀行合作的參考，展上會相對多元化，一方面是受到較少的政府限制，大多是由產業公會間自行至於實際運行方式則交由市場自由決定。

一般來說，採用市場驅動模式的國家，在商品發規範；另一方面則是因為參與者是自願參與，積極性較高也更容易激盪出多元的創新

火花。

(二)、政策鼓勵

政策鼓勵是指主管機關提出開放銀行的相關政策，形式可能為指導原則或白皮書，提供交換方式的建議或鼓勵金融業者主動開放 API，目的是為了加強跨業合作、鼓勵市場創新，進而達到金融創新的目的，代表國家如香港、紐西蘭以及東南亞國協的多數國家。

以香港為例，金管局在 2018 年 7 月發表了《Open API Framework for the Hong Kong Banking Sector》，內容包括四階段的 API 開放以及種類，但卻不強制銀行參與，由業者自行評估決定[37]。而新加坡也是類似的作法，在 2017 年提出《ABS-MAS Financial World： Finance-as-a-Service API Playbook》。由於台灣採取借鏡香港的作法，因此台灣的開放銀行也是屬於在這個類別之中。

(三)、法令強制

開放的目的是為了促進市場競爭以及鼓勵創新，或是為了實現消費者對個人資料的權利，例如歐盟的 PSD2、GDPR 以及澳洲的 CDR。

對銀行來說，法令強制的方式在初期或許對銀行造成巨大負擔和壓力，但主管機關通常會設計出更完整的配套措施，例如開放銀行制度設計、TSP 的資安規範、紛爭解決機制等等，藉由對 TSP 以及整體進行高度的品質管制，讓銀行和 TSP 之間的合作可以更加安全與穩定。

在這樣高度監管的環境下，產品的多元性會受到比較多的限制，例如主管機關可能會規定 API 開放的種類、時程、規格等等，但也因

[37] https ： //www2.deloitte.com/cy/en/pages/financial-services/articles/open-banking-around-the-world.html

為具有較完整的法源依據以及配套措施，會讓開放銀行的發展更加的穩固。

二、開放銀行框架項目說明

本研究在第二章第三節以及第三章第一節將分別介紹各國開放銀行發展，以及台灣開放銀行發展。內容除了簡介主管機關具體推動方式之外，會更進一步分析各國推動開放銀行的五大重點：開放的產業、API 開放範圍、參與者類別、資安標準以及監理規範，並進行各國發展的比較。以下先就這五項觀察重點進行說明。

(一)、監理規範

在研究開放銀行時，第一步必須先釐清主管機關是誰，因為主管機關的角色將會影響到該國開放銀行的發展方向以及推行的方式，例如修法與否，或是由業者制定自律規範即可，以及是否規定市場上的銀行都必須強制開放，這些都取決於主管機關的角色及看法。再來必須瞭解到該國的法源依據為何，這將決定開放銀行推行後各個參與者的權利義務以及運作方式。透過主管機關以及法源，就能夠大致上描繪出該國的開放銀行輪廓，才能夠進行更深入的分析與討論。

(二)、API 開放範圍

API 開放表示銀行將資料透過 API 提供給 TSP 串接，同時也賦予消費者行使個人資料的管控權，此為建立開放銀行金融生態系最關鍵的環節，讓平台之間的數據和服務可以重新組合，創造新的商業模式與價值，間接促成更強大的金融服務生態系[38]。因此，API 的開放

[38] http：//openbanking.org.tw/origin

範圍就決定了 TSP 可運用的資料種類，當 TSP 能夠串接越多 API，那他們就能夠整合更多的金融服務，為消費者提供更多元的創新內容。以新加坡為例，金融管理局(Monetary Authority of Singapore, MAS)和銀行公會(ABS)於 2016 年頒布《ABS-MAS Financial World： Financial As a Service API Playbook》詳細制定 API 的發展策略[39]。截至 2019 年底，新加坡共有 238 支交易功能的 API 以及 279 支資訊功能的 API 在金融市場上開放。

(三)、開放的產業

涉及產業可以大致上表示各國目前的發展階段，絕大多數的國家目前開放的產業只有銀行業，但有些國家已經將開放銀行的概念延伸至其他產業，例如英國和中國除了開放銀行之外，市場上也已經出現了開放保險的跡象，也就是保險業將 API 公開讓其他業者串接；另外澳洲也是比較特別的國家，由於澳洲發展開放銀行的法源為 CDR，其中規定消費者能夠將資料分享給他們授權的第三方業者，這樣的方式使得澳洲的開放銀行開放的產業較廣泛，包括能源業、電信業以及其他產業，都屬於澳洲開放銀行體系中的產業。

(四)、參與者類別

各國對於開放銀行架構中參與者的定義不同，將影響到參與者的資格與範圍。舉例來說，英國規定的參與者主體為銀行以及 TPP(等同台灣的 TSP)[40]，其中又指定 TPP 必須為帳戶資訊服務提供者(Account Information Service Provider, AISP)以及支付服務發起者(Payment

[39] https：//ec.ltn.com.tw/article/breakingnews/2812657

[40] 英國的 TPP 全名為 Third Party Provider，等同台灣開放銀行中的第三方服務業者 Third-party Service Provider, TSP。英國開放銀行中的 TSP 全名另外為 Technical Service Provider，為提供開放銀行資訊建置服務的廠商。

Initiation Service Provider, PISP)；而澳洲則是將參加者規定為資料擁有者(Data Holders)以及資料接收者(Data Recipients)。從這兩國對參與者的規定即可發現，澳洲對參與者的認定範圍更大，表示任何種類的業者都可以和銀行合作，相反的英國 TSP 則以資訊或支付公司為主，範圍明顯較小。

(五)、資安標準

資安問題是各國主管機關在推動開放銀行時都面臨的考驗，畢竟 TSP 並不屬於銀行業，在資安規範上或許不如銀行業嚴謹，例如銀行業需要對客戶做 KYC、AML，還有其他高強度的防駭環境等等。這些高度的資安標準對 TSP 來說，若比照辦理，可能會造成 TSP 的進入門檻太高；將門檻稍微降低，讓更多的 TSP 能夠加入，才能創造出更多元的金融生態。各國主管機關對此都嚴陣以待，深怕開放銀行反而對消費者個資產生不利影響，也因此本研究將針對各國所採用的資安標準進行整理，以供參考。

資安標準的作法一般可分為二種：第一為透過共用的規範，第二為由資訊業者提供相關資安標準。在共用規範上，可以為主管機關立法或制訂之資訊安全規範，例如以歐盟來說為 PSD2 的法定技術規範(Regulatory Technical Standards, RTS) [41]，以英國來說為 OBIE 提供的開放者標準(developer standards)。第二種較像美國的作法，是由資訊廠商設計相關規範後大家共同採用。

[41] https：//eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX：32018R0389&from=EN

第三節 各國開放銀行發展分析

一、英國

英國的開放銀行發展起源於 2016 年 CMA 對市場的調查報告，報告中發現市場遭到大型銀行壟斷，且客戶轉換度極低，銀行不需要做太多創新和品質提升，就可以穩穩地維持市占率。由於市場上缺乏競爭意識，挑戰者銀行亦無法輕易進入金融業，因此 CMA 在 2017 年提出一份行政命令(Order)，該命令要求英國市場上排名前九大銀行必須以安全且標準的形式將 API 開放給 TSP 串接，而其他銀行則不強制要求開放，這就是英國將開放銀行落地的開端，關於英國開放銀行法源與做法整理如下表。

表 3 英國開放銀行法源與做法[42]

(1) 法律依據	2017 支付服務案(Payment Services Regulations 2017, PSRs 2017)
(2) 主管機關	英國金融行為監理總署(Financial Conduct Authority, FCA)為 PSRs 2017 規定之主要監理機關，並以英國支付系統監理機構(Payment Systems Regulator, PSR)負責支付相關的監理。
(3) 具體作法	2017 年，英國競爭及市場管理局(Competition and Markets Authority, CMA) 發布了「零售銀行市場調查指令」(The Retail Banking Market Investigation Order 2017)，成為開放銀行的執行依據。另外，英國財政部也著手推動將 PSD2 寫入法規，並在 2017 年 7 月 19 日順利發布支付服務管理規定 2017(Payment Services Regulations 2017, PSRs 2017)，以英國金融行為監理總署為主要監理機關，英國支付系統監理機構則負責與支付相關的監理。 根據 CMA 的指令，英國市占率前九大的銀行及英國房屋互助協會 (下稱 CMA9)成為首波 API 開放的實施對象。另外，為了建置並維護開放銀行的 API 標準以及整體秩序，在英國競爭及市場管理局的管理下，由 CMA9 共同出資，成立了一間公司，登記名稱為 Open Banking Limited，一般將其稱為開放銀行執行組織(Open Banking Implementation Entity, OBIE)，主要的任務包括：建置 API 標準及相關資訊的規定與格式、管理及維護規定、更改及發布規定、支援用戶的使用結構及流程、處理開放銀行中應適用的條款及條件、負責開放銀行系統的指導原則，以及根據相關法律及監理規定來維護該系統，同時建立安全機制與管理架構。 上述任務的總預算為 200 萬英鎊，並於獲得 CMA9 的同意後，依照各銀行的市占率來分配出資額度。 英國除了透過強制的方式要求 CMA9 作為 API 的提供者之外，也開放第三方業者自願加入開放 API 的行列。第三方業者又根據業務種類不同，可分為支付服務發起商(Payment Initiation Service Providers,PISP)，以及帳戶資訊服務提供者(Account Information Service Providers,AISP),上述兩種業者均可透過 OBIE 的網站申請，經 FCA 審核後，待 OBIE 發行憑證即可上路。

[42] 政治大學金融科技研究中心整理

(一)、監理規範

最初的英國開放銀行的法源參考為歐盟的 PSD2，為了將 PSD2 轉納為國內法，英國於 2017 年時修正《支付服務法》(Payment Service Regulations 2017)，修正的內容包括使用帳戶之權利、第三方服務提供者及其監理方式等等。[43]

英國開放銀行的主管機關為 FCA 以及 CMA，實際執行機構則是 OBIE[44]。CMA 是 OBIE 的主管機關，2017 年 CMA 下令國內市占率前九大銀行[45]共同出資成立 OBIE，負責開放銀行相關的大部分業務，包括制定 API 標準及規範、建立安全機制以及爭端解決機制、維護管理架構等等[46]；另外，FCA 則是負責審查前來申請的 TSP 資格包括商業模式、服務細節、系統安全、資料存取以及其他政策相關規定[47]。FCA 也參照 PSD2 的規定，要求 TSP 必須要擁有職業責任保險(profession indemnity insurance)才具備申請資格，確保 TSP 的責任賠償能力，而目前市面上有部分職業責任保險已經將資安風險納入承保範圍內，增強 TSP 的保障。

(二)、API 開放範圍

在 CMA 於 2017 年頒布的行政命令當中規定了 API 開放的範圍以及內容，主要可以區分成兩大類：唯讀資料(Read)以及可讀寫資料(Read/Write)。其中唯讀資料包括銀行的總行地點及營業時間、分行的

---

[43] 谷湘儀，臧正運(2019)，變革中的金融科技法制。

[44] OBIE 在 2019 年後更名為 Open Banking Limited，但多數文件仍稱 OBIE 居多。

[45] 九大銀行，又稱為 CMA9，為 AIB Group UK (trading as First Trust Bank in Northern Ireland), Bank of Ireland (UK), Barclays Bank, HSBC Group (including First Direct and M&S), Lloyds Banking, Group (including Bank of Scotland and Halifax), Nationwide Building Society, NatWest Group (including NatWest, Royal Bank of Scotland and Ulster Bank NI), Northern Bank Limited (trading as Danske Bank), and Santander UK.

[46] http：//openbanking.org.tw/index.php/foreign_implement

[47] 薛丹琦(2019)，開放銀行金融創新之機制研究，世新大學財務金融學研究所碩士論文。

地點及營業時間、ATM 的地點、個人及企業活存帳戶、利息、中小企業借貸條款及條件[48]。而可讀寫資料則規範了交易面以及支付面的 API 類別，包括國內外交易發起、國內外交易同意、個人借貸等等各種相關應用[49]。除了唯讀資料以及可讀寫資料，英國從 2019 年底便積極討論是否要開放數位身分的 API，來解決開放銀行中身分認證的問題。

(三)、開放的產業

當初 CMA 在行政命令中，把提供開放 API 的業者稱之為帳戶支付服務提供者(Account Service Payment Service Providers, ASPSPs)，而這些 ASPSP 在一開始只有銀行，也就是說只有銀行才需要將帳戶資訊、交易資訊的 API 開放給 TSP 串接。然而隨著開放銀行體系的成熟，英國 FCA 在 2019 年 12 月發布了《開放金融-徵求意見書》，希望將開放的產業向外擴張至保險業、證券業，以及其他掌管著消費者帳戶的產業，例如財富管理帳戶或是退休金帳戶等等。使唯有多元的業者加入開放的行列才能建構出完整共榮的金融生態圈。

(四)、參與者類別

英國規定的參與者主體為銀行以及 TPPs[50]，其中 TPPs 的資格又可分為 AISP 或是 PISP，根據今年六月 OBIE 公布的訊息，目前共有 184 間 TSP 業者登錄在 OBIE，其中 84 間已經開始營業並且擁有客戶[51]，而未來 Open Finance 階段將有更多金融機構加入參與者的行列，這部分英國尚在研擬當中。由於 TPPs 的數量眾多且種類多元，OBIE

---

[48] https：//openbankinguk.github.io/opendata-api-docs-pub/v2.4.0/

[49] https：//openbankinguk.github.io/read-write-api-site3/v3.1.6/profiles/account-and-transaction-api-profile.html

[50] 英國的 TPP 等同台灣的 TSP，而在英國開放銀行的 TSP 為 Technical Service Provider，為資訊科技提供廠商。

[51] https：//www.openbanking.org.uk/wp-content/uploads/JUNE-Monthly-highlights.pdf

認為消費者和中小企業需要擁有更清楚的分類資訊，才能夠選擇更適當的服務來解決難關。在這樣的動機下，OBIE 於 2020 年 6 月推出了 Open Banking App Store，建立了一套 API 相關的搜尋服務，讓消費者或是企業可以更快速便利的找到正確且合適的 TSP 服務[52]，圖 6、圖 7 為 OBIE 的 App Store 實際畫面。

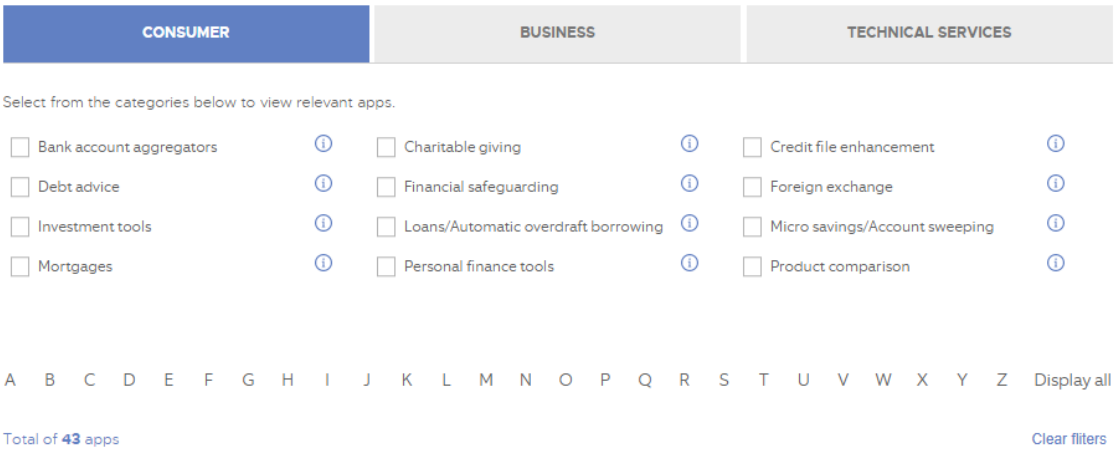


圖 6 OBIE Open Banking App Store 條件選取[53]

[52] https：//www.openbanking.org.uk/app-store/
[53] https：//www.openbanking.org.uk/app-store/

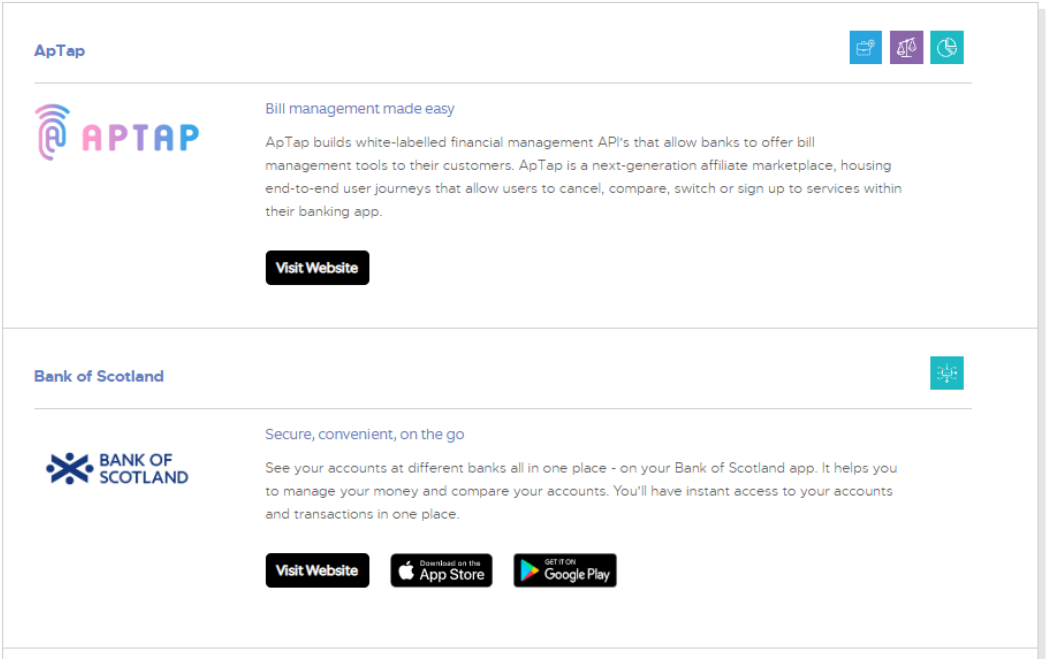


圖 7 OBIE Open Banking App Store 選取結果[54]

(五)、資安標準

英國資安規範依據：GDPR、PSD2 RTS、其他 OBIE 制定之標準所組成。主要有規範下列幾項：

1. SCA (Strong Customers Authentication) ： SCA 是 PSD2 中對消費者授權的嚴格規範，PSD2 和 RTS 將 SCA 定義為「對於使用者的知識(knowledge,只有使用者知道)、所有物(possession,只有使用者擁有)、固有屬性(inherence,使用者的屬性)，若要使用以上三種資料就必須要獲得授權，且三種資料授權相互獨立而不得混用，以保護資料授權的安全性」[55]

[54] https：//www.openbanking.org.uk/app-store/

[55] https：//www.advantio.com/blog/psd2-strong-customer-authentication-sca-and-pci-multi-factor-authentication-mfa-compliance

2. FAPI (Financial Grade API) Profile： FAPI 是一種 REST[56] API，負責提供代表高風險的 JSON[57] data。這類型的 API 會在 OAuth 2.0[58] 的架構下受到保護，並遵從[RFC 6749]、[RFC 6750]、[RFC 7636]以及其他相關規定[59]。
3. CIBA Profile： CIBA 全名為 Client Initiated Backchannel Authentication，由 OpenID 組織提出的 TSP 端驗證機制，其用途改善消費者體驗，讓消費者行使同意權後，可由銀行與第三方認證業者直接確認後續授權的流程。[60]

除了資安規範外，英國也提出了 conformance certification 的"一致性系統驗證"的機制。而在系統驗證中，分了四大類：

- 個資檔訊一致性：Security Profile Conformance
- 功能一致性：Functional Conformance
- TSP 端動態註冊一致性：Dynamic Client Registration Conformance
- 消費者體驗規範一致性：Customer Experience Guidelines Conformance

在 Security Profile Conformance，ASPSP 必須驗證其 API 系統必須符合 FAPI 與 CIBA 規範；而在 Functional Conformance 中，各個參與者則必須驗證其 API 系統符合 OBIE 的 Read 和 Read/Write 的 API 規格。但目前 Conformance Certification 是非強制性，而是採取自測或由

[56] REST，中文為"含狀態傳輸"，全名為 Representational State Transfer，是一種軟體架構設計風格。資源由 URI 指定，對資源的操作包括取得、創建、修改和刪除資源，這些操作正好對應 HTTP 協議提供之 GET、POST、PUT 和 DELETE 方法。
[57] JSON，全名為 JavaScript Object Notation，為網際網路應用的一種常見的輕量級資料交換格式。
[58] OAuth，中文為"開放授權"，OAuth 2.0 標準係指一個開放標準，允許消費者授權讓第三方服務提供者存取該消費者在授權機構上所儲存的受保護資料(又稱為保護資源)。
[59] https：//standards.openbanking.org.uk/
[60] https：//standards.openbanking.org.uk/

認證單位進行後呈 FCA 發佈。

二、 歐盟

歐盟認為支付服務應該滿足歐盟經濟區(EEA)內一致性、清楚的付款資訊、多元支付、消費者保護等項目。所以歐盟一直致力於建立一個單一支付區，使消費者和企業都能在支付區內安全的進行跨境支付，費用也應與境內支付相同。為了推行無縫支付環境，2013 年歐盟提出支付服務指令修正案(PSD2)，主要目的在於整合歐盟內部的電子支付市場，並為其提供統一的法律基礎和規則，讓歐盟內部的跨國支付就像在國內支付一樣快速、有效且安全。PSD2 提到，根據客戶的要求，銀行和其他帳戶支付服務提供商必須開放 API 給註冊後且取得消費者授權的 TSP，讓 TSP 能夠拿到消費者帳戶的讀寫權限[61]。此即 PSD2 為促進支付服務的良性競爭所採取之開放銀行政策，成為歐盟各國推動開放銀行的基礎。下表為歐盟推動開放銀行的法源與做法整理。

表 4 歐盟開放銀行法源與做法[62]

(1) 法律依據	支付服務指令修正案(Revised Payment Service Directives, PSD2)。
(2) 主管機關	歐洲銀行監理機關為 PSD2 之主管機關，依法應與歐洲中央銀行(European Central Bank, ECB)密切合作，並針對支付服務制定安全措施指南《Guidelines on the security measures for operational and security risks under PSD2》，負責建立一個可公開訪問的中央登記冊，以登記所有取得授權的支付機構。
(3) 具體作法	2013 年 7 月，歐盟執行委員會(European Commission)為了要修正原支付服務指令 PSD《Directive 2007/64/EC》，提出 PSD2《Directive(EU) 2015/2366》。又依據 PSD2 的法律約束力，歐洲經濟區(European Economic Area, EEA)內的 31 國(歐盟會員國及冰島、挪威、列支敦士登)，須在 2018 年 1 月 13 日前將 PSD2 的內容轉化為國內法。 2017 年 2 月 23 日，歐洲銀行監理機關又向委員會提交了 PSD2 之監管技術標準草案《Final draft RTS on SCA and CSC under PSD2》，以此制定嚴格的客戶認證(strong customer authentication, SCA)以及一般安全通訊標準(common and secure communication, CSC)。 PSD2 旨在優化 PSD，要求銀行將部分資料開放予第三方服務提供商(Third Party Service Providers, TPPs)以促進市場競爭，並強化消費者的權益和保障，而 EBA 所訂定的安全措施指南和 PSD2 之 RTS 草案，前者是針對銀行作業風險和資安問題防範的指導守則，後者則是對於資訊傳輸和客戶身分認證流程的規範。

[61] EU, PSD2 - https：//eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX：32015L2366

[62] 政治大學金融科技研究中心整理

(一)、監理規範

歐盟開放銀行的主管機關是歐洲銀行業管理局(EBA)以及歐洲中央銀行(European Central Bank, ECB)，根據 PSD2 第 95 條規定，EBA 和 ECB 應當密切合作，共同推動 PSD2。歐洲開放銀行業務由監管機構強制要求自上而下推動，主要原因是為了提高歐洲銀行業的競爭水平。開放銀行業務將為銀行創造一個戰略機會，使其能夠在競爭對手之間實現更大的差異化，為客戶提供更多元選擇。

除了 PSD2 之外，EBA 於 2020 年 2 月 7 日發布了 RTS 草案的最終版(Final draft on the Regulatory Technical Standards)，以確保在 PSD2 的環境下能夠安全的傳輸資料，同時也保障消費者授權的安全性(Secure Customer Authentication)。這份草案會再經由歐盟委員會(European Commission)審查，審查通過後則會被提交到歐盟議會(European Parliament)。一旦議會決議通過後將會在通過後 18 個月正式生效[63]。

(二)、 API 開放範圍

歐盟所開放之資料類型，可分為帳戶資訊服務(Account Information Service,簡稱 AIS)、支付發起服務(Payment Initiation Service, 簡稱 PIS)以及卡片支付服務(Card Based Payment Service,簡稱 CBPS)[64]。其中 AIS 是開放銀行中最基礎的，使 TSP 能夠取得消費者的帳戶資訊，並且讓 TSP 透過詳細的金融資訊幫助消費者提供分析與建議；PIS 則是讓 TSP 能夠代替消費者發起支付指令，簡化支付流程也提高應用性和方便性[65]；最後的 CBPS 也是一種支付服務，只是變成卡片

[63] https：//www.openbankingeurope.eu/news/final-draft-rts-published/
[64] BIAN (2020), Build the future of banking service, http：//bian.org/participate/bian-webinars/bian-apis-future-banking-api-standards
[65] https：//www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/

形式，表示 TSP 能夠在取得授權後，代替消費者以卡片形式進行付款。

(三)、開放的產業

目前歐盟仍只有銀行，然而英國在 2019 年底發布了《Call for Input》的意見蒐集報告，宣示準備朝向開放金融邁進，因此歐盟內部也開始有許多研究認為應該跟進，將開放的範圍擴展，而不限於銀行。歐盟委員會在 2020 年發布的資料策略報告《Data Strategy》中提到對於開放金融的概念與發展，希望在 2020 年第三季能夠公布計畫並實際推行[66]；另外歐盟也提到要開放金融業以外的產業，包括健康、電信以及能源[67]。

(四)、參與者類別

歐盟的 TSP 可以分成 AISP、PISP 以及 CPIIs，申請流程如圖 8，需要經過註冊、登入、權限申請、確認身分、符合 PSD2 規範，最終才能夠成為合格的 TSP 業者。比較特別的是，由於 AISP 的業務僅止於資訊整合，並不涉及金流轉移，因此並未設有最低資本額；相對來

[66] European Commission, European data strategy, https：//ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
[67] https：//www.finextra.com/blogposting/18517/the-ambitious-path-to-open-finance-and-open-data--how-europe-is-leading-the-way

說，PISP 需要經手金流的控管和支付，因此 PSD2 要求此類型業者須維持 50000 歐元的資本額[68]。

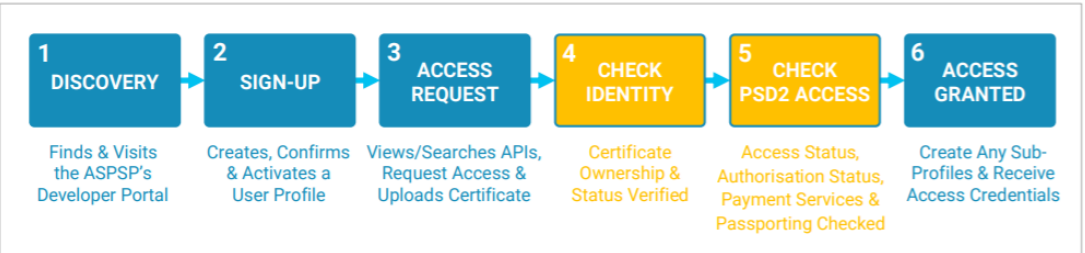


圖 8 歐盟 TSP 申請流程[69]

(五)、資安標準

歐盟的資安標準最主要規範在 PSD2 的 RTS 中，但是歐盟的資安標準並未規範像英國開放銀行規範技術層面。RTS 主要是以有關客戶認證和安全通信的資訊標準，這項標準將於 2019 年 9 月 14 日生效。該標準規定銀行和 TSP 應如何在提供消費者 API 時符合相關客戶認證與安全通信標準。

RTS 對於客戶認證的要求為 SCA (Strong Customer Authentication)，是指客戶必須提供二項以上的認證機制。而在安全通信標準上則必須採用歐盟核可 QWCA (Qualified Web Certification Authority)發行之憑證，再由銀行與 TSP 以 TLS 等級以上的通信傳輸進行資料交換。

三、 澳洲

澳洲早在 2014 年便開始提倡資料分享的好處，並於 2017 年發布《Review into Open Banking in Australia》，同年底開始推動 CDR，宣布消費者在交易和商品等數據可以交由第三方使用，另外實施順位以銀行最優先，接下來是能源、電信產業以及其他行業[70]。2018 年澳洲

[68] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。
[69] PRETA S.A,(2017),Third Party Provider User Management for PSD2 Access to Account.
[70] 薛丹琦(2019)，開放銀行金融創新之機制研究，世新大學財務金融學研究所碩士論文。

發布開放銀行建議書，修正《競爭與消費者法》，正式啟動開放銀行的建置計畫，並強制要求國內市佔共95%前四大銀行[71]必須加入開放銀行體系[72]。

[71] 澳洲四大銀為國民銀行、聯邦銀行、澳新銀行、西太平洋銀行。

[72] http：//openbanking.org.tw/index.php/foreign_implement

表 5 澳洲開放銀行法源與做法[73]

(1) 法律依據	競爭與消費者法(Competition and Consumer Act 2010)
(2) 主管機關	澳大利亞推行開放銀行制度之目的除促進交易便利、將資訊主導權回歸消費者以外，更肩負著兼顧市場安全與競爭的雙重目的，因此開放銀行之主管機關由澳洲財政部(Treasury)擔任。
(3) 具體作法	■ 由原則出發的法制設計 澳洲施行開放銀行制度的法制度設計，共可分為三層次： 1. 擇定欲修正之總綱 第一層次為法律層面(Legislation)，負責總綱的制度建立。澳大利亞選擇修正為現有之競爭與消費者法，而不選擇另訂定新法律之理由主要有二：首先，由於開放銀行僅為澳洲政府設定率先運用消費者資訊權(CDR)，旨在落實消費者資料主導權的第一項產業(銀行、能源、電信)，因此其希望設立一套通用於三項產業的法規範，故排除透過修正澳大利亞證券和投資委員會法(The Australian Securities and Investments Commission Act 2001)等金融法規；再者，有鑒於先前提及之開放銀行之雙重目的，政府認為隱私法(The Privacy Act) 並不足夠，立法重點不應放在單純的隱私權保障，此法規範之目的應在於促進金融市場競爭、提供更佳的金融服務，故最終選擇修正競爭與消費者法。 2. 法規命令之草擬與制定 第二層次為法規命令(Rules) 之制定過程。澳洲修正草案的擬定機構，主要由兩機關負責：澳大利亞競爭和消費者委員會(the Australian Competition and Consumer Commission， 下稱 ACCC)，以及澳大利亞信息專員辦公室(the Office of the Australian Information Commissioner， 下稱 OAIC)。ACCC 主要負責競爭與消費者層面，OAIC 則負責隱私層面的法規範修訂，又整體過程皆以 ACCC 為總領導機關，協同 OAIC 進行法規命令之擬定。 3. 相關標準之建置 第三層次為相關標準之制定(Standards)。前述標準係針對技術層面之標準，例如資料傳輸標準、資料儲存標準等，由政府委託各領域專家協助擬定之。

(一)、監理規範

澳洲開放銀行的法源依據來自於修正後的《競爭與消費者法》，主要原因為 CDR 規定銀行、能源以及電信業者都是優先設定開放的產業，這之中並不只有銀行業參與，因此澳洲希望能有一套適用三種產業的法源，最終選擇修正競爭與消費者法來做為法源。

澳洲開放銀行的主管機關主要有競爭和消費者委員會(Australian Competition and Consumer Commission, ACCC)、資訊專員辦公室(the Office of the Australian Information Commissioner, OAIC)以及聯邦科學與工業研究組織(Commonwealth Scientific and Industrial Research Organisation, CSIRO)。

[73] 政治大學金融科技研究中心整理

ACCC 主要負責競爭與消費者層面；OAIC 則負責隱私層面的法規修訂；CSIRO 則是由財政部指派負責制定 CDR 中提到的資料標準的單位，並且組成專家團隊 Data61，和 ACCC 並列為 CDR 的最高主管機關[74]。

ACCC 在管理開放銀行時特別注重 TSP 的消費者保護的保險內容，要求 TSP 在取得授權之前必須提供保單細節、為何投保該險種的判斷依據，並提供相關證明等等，為的就是確保消費者的權益以及 TSP 的賠償能力。而 ACCC 並未規定 TSP 需要投保哪些特定的險種，而是採用「適當的保險」來規範，因為 ACCC 認為為每家業者有其獨特的業務與體制，影響因素包括服務、商品、活動等 等，有些風險甚至需要客製化保險才能夠處理。因此若 ACCC 為業者建立確切的保險計畫，可能導致某些業者出現 under-insurance 或是 over-insurance 的情況。

(二)、 API 開放範圍

澳洲在 2018 年 5 月 25 日宣布將 API 開放進程分成三個階段，各階段開放的如下表所示。

表 6 澳洲 API 開放種類

第一階段	saving accounts、call account、term deposits、current accounts、Cheque accounts、debit card accounts、transaction accounts、personal basic accounts、GST and tax accounts、credit and charge cards
第二階段	home loan、personal loan、mortgage offset accounts
第三階段	business finance、investment loans、lines of credits、overdrafts、asset finance、cash management accounts、farm management accounts、pensioner deeming accounts、retirement savings accounts、trust accounts、foreign currency accounts 以及 consumer leases。

目前四大主要銀行的完成進度包括第一階段商品相關的資料(2019 年 7 月)、第二階段商品相關的資料(2020 年 2 月)，以及第三階

[74] https：//data61.csiro.au/en/Our-Research/Focus-Areas/Special-Projects/Consumer-Data-Standards

段商品相關的資料(2020 年 7 月)[75]。至於全部資料的完成時間預計要到 2021 年 7 月才能夠開放完畢。

(三)、開放的產業

銀行、能源、電信業是 CDR 中規定第一波開放的產業，但發展成熟後開放範圍也會擴及至其他產業。這樣的發展源自於澳洲的出發點是 CDR，因此消費者資料權的實現必須在各行各業，而非僅限於金融業[76]。

(四)、參與者類別

CDR 將參與者分為資料擁有者(data holder)以及被授權的資料接收者(accredited data recipient)。所謂的資料擁有者是指掌握消費者資料的一方，例如銀行，這些資料擁有者必須在消費者的要求下將資料移轉給資料接收者。而資料接收者是代替消費者來接收資料的業者，例如 TSP[77]。

(五)、資安標準

澳洲的資訊安全規範是在消費者資料標準(Consumer Data Standards, CDS)規範，而 CDS 是 CDR 的一部分，主要規定 API、資料與安全的相關規定[78]。澳洲的資安標準與英國非常相似，是採用 OIDC 與 FAPI 作為身份認證機制。澳洲的資安標準是採歐盟與英國的標準整合而成。

---

[75] https：//www.ausbanking.org.au/policy/the-future/open-banking/
[76] https：//www.lexology.com/library/detail.aspx?g=68acc1a2-6681-4e71-ad72-ec9c80a6e4fc
[77] https：//www.oaic.gov.au/consumer-data-right/cdr-participants/
[78] https：//consumerdatastandardsaustralia.github.io/standards/#introduction

四、 香港

對於開放銀行的發展，HKMA 採開放式態度，屬於政策鼓勵的推行模式。2017 年 9 月，香港金融管理局公布了七項措施，宣布推動香港邁向智慧銀行新紀元。而這七項措施分別為推出快速支付系統、監理沙盒升級、引入虛擬銀行、推出「銀行易」、促進開放應用程式介面(開放 API)、加強跨境金融科技合作，以及提升科研及人才培訓。其中第五項提到香港金融管理局將會制訂開放 API 政策，促進開放 API 在銀行業的應用，同時也透過銀行和科技公司之間的合作鼓勵創新並加強金融服務[79]。

為了推動開放銀行，香港金融管理局在接下來一年間舉辦多場討論會並蒐集業界回饋，最終在 2018 年 7 月發表《香港銀行產業開放式應用程式介面架構》(Open API Framework for the Hong Kong Banking Sector)，載明開放 API 的政策性指導方針以及目標[80]。

香港金融管理局建議將 API 開放分成四階段，第一階段是提供查閱產品與服務資料；第二階段開放接受銀行產品申請；第三階段賦予讀取或更改帳戶資訊的權利；第四階段則是接受客戶授權的銀行交易及支付服務。目前第一和第二階段已經於 2019 年完成，至於三四階段預計會在 2020 年公布一套技術標準，並訂定具體的實施時間表[81]。有關香港的開放銀行法源與做法整理如下表。

[79] https：//www.hkma.gov.hk/chi/news-and-media/press-releases/2017/09/20170929-3/

[80] HKMA (2018), Open API Framework for the Hong Kong Banking Sector, https：//www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/

[81] https：//www.hkma.gov.hk/chi/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/phase-approach/

表 7 香港開放銀行法源與做法[82]

(1) 法律依據	香港《外匯基金條例》和《銀行業條例》
(2) 主管機關	香港金融管理局(Hong Kong Monetary Authority, HKMA)於 1993 年 4 月 1 日成立，由外匯基金管理局與銀行業監理處合併而成。其主要職能由《外匯基金條例》和《銀行業條例》規定，協助鞏固香港的國際金融中心地位(包括維持與發展香港的金融基建)，因此依據被賦予的職權，Open API 涉及金融體系的穩定，由香港金融管理局主管。
(3) 具體作法	香港金融管理局目前針對 Open banking 採取開放式態度，鼓勵金融業在原有法律架構之下與第三方服務供應商(Third Party Service Provider， TSP)進行 Open API 的合作。在與相關業者(金融業、第三方服務供應商等等)研討並收集意見回饋之後，香港金融管理局於 2018 年 7 月 18 日發布「香港銀行產業開放式應用程式介面架構」，在報告中提出開放 API 架構、時間表以及第三方服務供應商治理等相關建議。

(一)、監理規範

香港金融管理局在 API 框架中指出，第一階段開放的讀取資訊敏感性和風險較低，因此 TSP 僅須通過銀行簡易的登錄流程，並遵守幾項規則，包括 TSP 應通知銀行其使用的資訊範圍、TSP 在蒐集資料時不得誤導客戶，以及對客戶充分說明產品和服務的風險[83]。

到了第二階段，涉及到銀行商品的申請，因此 API 框架中提到銀行應對 TSP 引入適當的評估流程，包括財務、管理、風險、技術、資料保護、網路安全等等，然而銀行不得使用簽署契約的方式提高 TSP 取用資料的門檻。[84]

(二)、 API 開放範圍

香港金融管理局在 API 架構中將 API 分為四大類，分別為產品/服務資訊、產品/服務的訂閱和新申請、帳戶資訊、以及交易。2019 年 1 月，13 間銀行[85]與銀聯通寶有限公司推出 API 交換平台 JETCO APIX，成為香港首個支援跨行業操作的開放 API 交換平台，服務對象為任何行業，包括銀行、第三方服務供應商以及程式開發機構。該平台可

[82] 政治大學金融科技研究中心整理

[83] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。

[84] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。

[85] 東亞銀行、交通銀行、花旗銀行、中國建設銀行、創興銀行、中信銀行、招商永隆銀行、大新銀行、富邦銀行、工銀亞州、華僑永亨銀行、大眾銀行，以及上海商業銀行。

為用戶提供簡易無縫的連接，讓他們可以在一個較為安全且標準化的環境中共同開發新產品，並且能以更低的成本，更快的速度推出產品和服務。從平台推出日開始，無論個人或機構均可於 JETCO APIX 的網站(www.apix.com.hk) 登記、建立戶口，還可使用沙盒測試產品[86]。

目前平台上將 API 分成存款、借貸、信用卡、抵押、地點、其他銀行服務、保險、外匯、商品資訊以及商品應用等十大類別， 提供超過 200 支 API 串接[87]。

(三)、開放的產業

根據 JETCO APIX 上列載的 API 提供者，有 14 間銀行、1 間證券金融科技業者，以及 1 間保險金融科技業者。雖說香港的發展方式極具彈性，卻也分成二個不同的生態系，中小型銀行透過 JETCO 加入開放 API 的行列，而大型銀行卻大多採自建 API 平台的方式進行。

(四)、參與者類別

目前 TSP 大多是金融科技業者，陸續也可以看到開放銀行的應用案例。例如 2019 年花旗香港和「易賞錢」合作，將花旗的紅利積分兌換功能和易賞錢平台整合，因此花旗銀行的信用卡客戶可以直接將積分使用在易賞錢上進行兌換和消費[88]。

(五)、資安標準

香港資安規範為參考非強制依據 API 架構，而香港對四大類 API 對應之保護要求整理如下圖。

---

[86] https：//www.edigest.hk/article/117710/%e7%86%b1%e8%a9%b1/%e9%8a%80%e9%80%9aopen-api%e5%b9%b3%e5%8f%b0-%e9%8a%80%e8%a1%8c-%e5%84%aa%e6%83%a0%e5%88%b8-jetco-apix/2/

[87] https：//sandboxportal.apix.com.hk/jetco/sb/categories

[88] https：//ctee.com.tw/news/finance/30806.html

Categories of Open API	*Protections required*
Product and service information	• Authentication of bank sites • Integrity of data • Authentication of TSPs
Subscription and new applications for product/service	• Authentication of bank sites • Integrity and confidentiality of data • Authentication of TSPs
Account information	• Authentication of bank sites • Integrity and confidentiality of data • Authentication of TSPs • Authorisation of customers
Transactions	

圖 9 香港對 API 之保護要求[89]

在技術與資安架構方面，有鑑於全球 API 介接多以 REST 的實用性以及廣獲業界接受，HKMA 建議以 REST 為通訊協定，並以 JSON 為資料格式[90]。API 框架中的安全標準如下圖所示。

Protection required	*Technology*
Authentication of bank sites and TSPs	X.509
Integrity and confidentiality of data	TLS
Authentication of customers	Bank's own method
Authorisation of customers	OAuth 2.0

圖 10 香港對 API 之安全標準[91]

五、 新加坡

MAS 和新加坡銀行公會(the Association of Banks in Singapore, ABS)於 2016 年 11 月 16 日發布《Finance-as-a-Service: API Playbook》(以下簡稱 Playbook)，作為新加坡開放銀行的指導手冊。Playbook 提

[89] https：//www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf p.5
[90] https：//www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf p.25
[91] https：//www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf p.26

出開放 API 的建議標準，並未強制要求業者遵循，由銀行自行決定開放哪些 API，也可以自行決定合作夥伴。

表 8 新加坡開放銀行法源與做法[92]

(1) 法律依據	《新加坡金融管理局法》(Monetary Authority of Singapore Act)
(2) 主管機關	新加坡金融管理局(Monetary Authority of Singapore)根據《新加坡金融管理局法》(Monetary Authority of Singapore Act)所授予的職權作為新加坡的中央銀行，以將新加坡發展成為國際金融中心作為目標。因此根據該法案，Open API 涉及銀行資訊與金融服務業，由新加坡金融管理局新創的金融科技與創新部(FinTech and Innovation Group，FTIG)主管。
(3) 具體作法	MAS 針對 Open Banking 採取鼓勵金融業者主動開放 API，在研討與回饋之後，MAS 於 2016 年發布「ABS-MAS Financial World｜金融即服務：應用程式介面腳本(Finance-as-a-Service：API Playbook)」，在此報告中提出對於應用程式介面的篩選、資料安全標準以及與第三方業者的合作規範等相關建議。

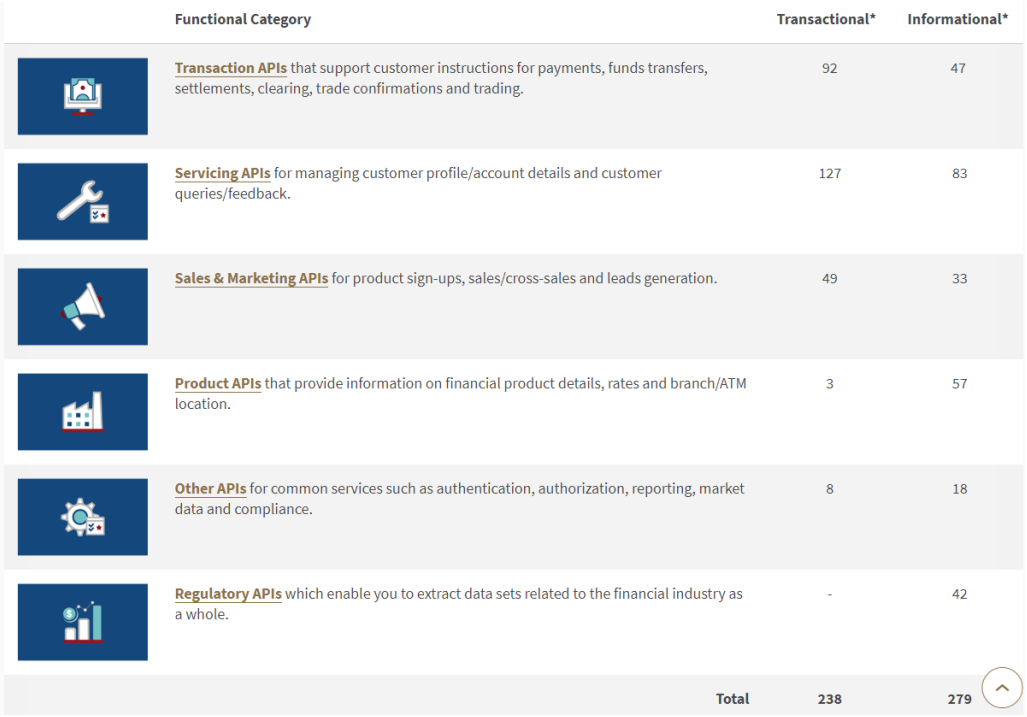
(一)、監理規範

為了推動開放銀行，新加坡金融管理局轄下新成立了金融科技與創新部，負責開放 API 的相關業務。新加坡政府並未透過法令強制推動，而是發布 Playbook 來引導業者使用 API 技術及對應資安規範，此做法和香港類似。另外 MAS 與東盟銀行組織(ASEAN Bankers Association， ABA)、國際金融公司(International Finance Corporation，IFC)共同成立的東盟金融創新網路(ASEAN Financial Innovation Network， AFIN)也推出 API Exchange (APIX)，作為一全球的開放架構 API 交換平台與市集[93]。

(二)、 API 開放範圍

根據 MAS 官網 2019 年 11 月的資料，新加坡的 API 開放可分為交易、帳戶服務、銷售、產品、其他以及監管等六大種類。每一類又可以細分為敏感度較高需要詳細審核的 Transactional，以及敏感度較低僅需檢易授權的 Informational。由圖 11 可見新加坡市場應用上最廣泛的 API 種類還是以交易和服務兩項為主[94]。

[92] 政治大學金融科技研究中心整理
[93] https：//apixplatform.com/aboutapix
[94] https：//www.mas.gov.sg/development/fintech/financial-industry-api-register



	Functional Category	Transactional*	Informational*
	Transaction APIs that support customer instructions for payments, funds transfers, settlements, clearing, trade confirmations and trading.	92	47
	Servicing APIs for managing customer profile/account details and customer queries/feedback.	127	83
	Sales & Marketing APIs for product sign-ups, sales/cross-sales and leads generation.	49	33
	Product APIs that provide information on financial product details, rates and branch/ATM location.	3	57
	Other APIs for common services such as authentication, authorization, reporting, market data and compliance.	8	18
	Regulatory APIs which enable you to extract data sets related to the financial industry as a whole.	-	42
	Total	**238**	**279**

圖 11 新加坡 API 開放數量統計[95]

(三)、開放的產業

根據 MAS 的資料顯示參與開放的業者有星網電子付款、星展銀行、華僑永亨銀行、花旗銀行以及渣打銀行[96]。 其中星展銀行算是發展最迅速的業者，星展於 2017 年就推出了 API 開放平台「DBS Developers」，上架超過 200 支 API。

(四)、參與者類別

新加坡的 TSP 除了金融科技業之外，已經有許多生活場景的業者成為銀行開放 API 的合作夥伴。以星展銀行為例，合作夥伴包括麥當勞、Grab 等等，實現金融服務走向生活場景的模式。

95 https：//www.mas.gov.sg/development/fintech/financial-industry-api-register
96 https：//www.mas.gov.sg/development/fintech/financial-industry-api-register

(五)、資安標準

依據新加坡 Playbook[97]規範，新加坡也是採用 TLS 與 OAuth 為主要 API 導入時的技術標準，主要也是依循了英國 open banking 的技術規範。

六、 美國

美國一直都是自由競爭市場的代表，在這樣的市場環境下，各家業者的競爭意識較為強烈，總是不斷推陳出新來吸引消費者並搶占市場。這樣的市場也讓美國對於開放銀行的推行方式不同於英國、歐盟，美國採用市場自由發展的方式來推動，而未強制要求銀行業者開放 API，政府僅作為提供建議的角色，頒布指導原則做為業者的參考。例如 2017 年美國的金融保護局(United States Consumer Financial Protection Bureau, CFPB)曾針對網路爬蟲的做法頒布「消費者授權的資料存取權」九項指導原則。由此可見美國政府肯認可金融消費者確實擁有將資料授權予第三方業者使用之權利，雖然當時規定的是網路爬蟲方式而非開放 API，但核心概念皆以消費者的資料可攜權為出發，實現消費者賦權[98]。

表 9 美國開放銀行法源與做法[99]

(1) 法律依據	《Dodd-Frank 法案》(Dodd-Frank Wall Street Reform and Consumer Protection Act)
(2) 主管機關	美國的監理架構極其複雜，並沒有專責主管機關來主導開放銀行。美國金融保護局(United States Consumer Financial Protection Bureau，簡稱 CFPB)是目前和開放銀行最為相關的主管機關，該單位是由 Dodd-Frank 法案授權成立，隸屬於美國財政部管轄，旨在建立普惠金融，並監管銀行、信用合作社以及其他金融公司，保護消費者的權益。
(3) 具體作法	美國屬於完全的市場驅動，例如花旗銀行早在 2016 年 11 月就宣布推出全球 API 開發者中心，是美國銀行業者自由開放的著名案例。 CFPB 曾在 2017 年針對網路爬蟲的做法頒布「消費者授權的資料存取權」九項指導原則。由此可見美國政府肯認金融消費者確實擁有將交資料授權予第三方業者使用之權利，雖然當

[97] https：//abs.org.sg/docs/library/abs-api-playbook.pdf P.34-41
[98] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。
[99] 本研究金融科技研究中心整理

	時規定的是網路爬蟲方式而非開放 API，但核心概念皆以消費者的資料可攜權為出發，實現消費者賦權。另外美國自動票據交換所協會(National Automated Clearing House Association)以及金融數據交換組織(Financial Data Exchange)，也都各自提出 API 標準供市場參考。

(一)、監理規範

美國的監理架構極其複雜，不像是台灣有金管會統一管理金融業的各種業務，在美國同一個銀行依據業務種類不同，需要面對多個不同的主管機關，如圖 12 所示。因此像開放銀行這種牽涉多種交易類別的制度，並不容易找到某個機關來專責主導，而是個別機關分別進行相關的標準制定以及研究報告。除了上述的 CFPB 之外，美國自動票據交換所協會(National Automated Clearing House Association,簡稱 NACHA)在 2017 年也曾組織 API 標準化行業組織(API Standardization Industry Group, ASIG)，制定帳戶資料分享、支付及詐欺等等 API 相關議題之標準，但此標準一樣不具強制效力。

美國正式提到開放銀行必須等到 2018 年財政部的報告，報告中認為資料共享的方式應該用 API 串接才更為安全，並建議政府消除法規中的不確定性，與民間共同研擬實務操作規則[100]。

目前美國唯一針對消費者獲取帳戶及交易資料的明文法為《Dodd-Frank 法案》的 1033 條規定，內容提到只要在符合 CFPB 管轄的範圍內，在消費者要求之下，金融從業人員必須將金融服務相關的資訊提供給消費者。除了該法案之外，美國尚未建立明確的開放銀行法源依據[101]。

[100] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。
[101] 谷湘儀，臧正運(2019)，變革中的金融科技法制，五南出版社。

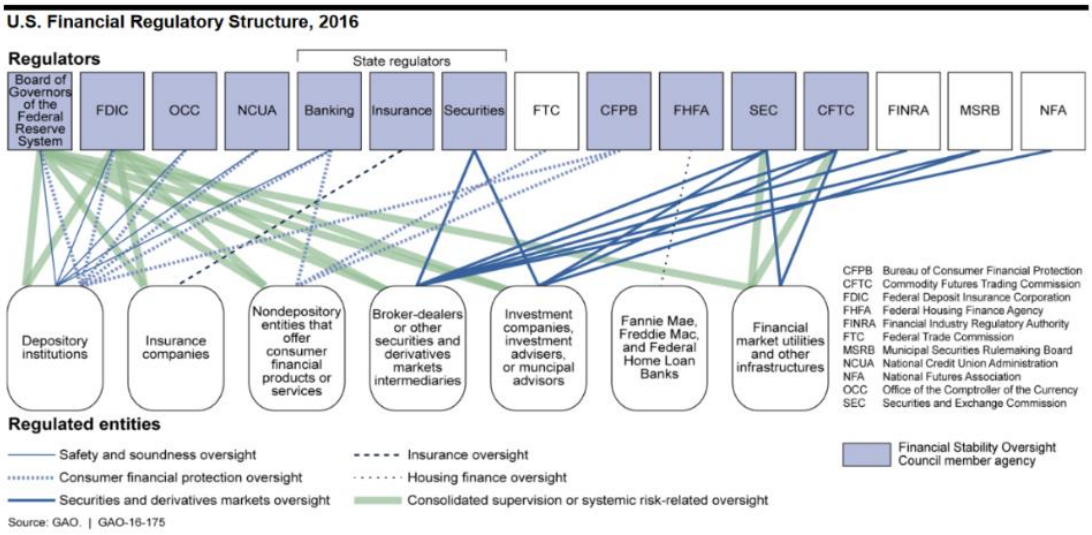


圖 12 美國金融監理架構[102]

(二)、 API 開放範圍

目前有多個組織同時進行制定 API 的標準以及範圍，例如部分銀行、金融科技業者自行組成的金融數據交換組織(Financial Data Exchange, FDX)，在 2020 年 3 月發布了 FDX API 的第四版更新，目的是加強串接的相互性並支援更廣泛的使用範圍[103]。另外，NACHA 和 Accenture 合作成立的標準化 API 行業組織(API Standardization Industry Group, ASIG) 也試圖使美國金融服務業能有標準化的 API 使用[104]，開放的種類包括帳戶確認(Account Validation)、媒體交換自動轉帳支付服務(ACH Payment Initiation)、銀連絡資訊(Bank Contact Information)、即時付款帳戶確認(Real-Time Billing Account Validation)、交易狀態(Transaction Status) APIs。

[102] https：//www.gao.gov/products/GAO-16-175

[103] https ： //www.financialdataexchange.org/FDX/News/Announcements/financial-data-exchange-releases-first-major-update-to-fdx-api-makes-fourth-version.aspx

[104] https：//www.nacha.org/afinis-interoperability-standards

(三)、開放的產業

目前為銀行業在領導開放 API，以花旗銀行為例早在 2016 年 11 月就宣布推出全球 API 開發者中心，是美國銀行業者自由開放的著名案例[105]。當時花旗已經透過開放式架構技術來發布 API，授權其他開發者可存取 8 個使用類別的 API，包括帳戶管理、分行資訊、轉帳服務、信用卡管理、信用卡紅利點數消費折抵、開戶辦卡、客戶服務等等，將金融服務結合不同領域，開發更多解決方案。而除了銀行之外，目前尚未看到保險業、證券業者等其他金融機構開放 API。

(四)、參與者類別

美國政府對於開放銀行的發展沒有多作干涉與強制，因此金融機構和外部(金融)科技公司就成為了推動開放銀行發展的主要推手。舉例來說，在 2017 年，富國銀行(Wells Fargo)與金融科技公司 Intuit 達成了數據交換的協議，推出名為 QuickBooks 的帳戶整合服務，而 Envestnet Yodlee 也提供了不同種類的 API 供客戶利用，可用於與金融機構介接，例如帳戶整合 API 與認證用 API，其他類似的還有科技公司 Plaid 與 Stripe 也提供自己的 API 文件(平台)讓第三方業者可以連接到金融機構進行帳戶訪問。

由於誰來串接、如何串接、串接後的應用等等都是由市場自行決定，因此美國開放銀行所提供的新金融服務可以說是相當多元且具有創意。

[105] https：//www.businesswire.com/news/home/20161114005729/zh-HK/

(五)、資安標準

美國對於 API 的資安規範依據 NACHA 和 FDX 分別發布的 API 標準建議大不同，且不具法令強制性，主要是以加入組織必須遵守的技術標準為主。彙整如下：

1. NACHA 建議的內容：比較像是研究報告，沒有真正提出建議的標準，目前內容僅提到架構採用 RESTful APIs，而資料交換格式為以 ISO 20022 為標準的 JSON 格式。
2. FDX 僅針對 API 進行相關規範，並未建議資訊安全規範。

七、 加拿大

2018 年，加拿大的監管機關首次將開放銀行相關計畫納入聯邦預算的討論項目當中。2018 年 9 月財政部長任命成立一開放銀行諮詢委員會，委員會於 2019 年 1 月發佈《開放銀行價值評估》(A Review into the Merits of Open Banking)，開始廣徵各方利益相關者(包括消費者、中小企業主、民間組織等)對於開放銀行第一階段的意見，收到了超過 130 份回應諮詢文件的書面意見，在這期間也通過會議方式與數百名利益相關者進行討論。主要目的在於衡量開放銀行相關服務是否能為加拿大人帶來實質的好處，以及政府在實施過程中應扮演何種角色[106]。在第一階段的評估完成後，2020 年 1 月委員會發表了《消費者導向金融：金融服務的未來》白皮書[107]，結論是以數據驅動的服務可以幫助人們在預算內獲得更負擔得起的金融服務，另外開放銀行業務應被重新命名為「消費者導向金融(consumer-directed finance)」以更精

[106] https：//www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/submissions.html
[107] https：//www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html

確描述其理念本質[108]。目前委員會的評估進入第二階段，重點將放在開放銀行相關的數據安全及隱私議題，預計蒐集結果將於 2020 年底提交給財政部長。

加拿大在發展開放銀行方面最特別的是由政府層級來協助處裡身分驗證的問題。加拿大數位身分及驗證委員會 (Digital ID & Authentication Council of Canada,簡稱 DIACC)是由公私部門合作組成的非營利組織，主要負責發展加拿大的數位身分的認證系統和授權機制[109]，在 2016 年曾發布《Pan-Canadian Trust Framework》，成為加拿大發展數位化的基礎之一，而 DIACC 也正在為開放銀行這種未來的市場變化擬定長期的計畫[110]。目前加拿大政府的構想是建立一個結合公私部門的聯合式數位身分架構，個人的身分和屬性將儲存在不同的連接系統當中，透過分散式結構讓單點故障對系統的危害降到最低[111]。

表 10 加拿大開放銀行法源與做法[112]

(1) 法律依據	《個人資訊保護與電子文件法》(The Personal Information Protection and Electronic Documents Act,PIPEDA)
(2) 主管機關	加拿大財政部於 2018 年首次將開放銀行相關計畫納入聯邦預算的討論項目當中，目前也正在努力擬定 PIPEDA 的修正草案，因為現行的 PIPEDA 雖然有規範商業活動期間如何收集、使用和揭露個人資訊，但由於立法的年代久遠，很多標準已經顯得老舊過時。希望修正後 PIPEDA 能夠成為開放銀行在資料許可、資料管理及(業者的)揭露要求的法源框架。
(3) 具體作法	2018 年 9 月財政部長任命成立一開放銀行諮詢委員會，委員會於 2019 年 1 月發佈《開放銀行價值評估》(A Review into the Merits of Open Banking)，開始廣徵各方利益相關者(包括消費者、中小企業主、民間組織等)對於開放銀行第一階段的意見。在第一階段的評估完成後，2020 年 1 月委員會發表了《消費者導向金融：金融服務的未來》白皮書 ，結論是以數據驅動的服務可以幫助人們在預算內獲得更負擔得起的金融服務，另外開放銀行業務應被重新命名為「消費者導向金融(consumer-directed finance)」以更精確描述其理念本質 。目前委員會的評量進入第二階段，重點將放在開放銀行相關的數據安全及隱私議題，預計蒐集結果將於 2020 年底提交給財政部長。

[108] https：//www.mondaq.com/canada/financial-services/797350/open-banking-in-canada-current-regulatory-insights
[109] https：//www.businesswire.com/news/home/20190604005330/en/Digital-ID-Authentication-Council-Canada-DIACC-Announces
[110] Canadian Banks (2019), Open banking is coming, p.11
[111] https：//cba.ca/embracing-digital-id-in-canada
[112] 政治大學金融科技研究中心整理

(一)、監理規範

加拿大是以財政部作為開放銀行的主管機關。至於法源依據，Deloitte 的報告中指出，加拿大現行聯邦法中的個人資訊保護與電子文件法(The Personal Information Protection and Electronic Documents Act, PIPEDA)，雖然有規範加拿大省分進行商業活動期間收集、使用和揭露個人資訊，但由於立法的年代久遠，很多標準已經顯得老舊過時。因此加拿大目前正在努力擬定 PIPEDA 的修正草案，以期 PIPEDA 能夠成為開放銀行在資料許可、資料管理及(業者的)揭露要求的法源框架，目的即是為了加強透明度並確保一切皆基於客戶的同意[113]。

(二)、 API 開放範圍

現階段加拿大並無明確的 API 開放規範，但預計會開放的 API 包括消費者帳戶資訊、投資帳戶、信用卡，另外也考慮將定存、支付發起、數位身分的 API 納入開放範圍。

在 API 串接的標準方面，利害關係人在第一階段的白皮書中提到，行業有能力自己訂定技術標準，但應在政府監督下完成以確保公平性及消費者保護。不過對於政府要幫到什麼程度有不同的意見，有人說應該要由市場上的領導者組成技術諮詢小組，或者建立一個 API 管理中心組織，類似英國 OBIE 的角色。負責授權建立技術標準。而大多數人都希望政府能強制使用標準化的 API。簡單來說，就是技術標準應以市場為基礎、由行業主導，但要與政府目標保持一致。

[113] https：//www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca-open-banking-aoda-en.pdf

(三)、開放的產業

目前加拿大的推行進度仍處於研擬階段，在開放產業方面僅以銀行作為推行對象。

(四)、參與者類別

由於加拿大在推動上是以銀行產業為主，因此參與者是以金融機構以及金融科技業者為主。

(五)、資安標準

加拿大目前仍未明確規定開放銀行適用之資安規範，以下僅列出政府對 API 的相關規定：通信標準為 TLS 1.2 與身份授權為 OAuth 2.0。[114]

八、 日本

日本銀行業在 2018 年 3 月到 2020 年部署開放 API。在日本，開放銀行是由促進銀行業創新和現代化的政策目標所推動的，這是日本政府 2017 年發佈的成長戰略的一部分。主管機關和利益相關者認為，日本的金融服務業落後於其他地方，這使其更容易受到潛在的外部衝擊影響並因此影響其全球競爭力。此外，對現金支付的嚴重依賴[115]及過去嚴格的監管措施(例如：限制銀行在金融科技公司持有大量股份的能力)皆扼殺了金融業的創新能力，也因此，開放銀行及隨之而來的監管現代化(包括放寬與金融科技相關的投資限制)被視為是促進成長、提高競爭力和增進創新的關鍵因素之一。

[114] https：//www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html
[115] https：//www.frbsf.org/banking/asia-program/pacific-exchanges-podcast/open-banking-apis-japan/

表 11 日本開放銀行法源與做法[116]

(1) 法律依據	《日本銀行法》(Bank of Japan Act)
(2) 主管機關	日本金融廳(Financial Service Agency,簡稱 FSA)是開放銀行的主管機關,設置於中央政府內閣府之下,類似於台灣的金管會。
(3) 具體作法	日本銀行業在 2018 年 3 月到 2020 年部署開放 API。在日本,開放銀行是由促進銀行業創新和現代化的政策目標所推動的,這是日本政府 2017 年發佈的成長戰略的一部分。日本在 2017 年 5 月修訂的銀行法中建立第三方服務機構的登錄系統,以及與銀行之間的自願性合作架構。新銀行法鼓勵銀行在 2020 年前開放 API,以便在東京奧運來到之前建立數位支付系統。然而也有人認為,日本的銀行法在資料可攜權方面缺乏明確規範,法律上仍有調整的空間

(一)、監理規範

日本金融廳(Financial Service Agency, FSA)是開放銀行的主管機關，設置於中央政府內閣府之下，類似於台灣的金管會。法源依據則是銀行法，日本在 2017 年 5 月修訂的銀行法中建立第三方服務機構的登錄系統，以及與銀行之間的自願性合作架構。新銀行法鼓勵銀行在 2020 年前開放 API，以便在東京奧運來到之前建立數位支付系統。然而也有人認為，日本的銀行法在資料可攜權方面缺乏明確規範，法律上仍有調整的空間。

(二)、 API 開放範圍

在早期階段，已有大約 20 家日本公司使用開放 API 提供帳戶資訊查詢的服務。另外個人化理財與企業會計服務也有望成為開放 API 的顯著受益者，其他機會也可能有例如 P2P 支付平台及個人電子貨幣帳戶的發展等[117]。

(三)、開放的產業

目前開放的產業以金融業為主，包括銀行以及證券業，例如三菱日聯銀行、瑞穗銀行、三井住友銀行、樂天銀行、樂天證券、日興證券等。

[116] 政治大學金融科技研究中心整理

[117] https：//www.frbsf.org/banking/asia-program/pacific-exchanges-podcast/open-banking-apis-japan/

雖說日本目前共有 130 間銀行，但根據 FSA 2019 年 9 月發布的報告，其中有 73 間沒有任何進展，也就是沒有和任何的 TSP 合作；而其他 57 間有實際和 TSP 合作的銀行當中，有 50 間銀行都只簽署了 4 份協議，只有 7 家銀行簽署了 5 份以上的協議，簽了最多份合作協議的則是 Sumishin Net Bank 的 9 份。所有金融機構的協議總數為 151 份，相當於每間銀行一份多一點。

(四)、參與者類別

參與者主要是金融科技業者以及電信業者，例如 Money Forward 、Moneytree、Line pay 等。其中有一間科技公司 NTT DATA 在 2017 年 9 月開始提供名為「Open Canvas」的開放銀行平台，除了 API 的管理平台以外，也提供 API use cases、外部公用雲及公共/企業網路的安全連接協助等等顧問型的服務，並定期舉辦論壇為金融機構、金融科技公司/外部營運商(external operators)提供媒合機會。

目前已有 59 間的 TSP 註冊，和銀行端的開放情況一樣，都有集中化的趨勢。前五名就佔據了 75%的市場份額，其中 Money Forward 以 35 個合作夥伴關係領先，其次是 Zaim、Money Tree、free 以及 Nest Egg；除此之外，市場上還有 34 間 TSP 並沒有簽訂任何協議，表示有 57%的業者加入開放銀行架構中卻找不到銀行合作，本研究認為這是台灣在發展上務必要注意的議題。

(五)、資安標準

日本在資安的衡量方法主要是依據日本的「公營財團法人金融訊息系統中心(The Center for Financial Industry Information Systems ,簡稱

FISC)」所公布的「API 連接檢查清單(API 接続チェックリスト)」[118] 。而清單中提到須遵守的規範如下第二點所列。

1. 規範依據：JBA”Report of Review Committee on Open APIs”、FISC Security Guidelines
2. OAuth 2.0

九、 中國

中國和美國一樣都是由市場驅動的模式來發展開放銀行，而政府方面尚未建立相關規範，然而根據中國互聯網金融協會針對 51 間商業銀行的調查發現，有 65%的銀行業者已建立起 API 開放平台，並各自和 TSP 業者合作。有鑑於市場上出現開放銀行的趨勢，中國互聯網金融協會在 2019 年 12 月發布《開放銀行發展研究報告》，探討中國開放銀行的現狀與未來發展[119]。

根據中國互聯網金融協會的報告，早在 2003 年淘寶推出支付寶服務時，各家銀行就陸續開放 API 與其串接；2013 年中國銀行推出中銀開放平台並開放串接 1600 多個 API；到了 2018 年許多銀行陸續表態將發展開放銀行，包括浦發銀行、工商銀行、招商銀行和建設銀行等等。銀行業認為開放銀行包含了「走出去」和「引進來」，不只是自家的金融商品能夠走進消費者的生活，也要讓其他業者的商品引入自己的生態圈。由此可見，政府勢必要加快腳步制定規範，包括開放甚麼、開放給誰、如何開放等等，才能夠滿足銀行業的發展趨勢[120]。

[118] https：//www.trustbind.jp/security-information/api-security/webapi.html
[119] 開放銀行研究報告，中國互聯網金融協會，2019
[120] 開放銀行研究報告，中國互聯網金融協會，2019

表 12 中國開放銀行法源與做法[121]

(1) 法律依據	無，目前中國的主管機關或是公會並沒有建立開放銀行的政策以及自律規範
(2) 主管機關	中國人民銀行為目前開放銀行的主導機構，曾於 2019 年 9 月發布《金融科技發展規劃》，成為中國金融科技基礎。
(3) 具體作法	中國開放銀行屬於市場驅動，早在 2003 年淘寶推出支付寶服務時，各家銀行就陸續開放 API 與其串接，一直到 2019 年中國政府才開始正式研擬相關規範。除了上述的中國人民銀行，中國互聯網金融協會(由中國人行、銀保監會、證監會、工信部、公安部、工商總局等等 10 部委聯合要求而成立的國家及互聯網金融行業自律組織)也在 2019 年 12 月發布《開放銀行發展研究報告》，報告中除了調查目前市場上的 API 開放狀況，更呼籲政府必須要盡快建立相關標準，以利市場發展。

(一)、監理規範

目前中國的主管機關或是公會並沒有建立開放銀行的政策以及自律規範，只有一些研究報告提到開放銀行的概念並呼籲政府建立相關標準，例如上述中國互聯網金融協會的《開放銀行發展研究報告》，以及中國人民銀行在 2019 年 9 月發布的《金融科技發展規劃》。

(二)、 API 開放範圍

由於中國屬於市場驅動的發展模式，因此要開放那些 API、開放給誰使用都是銀行業者自行決定，在推動開放上不是從消費者賦權的角度出發，反而更偏向於商品和服務的角度。目前市場上開放的 API 種類包括銀行資訊、消費者帳戶及企業帳戶、借貸、支付、投資和財富管理，以及外匯交易[122]。

(三)、開放的產業

目前中國只有銀行業有開放 API，其中包括中國工商銀行、中國銀行、中國光大銀行、上海浦東發展銀行、中信銀行、中國民生銀行、江蘇銀行、深圳前海微眾銀行、四川新網銀行、重慶富民銀行、中信

[121] 本研究金融科技研究中心整理
[122] Build the future of banking service, BIAN

百信銀行以及京東數科，都將開放銀行納為發展策略並持續實踐當中[123][124]。

(四)、參與者類別

由於中國的開放銀行是以銀行作為發動主體，並且搭配金融科技業者，共同打造許多種類的場景平台。圖 13 整理了中國的市場現況，可發現其實參與的業者並不多，有一部分原因是因為銀行雖然同意開放 API 給 TSP 串接，但中國的銀行業者並不擅於透過場景來聯想服務並找到合適的合作對象，在建立合作關係方面的主導能力不夠強大，也因此導致 TSP 以及實際推出的服務並不算太多[125]。



圖 13 中國開放金融市場現況[126]

(五)、資安標準

2020 年 2 月 13 日，中國人民銀行發佈了《商業銀行應用程序接

123 http：//www.woshipm.com/evaluating/3171726.html
124 開放銀行研究報告，中國互聯網金融協會，2019
125 https：//insights.thoughtworks.cn/open-banking-china/
126 https：//www.analysys.cn/article/detail/20019586

口安全管理規範》(JR/T 0185 - 2020)金融行業標準，作為中國開放銀行的標準參考。[127] 標準規定了商業銀行 API 的類型與安全等級、安全設計、安全部署、安全集成、安全維運、服務終止與系統下線、安全管理等安全技術與安全保障要求。

此份規範比較像台灣開放銀行的資訊安全規範，有明訂相關銀行與 TSP 必須執行的相關資安作業。另外，按照《規範》中，可將 API 分為三種類型：內部 API、企業 API 與外部 API。

1. 內部 API(Private APIs)指銀行內部系統間的 API，促進了業務系統間的資訊互通，僅供銀行內部使用；
2. 企業定制 API(Partner APIs)指銀行與特定合作夥伴之間定制集成，目標是支援特定的業務流程或產品的 API，甚至使用私人網路絡進行通信；
3. 外部 API(Public APIs)指銀行廣泛地向應用方提供標準介面，供外部合作夥伴使用的 API。較前兩類 API 更深入、更廣泛地向外部合作者提供服務。外部機構可通過互聯網管道，調用外部 API，獲取商業銀行提供的各類金融業務場景服務。

第四節 國外開放銀行案例

根據英國 OBIE 官網資訊，目前英國的開放銀行 TPPs 可大致區分為面向中小企業、面向消費者等兩大客群，並且將其分為以下類型，如下

[127] 商業銀行應用程序接口安全管理規範，中國人民銀行

表 13、表 14[128]。

[128] 此兩表取自黃柏堯，碩士論文 working paper,(2021)。整理自 https://www.openbanking.org.uk/app-store/

表 13 OBIE 分類的開放銀行應用場景-企業

帳戶存取與稅務 負債管理	存取帳戶以及交易資料，管理稅務、債務
借貸	迅速評估借款者的帳戶歷史與還款能力
現金流管理	提供當前與未來的現金流觀點，推薦適合的金融商品
數位支付	提供即時付款服務，而非傳統的卡式交易
SME 財務顧問	自動執行傳統的財務功能，例如發票管理、薪資管理、追蹤付款，並進行現金流預測
資料分析與存取管理	將財務數據進行分類與分析，並控制存取全線以及投資決策
身分驗證	確保資料共享的安全，以執行反洗錢、詐欺偵測和 KYC

表 14 OBIE 分類的開放銀行應用場景-消費者

銀行帳戶總覽	讓消費者能夠在單一介面瀏覽不同銀行的帳戶
負債建議	讓消費者不必提供過去詳細的金融紀錄，即可獲得適當的負債建議；另外也可以協助制訂彈性的還款計畫
投資顧問	透過個人資料的取得，可以給予客製化的投資建議，另外也可以做到自動投資。
抵押申請	將抵押流程數位化、無紙化，可減少決策時間
慈善捐款	將消費者的每日消費連結至慈善捐款
金融保全	提供消費行為異常的偵測以及警示系統
借貸 自動透支借貸	貸款方可以取得借款方的帳戶歷史資料，以加速借貸流程並降低成本，並提供自動透支借款，避免消費者被收取高額的透支費用。

消費顧問	分析日常消費，另外可依據預算提供消費計畫或是商品建議。
信用評等	信評公司可以取得更完整的消費者資料，藉此改善信用分數並且讓整個過程更加透明化
外匯交易	更容易取得較佳的匯率
自動小額儲蓄	自動將帳戶內的錢移轉至較高利率的商品，並且將每日消費後的剩餘金額投入存款或是投資帳戶
產品比較	依據消費者狀況找到最適商品

由於目前台灣開放銀行 API 開放範圍主要是以帳戶(account)為主，支付(payment)部分則有待第三階段推出，且因核身機制等原因，尚未開放中小企業運用開放銀行 API。故本研究將針對以上三項常見情境提供說明，並列舉部分代表供我國參考，以下分類為本研究中心參考英國 FCA Call for Input: Open finance 整理 。

一、 帳戶類型情境

個人理財管理(Personal finance management,PFM)仍是開放式銀行業務實踐中最常見的情境。其中又可以依據其所獲取資訊，提供不同的相關服務情境。

1. 財務訊息彙總:

   消費者透過開放銀行將多間銀行帳戶的資訊整合至單一瀏覽平台，提高客戶對其財務狀況的瞭解/參與度。這可以讓他們節省更多或更好瞭解他們的支出。提供消費者財務狀況總體資訊的服務，減少財務顧問瞭解消費者情況所需的時間和精力。

使用的 API 項目:

Read: 產品功能、消費者資訊、使用資訊

代表業者: Mint,Revolut,Numbers

2. 智能轉帳管理:

這類商品多半搭配前項情境，提出替代產品建議或協助切換到替代產品，並協助帳戶之間轉帳，協助消費者做出更好地滿足其需求的決策，例如如何在現金之間分配儲蓄，便於使用。或是協助消費者自動化處理其規律性的轉帳活動。

使用的 API 項目:

Write: 產品服務轉換、服務開關、產品的銷售兌換及購買

代表業者: Asto,Plum

3. 貸款評估、信用評等:

顧客不再需要調閱各項資訊，銀行或其他放貸機構可以在消費者同意下直接調閱其金融資訊或信評資料等。改善了流程及資料來源等機制，放貸機構更為相信相關資訊，因而大幅度提升效率及消費者體驗，提高信用度/可負擔性/資格的檢查效率。

使用的 API 項目:

Read: 可以存取消費者財務餘額/交易資料和其他收入、產品資料和過去使用紀錄、消費者資訊。

Write: 進行付款或是轉移餘額、切換產品、調整信用額度等

代表業者: TALA、Credit Passport (CRIF)、iwoca、Funding Options

二、 支付類型情境

透過 API，可將支付服務內嵌於消費情境，有效提升客戶體驗同時增進數據蒐集與分析。支付場景目前可大致分為以下幾項:

1. 白牌支付系統:

   提供無商標的支付系統，供不同的通路業者使用。這類公司往往專注於技術底層及串接通路，並交由專屬通路商進行相關行銷規劃。

   代表業者: fire

2. 支付獎勵導購:

   串聯銀行帳戶、信用卡帳戶進行支付，並以點數、現金回饋等方式鼓勵消費者購買特定商品或服務。常見與利益團體(環保組織、宗教組織等)或特定店家聯盟等合作。

   代表業者: koinrewards、loyalBe、pledjar

3. 跨境轉帳:

   透過 Openbanking、PSD2，協助消費者跨境無縫進行支付、轉帳、匯款。

   代表業者:Revolut、TransferWise、

4. 跨通路收款整合

   整合企業、店家以及所有角色，利用 API 串接收款，強調在各種支付場景下均可提升體驗。通常這類業者會強調其服務可以輕易地嵌入中小企業現行的服務內，協助其金流建置。

   代表業者: adyen、Stripe、citizen

三、 中小企業相關情境

開放銀行下常見面向中小企業的情境，多半是基於財務資訊的整

合、分析。並且針對自身及客戶進行進一步的身分認證服務。

1. 帳務財務彙總:

   開放銀行協助公司可以一站式的查詢所有帳戶，幫助公司更快速的了解其財務狀況，並協助公司做財務相關決策。

   代表業者: DirectID Insights、Ordo、Vat Direct

2. 自動化會計:

   將財務、會計、審計模式直接連接到中小企業銀行帳戶，在極短的時間內管理會計報表，或填寫相關表單(稅務、商品申請)。

   代表業者:Circit、Audapio、Armalytix、QuickFile、Reckon One

3. 信評借貸能力:

   利用開放銀行存取企業的金融資訊，更快地做出更精準決策，同時簡化信評、放貸流程，協助中小企業取得放貸或相關信評需求。

   代表業者:MyBuget、Credit Kudos、Creditspring、Affordability Passport

第三章 台灣開放銀行發展剖析

目前台灣開放銀行，已經進行到第二階段。金管會於 2020 年 6 月 24 日核備了開放銀行第二階段的相關文件。政治大學金融科技研究中心也在 2020 年 4 月與 5 月先後完成了開放銀行 TSP 第二階段輔導說明會，其中針對技術標準與資安標準相關文件分析，並以此為基礎設計針對合規 TSP 的輔導計畫。

第一節 台灣開放銀行發展分析

2019 年 6 月，金管會拍板定案，台灣比照香港採用以不修法、不強制的模式，由銀行與第三方業者合作推動，並將開放銀行推動進程分成 3 大階段：[129]

- 第一階段：公開資料查詢。目前已開放業者測試，如比價網之類的第三方平台，可透過 API 串接各銀行的商品資訊，像是定存利率、貨幣匯率、房貸利率等，民眾可直接在網站中，比較各銀行的利率。
- 第二階段：消費者資料查詢。包含帳戶開戶與附屬業務申請、信用卡及附屬業務申請、消費者個人資料查詢等。用戶可以將個人資料打包帶走，例如在 A 銀行填寫過的個人金融資料，可以直接拿去申請 B 銀行的戶頭，不必重複填寫資料。
- 第三階段：交易面資訊。包含貸款清償、扣帳授權等。用戶可以透過第三方業者的 App，直接連結帳戶扣款、消費支付，以及整合不同帳戶的資金。

針對開放銀行的推動，金管會已委託財金公司(前身為財政部設

[129] https：//www.bnext.com.tw/article/55095/global-open-banking-taiwan

立的「金融資訊服務中心」，後改制為「財金資訊公司」)，協同銀行和第三方業者參與討論，並交由財金公司制訂 API 標準，圖 14 整理出財金公司 2020 年 5 月 26 時公布之推動進程。

第一階段的 API 已由財金公司在 2019 年 6 月間，完成第一階段技術與資安標準制定，統合 13 家銀行與業者需求，訂出通用的 API 規格。根據財金公司公佈的規格，第一階段開放的 API 總數有 18 支，而 API 類型分成存款、貸款、投資理財、其他銀行服務四大類。至於開放銀行第二階段「消費者資訊查詢」，已於 2019 年 12 月完成技術與資安標準制定，並在 2020 年 6 月核備[130]；第三階段「交易面資訊」，依原訂時程則會在第二階段實施 6 個月後，完成技術與資安標準訂定。

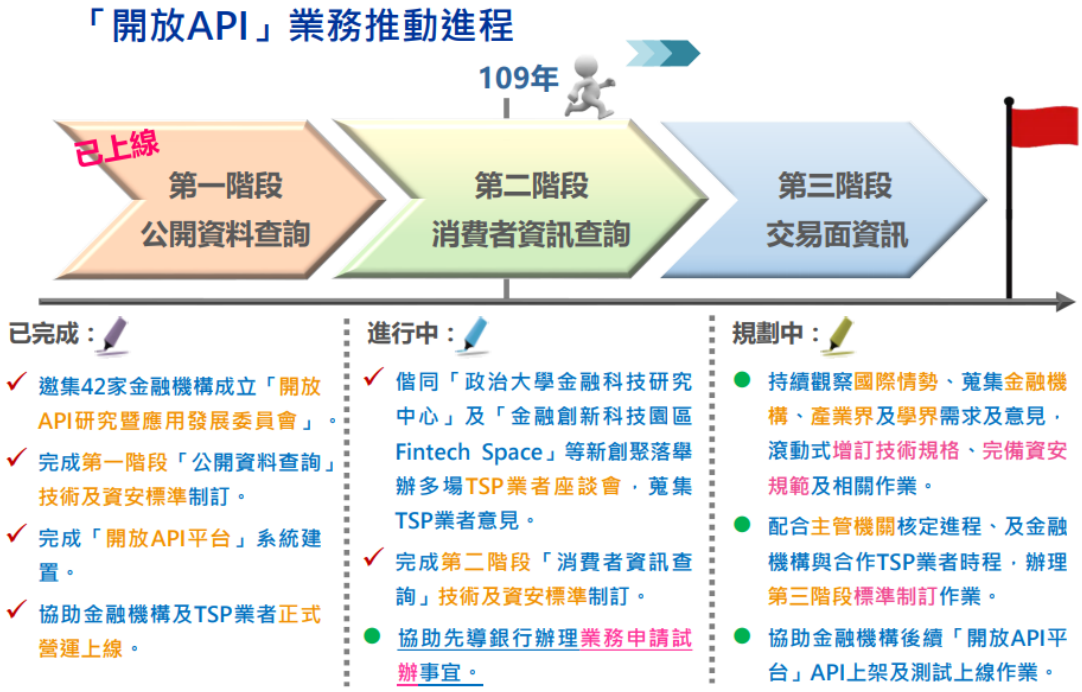


圖 14 「開放 API」業務推動進程[131]

[130] 根據財金公司所提出的《開放應用程式介面(Open API)技術標準規格文件 V1.0》及《開放應用程式介面(Open_API)技術標準規格文件 V2.2》，我國第一階段公開資料查詢總計 18 支 API，第二階段消費者資訊查詢開放總計 18 支 API，並另提供 4 支 API 規格供銀行與 TSP 進行認證授權使用。

[131] 財金公司，2020 年 5 月 26 日政治大學金融科技研究中心 OPEN API 技術合規與測試說明會，http：//www.ftrc.nccu.edu.tw/wordpresseng/?p=10997。

因第二階段「消費者資訊查詢」涉及使用者個人金融資訊，財金公司為穩健辦理業務營運事宜，擬透過金融機構進行業務核備與試辦，以實證第二階段之自律規範、技術及資安標準，並將實證結果陳報主管機關據以參考，以進一步落實金融科技創新成果，並加速金融產業與科技新創業者之媒合。[132]

第二節　台灣開放銀行法令基礎

目前台灣開放銀行在推動上，銀行與 TSP 與銀行合作關係是以銀行公會的「銀行與第三方服務業者合作自律規範」(以下簡稱為自律規範)為依據，而此自律規範的條文又以「金融機構作業委託他人處理內部作業制度及程序辦法」為基礎，因此台灣開放銀行的推動是將 TSP 定位於銀行委外合作關係，整體生態系的架構如下圖所示。

- 銀行與TSP合作，基於：
  - **銀行與TSP合作自律規範**
- 自律規範中提到
  - TSP必須和銀行簽定**合約**
  - TSP必須符合技術與資安標準
  - TSP必須符合ISO 27001或相當認證
- 二個標準
  - 技術標準：**Open API技術規格文件**
  - 資安標準：**業務安全控管作業規範**

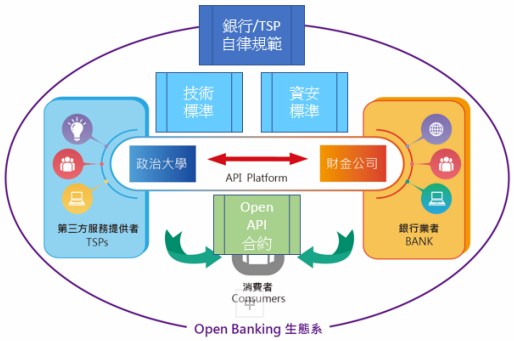


圖 15 台灣開放銀行推動架構[133]

在此自律規範第三條第一款中定義：” 第三方服務提供者：係指與會員銀行簽署業務合作契約，透過開放應用程式介面取得會員銀行金融產品及服務資訊、金融往來資訊暨申請金融產品及服務的業者。

[132] 財金公司，財金公司，2020 年 5 月 26 日政治大學金融科技研究中心 OPEN API 技術合規與測試說明會，http：//www.ftrc.nccu.edu.tw/wordpresseng/?p=10997。

[133] 政治大學金融科技中心整理

”因此，TSP 與銀行合作必須簽訂業務合作契約。另外，在第四條第四款明訂：”第三方服務提供者應符合會員銀行與第三方服務提供者業務合作應適用之開放應用程式介面技術標準規格及業務安全控管作業規範”。由自律規範可以明確了解 TSP 與銀行合作前必須先確認通過相關技術與資安標準，才能與銀行簽訂合約進行開放銀行情境的合作。

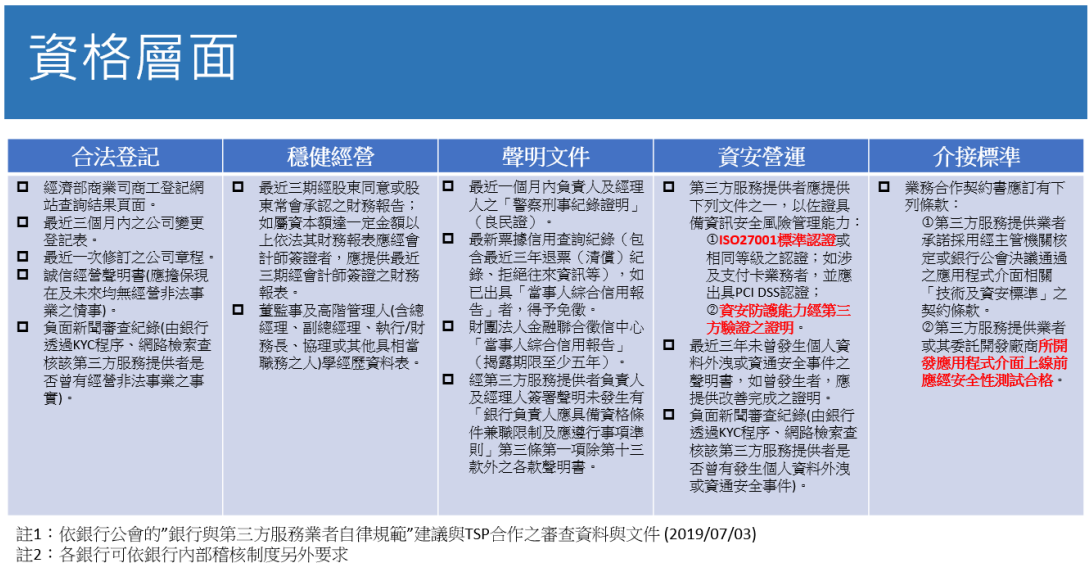
除此之外，依據自律規範第四條第三款：”第三方服務提供者應具備網路安全與資訊控管之風險管理能力”，以及第九條：”會員銀行與第三方服務提供者業務合作時，應訂定有關內部控制制度及稽核程序之內部規範。”這二條在實務上，TSP 必須提出 ISO 27001 或由銀行認可之相同等級驗證，才能符合自律規範的條件。

而針對消費爭議處理機制，在自律規範的第十條也明訂”消費者與第三方服務提供者或會員銀行發生消費爭議時，會員銀行應提供消費者申訴管道，並應提供消費者協助，以妥適處理消費爭議。會員銀行應與第三方服務提供者約定，如消費者向會員銀行提出因其與第三方服務提供者所生之消費爭議而受有損害者，除會員銀行得證明消費者有故意或過失者外，於一定金額內由會員銀行先償付消費者，再依業務合作契約之約定向第三方服務提供者求償。”

而彙整自律規範各項要求，銀行公會有提出第三方服務業者必須提出如下

表 15 的申請資格文件供銀行審查

表 15 台灣銀行與 TSP 業者合作之建議審查資料與文件[134]



資格層面

合法登記	穩健經營	聲明文件	資安營運	介接標準
◘ 經濟部商業司商工登記網站查詢結果頁面。 ◘ 最近三個月內之公司變更登記表。 ◘ 最近一次修訂之公司章程。 ◘ 誠信經營聲明書(應擔保現在及未來均無經營非法事業之情事)。 ◘ 負面新聞審查紀錄(由銀行透過KYC程序、網路檢索查核該第三方服務提供者是否曾有經營非法事業之事實)。	◘ 最近三期經股東同意或股東常會承認之財務報告；如屬資本額達一定金額以上依法其財務報表應經會計師簽證者，應提供最近三期經會計師簽證之財務報表。 ◘ 董監事及高階管理人(含總經理、副總經理、執行/財務長、協理或其他具相當職務之人)學經歷資料表。	◘ 最近一個月內負責人及經理人之「警察刑事紀錄證明」（良民證）。 ◘ 最新票據信用查詢紀錄（包含最近三年退票（清償）紀錄、拒絕往來資訊等），如已出具「當事人綜合信用報告」者，得予免徵。 ◘ 財團法人金融聯合徵信中心「當事人綜合信用報告」（揭露期限至少五年）。 ◘ 經第三方服務提供者負責人及經理人簽署聲明未發生有「銀行負責人應具備資格條件兼職限制及應遵行事項準則」第三條第一項除第十三款外之各款聲明書。	◘ 第三方服務提供者應提供下列文件之一，以佐證具備資訊安全風險管理能力： ①ISO27001標準認證或相同等級之認證；如涉及支付卡業務者，並應出具PCI DSS認證； ②資安防護能力經第三方驗證之證明。 ◘ 最近三年未曾發生個人資料外洩或資通安全事件之聲明書，如曾發生者，應提供改善完成之證明。 ◘ 負面新聞審查紀錄(由銀行透過KYC程序、網路檢索查核該第三方服務提供者是否曾有發生個人資料外洩或資通安全事件)。	◘ 業務合作契約書應訂有下列條款： ①第三方服務提供業者承諾採用經主管機關核定或銀行公會決議通過之應用程式介面相關「技術及資安標準」之契約條款。 ②第三方服務提供業者或其委託開發廠商所開發應用程式介面上線前應經安全性測試合格。

註1：依銀行公會的"銀行與第三方服務業者自律規範"建議與TSP合作之審查資料與文件 (2019/07/03)
註2：各銀行可依銀行內部稽核制度另外要求

第三節 台灣開放銀行業務限制

透過檢視自律規範，並訪談參與開放銀行的多家銀行與 TSP 業者，可以發現目前台灣開放銀行在業務上有以下限制：

一、銀行篩選 TSP 限制

台灣的 TSP 並無英國開放銀行的註冊制，並非透過申請或註冊方式取得成為 TSP 的資格，而必須透過銀行篩選後才能加入，導致銀行責任過大且須負責把關 TSP 業者資格，無形中限制了 TSP 和開放銀行生態圈的發展。以英國而言，TSP 可以 AISP、PISP 或金融科技公司不同角色註冊申請，註冊作業過程明確清楚。銀行和消費者可以從單一窗口確認 TSP 業者之資格與核可範圍，有助於健全開放銀行生態系。

[134] 政治大學金融科技中心整理

二、篩選條件的不明確

在自律規範第四條會員銀行對合作之第三方服務提供者遴選原則中，銀行在 TSP 的遴選原則除了要符合一定資安能力，另有兩個原則：(1). 第三方服務提供者應為合法登記之法人組織，其實收資本額或營運資金應與其業務合作規模相當，且不得經營非法之營業項目；以及(2). 第三方服務提供者或其經營團隊應具備穩健經營之能力、適足之經驗及專業能力。

除了金融科技公司外，其它如電信業者、徵信業者和第三方支付業者等也想加入生態圈，但不同業者因產業不同，公司的營業項目、資本額亦大不同，自律規範中因欠缺更明確的規範，會導致銀行可能傾向與大型產業如電信公司合作，不利於金融科技新創業者的合作。

三、銀行僅為資料提供角色

在自律規範中的定義中，第三方服務提供者係指與銀行簽署業務合作契約，透過開放應用程式介面(API)取得會員銀行相關資訊的業者。在此一定義下，TSP 被定義為資料接收者的角色，並無資料提供者的角色。也因此，目前台灣開放銀行的應用情境大部份是透過 TSP 取得消費者在銀行端的現有資料。

四、無資料交換的應用情境

依目前自律規範僅在第七條第三段中有提到”第三方服務提供者不得將消費者之資料再提供予第三人，但經消費者同意提供予其他會員銀行申請金融產品及服務者，不在此限”。目前台灣開放銀行的應用情境應用僅考慮單一方向的資料交換，並未考慮銀行進件/收件時的合作情境，僅提供了銀行可以透過 TSP 互換資料的可能性。

因此，在單一方向的資料交換，銀行是資料提供者，消費者資料

是由銀行交給 TSP 端，可能衍生較高資訊風險環境，造成銀行對於小型的 TSP 合作意願不高，不利整體金融科技創新。

第四節 台灣開放銀行資安要求與問題

台灣開放銀行的二份標準文件，分別為技術標準—Open API 技術規格文件(簡稱 API 規格)，以及資安標準—業務安全控管作業規範(簡稱安控規範)。針對台灣開放銀行資訊安全要求，主要是以資安標準的安控規範為主；再搭配技術標準的 API 規格中，有關訊息簽章與加密的保護。

首先探討安控規範中的各項條文。安控規範文件可分為五個章節如下圖：

章節	內容摘要
一	明定本作業規範之法源依據、適用對象與範圍、用詞定義。
二	(安全控管要求) 消費者註冊時之身分確認安全設計、消費者資訊查詢之身分確認安全設計、網路型態與其安全設計、設計原則之共通要求與各類安全要求。
三	(資訊系統標準) 應訂定組織、人員及設備安全之相關管理措施；應就機房、營運、網路、金鑰、系統生命週期、資安事故、營運持續管理等採取資訊安全維護措施。
四	(配套監理措施) 應於業務申請時及其後每年由[redacted]進行檢視，提出「資訊系統及安全控管作業評估報告」。 公正第三方
五	明定本作業規範施行日期。

圖 16 業務安全控管作業規範[135]

第一章為定義說明。第二章主要規範是安全控管要求，此章在說明開放銀行的資訊架構，其中包含了 TSP 端資訊架構與資安要求、與銀行端的連線架構與資安要求，以及銀行端對於消費者的身份認證作業。第三章主要規範是資訊系統標準，此章在呼應銀行自律規範中的 TSP 必須具備網路安全與資訊控管之風險管理能力。基本上，此章的

[135] 政治大學金融科技研究中心整理

條文也是對應到 ISO/CNS 27001 的管理需求。第四章則是銀行的配套監理措施，TSP 被要求每年必須進行內部自檢稽核一次，並配合銀行與主管機關不定期的外部稽查作業。

而安控規範的第二章內容，以下列簡易資訊示意圖說明：

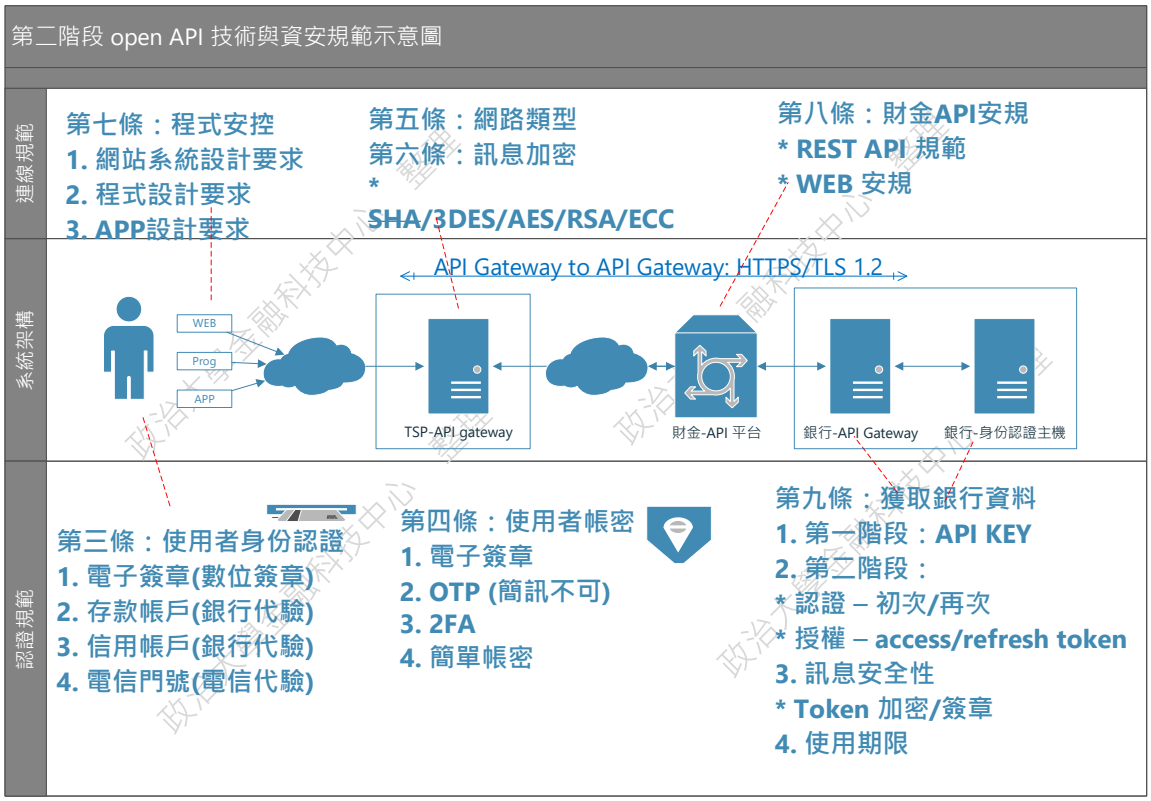


圖 17 第二階段 open API 技術與資安規範[136]

由於在第二階段涉及使用者個人金融往來資訊，因此在資訊安全的規範與要求上，針對身份認證與授權作業有詳盡的規範，整個開放銀行的資訊架構也相對完善。財金公司研究指出第二階段金融機構與 TSP 之間的技術運作方式，主要有三大重點，訊息處理、憑證作業和認證機制的要求。[137]

在訊息處理部分，因應各金融機構 OAuth 處理機制不同，同時為簡化連線方式，OAuth 訊息由 TSP 業者直連金融機構。而 API 訊息

136 政治大學金融科技研究中心整理
137 本研究說明會，內容引用：https：//www.ithome.com.tw/news/137909

則由 TSP 業者介接財金後，再由財金轉接金融機構。

在憑證作業部份，銀行、TSP、財金公司端皆採用 TLS 雙向認證，而雙向認證會用通訊憑證辦理。所以，當 TSP 與金融機構簽署合作並完成註冊時，金融機構將先取得 TSP 通訊憑證。而金融機構 API 訊息如果是經由財金公司介接，則須提供銀行通訊憑證與先前取得的 TSP 通訊憑證給財金公司，做雙向憑證設定。接下來，財金公司將提供通訊憑證給金融機構，金融機構再將財金通訊憑證交付給 TSP 業者。

而根據安控作業規範，在認證機制上，TSP 業者的代理存取端與金融機構的資源伺服器或授權伺服器間，應建立認證機制。要遵循 TLS 雙向認證或是以簽章的 JSON Web Token(JWT)作認證，採用憑證者，則要驗證憑證的正確性與有效性。另一個是，要用事先設定的來源網路位置(IP)正面表列管制。

在財金公司規劃的重點中，欠缺了對消費者身份認證的作業。造成欠缺身份認證作業的主要原因有二。第一、是財金公司是依國際標準採用 OAuth 2.0 作為授權(authorization)作業，但在 OAuth 2.0 中本身就欠缺身份認證(identity authentication)的作業，這也是英國採用了 OIDC (Open ID Connect)作業身認證的機制補強的原因。第二、雖然台灣現行有自然人憑證作為電子身份認證，但台灣銀行業目前並未有規定的第三方認證機構或方式，自然人憑證僅可作為金融業做為業務申請的依據，且採用自然人憑證核身對於使用者體驗影響甚鉅。

根據財金公司的規劃，消費者的身份認證與授權是由 TSP 透過導向至銀行後，由銀行端負責。因此，在整個資安要求上，身份認證會連結至消費者賦權的議題上。因此，這邊先簡述身份認證對於開放銀行商業模式上的不便進行說明。

一、身份認證

以現行作法，消費者必須是銀行的現行客戶才能由銀行進行身份認證。第一、身為現行客戶部分，消費者透過 TSP 取得消費者在銀行端的現有資料，身份認證是由銀行端進行。但由於身份認證是由個別銀行認證，消費者如有多個帳戶，必須一一登入確認，對於使用者體驗會造成很大的不便。第二、如果消費者如果想透過 TSP 傳送個資給銀行，在目前的銀行作業規範是否可以接受第三方的外部 eKYC 作業，另外個資的資安責任歸屬並未在現行自律規範或安控規範中規範。

二、第三方身份認證

在現行安控規範中，TSP 已有規定對消費者進行身份認證，但並未確認如何落實。以銀行進件(例：信用卡申請)，對新客戶部分，銀行必須信任 eKYC 流程中由 TSP 透過第三方身份認證(如：透過台網、集保、電信業者 Mobile ID 或 FIDO)之核定。在 eKYC 流程上，銀行如何在消費者授權情況下，信任並接受由 TSP 傳來的資料是一個問題。

第五節 TSP 輔導方案與說明

自 2019 年 10 月第一階段上路後，金管會曾提出，對於敏感的資料開放要以銀行級的資安標準來要求。銀行公會和財金公司開始討論第二階段的相關技術與資安標準規範，並與十多家銀行討論，而政治大學金融科技研究中心也參與這個過程，深入了解銀行端對於 TSP 業者的要求以及顧慮。同時，也把這些顧慮納入至規範的 TSP 輔導範圍，讓新創公司能達到第二階段合規的要求。輔導的目標期望達到法令遵循(compliance)與介接一致(conformance)二個要求。



圖 18 台灣 TSP 合規範圍[138]

在協助 TSP 與銀行媒合的過程之中，本研究發現，第二階段的挑戰是，有些 TSP 業者與銀行談妥業務面、資訊面議題後，最後卻在法遵面失利，比如後續稽核，過不了銀行那關。所以，TSP 應從法遵面開始，先符合銀行要求的技術、營運與監理層面，再往下進行業務面的討論與資訊面的調整。「先求合規，再求合作。」讓 TSP 成為一個合規的第三方服務業者(Qualified TSP,QTSP)，再來與銀行談業務上的合作，如圖 18 所示。

而在 Open API 的法令架構上，銀行與 TSP 合作須基於銀行公會訂定的自律規範。目前自律規範中提到，TSP 必須與銀行簽訂合約、符合技術與資安標準、符合 ISO 27001 或相當認證。而在財金公司訂定的技術與資安標準中，銀行則要遵守 Open API 技術規格文件，以及業務安全控管作業規範。

在安控規範中已明確列出了銀行與 TSP 合作時的規則。其中，第一個是安全控管要求，包括消費者註冊以及資訊查詢時的身分確認安全設計、網路型態與其安全設計、設計原則的共通要求與各類安全要求。第二是資訊系統標準，要訂定組織、人員與設備安全的相關管理措施；應就機房、營運、網路、金鑰、系統生命週期、資安事故、營

[138] 政治大學金融科技研究中心整理

運持續管理等採取資訊安全維護措施。第三則是配套監理措施，需在業務申請時及其後每年由公正第三方進行檢視，提出資訊系統及安全控管作業評估報告。此部份，在執行層面上並無太大的問題，主要是投入成本的因素。

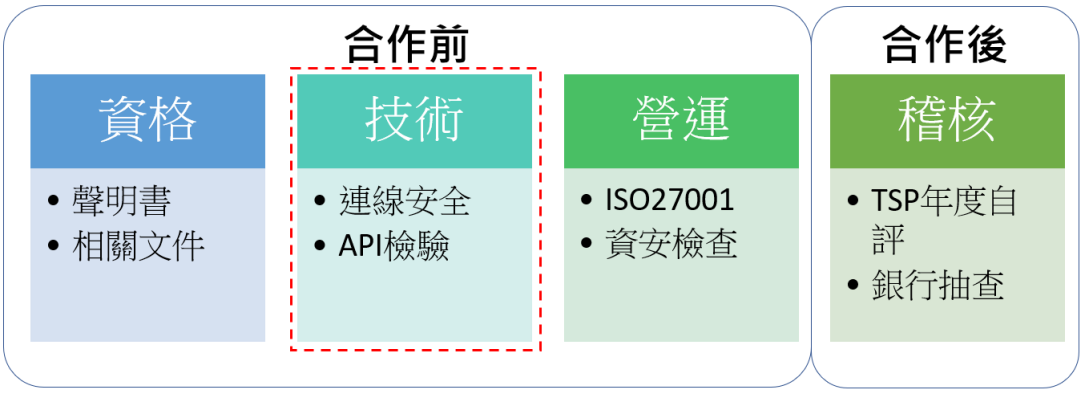


圖 19 台灣 TSP 合規項目[139]

在輔導規劃中發現，對 TSP 而言，在合規上，合作前有三大重點工作，包括資格、技術、營運，如圖 19 所示。在資格部分，必須是合法登記公司，具備穩健經營的證明，並提供聲明書與相關文件。在技術層面，包括連線安全、API 檢驗等項目都要合規，TSP 業者或其委託開發廠商所開發的應用程式介面，上線前要經安全性測試合格。而營運部分，TSP 業者則須提供 ISO 27001 標準認證或相同等級的認證，以及資安防護能力經獨立公正第三方驗證的證明。

與銀行合作後的合規重點則是稽核，包括 TSP 每年四前底前必須進行年度自行查核，以及銀行內稽抽查。在 TSP 內部稽核措施，本研究建議，先由原 ISO 27001 驗證單位進行檢視，並提供報告。而對於銀行內稽核抽查，本研究則建議由銀行視必要性委任其他單位，對 TSP 做外部稽核檢視。比如，可委託配合的會計師事務所，也可參考

[139] 政治大學金融科技研究中心整理

IASME[140]框架進行外部查核。

在 TSP 技術與資訊驗證部份，本研究也完成相關的合規標準，如圖 20 所示。



圖 20 台灣 TSP 技術/資訊驗證[141]

綜合以上各章節，可以發現台灣開放銀行在資安技術執行與落實上規範的很完整，但主要的問題集中在法令限制與商業模式不易推動上，下個章節就針對金融科技中心在輔導時觀察到的問題進行剖析。

第六節 TSP 輔導問題觀察

政大金融科技研究中心，在協助財金公司推動開放銀行時，與多家銀行與第三方服務業者有進行訪談與輔導。以下就幾個案例說明目前在推動台灣開放銀行的狀況。

[140] IASME 為英國成立的中小企業資訊確認聯盟，全文為 Information Assurance for Small and Medium Enterprises Consortium，IASME 的主旨在提供中小企業以及工作室一個資訊安全的評鑑確認機制，其中主要的二項工作為 Cyber Essentials 與 IASME Governance。Cyber Essentials 為對於中小企業資安的最基本要求，而 IASME Governance 為基於 ISO 27011 的中小企業的資安治理框架。詳細資料可至官網查詢：https：//iasme.co.uk/。

[141] 政治大學金融科技研究中心整理

案例一：

A 公司為國際金融科技公司，主要業務為信用卡比價，希望透過開放銀行 API 直接收集銀行信用卡資訊，因此一來可以省去至各家銀行網站用爬蟲收集資料的方式。該公司也願意配合台灣相關法令，通過 ISO 27001 的認證，但後來經評估，發現各家銀行對於可以提供的信用卡資料並未統一；就算通過法規的要求，仍必須要和各家銀行一家家簽約，對於業務的推動緩不濟急。

案例二：

B 公司為國內資本額超過上百億的上市櫃公司，已經有 ISO 27001 認證，想透過開放銀行 API 與銀行進行業務合作。在準備相關文件時，發現了各家銀行對於文件要求不同。如：以聲明文件中規定的負責人及經理人必須提供最近一個月內之「警察刑事紀錄證明」(良民證)，有些銀行認為一定要董事長，而有些銀行認定合作單位的最高經理人即可。另外，有些銀行認定 ISO 27001 必須重新認證，而有些銀行則採用現行認證即可。

案例三：

C 公司為金融科技新創公司，擁有客戶電話帳單相關資訊，想透過國外類似案例，與銀行合作針對金融小白提供小額貸款，但目前規範中銀行無法接外部的業務申請和相關的信評資料。

本研究彙整 TSP 在進行開放銀行生態系時所碰到的問題如下：

1. 法源關係：TSP 基於委外關係與銀行合作，在法源上不利開放銀行長遠發展。
2. 審查不易：台灣非註冊制，目前審查作業標準不一，TSP 必須

送件至各家銀行進行篩選，再由各家銀行進行審查，最後再由銀行內部會議決議後，再報部通過。

3. 開放資料不完整：台灣第一階段的開放銀行資料，在國際上有許多行銷案例可引用，但台灣各家銀行提供的資料品質不一，無法讓 TSP 利用以及和國際接軌。
4. 消費者賦權：台灣個資法不利於資料交換，資料交換無特定法源。
5. 資料交換：讓金融業者由資料提供者，同時也成為資料接收者，達到互利的生態圈。
6. 身分認證：現行開放銀行採用 OAuth 的身份認證流程作業，此作業係由銀行進行認證。在國外經驗，銀行必須相信外部第三方認證以利資料的交換，以提升消費者體驗。

整體而言，綜觀以上問題，可能會導致有些銀行以個資法保護資料義，不願意將客戶資料輕易給出，因此會要求 TSP 必須要達到銀行等級的資訊安全要求才會提供資料。其次，銀行僅為資料提供者，沒有進件類的業務合作，這也會導致銀行沒有馬上導入 open API 的利基點。最後，由於台灣的開放銀行是採用鼓勵性質，因此大型銀行會自行建立自己生態系，並不一定要加入 Open API，如此將較無法落實開放銀行想達成的普惠金融目的。

第四章 國外開放金融之新金融生態系

國際開放銀行的三大趨勢說明如下：

1. 由開放銀行發展至開放金融生態系

   雖然各國金融法制不盡相同，但都發現開放銀行必須整合銀行、保險、證券才能提供完整的金融服務。新加坡早在 2017 年的 MAS Playbook 就包含了證券/保險的 API，而英國於 2019/12 月提出開放金融徵求意見書，提出有關信評、借貸、保險、退休金、投資與非投資型儲蓄等應用場景。

2. 消費者賦權

   開放銀行是以消費者為導向的開放金融制度，因此在消費者同意下透過第三方服務業者獲得金融服務。而資料權是由消費者擁有，資料可在不同機構間交換，獲得更便利的金融服務，降低機構間資料處理成本。澳洲是最早提倡資料所有權議題的國家，透過修法提出 CDR。

3. 跨業資料共享

   澳洲在 2019 年通過 CDR，該法案包含金融、能源、電信以及其它產業資料的使用。透過各產業不同機構設定資料標準，而金融機構的 API 由 DATA 61 的三方機構制定實施。因此，金融機構資料透過規定的身份認證機制，在消費者同意下，可以進行跨業資料的交換，而澳洲規劃於 2020 年七月推動開放銀行 API。

以下章節將就這國際發展的三大趨勢進行說明，並透過與台灣現行法令或產業現況進行交叉分析。

第一節 新金融生態系對未來金融服務的影響

自 2015 年英國財政部(HMT)為促進零售銀行市場之競爭，首次提出 Open API 與 Open Banking 概念以來，英國一直都是國際上開放銀行領域領航者，經過五年的發展，目前英國的開放銀行體系已成為英國金融科技市場上最重要的創新驅動力，這是英國銀行 200 年以來，不曾出現的金融創新速度[142]。

英國 FCA 在開放銀行推行之初即設想了幾種服務，其整理及觀察如表 16 所示：

表 16 新金融服務發展進度[143]

先前設想服務已開發	非先前設想服務已發展	先前設想服務 仍在為發展或在早期階段
帳戶整合	普惠金融	自動產品轉換
帳戶資訊訪問告知貸款決策	對財務脆弱成員的保護	餘額轉帳管理(信用卡)
個人財務管理	法律扶助和福利支持建議	高帳戶餘額投資
中小企業財務管理	慈善禮品援助稅務追朔	現金流優化
使用 PIS 服務進行轉帳	多重 API 整合服務進入市場	利息最大化
		通路採用 PISP 支付
		CBPIIs[144]提供支付服務

開放銀行所帶來的驚人金融創新能量，吸引世界各國開始積極的投入。而目前幾大開放銀行領域領先國家則希望將開放銀行的創新能量擴及到整個金融產業。因此作為全球開放銀行的領航者之一，英國 FCA 在 2019 年 12 月 17 日率先的提出了 Call for Input： Open finance[145]，將開放銀行的資料共享原則擴展到更加廣泛的金融領域，包含存款、抵押擔保、消費信貸、投資、退休養老金和保險。

[142] https：//www.ithome.com.tw/news/127558
[143] https：//www.fca.org.uk/publications/calls-input/call-input-open-finance
[144] CBPII 全文為 Card Based Payment Instrument Issuers，為信用卡發卡機構。
[145] https：//www.fca.org.uk/publications/calls-input/call-input-open-finance

Call for Input： Open finance 中提到，在未來開放金融的架構下，消費者和企業都能夠放心的將數據存取權利託付給值得信任的第三方，從而獲得或是推廣更廣泛、細緻的商品以及服務；另外消費者也能夠確實掌握自己的數據資料，做出更好的決策[146]。報告中亦提出以下四種開放金融未來的場景應用。

1. 個人財務管理儀表板：財務管理涉及廣泛且多元的產業，包括現金、存款、投資、退休金等等，而這些財務資訊未來可能會聚集至同一個平台，為消費者提供一個整合性的財務入口。這就好比汽車的儀表板一樣，可以看到關於汽車狀態的所有資訊，讓消費者能夠確實掌握財務資訊，並做出更好的財務決策。
2. 自動轉換和更新:減少消費者和金融服務提供者之間的摩擦，讓消費者能夠獲得更符合自己需求的商品服務和價格，進而鼓勵消費者獲取更多的金融服務[147]。
3. 新的財務顧問和支援服務：在財務儀表板的基礎上，財務顧問能夠為消費者提供更全面的建議和服務。
4. 更精準的信用評估：第三方能夠全面審查現金流量，為企業和消費者確認合適的信貸商品，因此消費者能夠獲得更低的融資成本、量身訂製的貸款建議，也可以讓目前市場上無法貸款的消費者(例如社會新鮮人缺乏金融數據，導致銀行不敢借款，俗稱金融小白)用其他的方式來評估其信用風險，協助其獲取貸款服務。

[146] FCA (2019),Call for Input： Open finance.

[147] 原文 automating switching and renewals that remove friction and encourage shopping around. This could help consumers get a better deal and increase competition. Access to data could give customers more competitively priced quotations based on the product features they are most interested in.

由上述英國 FCA 提供的場景可發現，其實在開放金融體系下，追求的是資料的即時性以及全面性，主要原因為金融商品的交互作用性質太高，某一種商品的多寡漲跌都會產生截然不同的財務策略，因此唯有消費者全面且即時的掌握相關資訊，才能夠為消費者帶來極大化利益[148]。而為了達到全面性，未來勢必會出現一站式的大平台，讓消費者能夠在單一入口查看所有的資訊，以及各種相關的服務。

整合服務平台是開放銀行和開放金融下的重要經濟模式，能夠容納多種不同的服務供給者，加速消費者和供給者之間的互動並創造價值，具有媒合的關鍵功用。以開放金融的架構來看，服務提供者就像是金融業以及其他的 TSP，透過 API 串接形成一個巨大的平台，如圖 21 所示。這個平台可以是銀行建立、TSP 自建或是政府主導，但不論如何，消費者都能夠透過該平台精準地找到對應的服務來滿足需求。而平台之中最關鍵的環節就是身份辨識，必須建立一套每個參與者都能夠信任的身分驗證機制，也就是相信對方所做的 KYC，如此一來才能夠讓消費者的體驗最佳化，使用流程也會更順暢。

[148] Open finance ： shaping the future of financial services

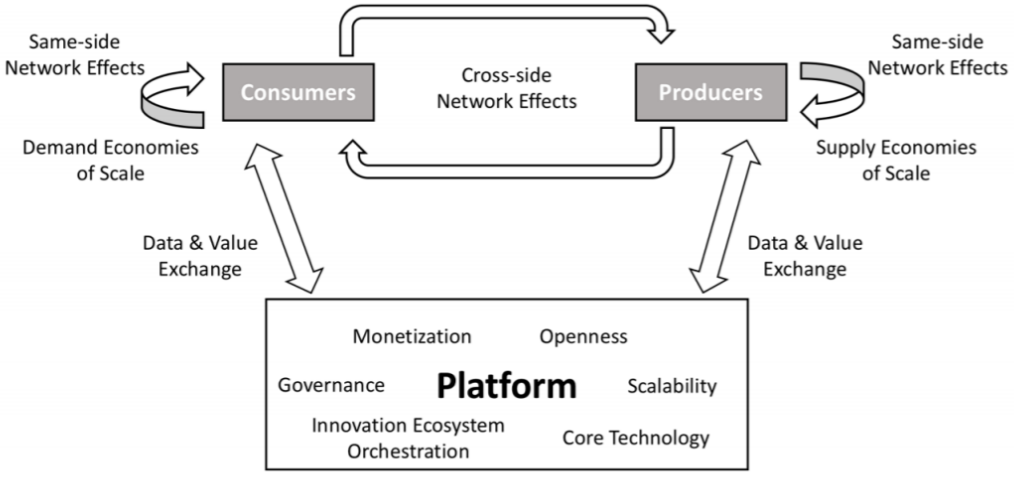


圖 21 平台經濟模式[149]

而在開放金融這種高度整合的空間，政府的監管就非常重要，上圖的平台中也納入了監視、管理等元素。要如何確保平台參與者的安全性是一大難題，是消費者產生信心的關鍵，但顧及安全性的同時又需要考慮不同角色之間的差異性，此外也必須注意不能因為過度規範而大幅降低消費者的體驗，這將會是開放金融發展中的一大難題，也是各家英國 TSP 在回應 Call for Input 時皆提及的重點。另外政府或是業者之間也必須要建立良好的溝通以及責任機制，當資料外洩、服務糾紛發生時，消費者究竟要聯繫哪個窗口，又該向誰求償，在跨業合作的情景下，爭端機制處理更加重要，這都是未來在開放金融生態圈下需要特別留意的問題。

除了資安風險以及安全性問題之外，開放金融體系下也需要注意是否會產生排擠現象。例如某間公司不願意加入開放行列，是不是會漸漸的被排除在市場之外，等於變相的潛在強制業者參加；又或者是當 Google、Amazon、Facebook 等國際級科技公司想要加入開放金融

[149] The book on open banking, Bud, 2018

市場時，是否又會挾帶龐大的網路資源直接壟斷整個金融市場，排擠掉原本存在於市場中的企業。

綜合來說，開放金融和開放銀行談的都是「整合」這件事，不只是商品、服務、產業需要整合，現存服務提供者、新服務提供者、企業用戶、消費者以及監理機關也都需要在這個生態系中整合[150]，才能夠建立全面的服務以及足夠的信任。而最終開放金融並不會只發生在金融業，而是以金融業為起點向外發散，能源業、電信業甚至是公部門都有可能加入。例如政府的退休金、能源和工業部門，或是各國政府在推行的智慧政府，都和開放金融息息相關。這正是開放金融的迷人之處，不同的角色與多元的產業在大熔爐，共同建構出嶄新的金融生態圈。

第二節 消費者賦權的發展與因應

隨著網路發展成熟，各式各樣的資訊都會被放到網路上，創造出資訊爆炸的時代。根據統計，人們每天通過搜尋引擎、email、網購、使用社群，產出 25 億 gigabytes 的資料量，龐大的數據量全部都被記載在服務提供者的手中，例如提供搜尋引擎的 Google、提供社群軟體的 Facebook，以及其他各式各樣的業者，都掌握著消費者的數據，藉此分析消費者的行為，進一步思考如何提升服務品質改善消費者體驗，這就是目前最夯的大數據。

但是，隨著越來越多的不肖業者發生資料濫用或是資安漏洞，使得消費者的權利意識不斷提升，開始會在意自己的資料是誰在使用、如何使用，希望自己能夠明確的知道並確實掌握，而這樣的概念其實就是消費者的「資料權」。

[150] From open banking to open financial service ： the long view

資料權在開放銀行中扮演極其重要的角色，甚至可說是發展開放銀行的首要基礎。開放銀行的核心理念在於將銀行的資料開放給 TSP 使用，這部分涉及到資料交換的議題，進一步連結到究竟是誰可以決定是否要交換資料，是消費者自己還是銀行? 消費者會認為這些資料都是與自己相關的，銀行只是代為保管，因此資料的掌握權在自己手中；而銀行此時業會反駁，消費者資料到了銀行會有許多分析、加工，例如信用分析、財務報告等等，主張這些資料的使用權利在銀行身上。

一旦無法明確界定資料權的主體是誰，那麼開放銀行在執行上就會面臨極大挑戰，當 TSP 來跟銀行串接資料時，如果銀行具有資料權，那銀行就可以拒絕 TSP 的請求，導致開放銀行形同虛設。若要讓開放銀行能夠順利運作，必須讓消費者成為資料權的主體，掌握資料的使用者、使用方式，這也就是本節要討論的「消費者賦權」的法令基礎的差異，探討國外消費者賦權的規範、目的、作業(包含消費者行使意權，進一步作為台灣修法或是配套的參考。

以下二個章節，會先分析國外消費者賦權的法令架構，透過五項：法律規範、資料使用範圍及目的、明示同意、資料交換機制以及資安規範進行說明。再來，透過同樣的架構進行台灣在消費者賦權的現況，由於台灣是以個資法為主要法令，因此會以個資法對台灣開放銀行進行差異分析之說明。此部份的差異是以行動研究法發現問題後，由政治大學金融科技研究中心的專家學者進行相關的研究之後摘錄而成。

一、國外消費者賦權法令分析

1. 法律規範

歐洲的 GDPR 和澳洲的 CDR 是消費者賦權的代表國家，將資料

權寫入法條當中，明定消費者對於資料具有可攜權與自主權。詳細說明請參閱本研究第二章第一節第三項。

2. 資料使用範圍及目的

歐盟 GDPR 第五條提到兩項重要的個資處理原則，分別為目的限制原則(purpose limitation)以及資料最少蒐集原則(data minimisation)。目的限制原則規定資料蒐集目的需特定、明確及合法正當，且不得為目的以外之進階處理；而資料最少蒐集原則是指處理個人資料應適當、相關且限於處理目的所必要。綜合以上兩條，GDPR 嚴格規定資料使用的目的必須「特定」且「必要」，防止業者濫用，同時在第 6 條也規定蒐集個人資料時確定使用目的並告知當事人，這也成為開放銀行中約束 TSP 和銀行的重要依據[151]。另外在 PSD2 中也有資料最少蒐集原則的規定，支付服務提供者只能夠在「必要」時接觸、處理及留存個人資料[152]。

3. 明示同意

依據 GDPR 第 7 條規定，同意必須是資料主體所為之具體、肯定、自由、明確且受充分告知及非模糊之指示；若為單純沉默或是預設選項為同意，均不構成同意。另外本條文也規定若資料之處理具有多重目的時，全部目的均應取得同意[153]，此規定類似於香港《個人資料(私隱)條例》第 2(3)條規定「同意不應為綑綁式同意」，表示業者不應該將所有使用目的強制打包，並要求消費者一次同意，必須讓消費者擁有拒絕無關使用目的之權利。由此可見，歐盟和香港將明示同意

[151] 歐盟「個人資料保護規則」導讀，蔡柏毅
[152] 變革中的金融科技法制，谷湘儀，臧正運
[153] 歐盟「個人資料保護規則」導讀，蔡柏毅

視作使用資料的最大前提，相較之下，台灣目前個資法在同意的規定，並沒有強制明示同意，仍有默示同意之適用空間[154]。

4. 資料交換機制

資料交換是開放銀行落地的基礎，可分為資料存取以及資料移轉，涉及層面相當廣泛，例如誰可以存取資料、哪些資料可以存取、移轉的機制、消費者同意權的行使方式等等，需要法令和技術規範互相配合才能夠建立一套共通的標準和監理架構。例如近年很常見的網頁爬蟲技術，屬於資料交換的一種，然而卻涉及了隱私權保護、網頁內容著作權歸屬以及網頁使用者協議等問題，另外還有可能會影響網站的運作，這些都屬於資料交換機制的一環。目前開放銀行是採用 API 來進行資料交換，在法律和技術的規範上和爬蟲所遇到的問題並不會完全相同，但資料存取以及資料移轉仍是如何實現資料交換的兩大關鍵。

5. 資安規範

根據 Royal Statistical Society survey 調查，70%的受訪者認為企業沒有足夠動機來保護消費者的資料，另外有 71%的消費者在確保資訊不會被隨意分享之後，願意提供更多資料，顯示出消費者對於保護個資安全的重視，唯有業者建立足夠強度的資安標準，消費者才會願意交付資料。以香港為例，香港金融管理局在 2018 年提出的 API 框架中認為銀行業應該提供最高強度的資安標準來控管，因此 API 框架附件 B 中列出各項流程的建議標準，另外也有載明消費者保護的要求，建立一套完整而詳細的資安規範，相關標準細節請參考第二章第三節第四小節。

[154] http：//www.leeandli.com/TW/NewslettersDetail/6028.htm

二、台灣個資法與開放銀行關係與問題

針對資料賦權或消費者賦權這個議題，透過分析現行台灣個資法與國際資料賦權中的差異，並針對台灣要利用 open API 這個平台，透過資料賦權進行資料交換時必須要考量的事項。

1. 法律規範

我國開放銀行個人資料保護的法令，基本上是基於「個人資料保護法」(以下稱為個資法)為主要的法源依據。

2. 資料使用範圍及目的

個資使用目的可根據個資法第一條：”為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。”

又，在第二條第一款中定義：”個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。”而個資法的適用範圍只要是個資的蒐集、處理、以及利用，都會適用個資法。

3. 明示同意

在個資法中第七條有明定”同意”必須經過當事人經蒐集者” 明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後”的表示之認同行為。而告知的事項必須包括：

(1). 公務機關或非公務機關名稱。

(2). 蒐集之目的。

(3). 個人資料之類別。

(4). 個人資料利用之期間、地區、對象及方式。

(5). 當事人依第三條規定得行使之權利及方式。

(6). 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

而其利用目的必須為個資法中特定目的的必要範圍，並符合以下情形：

(1). 法律明文規定。

(2). 與當事人有契約或類似契約之關係，且已採取適當之安全措施。

(3). 當事人自行公開或其他已合法公開之個人資料。

(4). 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

(5). 經當事人同意。

(6). 為增進公共利益所必要。

(7). 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

(8). 對當事人權益無侵害。

4. 資料交換機制

在台灣的個資法中並未明定資料交換的架構，但在本研究的研究中，現行的資料交換模式可用直接蒐集方與間接蒐集方來說明。直接蒐集方必須依個資法中的特定目的行使資料彙集的行為，而間接蒐集方則必須要滿足個資法第二十條的使用要件。在告知資料當事人使用目的後，就可以進行資料的蒐集。如下圖所示。

而所謂的特定目的地指定，也可以由法務部會同中央目的事業主管機關指定而定之。

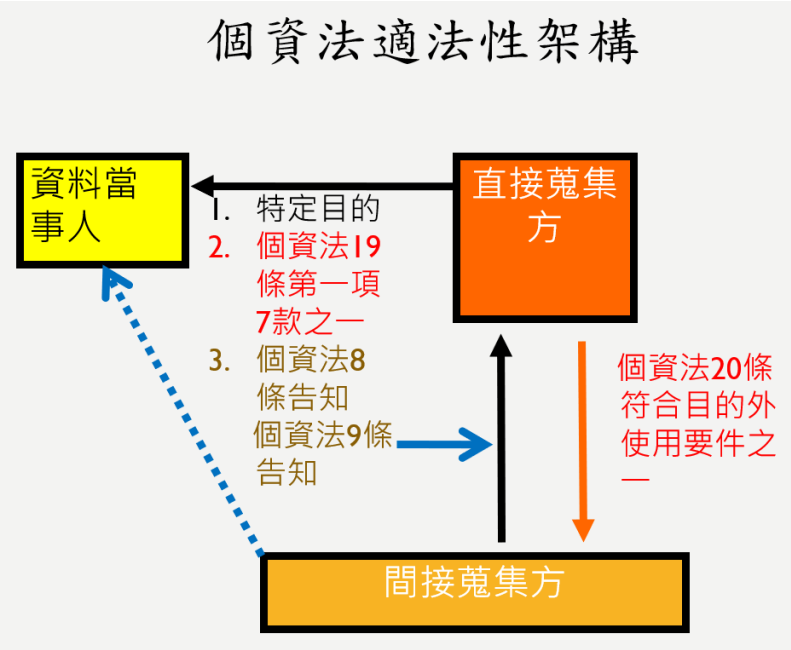


圖 22 個資法適法性架構

5. 資安規範

在個資法中規定，個人資料的取得必須透過個資法。不同於歐洲 GDPR 與澳洲 CDR 的消費者賦權，台灣的個資法的重點是在於個人資料的保護，因此台灣個資法規的主體在於資料的蒐集、處理、利用。雖然在個資法中並未討論到資訊安全的部份，但在台灣開放銀行的安控規範中第二條，有針對訊息的防護措施區分如下[155]：

(1). 訊息隱密性(Confidentiality)：指訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性。

(2). 訊息完整性(Integrity)：指訊息內容不會遭篡改而造成資料不正確，即訊息如遭篡改時，該筆訊息無效。

[155] 金融機構與第三方服務提供者辦理開放應用程式介面(OPEN API)業務安全控管作業規範

(3). 訊息來源辨識性(Authentication)：指傳送方無法冒名傳送資料。

(4). 訊息不可重複性(Non-duplication)：指訊息內容不得重複。

(5). 訊息不可否認性(Non-repudiation)：指無法否認其傳送或接收訊息行為。

以上各項訊息保護措施必須透過必要的對稱式或非對稱式的加密運算或數位簽章。例如在安控規範中訊息隱密性：應採用 3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同(含)以上之演算法進行加密運算，並採用 TLS 1.2(含)以上之通訊協定並使用 Elliptic Curve Diffie-Hellman Exchange 方式進行金鑰交換。又如訊息不可重複性：應採用序號、一次性亂數、時間戳記等機制產生。

除此外，在財金公司公佈的開放應用程式介面(Open API)技術標準規格文件中，也規範銀行提供資料時必須透過必要的加密機制。由於台灣開放銀行是採用 RESTful 架構，因此訊息交換的資料格式為 JSON (JavaScript Object Notation)。針對銀行提供消費者 JSON 訊息交換時，必須符合國際的 RFC 7516 JWE (JSON Web Encryption)的加密標準與 RFC 7515 JWS (JSON Web Signature)的簽章標準。

第三節 開放銀行的 TSP 管理與平台

全球各國針對開放銀行的 TSP 業者管理，以及 TSP 和銀行間的資料交換平台作法大有不同，與其推動方式有極大關聯。

一、國際各推動方式作法

(一)市場驅動

在全球政府中，美國是最不可能頒布開放銀行監管的國家，是市場驅動型的開放銀行典型。考慮到市場驅動無國家級機構介入的前提下，並不容易出現單一集中式的 TSP 業者管理機構或是資料交換平台。

但金融科技業者與金融機構受市場需求驅使，主動的尋求合作推動開放銀行的發展，開始出現單間機構合作、上架第三方資料平台、共組聯盟提出協定等模式。

單間機構合作的案例如：2017 年 Wells Fargo 與帳戶整合業者 Intuit 簽訂資料交換協議[156]。上架第三方資料平台案例如： Envestnet Yodlee 提供財務數據 API 平台，讓第三方開發人員存取金融機構數據的媒介。 Plaid 與多家銀行串聯，為第三方服務業者提供了一個 API 平台[157]，可以連接到金融機構進行帳戶訪問和身份驗證，並由 Plaid 作為金融機構外包服務商提供 API 標準[158]。另外還有其他相關廠商 Stripe、DirectID。

共組聯盟提出協定者，由金融機構及相關業者共同提出數據共享標準，例如 2017 年美國的國家自動票據交換所協會(NACHA)與埃森哲(Accenture)合作創建了 API 標準化行業小組(ASIG)，並於 2018 年 9 月與 IFX Forum 合併改名為 Afinis Interoperability Standards[159]，多半簡稱為 Afins，目前 Afins 已有 61 家會員公司跨及銀行、國際信用卡清算組織、證卷業者、金融科技業者、科技巨擘等[160]。並由 Afins 提供一系列的資料交換規範，包含 API 經濟、Blockchain 等。

156 https：//www.businesswire.com/news/home/20170203005316/en/Intuit-Signs-New-Data-Exchange-Agreement-Wells-Fargo
157 https：//www.pymnts.com/visa/2020/visa-buys-fintech-plaid-for-5-3-billion/
158 https：//www.bnext.com.tw/article/58109/visa-plaid-open-banking
159 https：//www.nacha.org/system/files/2019-05/Afinis-2018-Report-FINAL%20%281%29.pdf
160 https：//www.afinis.org/

(二) 政策鼓勵

香港與東協是政策鼓勵的典型，而這兩國家的資料交換標準及治理平台有異曲同工之妙。香港金融管理局僅訂定開放範圍、資安標準、監理標準等，並未提供 API 標準格式，或單一開發人員入口網(API Portal)。但有意願投入開放銀行的銀行可將所開立的 API 格式等資訊上架於具官方色彩的香港科技園公司的 Data Studio Portal，截至 108 年 8 月 16 日止已有 21 間銀行及 4 間 TSP 業者將相關資訊放於其上。另外銀聯通寶有限公司於 2019 年 1 月推出的 API 交換平台 JETCO APIX，銀聯通寶有限公司是香港最大的自動櫃員機、線上支付平台的服務商，目前 JETCO APIX，已有 14 家銀行及 1 家保險銷售通路投入[161]，提供統一的 API 瀏覽模式及免費的沙盒測試環境。

無獨有偶的，同屬政策鼓勵的典型，2018 年東盟金融創新網路 ASEAN Financial Innovation Network (AFIN)由東盟銀行組織(ASEAN Bankers Association, ABA)， 國際金融公司(International Finance Corporation, IFC)及新加坡 MAS 共同成立，隨即推出 API Exchange (APIX)[162]，截至目前截至 108 年 8 月 16 日止已有 51 間金融機構及 327 間新創業者投入平台。

(三) 法令強制

如同本報告第二章第二節說明，在法令強制的推行架構下，主管機關通常會設計出更完整的配套措施，這也就包 Open API 的資料交換標準與治理平台。以法令強制的典型代表為英國為例，2017 年英國推行開放銀行之初，在英國競爭及市場管理局(CMA)的管理下，由英國九大銀行及英國房屋互助協會(CMA 9)共同出資成立 OBIE，建置

[161] https：//sandboxportal.apix.com.hk/jetco/sb/categories
[162] https：//apixplatform.com/aboutapix

API 標準及相關資訊的規定與格式、管理及維護規定、更改及發布規定、支援用戶的使用結構及流程、處理開放銀行中應適用的條款及條件、負責開放銀行系統的指導原則，為其主要職能。

第三方服務業者則回歸英國 FCA 進行審核，將依照讀取及寫入權限及所存取的項目等提供不同程度的監理[163]，大致可分為 AISP 及 PISP 兩種。

除了統一的 API 標準公告外[164]，針對第三方服務業者(TPPs)及開放銀行技術服務提供商(TSP)也建置了 APP STORE 提供快速的篩選機制，加速消費者、企業用戶、金融機構與第三方服務業者互相聯繫。

二、台灣 API 管理平台作法

台灣開放銀行的 API 管理，在前面章節說明是以財金公司為銀行與 TSP 業者之間的平台橋樑。而台灣開放銀行本來就是採取政策鼓勵，因此財金公司的角色與香港的 JETCO APIX 平台類同，財金公司除了提供了 API Portal 供 TSP 測試與介接，也負責也協調與銀行之間的測試。除了技術支援外，財金公司本身也因在 Open API 委員會中，協調各家銀行針對要開放的 API 項目進行討論與設計。

在台灣的開放銀行作法，以財金公司為 API 管理平台的作法相對合理且有效益，但以財金公司為平台的問題主要不在財金公司角色與功能上，而會在於 TSP 在加入開放銀行平台時，由於是單獨與各家銀行簽約後再跟財金介接，所以 TSP 每次與新的銀行介接，仍要透過財金公司進行介接的測試。在這部份在政策強制的國家，基本上為了要

[163] https：//www.ithome.com.tw/news/133675
[164] https：//openbanking.atlassian.net/wiki/spaces/DZ/overview

維持介接的一致性，通常會由第三方驗證公司協助此部份的驗證，而API 平台只需專注在平台營運的執行。

第五章 台灣開放銀行政策建議

台灣在金融科技的發展上，最早的金融科技發展在金融科技創新實驗條例下的監理沙盒下，其創新的速度受到法令修改之限制，雖然最後通過 12 件案例，但實際執行上仍待法令解套。而開放銀行在金融科技發展方面，是採較實際的作法，讓現行的業務在一開放的 API 平台執行，因此開放銀行政策可視為金融科技落地情景的實現，也可以促進台灣未來的金融科技發展。

本研究建議台灣開放銀行在進入第二階段應採「法制調適、跨業開放」的作法，針對第一階段運行之問題與經驗研議必要的法規開放。第二階段是法規調試與健全體制的重要關鍵期，包括建立技術標準、資安風控、技術認證、法遵合規、稽核查驗、爭議處理、責任歸屬與資安保險等等議題。

而金管會在近期也公佈金融科技發展路徑圖(以下簡稱路徑圖)，路徑圖中有針對開放銀行下一個階段的發展提供了規劃與里程碑。因此，以下會先就路徑圖提出的作法進行說明，再就開放銀行之法令面、政策面與技術面三個層面進行政策的建言。

第一節 金融科技發展路徑圖將促進開放銀行之發展

金管會於 2020 年 8 月 27 日發布「金融科技發展路徑圖」，以 3 年提升數位金融服務效率、可及性、使用性及品質。金融科技發展路徑圖，包含四目標、三原則及八推動策略，說明如下圖：[165]

[165] 「金融科技發展路徑圖」政策：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202008270008&dtable=News



圖 23 金融科技發展路徑圖

一、 推動目標：

(一) 普惠：推動金融服務滿足各類型企業與民眾的不同需求，達到便利性與普及性。

(二) 創新：秉持「鼓勵創新與預防風險」衡平原則，推動負責任創新，提升金融產業新價值。

(三) 韌性：確保金融服務提供者的資本適足及業務財務健全經營，落實誠信的經營文化，並透過完善風險管理措施，提升金融體系韌性。

(四) 永續：推動金融服務提供者善盡社會責任，促進永續平衡，致力創造經濟、環境、社會三贏。

二、 推動原則

(一) 功能及行為監理：將金融監理思維框架由機構管理導向，轉化為功能及行為導向，鼓勵創新商業模式研發，並有效識別及管控風險，維護金融市場使用者權益。

(二) 科技中立：鼓勵運用技術精進經營效率及效能，建立公平競爭環境，增加消費者福祉及提高產業競爭力。

(三) 友善創新：提供創新及創業資源之政策支持，打造充滿活力的金融科技生態系統。

三、 推動策略

在推動策略的前三項，跟本研究的相關建言有關，如下所示，：

(一)金管會將強化創新中心作為議題溝通窗口及跨部會合作之平台，協助業者解決共通性議題，並由周邊單位協力設置金融科技共創平台，協助推動金融科技發展事項。

(二) 調適數位金融相關法令，因應跨業跨域及場景金融之發展。

(三) 整合政府與民間資源，共同創造數據價值及提供貼近消費者需求的金融服務。

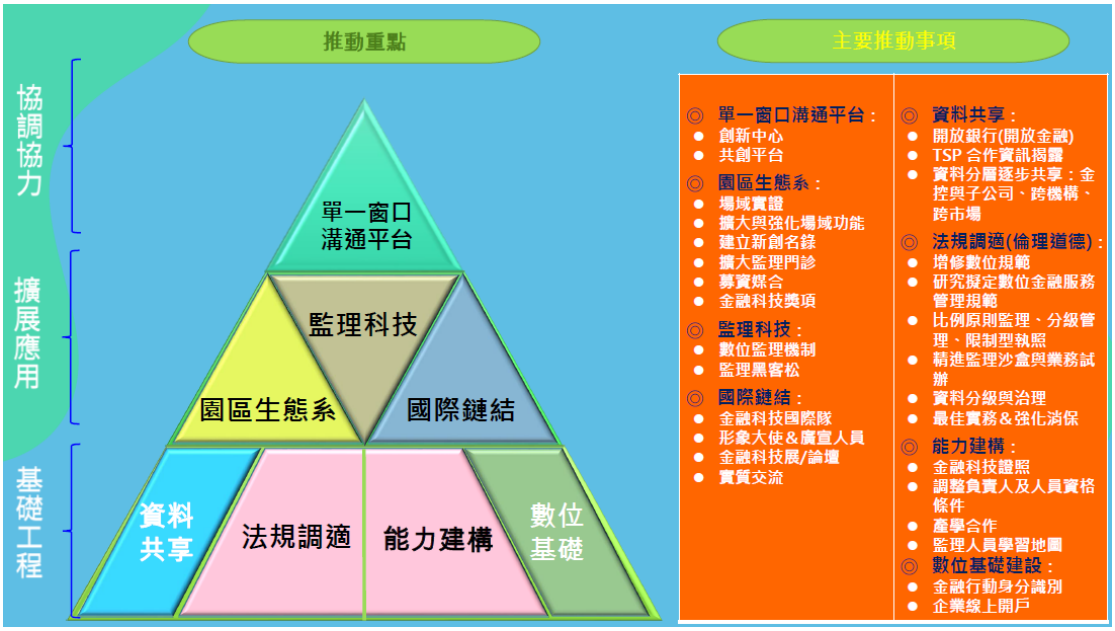


圖 24 金融科技發展路徑圖推動策略

而依據上述目標與原則，路徑圖將以三年為期，推動八大面向與其重要措施。而「開放銀行」第二階段已於 2020 年 11 月啟動，目前仍是金管會之重要發展政策，並在「資料共享」面向規劃中持續推動

開放銀行，包括建立與第三方服務機構合作資訊揭露制度；訂定金控轄下子公司客戶資料共享之相關機制與規範；訂定金融市場跨機構間客戶資料共享之相關機制與規範；訂定跨市場客戶資料共享之相關機制與規範。

第二節 法令與政策層面建議

目前的開放銀行是採用委外制度的法令基礎，現行開放銀行是以銀行自律規範在推動開放銀行的政策，鼓勵銀行跟第三方服務業者合作。然而，在開放銀行中更重要的是開放的目的及意義，是希望能夠將銀行的資料以及服務透過一個共通平台，提供更便利更有效率的金融服務。

因此，本研究建議在法令與政策層面上，金管會依金融科技發展路徑圖的政策持續推動，並持續鼓勵銀行與 TSP 業者合作，協助推動開放銀行以及未來開放金融的發展。以下針對在法令與政策層面說明。

一、鼓勵 TSP 治理制度的建立

金管會的金融科技路徑圖內，已有提出單一窗口服務機制、開放銀行政策推動上建立 TSP 合作資訊揭露制度，我們認為單一窗口服務機制的精神也可以套用到開放銀行推動之上。

本研究認為在第三方服務業者之治理，可從根本的參與機制著手，建議可由進行 TSP 本身的治理開始著手。[166]本研究建議透過 TSP 業者組成一個聯盟的方式，聯盟建立統一註冊機制並推動必要的分級管理，由主管機關可提供必要的協助，將 TSP 定位為銀行在金融科技上的策略夥伴角色參與開放銀行，該聯盟可配合銀行公會和財金公司共

[166] 以澳洲為例，澳洲開放銀行是由銀行公會與澳洲金融科技聯盟共同推動，合作內容可考：https://www.accc.gov.au/system/files/Fintech%20Australia%20%286%20August%202020%29.pdf

同推出單一窗口進行註冊服務、分級管理和定期稽核機制。在推動上，該聯盟可明確訂定相關自律規範及治理制度，依能力與營業項目推動必要的分級管理，並提供 TSP 註冊機制及分級標準後，提供銀行遴選第三方服務業者為依歸。

業者須符合金管會在開放銀行下的業務範圍以及資訊安全要求，方可取得第三方服務業者的資格。其次，建議公開統一的分級審查規範，針對依能力與營業項目推動必要的分級管理。最後，每年定期透過第三方公證的認證單位進行相關的第三方服務業者業務稽查作業並將稽查報告放於單一窗口，已合作銀行們不需要重複進行全部稽核項目，相關報告提供給所有已合作銀行審視，亦可提供其他銀行評估未來合作之風險。

透過以上的註冊、分級與審核制度，TSP 業者也可以有明確的依據。主管機關也可以統一各權責機構責成相關單位，對 TSP 業者進行統一的審查作業。在此制度下，銀行可以減少與 TSP 合作下的繁雜的審查作業，快速的進行 TSP 業者的篩選，再也不需要摸索相關法規解釋範圍，積極的進行試辦，加速導入相關服務；從消費者的角度出發，則可以更加放心的使用經審核把關的開放銀行服務，正所謂四贏局面。

而分級管理的設計，本研究建議參考國際開放銀行的做法，並利用風險控管為基礎的分類分式，如下圖所示。開放銀行第一階段服務業者，因均為公開資料，無個資外洩等疑慮，應放寬資格限制，僅需註冊報備之後就可以跟相關的銀行進行資料介接；針對第二階段以及未來第三階段的第三方服務業者，須具備 ISO 27001 以及 PCI DSS 的相關證照，並依照其情境開放項目、風險承擔能力等分級控管。

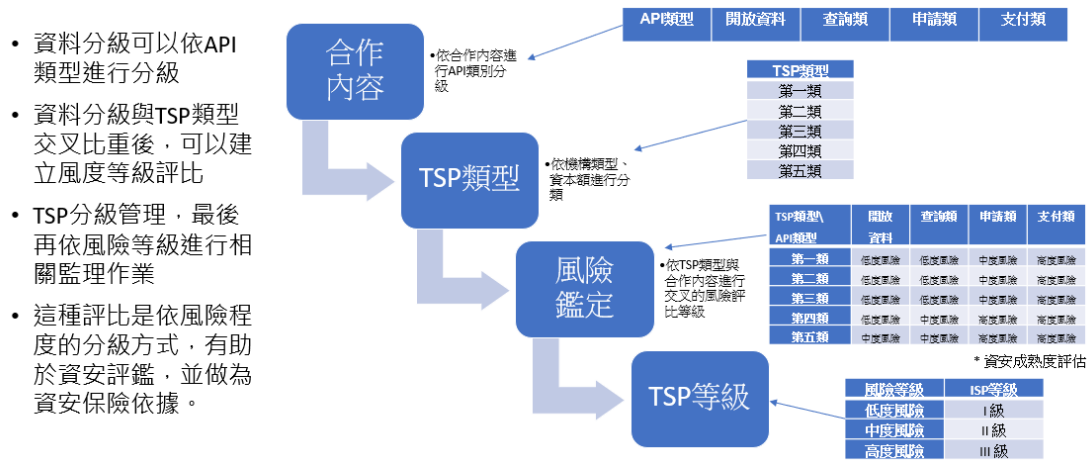


圖 25 基於風險管理基的 TSP 業者分級制度[167]

針對推動 TSP 治理制度，有利讓 TSP 了解自身責任與申請作業，提供新創業者進入的機會，但其管理機制至少須包括：

- 建立標準的認證與查核機制：對 TSP 業者進行技術與資安查核認證
- 定期公布查核的結果：查核資料必須儲存及透明公開
- 第三方查核機構協助釐清銀行與 TSP 之間的責任歸屬：並建立紛爭處理機制

二、建立資料賦權機制推動公開資料範圍與簡化交易確認作業

數據資料的整合與資料共享是金融科技發展重要關鍵，而金管會的金融科技發展路徑圖中也已規劃未來將走向資料共享。台灣若要實現 API 經濟與資料共享生態系，建立資料賦權機制是非常重要的。在資料賦權的部分，可以分為兩個部分來說明：第一是開放銀行中針對銀行的產品與服務之相關開放資料，第二才是針對消費者本身個人資料的部分。

以開放銀行第一階段的開放資料，既然已是開放之公開資訊，本

[167] 政治大學金融科技研究中心整理

研究建議可以仿效英國以及澳洲的方式要求全部開放，或是由市占率大的銀行領頭公開，而且公開資料的格式建議應效法澳洲開放銀行CDS(Customer Data Standards)作法，建立標準的資料格式提供資料交換使用，也有利與國內外廠商合作使用， 建立一致性的資料欄位，以利國內外的廠商使用。

開放銀行第二階段有關消費者個人資料的部份，在現行開放銀行規範下，係以銀行的網路銀行或行動銀行作為身份認證，第三方服務業者必須取得消費者的明示同意之下才能拿到銀行端的資料。因此，目前銀行與 TSP 進行資料交換時，由於目前金融業沒有通用的身份認證機制的公開金鑰基礎建設（Public Key Infrastructure, PKI），不利消費者體驗之提升。因此，在金管會的發展路徑圖也規劃研擬使用 FIDO 做為金融業的身份認證標準。本研究建議在未來金融產業導入 FIDO 後，可以利用 FIDO 作業多因子身份認證其中一項因子；另外也可以在 Open API 模式作為交易確認，建立消費者賦權所需要的同意授權(consent management)法制條件。例如：在相關金融法規下規範個人資料保護；另外，也必須建立以消費者賦權的 KYC 作業流程，在消費者同意授權後，使消費者能夠合理且有效的使用自身數據。

為實現資料共享，並促進開放 API 金融生態系之建立，建議未來在 Open API 或 Partner API 模式下，應建立消費者賦權所需要的同意授權(consent management)法制規範，例如在相關法規中增修對資料當事人資料賦權之可攜權相關條文，使消費者能夠合理使用自身數據，並透過統一的身份認證機制建立消費者賦權的 KYC 作業標準流程，讓消費者方便行駛授權，使個人資料可透過 API 開放給銀行、保險與證券等相關金融產業應用，也讓金融業者也合理使用個人資料，以促進資料共享生態系。

三、建立個資去識別化標準與資料交換中心

目前台灣個人資料之蒐集處理與利用必須嚴格遵照個資法之規定，台灣個資法有關人格權保護之基本概念形成甚早，目前面對金融科技之發展變革，許多個資保護之機制已難以因應金融科技時代所需。建立資料賦權開放資料交換的機制，這部份可能必須修改消費者保護法及個資法規，開放消費者數據可跨產業使用，讓金融業可使用健保、醫療、戶籍、交通安全、能源、交通和電信等相關數據資料，仍需待政府跨部門協調推動。但為解決個資法對金融科技發展之限制，並取得監理安全之衡平，建議未來可適時檢視鬆綁個資法。短期而言，可利用個資法中對事業主管機關之授權空間進行彈性監理。例如個資法中有諸多法條規定，只要是履行法定義務必要範圍內，得排除個資法之規定，即可據此針對金融保險業適用之規範進行訂定。

未來在消費者賦權的前題之下，根據國外的發展，消費者的個人資料應該可以再利用，讓銀行與第三方服務業者透過人工智慧以及大數據分析，為客戶提供更方便更有效率的金融相關服務。從金融科技路徑圖內，金管會也將資料共享作為未來兩年的主要推動項目，分三個階段推行。先由金控與子公司可以進行資料共享，再由金融業內共享，最後發展至跨業共享，如此可以加速提升資料再利用的綜效。而且，本研究建議在推動的資料共享目標外，應該可以針對資料共享的資料，納入開放銀行可落地的資料交換情境。因為資料共享是由金融業將現行的客戶金融資料整合再利用，但資料交換是希望可讓金融業者透過 TSP 業者收集新的資訊做為創新金融服務。舉例來說，針對大學剛畢業的信用小白，應可以透過電信公司帳單進行簡單的信用評比，進而提供微型貸款。

四、提升數據治理促進跨產業資料共享平台

目前台灣的金融科技發展非常仰賴大數據與人工智慧之應用，要解決目前數據孤島問題必須先要有數據治理。首先，建議監理機關指派單一專責機構持續負責明確數據治理策略，對個人與企業數據蒐集範圍與共享的界定、數據隱私定義與保護、及法律規範調適；其次，對於受監管單位而言，由於數據共享的範圍可以是受監管單位內部(如：金控轄下子公司)或是與外部跨機構之間，因此受監管單位在配合監理機關政策推動(如：開放銀行)及法律規範的要求下，建議應設立數據治理委員會，負責組織內部數據治理計畫的訂定，包含：數據治理策略與組織數位化轉型主題的關聯性、數據域優先級界定、組織內數據共享管理、跨業間數據共享與隱私保護措施等。此外，建議未來在個資法中界定資料分級(例如分為:核心資料與非核心資料)，所分類的資料包括企業自身資料與客戶提供資料，開放對外數據共享，跟其他行業的數據中心合作(例如:電信業)，或學術研究機構整合去識別化之資料數據後供大眾使用。借鏡國際發展，未來資料共享應該要發展到跨產業(金融、醫療、能源、交通和電信等)之資料庫互惠使用，例如：銀行業與保險業可使用戶籍、健保、醫療、交通安全等相關數據資料。同時，透過監理科技的技術發展，強化資安防護機制以消除業者與監理單位在個資(數據)使用上的疑慮。尤其，台灣金融產業擁有許多交易中介機構，例如：財金公司、聯徵中心、證券交易所、保發中心與集保公司等，因此在推動資料開放時應考量此特殊性。若資料賦權的架構發展完備，不但能夠解決跨金控子公司共同行銷，以及銀行業與第三方服務業者單方向資料交換問題，還能夠讓消費者資料發揮最大的效益。

總體而言，金管會的金融科技發展路徑已積極納入這二年金科技

業者所面臨的問題，並提出相關可能的解決方案及未來發展方向，以提升整個金融產業創新發展的效應。而本研究本著支持與協助政策推動的立場，對台灣未來開放銀行在不同階段導入時，提出可以借鏡國外制度發展經驗之相關建議。

第三節 業務推廣層面建議

台灣開放銀行在跨業合作上，必須應借鏡國外經驗，在心態上將TSP 視為開放銀行生態系的參與者，而不是銀行的委外機構，因此必須簡化進入的門檻，以及提供可實際上以數據為導向的應用場景。

在上個章節已有討論可以透過 TSP 的聯盟或協會加強 TSP 本身的治理，而且此個聯盟可以透過建立合作平台更積極發展相關的配套措施。因此，在業務層面，本研究建議以下配套措施的作法。

一、成立 API 管理中心

開放銀行要持續發展，產業間必須建立一套共同遵守的規範，該規範應可以隨時彈時因應不同情境，新增必要的 API。本研究建議參照國際間英國的做法，成立類似 OBIE 的 API 管理中心，負責維護開放銀行標準 API 及資料交換的格式。由單一 API 管理中心負責管理系統，以利監控平台的運作，搜集各種服務的使用數據，發布管理報表。對主管機關可用較低成本推行監理科技，對銀行及 TSP 業者可以有 API 規格與標準的最高權責機構，在相關情境技術開發時可以有所依歸。

目前財金公司已經擔任類似的角色了，但未來可能會面臨到像以市場驅動的 API 平台整合業者(如美國的 Plaid)進入台灣，這時也許要有個中間機構負責推動 API 相關管理工作。

二、建立一致性的驗證機制

開放銀行的成功因素之一在於將 API 標準化後可以快速的交換資料，但必須要再進一步的確認 API 標準化的技術檢驗，目的是為了要減低 TSP 與銀行合作時重覆的測試工作。本研究建議應參考英國、法國與德國在推動開放銀行時皆有驗證單位(certification body)。舉例，以英國有 OBIE 的驗證、法國有 STET 的驗證以及德國有 Berline Group 的驗證，這些驗證單位可以協助主管機關與銀行進行把關的機制。

三、建立合規雲端服務平台與設立合規服務提供廠商名單

參考國外經驗，未來可以讓新創業者透過合規的雲端服務與金融業者進行資料交換，將資訊安全建立的成本攤轉至營運的費用上，對於新創業者的進入門檻會相對較低。銀行與 TSP 間的合作可利用雲端平台作為資訊資源共享與交換的平台，雲端運算包含虛擬化、網絡計算、寬頻網路等架構與服務，帶動業務轉型，能加速金融科技的試驗和轉型，更能建立單一的雲端稽核查驗制度，減少銀行與新創業者之間的管理成本。

在此平台上，也可以參考國外的作法，把可以提供此平台功能業者列為英國技術服務提供業者，在台灣應可稱為 TISP (Technical Infomration Service Provider)，協助整合 TSP 端的通用型服務。

在現行開放銀行的安控規範的第二十條也允許 TSP 透過委外廠商進行必要的營運，所以利用雲端平台本身沒有適法性問題，然而卻會有資安查核的議題。首先，TSP 仍必須要有完整的風險管理與資訊安全管理機制，其次，TSP 和銀行必須要有實地查核的權利，必要時可聯合委託第三方公證單位查核雲端業者。最後，在雲端平台必須要有明確的資料保以及加密機制，確保除了 TSP 業者外沒有人可以存

取到消費者資料。

四、推動資安保險

在現行開放銀行的規範中，銀行必須負最後的紛爭責任，但開放銀行的資安與個資責任不應全由銀行全部承擔。在現行的安控規範中，除對 TSP 業者資安基本標準外，後續也有定期稽核追蹤，並建立透明的資訊公布機制。因為在安控標準中有要求 TSP 業者提供資安評估報告，此資安評估報告可以依成熟度評分後，做為資安保險的風險模型評估標準。所以，在現行架構下，可以要求銀行與 TSP 業者購買資安保險，由認證機構與外部稽核機構協助提供評估與分析報告，建立資料庫供保險公司與金融機構使用。如下圖所示。



圖 26 TSP 資安保險類別[168]

而資安保險在過去不易推動是因為資訊安全的評鑑是以承保公司自行填寫，沒有公訂標準，故不易進行定價。而在開放銀行下，提供給 TSP 資安保險沒這個問題，因為 TSP 都必須具備 ISO 27001 認證，會由公正第三方提供資訊安全的評鑑報告。保險公司可以依據 ISO 27102 – 資安保險準則，以 ISO 27001 的資安評鑑報告，建立資

[168] 政治大學金融科技研究中心整理

安保險必要的資安成熟度標準，進而精算資安保險的定價模型。而 TSP 資安保險的範圍可依開放銀行(1).資訊安全要求 和(2).消費者爭議處理二個部份進行評估。

五、建立開放銀行生態系

加速推動 Open API 生態系，必須從協助 TSP 業者如何進開放銀行生態系開始；因此，如何有效地將 TSP 業者的整體配套整合將會有助於降低金融產業發展基礎建設經營成本。綜合上述各點，本研究建議對 TSP 應該要有更完整的規劃，現行台灣規劃的 TSP 業者比較像英國的 AISP 與 PISP，但欠缺技術服務業者的角色。因此，透過與合規的 TISP 業者與雲端業者服務，可以有效的整合不同的 TSP 業者，協助推動整個開放銀行生態系，並可在未來開放消費者數據可跨產業之資料庫互惠使用，例如銀行業與保險業可使用戶籍、健保、醫療、交通安全等相關數據資料。如下圖所示：

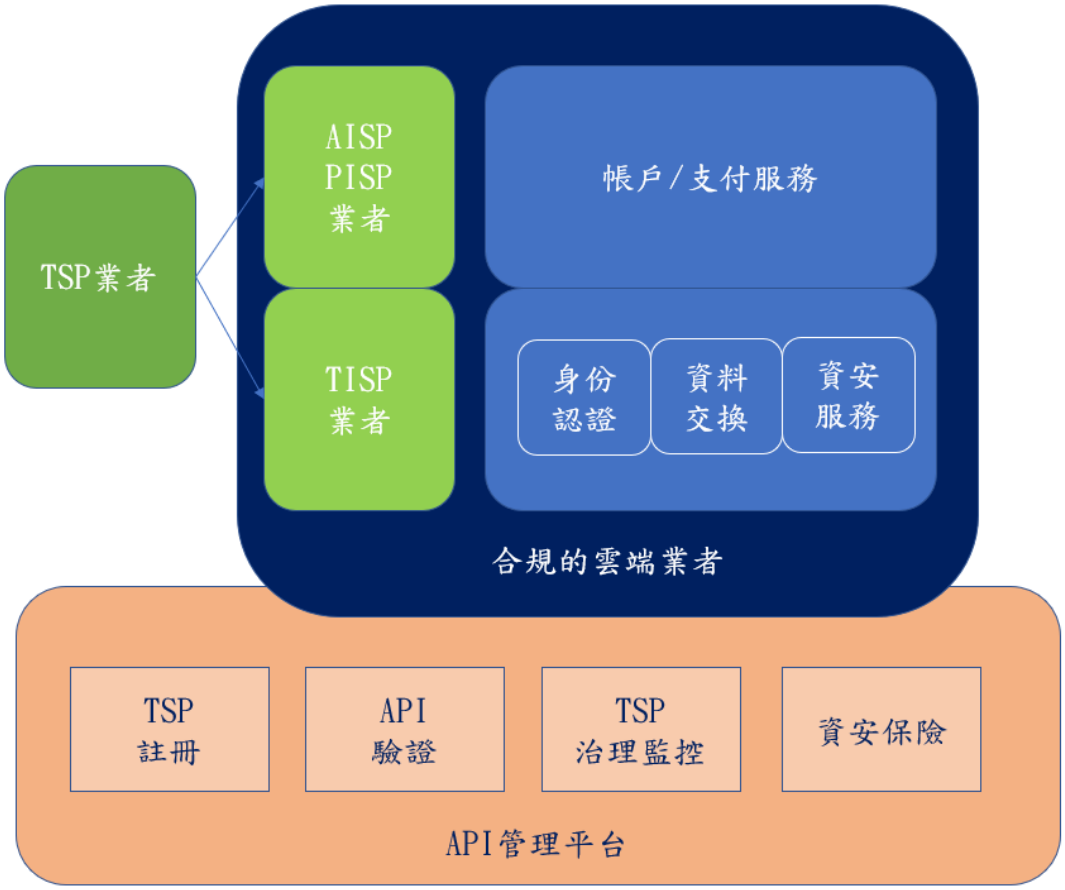


圖 27 開放銀行生態系 TSP 合作與監管示意[169]

有效地整合不同 TSP 業者，也有利解決銀行一定要找資本足夠的 TSP 合作的窘境，因為目前台灣大多數的新創業者資本額不會太多，但如何提供一個完整的進入機制、可營運的平台以及可被監理的機制就會相當重要的議題。

第四節 技術層面建議

就技術層面，開放銀行現行的資訊安全規範已相當完整，缺乏一樣是相關配套措施。例如現行開放銀行作法，消費者的身份是由銀行代驗，因此銀行無法透過 API 進行進件相關的業務推廣。因此，第三方身份認證或外部 eKYC 就是必須要有的配套措施。

[169] 政治大學金融科技研究中心整理

一、第三方身份認證

從金融科技路徑圖內，金管會也發現金融科技的推動和身分認證這類基礎架構建設息息相關。現階段的開放銀行身分認證機制，消費者仍需進行多次對多家銀行的身分驗證，而且以現行的身份認證大多是以簡單的帳密驗證方式，不僅影響服務體驗，其安全性亦不足。為解決問題，如何將多重認證機制(MFA, multiple factors authentication)納入至行動裝置的生物辨識作為身份認證與簽章使用，為當前必須要解決的議題。

目前依開放銀行安控規範，TSP 可以透過自然人憑證、金融卡、信用卡以及手機 SIM 卡等方式進行身份確認，然而現行身份認證方式，並未支援行動裝置和連結 eKYC 作業。因此，本研究建議金管會應開放銀行多元身份認證方式，並透過現行 open API 平台進行多方的驗證機制。將消費者的身份(identity)行動化，然後提供憑證(authentication)、授權(authorization)與簽章(signature)功能。

在金管會的路徑圖亦有規劃了第三方身份認證，金管會建議由金融機構共同 籌組金融行動身分識別聯盟 F FIDO，研議規劃導入國際 FIDO 標準[170]，初期針對中低風險之金融服務，提供通用之行動身分識別與簽署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。

然而，路徑圖中相關措施是以身份認證為主，並未規劃相關的 eKYC 作業。

[170] FIDO（Fast Identity Online）聯盟，它是在 2012 年成立，屬於非營利的產業聯盟，目標是為各種網站和行動服務提供一套開放、互通的標準，以解決近年身分認證技術彼此之間，缺乏互通性的問題，並希望讓使用者不用再以傳統的輸入密碼方式，來進行身分辨識。

二、強化法遵與監理科技

開放銀行與純網銀是帶動法遵與監理科技應用的切入點。未來必須建立開放銀行「數位監理申報(Digital Regulatory Reporting, DRR)」，讓業者給監理機關的報告能自動化產生。主管機關拿到的報告必須能夠「機器可讀可處理(machine readable & executable)」。

另外，提供開放銀行 TSP 與銀行之間的 API log 分析能力，並提供交易資訊的 KYC/AML 等的資料分析能力。

第五節 總結

開放銀行實現「消費者賦權」，使消費者獲得更多元的金融服務，也使金融機構透過「資料共享」，快速串聯大數據和人工智慧等技術，加速數位金融創新。尤其，臺灣有財金公司、聯合徵信中心、集保結算所、保發中心等金融周邊單位，在 Open Banking 上應該可以走得比國外更為穩健。而未來在開放金融數據共享下，金融機構與金融科技公司可由競爭轉為合作形成「互利共榮的金融生態圈」，將更有助於台灣的金融科技產業發展 。

台灣未來開放銀行第二階段之後應逐漸採行「法制調適、跨業開放」，總結如下：

1. 針對 TSP 業者加強相關治理制度規劃，並透過聯盟建立合作平台的作法，規劃 TSP 的相關配套措施，提供便捷的導入與驗證作業。
2. 為強化並普及開放銀行的推動，建議將開放銀行第一階段資

料開放設為強制項目，讓中小型的銀行也可以透過導入開放銀行，進行資訊架構與能力的升級。

3. 參酌國際模式，將開放銀行作為跨業資料開放的示範場域，在消費者授權的前提下，以及資料交換雙方業者自願互惠的基礎下，進行跨產業的資料共享與開放。
4. 建議金管會可以鼓勵金融機構積極參與，以試辦方式加速進行更多創新。

本研究期待我國加速推動開放銀行生態系法規、政策上的健全，使開放銀行成為我國金融領域創新驅動力，提供消費者更加便利、更加親民、更加普惠的金融服務。

附錄. 參考資料

- 中國人民銀行(2020.02.13), 商業銀行應用程序接口安全管理規範
- 中國互聯網金融協會(2019),開放銀行研究報告
- 王宏仁 (2019.10.16),【開放銀行特別報導】財金開放 API 平臺終於上路 23 家銀行與 6 家 TSP 搶先布局，但下一階段才是更大的挑戰,https://www.ithome.com.tw/news/133650
- 王宏仁(2019.10.18), 【開放銀行特別報導】跨海專訪英國 Open Banking 推手：英國開放銀行有成，API 呼叫破億次觸及 99%全英金融市場, https://www.ithome.com.tw/news/133675
- 王儷玲(2019)，台灣發展 Open API 的機會與挑戰,http://www.ftrc.nccu.edu.tw/wordpresseng/?p=9015
- 李靜宜(2018.12.09), 為何英國堅持開放銀行？英國開放銀行推手點出關鍵：就是為了改變銀行的懶惰心態, https://www.ithome.com.tw/news/127558
- 肖然(2020.02.12),开放银行中国实践探索
- 谷湘儀，臧正運(2019)，變革中的金融科技法制。
- 孟潔(2020.03.10),評析澳大利亞《消費者數據權利規則》及對我國立法與產業的啟發，http：//pkulaw.cn/fulltext_form.aspx?Db=lawfirmarticles&Gid=801176401

a6b24e205b3b43963cb1057bdfb&keyword=&EncodingName=big5&Search_Mode=accurate&Search_IsTitle=0

- 易观分析(2019.12.05), 2019 中国开放银行发展专题分析（案例篇）, http://www.woshipm.com/evaluating/3171726.html
- 林鎧勳(2019.04),淺談 API 應用與經濟發展, 叡揚 e 論壇 第 93 期
- 花旗(2016.11.14),花旗推出全球 API 開發者中心，實現開放式銀行業務, 花旗推出全球 API 開發者中心，實現開放式銀行業務 | Business Wire
- 金管會(2020.08.27),金融科技發展路徑圖
- 政大開放銀行創新平台-背景介紹,http：//openbanking.org.tw/origin
- 英國 OBIE 網站,https：//www.openbanking.org.uk/
- 財金公司，2020 年 5 月 26 日政治大學金融科技研究中心 OPEN API 技術合規與測試說明會，http://www.ftrc.nccu.edu.tw/wordpresseng/?p=10997
- 財金公司新聞稿(2019.10.16),創新數位金融新契機　開放 API 平台正式啟動,
- 高敬原(2019.10.16), 開放銀行...怎麼全世界都在熱？圖解全新金融生態系帶來的大變革,

https://www.bnext.com.tw/article/55095/global-open-banking-taiwan

- 陳伯璋（1998）。教育研究方法新取向：質的研究方法，南宏圖書有限公司。
- 曾更瑩(2018.02.26), 企業應儘速評估歐盟個資法遵循事宜, https://www.leeandli.com/TW/NewslettersDetail/6028.htm
- 黃亞森(2020.06.16), 從 Visa 併購 Plaid 案件談台灣開放銀行的發展, https://www.bnext.com.tw/article/58109/visa-plaid-open-banking
- 資策會(2020)，開放銀行發展趨勢與展望。
- 資策會產業情報研究所(2019)，開放銀行發展簡報。
- 銀行公會『開放 API』研究暨應用發展委員會開放 API 諮詢小組(2019.12.26),金融機構與第三方服務提供者辦理開放應用程式介面(OPEN API)業務安全控管作業規範
- 蔡柏毅(2018), 歐盟「個人資料保護規則」導讀, https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMTY4OC8yZTAzODExMS02NGRkLTRlZGMtYWZlZC05N2MzOTNhYzE5ZjUucGRm&n=5q2Q55uf5YCL5Lq66LOH5paZ5L%2Bd6K236KaP5YmH5bCO6K6ALnBkZg%3D%3D&icon=..pdf
- 薛丹琦(2019)，開放銀行金融創新之機制研究，世新大學財務金融學研究所碩士論文
- ACCC, Competition and Consumer (Consumer Data Right) Rules

2020.

- Afinis(2018), Afinis Interoperability Standards
- Alliedmarketresearch Acess,https：//www.alliedmarketresearch.com/library-access
- APIX 官網, https：//apixplatform.com/
- Arturas Vegelius(2020.04.01),PSD2 Strong Customer Authentication (SCA) and PCI Multi-factor Authentication (MFA) compliance,https：//www.advantio.com/blog/psd2-strong-customer-authentication-sca-and-pci-multi-factor-authentication-mfa-compliance
- Barend, G. (2019), Establishing a Durable Environment for Digital Financial Services.
- BIAN (2020) ,Global Open Banking Initiatives and the added value of the BIAN Open Standards,https：//bian.org/participate/bian-webinars/global-open-banking-initiatives-added-value-bian-open-standards/
- BIAN (2020), Build the future of banking service, http：//bian.org/participate/bian-webinars/bian-apis-future-banking-api-standards
- Bill Streeter (2020.10.05),U.S. Financial Institutions Now Lead Europe in Open Banking (Here's Why), https://thefinancialbrand.com/102918/u-s-financial-institutions-now-lead-in-open-banking-api-token-mobile-app-screen-scrape/

- Bud Financial Limited(2018), The book on open banking
- Businesswire(2017.02.03),Intuit Signs New Data-Exchange Agreement With Wells Fargo, https://www.businesswire.com/news/home/20170203005316/en/Intuit-Signs-New-Data-Exchange-Agreement-Wells-Fargo
- Businesswire(2019.06.04),Digital ID and Authentication Council of Canada (DIACC) Announces the Appointment of Six Board Members,https://www.businesswire.com/news/home/20190604005330/en/Digital-ID-Authentication-Council-Canada-DIACC-Announces
- Canadian Bankers Association(2018), Canada's Digital ID Future - A Federated Approach
- Canadian Banks (2019), Open banking is coming
- Capgemini & BNP Paribas,《World Payment Report 2018》
- CMD - Retail Banking Market Investigation, https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk.
- Daniel Leslie(2019.04.10), Canada: Open Banking In Canada – Current Regulatory Insights,https://www.mondaq.com/canada/financial-services/797350/open-banking-in-canada-current-regulatory-insights
- Data61-Austrilia(2020),Consumer-Data-Standards(2020), https://data61.csiro.au/en/Our-Research/Focus-Areas/Special-Projects/Consumer-Data-Standards
- Deloitte,Creating an open banking framework for Canada
- Deloitte,Open Banking around the

world,https://www2.deloitte.com/cy/en/pages/financial-services/articles/open-banking-around-the-world.html

- Deutsche Bank (2018), Unlocking opportunities in the API economy
- EBA, Open Banking：advancing customer-centricity.
- European Commission, European data strategy,https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
- FCA(2019.12.17),Call for Input: Open finance
- Federal Reserve Bank of Boston(2020),Developments in Open Banking and APIs：Where Does the U.S. Stand?
- Financial Industry API Register, Financial Industry API Register (mas.gov.sg)
- FinancialDataExchange(2020.03.19),The Financial Data Exchange Releases First Major Update to FDX API, Makes Fourth Version Available,https：//www.financialdataexchange.org/FDX/News/Announcements/financial-data-exchange-releases-first-major-update-to-fdx-api-makes-fourth-version.aspx
- FinancialDataExchange,The Financial Data Exchange Releases First Major Update to FDX API, Makes Fourth Version Available
- Finextra(2020),The ambitious path to Open Finance and Open Data..how Europe is leading the way, https://www.finextra.com/blogposting/18517/the-ambitious-path-to-open-finance-and-open-data--how-europe-is-leading-the-way

- GDPR,https://gdpr-info.eu/art-1-gdpr/
- Government of Canada(2020.07.27), Government of Canada Standards on APIs
- Government of Canada,Submissions for Consultation Paper on Open Banking, https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/submissions.html
- HKMA (2018), Open API Framework for the Hong Kong Banking Sector, https：//www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/
- Hong Kong Open API Exchange Platform Categories, https://sandboxportal.apix.com.hk/jetco/sb/
- IBM，Evolution of the API economy,https://www.ibm.com/downloads/cas/XG8RYO63
- IGI Global, https://www.igi-global.com/dictionary/consumer-empowerment/40673
- MAS(2018),ABS-API-Playbook
- Nacha,Afinis Interoperability Standards,https：//www.nacha.org/afinis-interoperability-standards
- Open Banking Limited (2019),Openbanking Developer Zone, https://openbanking.atlassian.net/wiki/spaces/DZ/overview
- Open Banking Standard(UK),https：//standards.openbanking.org.uk/
- OpenBankingExpo, Open Finance report: shaping the future of financial services

- Opendata-Api-Docs-Pub(Australia),https：//openbankinguk.github.io/opendata-api-docs-pub/v2.4.0/
- Peng Khim Ng(2019,06),新加坡星展銀行從 Open Data 到 Open Banking,台灣銀行家第 114 期
- PENSER(2019.05),AIS AND PIS – A STATUS UPDATE ON OPEN BANKING LICENSES ISSUED IN THE UK,https://www.penser.co.uk/business/ais-and-pis-a-status-update-on-the-licenses-issued-in-the-uk/
- PRETA S.A,(2017),Third Party Provider User Management for PSD2 Access to Account.
- PYMNTS(2020.01.04), VISAVisa's $5.3B FinTech Play, Wrapped In Plaid, https://www.pymnts.com/visa/2020/visa-buys-fintech-plaid-for-5-3-billion
- Sean Creehan and Paul Tierno(2019.05.02), The Slow Introduction of Open Banking and APIs in Japan, https://www.frbsf.org/banking/asia-program/pacific-exchanges-podcast/open-banking-apis-japan/
- Trustbind(2020.03.09), Web API の公開はセキュリティが不安… 安全に API を公開する方法とは？, https://www.trustbind.jp/security-information/api-security/webapi.html
- United States Government Accountability Office (2016.02),FINANCIAL REGULATION Complex and Fragmented

Structure Could Be Streamlined to Improve Effectiveness

- Upwork, The API Economy, Upwork.