FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

2024年六月

FSDC Paper No. 64

善用數碼身份：促進香港金融服務業的數碼轉型

目錄

引言 **4**

1.1 數碼身份助力數字經濟邁向新高度 4

1.2 整合數碼身份，釋放經濟價值，解鎖發展路徑 6

數碼身份的基本原理 **9**

2.1 支撐數碼身份的核心原則與技術 9

2.2 數碼身份格局：不同數碼身份管理方法 11

2.3 賦予個人權利：混合式去中心化管理方法 12

數碼身份的功能及其在金融服務業的應用 **14**

3.1 數碼身份在金融服務業的作用及特點 14

3.2 與金融服務業數碼身份相關的基本資料元素 16

3.3 評估資料模式，整合強大數碼身份 19

3.4 身份核實轉向以用戶為中心— 去中心化身份及自主身份管理 21

採用數碼身份的風險與挑戰 **24**

4.1 實施數碼身份解決方案的關鍵考慮因素 24

4.2 應對去中心化身份的複雜局面：潛力與挑戰 27

政策建議 **30**

建議 1：公私協同 — 探索「智方便」計劃更全面貫通實施，並賦能私營數碼身份錢包的發展 31

建議 2：為數碼身份生態系統制定數位身份信任框架 32

建議 3：雙管齊下促互通：改善基建及法律框架提升數位身份的互聯互通能力 33

建議 4：協調數碼身份認證標準，實現跨境身份認證機制的無縫對接 34

建議 5：增強對可信數碼身份採用的教育宣傳和推動社會賦權 35

結語 **38**

附件 1：持份者在各種數碼身份模式中的作用 **39**

附件 2：全球數碼身份發展的關鍵考慮因素：驅動力與案例研究 **40**

數碼身份發展與應用案例研究 41

中國內地 41

新加坡 42

印度 43

澳洲 44

歐盟 45

附件 3：評估香港的數碼身份生態系統及其實施準備情況 **48**

中文譯本僅供參考。如中、英文版本有任何抵觸或不相符之處，概以英文版本為準。

報告摘要

在現今不斷演變的全球市場環境中，科技的進步正從根本上重塑商業運營和經濟格局。應對這些變化對提升城市競爭力尤爲關鍵，特別是在瞬息萬變的金融領域。香港正策略性地提升創新科技發展，鞏固其作為領先國際金融中心和科技創新樞紐的地位。

數碼經濟的快速增長，特別是在後疫情時代，標誌著消費者對數碼渠道的接受度和使用率顯著提高。數碼身份（digital ID）系統擔當起核心角色，支持香港數碼經濟的持續擴展。[1]這些系統透過提高交易安全和效率、拓寬金融服務渠道、促進普惠金融，以及推動新業務模式和服務交付機制的發展，引領新時代的金融服務發展。

數碼身份滿足了金融行業的迫切需求，如減輕網絡安全風險及滿足嚴格的資料保護法規。此外，它們促進了更高效、更安全的在線交易，這對維護客戶信任和市場競爭力至關重要。透過採用生物特徵識別及密碼學等先進技術，數碼身份可以改善客戶核實流程，確保符合監管標準。另外，數碼身份能簡化開戶流程、降低營運成本，並透過提供更加個人化和便捷的服務提升客戶服務體驗，進一步推動金融普及與行業創新。

在香港，「智方便」等舉措體現了其對數碼身份概念的接納。它與目標更廣泛的數碼身份一致，通過增強在線安全性、簡化交易流程，並為公共和商業服務提供更便捷的訪問。《2023 年施政報告》及數字化經濟發展委員會隨後於 2024 年 2 月提出的建議均強調香港推動數碼經濟的策略方針。這些舉措涵蓋多個主要範疇，例如提升數碼基建、促進數據跨境流通、支援企業數碼轉型及人力資源配套。[2,3]當中的部分措施與數碼身份系統密切相關，並強調有必要制定統一的策略框架，從而為經濟及營運帶來更大的效益。

在肯定香港特區政府積極推動數碼經濟轉型的同時，我們亦應重視數碼身份所面臨的機遇及需要加強的環節，特別是在數碼基建及監管架構方面的不足。有見及此，香港金融發展局（金發局）成立由業界專家組成的專項工作小組，展開綜合研究，明確在金融服務領域發展及應用數碼身份系統所面臨的挑戰，並提出應對措施，供政府及公眾持份者考慮。主要考慮事項包括：

i) 探索「智方便」計劃的全面實施，並賦能私營數碼身份錢包的發展；
ii) 為數碼身份生態系統制定數位身份信任框架；
iii) 透過改善基建及法律框架提升數位身份的互聯互通能力；
iv) 協調數碼身份認證標準，實現跨境身份認證機制的無縫對接；及
v) 增強對可信數碼身份採用的教育宣傳和推動社會賦權。

[1] 在本報告中，「數碼身份」一詞主要指與個人官方或法定身份證明掛鉤且獲政府正式承認的個人身份。凡提述與公司或企業相關的數碼身份時，會明確說明
[2] 香港政府。（2023 年 10 月 25 日）。*《行政長官 2023 年施政報告》*。https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf
[3] 香港特區政府數字化經濟發展委員會。（2024 年 2 月）。*《數字化經濟發展委員會核心建議》*。香港特區政府。https://www.itib.gov.hk/assets/files/DEDC_Core_Recommendations_Eng_issued.pdf

引言

數碼經濟正在重塑全球商業運作及社會互動,掀起數碼市場顛覆性轉變。數碼平台與日俱增，已形成龐大的互聯生態系統，提高服務及交易效率。在此數碼生態系統中，通訊以各種數碼形式進行，並透過高速全球網絡將用戶連接起來。

數碼身份是數碼經濟蓬勃發展的核心，對安全高效地參與網上活動至關重要。數碼身份為驗證個人及商業實體的網上身份提供可靠框架。數碼身份不單是一種電子憑證，亦有可能發揮虛擬護照的功能，引導用戶從容應對複雜的數碼環境。

本報告旨在強調數碼身份在數碼經濟中的重要作用，重點關注數碼身份對金融服務業的影響。透過深入分析，探討營造有利於數碼身份穩健發展的生態系統的重要性。本報告亦將研究數碼身份如何從根本上促進融入性、拓寬服務可及性,並推動經濟全面發展,特別是在金融領域的貢獻。

1.1 數碼身份助力數字經濟邁向新高度

在快速發展的數碼經濟中，建立安全可靠的數碼身份日益重要，尤其是在充滿活力的金融服務業。受顛覆傳統模式及業務的數碼創新驅動，金融服務業正處在轉型變革的風口浪尖上。行業研究已指出這一轉變；其中，畢馬威會計師事務所的一項研究顯示，近半數受訪金融服務提供商準備在未來三年內進行徹底的數碼轉型。[4]另一項市場研究得出類似結論，稱 90% 的受訪專家認同數碼創新正在重塑金融格局。該等專家包括來自全球多個組織的企業高管、經理及分析師。[5]

根據國際貨幣基金組織的一份研究報告，數碼經濟指一系列以數碼化資訊和知識為主要生產要素的經濟活動。該等活動依靠先進的通信網絡，並利用資訊科技促進增長。[6]雖然科技與金融早有交集，但過去十年科技投資激增，促使近年來的創新步伐不斷加快。例如，作為全球金融科技行業表現的基準，MSCI ACWI IMI 金融科技創新指數在過去十年增長了近四倍，到 2024 年 4 月達到 491.94 點。[7]此外，隨著金融業採用人工智能、分布式分類帳技術、雲端計算及數據分析等技術，預計從 2022 年至 2028 年，金融科技行業的營收將達到傳統銀行業的三倍。[8] 新技術正在重塑企業營運和客戶參與模式，使新的參與者敢於破舊立新。

[4] 畢馬威會計師事務所。(2020 年 9 月)。*Digitalisation in banking beyond COVID-19*。https://assets.kpmg.com/content/dam/kpmg/be/pdf/2021/Digitalization-in-banking-beyond-Covid-19.pdf

[5] 德勤。(2017 年)。*Digital transformation in financial services*。https://www2.deloitte.com/tr/en/pages/financial-services/articles/digital-transformation-in-financial-services.html

[6] 國際貨幣基金組織。(2022 年 9 月 29 日)。*Experimental indicators of digital industries in select countries: Definitions, methods, and results*。https://www.imf.org/en/Publications/WP/Issues/2022/09/29/Experimental-Indicators-of-Digital-Industries-in-Select-Countries-Definitions-Methods-and-524035

[7] 摩根士丹利資本國際公司。(2024 年)。MSCI ACWI IMI 金融科技創新指數（美國）淨收益[概況]。https://www.msci.com/documents/10199/97543aa0-0ade-1dd6-1f12-fd2320479433

[8] 麥肯錫諮詢公司。(2023 年 10 月 24 日)。*Fintechs: A new paradigm of growth*。https://www.mckinsey.com/industries/financial-services/our-insights/fintechs-a-new-paradigm-of-growth

轉型期間，全球疫情加快了金融服務業的數碼化進程，因為受出行管制及保持社交距離的影響，人們對數碼服務的需求增加。世界銀行的一項研究同樣顯示，在疫情期間，特別是在發展中國家，該等國家的金融帳戶和進行電子交易的情況有明顯增加。[9]現今，全球三分之二的成年人口使用數碼支付方式。疫情對發展中國家的人們採用該等數碼方式的影響尤為顯著。不包括中國在內的開發中國家，約 40% 的成年人口表示首次使用數碼支付是受到疫情的影響。[10]此轉變更突顯了一套完善的數碼身份識別及支付系統的重要作用。該等系統不僅能擴大金融服務的覆蓋範圍，尤其是擴延至過去未被受服務的人而言，同時亦能為社區帶來新的經濟機遇。

貿易方面，2022 年貨品與服務的電子交易額達 3.82 兆美元，佔全球服務貿易總額的一半以上。[11]隨著企業及消費者在數碼市場的參與度不斷提升，制定可靠數碼身份解決方案的尤為重要。數碼身份指「*與個人／企業的『官方』或『法定』身份掛鉤且獲政府正式承認的*」獨特網上資料。[12]它為個人進行數碼互動及交易保駕護航。對企業而言，穩健的數碼身份系統對建立信任及在金融領域保持競爭優勢至關重要。

數碼身份的概念不再是簡單的身份驗證；隨著數碼世界與實體世界相融合，數碼身份成為促進包容性及協調各種交互的基礎，帶來全新機遇。正視這一融合趨勢至關重要，因為數碼互動日漸滲透到日常生活中，促進了推動全球數碼公民身份的萌芽。

在此背景下，採用前瞻性的方法構建數碼身份基建及監管框架至關重要。該系統必須靈活敏捷，既能滿足當前需求，又能順應未來技術發展。在以創新驅動的數碼經濟中，除了信任以外，隨機應變的數碼身份解決方案對個人及企業有效駕馭新興經濟環境至關重要。

香港已認識到數碼經濟促進優質發展的潛力。《2023 年施政報告》概述了旨在促進數碼經濟發展的各項舉措，包括在數字化經濟發展委員會的指導下，提升數碼基建、促進數據跨境流動、推動企業轉型及加強人力資源建設。[13] 鑒於善用數碼能力的重要性不言而喻，香港必須加倍努力。當前，打造有利於數碼身份發展及應用的生態系統刻不容緩。香港的當務之急是建立數碼身份系統。這不是錦上添花之舉，而是在數碼轉型中站穩陣腳、確保城市經濟活力及促進市民與全球互聯互通的根本措施。

[9] 世界銀行。（2022 年 7 月 21 日）。*COVID-19 boosted the adoption of digital financial services*。https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services
[10] 世界銀行。（2022 年 7 月 21 日）。*COVID-19 boosted the adoption of digital financial services*。https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services
[11] 國際貨幣基金組織。（2023 年 12 月 13 日）。*Why Digital Trade Should Remain Open*。https://www.imf.org/en/Blogs/Articles/2023/12/13/why-digital-trade-should-remain-open
[12] 普及金融聯盟 (Alliance for Financial Inclusion)。（2021 年 9 月 9 日）。*Policy model for digital identity and electronic know your customer (e-KYC)*。https://www.afi-global.org/publications/policy-model-for-digital-identity-and-electronic-know-your-customer-e-kyc/
[13] 香港政府。（2023 年 10 月 25 日）。*《行政長官 2023 年施政報告》*。https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

1.2 整合數碼身份，釋放經濟價值，解鎖發展路徑

數碼身份系統對適應數碼經濟及促進經濟增長至關重要。麥肯錫全球研究所的報告強調了數碼身份的潛在影響，預計到 2030 年，數碼身份的全面普及有望釋放相當於國內生產總值 3–13% 的經濟價值。[14]此外，根據普華永道諮詢團隊的研究，全球數碼身份市場正在快速擴張，預計該市場將從 2020 年的 160 億美元增加一倍至 2025 年的 330 億美元，複合年均增長率達 16%。[15]

該等預測突顯了數碼身份在推動經濟活動打破傳統界限方面的變革性潛力。透過消除多種障礙，例如人工操作或「了解客戶」法規、缺乏受多個多個司法管轄區的共識的信用資料及高昂的營運成本，數碼身份有望或促進數碼經濟的構建更加包容性的環境，讓更多人參與其中並從中受益，尤其是在發展中地區。整合數碼身份能簡化金融機構的營運，從而節約成本、降低風險及把握市場拓展機會。

數碼身份的預期經濟效益巨大，可以為公共服務部門節省多達 1,100 億小時的工作時間，企業開戶的成本減少 90%，並在薪資詐騙方面節省大量資金—每年可達 1.6 萬億美元。[16]此外，生物特徵識別在數碼身份解決方案中的應用日益廣泛，其進步有望加快數碼開戶的速度，實現近乎即時的身份核實，顯著提升用戶體驗及營運效率。[17]因此，數碼身份解決方案是未來實現互聯互通和經濟繁榮的基礎。

數碼身份對培養數碼信任的作用

信任是數碼經濟發展的基礎，亦是促進增長、創新及互動的核心驅動力。在數碼身份方面，信任是提升經濟抗逆性及社會包容性的必要條件。政府實體及私營組織均認識到這一點，並承認維護消費者及公民的信任是一項長期挑戰。

網絡安全威脅日趨複雜，Gartner 展開的一項研究指出，人們擔心傳統的身份核實方法即將過時，將有約三分之一的企業認為該等解決方案在 2026 年時已不再可靠。[18]無獨有偶，加拿大網絡安全中心強調該等問題的迫切性，網絡釣魚、惡意軟件及社交工程陷阱等複雜威脅日益普遍，威脅著個人資料的安全。[19]此外，生物特徵識別資料洩露及系統漏洞事件頻發，亦突顯採取有力數據保護措施的緊迫

[14] 麥肯錫全球研究所 (McKinsey Global Institute)。(2019 年 4 月 17 日)。*Digital identification: A key to inclusive growth*。https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-In-brief.pdf
[15] 思略特。(2021 年)。*Digital Identity: Opportunities and challenges – A perspective for telecom operators, banks, industrial companies and government institutions*。https://www.strategyand.pwc.com/jp/ja/publications/digital-identity-e.pdf
[16] 麥肯錫諮詢公司。(2023 年 10 月 24 日)。*Fintechs: A new paradigm of growth*。https://www.mckinsey.com/industries/financial-services/our-insights/fintechs-a-new-paradigm-of-growth
[17] Innovatrics。(日期不詳)。*Traditional versus digital onboarding in banking*。https://innovatrics.com/trustreport/traditional-versus-digital-onboarding-in-banking/
[18] Gartner。(2024 年 2 月 1 日)。*Predicts 2024: AI & Cybersecurity — Turning Disruption into an Opportunity*。https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-ID-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026
[19] 加拿大網絡安全中心 (Canadian Centre for Cyber Security)。(2022 年)。*An Introduction to the Cyber Threat Environment*。https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

性。2022 年，每四間銀行中就有一間遭遇超 100 宗身份詐騙事件，常見犯罪行為包括偽造證件及篡改身份證明，每宗事件平均導致行業損失 31 萬美元。[20]

2023 年初，香港的可疑數碼詐騙交易比率達 18.3%，在調查涵蓋的市場中位居榜首。由此可見，該等問題無分地域和行業。[21]隨著技術的進步和資料可存取性的增加，網絡攻擊呈現上升趨勢。以最近的一件案件為例，某家國際公司蒙受了約 2 億港元的損失，只因詐騙者在視頻會議期間操縱視頻和音頻，模仿高階管理層，最終導致欺詐性的金融交易得以進行。[22]

鑒於網絡安全威脅的複雜性和頻率不斷升級，實施有效的數碼身份解決方案可築起重要的安全防線。定期的安全檢查對於預防潛在漏洞也至關重要。穩健的數碼身份系統既要注重生物特徵識別等安全因素，亦要特別關注個人私隱保護，嚴格遵守國際私隱專業協會的指引。[23]數碼身份不僅對消費者交易重要，也關乎僱員、業務合作夥伴及聯網設備的穩定運作。因此，身份管理是企業的策略性要務。在金融服務業，根據財務行動特別組織 (FATF)的指引進行身份核實尤為重要，有助防止詐騙及提升客戶體驗。採用全球統一的標準來加強數碼身份系統的安全性和效用，有望打擊全球的數碼欺詐，提供更加統一和具有韌性的框架。

此外，人工智能及機器學習等技術的加入正在徹底改變數碼身份管理的格局。該等工具促進身份管理系統的自動化及可擴展性，提供隨機應變的解決方案，滿足不斷變化的網絡安全要求及身份核實需求。[24]數碼身份在數碼生態系統中的作用日趨重要，促進信任、包容及安全，而這些正是塑造數碼化未來的核心要素。

整合數碼身份，建設共融社會，賦予個人權利

實施數碼身份系統對提升經濟與社會的包容性具有重要意義。該等系統可改變個人與政府實體的交流互動、以及獲取公共服務及參與全球市場的方式。

儘管歐洲私營機構在服務數碼化方面取得了明顯進展，但數碼身份識別框架的不足，阻礙了公共部門前行步伐。完善的數碼身份系統有助於進一步簡化政府與公民之間的互動，特別是藉助流動技術及分

[20] Regula。(2023 年 3 月 29 日)。*Global Survey: Identity Fraud Cost Nearly Half a Million US Dollars to Every Third Bank Last Year*。https://regulaforensics.com/news/ID-fraud-cost-nearly-half-a-million-us-dollars-to-every-third-bank/
[21] 環聯。(2023 年 10 月 4 日)。*2023 年上半年全球每 20 宗數碼交易中即有超過一宗屬可疑詐騙 — 本港旅遊及休閒業的可疑數碼詐騙比率最高*。 https://newsroom.transunion.hk/more-than-one-in-20-global-digital-transactions-were-suspected-fraudulent-in-the-first-half-of-2023-in-hong-kong-highest-fraud-rate-in-travel--leisure-industry/
[22] 有線電視新聞網。 (2024 年 2 月 4 日)。 *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*。https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[23] 國際私隱專業協會 (International Association of Privacy Professionals)。(日期不詳)。*Biometrics*。https://iapp.org/resources/article/biometrics/
[24] MarketsandMarkets。(2024 年)。*Global identity verification market size, trends, growth rate & industry share 2030*。https://www.marketsandmarkets.com/Market-Reports/ID-verification-market-178660742.html

佈式分類帳技術，確保數碼身份解決方案的安全性。[25]這些系統提高了個人對自身數據的所有權，亦為電子選舉及數碼醫療服務等應用提供支援。[26]

共享政府服務是推動社會包容及普及金融的關鍵。相關倡議旨在建立全球認可的數碼身份框架，同時符合聯合國《2030 年可持續發展議程》，確保為所有人提供合法身份。考慮到發展中國家還有相當多的人口缺乏官方身份證明，數碼策略對緩解此不平等現象至關重要。[27]

對不同社會階層而言，數碼身份將成為通往機遇的大門。當數碼身份結合穩健的管治框架，就有充分發揮其包容性，在全球範圍內改善公民與政府的關係，推動為個人賦能。

[25] IBM。（2022 年 9 月）。*The next evolution of digital ID: Scalable, secure, and trusted digital credentials*。https://www.ibm.com/downloads/cas/PEZANJ1N
[26] The Innovation In Politics Institute。（日期不詳）*Building trust and social inclusion with digital identities*。https://innovationinpolitics.eu/showroom/project/building-trust-and-social-inclusion-with-digital-identities/
[27] 聯合國貿發會議。（2023 年 9 月 14 日）。*UNCTAD supports small island nations to harness digital ID for inclusion*。https://unctad.org/news/unctad-supports-small-island-nations-harness-digital-id-inclusion

數碼身份的基本原理

2.1 支撐數碼身份的核心原則與技術

數碼身份系統建基於確保功能性、完整性及安全性的基本原則和技術。數碼身份是個人身份的電子記錄，透過驗證用戶身份，安全高效地實現在各個數碼平台上的互動。[28]數碼身份代表個人獨一無二的數碼檔案，包含各種個人憑證及屬性。這一數碼足跡是現代身份識別實踐的基礎，使個人能夠建立與其現實身份具有同等可信度和保障的網上身份。

隨著數碼互動日益普及，數碼身份系統亦在不斷發展，以滿足大眾對可靠身份核實的需求。這些系統讓便利性與強大的安全措施完美結合，讓大眾能夠方便地融入數碼世界。國際組織如世界銀行等已制定全面標準，以道德及務實的原則約束數碼身份的使用。該等標準旨在為包括公共和私營機構在內的所有持份者，建立包容、安全及互利的數碼身份系統。[29]

各國政府透過制定核心原則，在塑造數碼身份生態系統方面發揮著舉足輕重的作用。例如，英國數碼身份策略委員會 (Digital ID Strategy Board) 於 2020 年已經提出關於發展數碼身份框架的六項指導原則。該等原則對數碼身份的基本要素提供詳細建議，涵蓋多個類別。[30] 同樣，2023 年 9 月，澳洲聯邦政府就關於建立全面數碼身份系統的立法草案，發佈徵求意見稿，其中提出了四項類似原則。[31] 關於數碼身份系統的首要設計原則，政府的觀點及學術界和業界的深入研究結論，[32]大致可以歸納為三點：

- **包容**：設計完善的數碼身份框架應努力實現普及性，確保人人都能公平接達。目標是創建不因社會經濟地位或地理位置等因素而有所區別的系統。透過實現這一目標，營造每位用戶都能充分參與數碼經濟的環境，縮小地區之間的服務差距。
- **信用**：信任是培養用戶信心的基礎。建立健全的數碼身份系統，離不開嚴密的安全措施，以保護個人資料免遭洩露及未經授權的取用。清晰的管理流程及負責的系統監督人員同樣重要。如果用戶對系統的健全性有信心，相信自身資料受到保護，私隱得到尊重，自然會產生信任。
- **實用**：此原則強調數碼身份的實際益處。系統應簡化用戶與公共和私營部門之間的互動，帶來更順暢的交易，及提高服務交付效率。有效的數碼身份不僅要實現固有功能，亦要能提升用戶體驗，促進採用率及滿意度。

[28] 麥肯錫全球研究所 (McKinsey Global Institute)。(2019 年 4 月 17 日)。*Digital identification: A key to inclusive growth*。https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20
[29] 世界銀行「身份識別促發展項目」(ID4D)。(日期不詳)。*Principles*。*In Identification for Development: Practitioner's Guide*。https://id4d.worldbank.org/guide/1-principles#:~:text=Establishing%20a%20robust%E2%80%94unique%2C%20secure,ensuring%20vendor%20and%20technology%20neutrality.
[30] 英國政府。(2020 年 9 月 1 日)。*Next steps outlined for UK's use of digital ID*。https://www.gov.uk/government/news/next-steps-outlined-for-uks-use-of-digital-ID
[31] 澳洲聯邦議會。(2023 年 9 月)。*Exposure draft of the Digital ID Bill 2023*。https://www.digitalID.gov.au/sites/default/files/2023-09/Exposure%20draft%20of%20the%20Digital%20ID%20Bill%202023_0.pdf
[32] The Sorvin Foundation。(2022 年 9 月)。*Principles of SSI V3*。https://sovrin.org/principles-of-ssi/

數碼身份的解決方案可以是整合各種不同資料點及數碼交互的複雜網絡。密碼、出生日期和生物特徵識別資料等關鍵要素與電子護照、數碼錢包及流動身份相輔相成，形成符合個人偏好及要求的綜合數碼檔案。[33]

個人資料保護同樣至關重要，需要建立一個以、安全及私隱為基礎的穩健架構。在個人化與保護私隱之間達到最佳平衡，是構建令人信任的數碼身份解決方案的關鍵。安全且以用戶為中心的數碼身份系統需借助各種先進技術，包括但不限於：[34、35、36]

- **密碼技術**：利用公鑰基礎設施（PKI）等技術確保電子身份的安全，利用數碼簽署驗證文件，及利用散列算法維護資料完整性與機密性。
- **生物特徵識別驗證**：利用獨特的身體或行為特徵進行核實，如指紋掃描、面部識別、語音驗證及虹膜掃描。
- **分佈式分類帳技術**：提供不可改變的交易記錄，支持自主身份模式，允許個人在不可更改的公共分布式分類帳上自主控制自己的數碼身份。
- **人工智能與機器學習**：透過檢測詐騙模式加固安全協議，及利用先進的活體偵測功能完善生物特徵識別系統。
- **行動身份錢包**：為智能手機數碼憑證提供安全的儲存空間，具有選擇性披露功能，以保護私隱。
- **高級加密標準**：透過高強度加密功能保護儲存的資料，使未經授權的用戶無法讀取。
- **零知識證明**：在不披露相關數據的情況下核實資料真偽，既能保護私隱，又能增進信任。
- **聯合身份管理**：促進身份在不同系統及服務之間的遷移，提高互通性，方便用戶使用。

透過整合該等技術，數碼身份系統可以降低身份盜用及詐騙風險，同時確保提供順暢的用戶體驗。該等系統完美兼顧安全性與用戶便利性，有望徹底改變身份核實領域。

然而，數碼身份系統的成功並非完全取決於技術進步，亦離不開完善的政策、有效的管治以及對以用戶為中心的設計理念的重視。周全的數碼身份管理方法既需考慮技術創新，亦需考慮社會因素，力求實現用戶積極參與、社會廣泛接受的目標。

[33] 亞略特科技。（2023 年 5 月 30 日）。*Digital Identity: What It is and Why It Matters in Today's World*。https://www.aratek.co/news/digital-identity-what-it-is-and-why-it-matters-in-todays-world
[34] 亞略特科技。（2023 年 5 月 30 日）。*Digital Identity: What It is and Why It Matters in Today's World*。https://www.aratek.co/news/digital-identity-what-it-is-and-why-it-matters-in-todays-world
[35] IBM。（2023 年）。*The next evolution of digital identity: Scalable, secure, and trusted digital credentials*。https://www.ibm.com/downloads/cas/PEZANJ1N
[36] 泰雷茲集團。（日期不詳）。*Trusted digital identity by Thales*。https://www.thalesgroup.com/en/markets/digital-ID-and-security/government/ID/digital-ID-services/trends

2.2 數碼身份格局：不同數碼身份管理方法

數碼身份採集個人獨特屬性，用於識別數碼身份，是網上交易不可或缺的一部分。下表簡述數碼身份管理格局的演變，展示一系列針對數碼時代需要而設計的模式。該等方法既有以高效流程和集中控制著稱的集中模式，也有賦予用戶數據主權的去中心化模式。每種框架都有不同的優勢及考量（見圖表 1）。

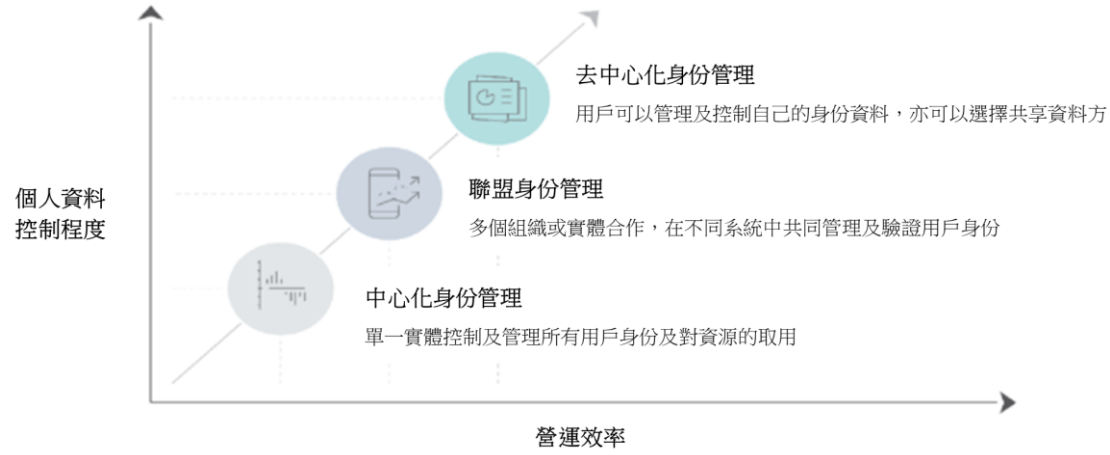
數碼身份的類型	詳細說明	擁有權
政府主導的中心化身份管理法	由政府全面監督及控制身份核實、管理及驗證過程的綜合系統。常見應用包括稅收、醫療保健、選舉等官方職能。	政府擁有及控制。該模式指定國家為收集資料、簽發數碼身份及驗證用戶身份的唯一權威機構。
半集中式聯盟身份管理法	用戶能透過多個認可提供商生成數碼身份的互聯系統。該身份普遍適用於各種服務，在促進互通性的同時保留一定程度的集中監督。	透過多個提供商的中央樞紐協調下進行管理，在可信框架內為用戶提供靈活性。
去中心化開放身份市場	該方法以市場為導向，採用去中心化身份核實及管理，用戶可以出於不同用途保留多個身份。該模式順應分佈式分類帳等新興技術，可提高安全性及私隱性。	身份資料歸個人所有，可在整個網絡上分發，無需中央授權。參與者在自主調節的市場中遵守一套標準規則或協議。
用户自主身份管理	用戶能為個人為中心，自設身份屬性，常見於更重視便捷性且不需要嚴格核實身份的環境，如社交網絡及電商平台。	個人保留對其數碼身份的自主權，外部驗證機構的監督作用極小。

資料來源：奧緯咨詢公司分析

圖表 1— 數碼身份的類型[37、38、39]

[37] 國際電信聯盟。（2018 年）。*Digital ID in the ICT ecosystem: An overview*。https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.ID01-2018-PDF-E.pdf
[38] 思略特。（2021 年）。*Digital Identity: Opportunities and challenges – A perspective for telecom operators, banks, industrial companies and government institutions*。https://www.strategyand.pwc.com/jp/ja/publications/digital-identity-e.pdf
[39] 世界銀行 ID4D。（日期不詳）。*Types of ID systems*。https://id4d.worldbank.org/guide/types-id-systems

數碼身份管理模式包括集中式系統與去中心化系統，每種模式會帶來不同的營運效率。去中心化系統憑藉穩健的控制權及數據分配，一般能提高營運效率。其高效特徵源於用戶對自身資料的自主權，以及利用分佈式分類帳技術帶來快速安全的身份驗證能力。相反，集中模式雖然結構更為簡單，但由於程序繁複，靈活性或被削弱（見圖表 2）。對該等模式的抉擇關乎用戶信任及參與度。決策者面臨的挑戰是平衡去中心化系統的效率和用戶賦權優勢與對普遍可用的直觀系統的需求。



資料來源：穆迪投資者服務公司

圖表 2– 數碼身份系統及其集中程度[40]

2.3 賦予個人權利：混合式去中心化管理方法

中心化身份管理管理系統基於政府人口統計資料庫，在身份驗證流程管理上較為簡單直接。然而，,隨著私隱保護、個人控制及數據自主傾向全球性趨勢，在身份管理模式均顯示出這一轉變趨勢。例如，愛沙尼亞將私營數碼身份提供商納入中央系統；以色列採取中央主導但分散程度不同的模式。[41]兩種模式雖不相同，但均致力於賦予個人管理數碼身份的權力。

而去中心化身份管理系統的出現，標誌著身份管理格局的巨大轉變。其將控制權交給個人，由個人擔任自己數碼身份的管理人。[42]透過數碼錢包，用戶可以安全地管理憑證，採用自主身份模式，減少對中央機構的依賴。該方法降低了與集中儲存數據相關的風險，如重大數據洩露事件。[43]

[40] 穆迪投資者服務公司。（2023 年 9 月 21 日）。*Decentralised Finance and Digital Assets - Cross Region: Decentralised digital ID has rich potential but wider adoption faces obstacles*。. https://www.moodys.com/research/Decentralised-Finance-and-Digital-Assets-Cross-Region-Decentralised-digital-ID-Sector-In-Depth--PBC_1370639
[41] Digital Government Exchange。（2022 年）。*Digital Identity and Verifiable Credentials in Centralised, Decentralised and Hybrid Systems*。https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX%20DIWG%202022%20Report%20v1.5.pdf
[42] ProofID。（日期不詳）。*What is decentralised ID?*。https://proofid.com/what-is-decentralised-ID/

採用去中心化身份系統亦能讓企業受益。這些系統簡化了客戶資料核實，提供更加高效及完善的用戶體驗。此外，該等系統只共享特定交互所需的資料，有助於公司達到資料保護標準，如《通用數據保障條例》(GDPR)規定的標準。[44]雖然半集中式聯盟身份管理系統亦有類似優勢，但去中心化模式在最大限度地減少收集的數據及加強個人對自身資料的自主權方面更勝一籌。[45]

隨著用於管理憑證的數碼錢包日益普及，為確保平台之間的互通性，採用統一的監管框架及協議勢在必行。雖然去中心化可能意味著政府監督有限，但政府在策略性上的參與可以加強數碼身份基建，完善核實與驗證流程。

整合來自「黃金源數據」(golden source) 的可核實憑證，可以兼顧用戶自主權與中心化身份管理的可信度（本報告後面章節將進一步討論「黃金源數據」的概念）。該等憑證對照中央資料庫進行驗證且附帶數碼簽署，儲存在數碼錢包中，在需要時進行對應，因此無需不斷向中央資料庫核查。憑證的加密簽署亦可證實其真偽。[46]

然而，去中心化身份儘管潛力巨大，亦遇到了一些障礙，包括技術複雜性、安全風險、兼容性問題以及潛在的數據濫用。[47]倘若不能克服該等挑戰，去中心化身份可能難以在全球範圍內推廣及獲廣泛接受。

為消除該等阻礙，混合模式的概念應運而生。其將提高安全性與賦予用戶權利相結合，提供平衡的解決方案。該等模式融合集中式系統與去中心化系統的優勢，簡化技術、提高可接達性及降低使用門檻。混合模式透過將集中式安全措施與去中心化加密技術相結合，增強信任。政府與私營實體攜手合作，對開發標準化框架、確保順暢的互通性及堅持問責原則至關重要。澳洲、加拿大及芬蘭等國家是運用該種合作生態系統的典範，它們利用精準的監管及私營部門的創新，打造安全、好用且能隨機應變的數碼基建。[48]

---

[43] Allen, C。（2020 年 4 月 25 日）。*The path to self-sovereign ID*。https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-ID/
[44] ENISA。（2021 年）。*Decentralised Identities: a new reality for the EU citizens*。https://www.enisa.europa.eu/events/trust-servicies-forum-ca-day-2021/trust-service-forum-presentations/daniel-du-seuil-pierre-marro-enisa-trust-services-forum-2021.pdf/@@download/file/Daniel%20Du%20Seuil%20-%20Pierre%20Marro%20-%20ENISA%20Trust%20Services%20Forum%202021.pdf
[45] 穆迪投資者服務公司。（2023 年 9 月 21 日）。*Decentralised Finance and Digital Assets - Cross Region: Decentralised digital ID has rich potential but wider adoption faces obstacles*。https://www.moodys.com/research/Decentralised-Finance-and-Digital-Assets-Cross-Region-Decentralised-digital-ID-Sector-In-Depth--PBC_1370639
[46] 花旗。（2023 年 3 月）。*Money, Tokens, and Games: Blockchain’s Next Billion Users and Trillions in Value*。https://www.citifirst.com.hk/home/upload/citi_research/rsch_pdf_30143792.pdf
[47] 穆迪投資者服務公司。（2023 年 9 月 21 日）。*Decentralised Finance and Digital Assets - Cross Region: Decentralised digital ID has rich potential but wider adoption faces obstacles*。https://www.moodys.com/research/Decentralised-Finance-and-Digital-Assets-Cross-Region-Decentralised-digital-ID-Sector-In-Depth--PBC_1370639
[48] Digital Government Exchange。（2022 年）。*Digital Identity and Verifiable Credentials in Centralised, Decentralised and Hybrid Systems*。https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX%20DIWG%202022%20Report%20v1.5.pdf

數碼身份的功能及其在金融服務業的應用

3.1 數碼身份在金融服務業的作用及特點

在金融服務業，嚴格確保資料完整性並採用先進的防護技術才能應對瞬息萬變的市場環境。隨著網絡威脅激增，依靠高成熟度的安全功能來有效保護個人敏感資料和財務數據變得不可或缺。隨著行業追求更安全的網上交易，網絡安全的應用亦發生了重要轉變。與此同時，消費者對便捷的遙距銀行服務的需求不斷增長。如何在快速處理交易與提供安全保障之間取得平衡，是數碼身份解決方案需要面對的難題。

實施數碼身份系統旨在轉危為機，例如提高營運效率、構築安全屏障及擴大服務可及性，覆蓋不同客戶群。

採用數碼身份將推動金融服務的核心職能的變革，內容主要包括：

加強客戶盡職審查：數碼身份可提升在開戶過程中的客戶識別及核實效率，以及在接達帳戶時的身份驗證。

- 簡化核實流程：透過利用先進數碼技術，包括生物特徵識別資料及加密方法，簡化流程。該等技術加強了對身份證件及持證人真實性的核查，從而減少詐騙和身份盜用事件的發生。
- 持續盡職審查：數碼身份系統有助定期更新客戶資料，協助金融機構進行持續監察。確保觀察到的金融行為與客戶檔案及預期活動相符。該等持續盡職審查對維護金融系統的完整性及遵守監管標準至關重要。

減少人為管控失誤：傳統的身份識別方法往往倚賴金融機構職員的主觀判斷，而職員可能缺乏檢測偽造文件的工具及專業知識。

- 專業核查：透過先進的自動化系統進行數碼身份核實程序，能夠精準識別偽造或篡改過的文件。依靠技術可減少人工參與驗證文件的必要性。此外，數碼身份系統也能確保在連接帳戶時採用統一、可靠的身份驗證方法。

成本效益及交易監測：

- 降低成本：簡化數碼核實流程可在客戶開戶方面節省大量成本。[49]由於開戶費用減少，金融機構可以將資源重新分配到其他合規職能上，及向客戶提供更多服務。

[49] 麥肯錫全球研究所 (McKinsey Global Institute)。（2019 年 4 月 17 日）。*Digital identification: A key to inclusive growth*。https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20

- 交易監察：即時核實有助於識別及報告可疑活動。此外，整合地理位置及行動裝置識別碼等其他資料有助於創建詳細的客戶檔案及識別異常交易模式，從而改善機構在打擊詐騙及洗錢方面的情況。

提升客戶體驗：

- 簡化客戶准入流程:數碼身份系統省卻客戶親自前往分行的不便及相關等侯時間，簡化客戶開戶體驗。這一流程加快了服務交付速度，提高了客戶滿意度，有助在競爭激烈的金融環境中提升客戶忠誠度。
- 量身定製金融產品及服務：策略性地使用數碼身份使金融機構能收集及分析特定客戶資料，深入洞悉消費者的行為與需求。這一數據驅動型方法使銀行與金融科技公司有能力開發個人化的金融產品及服務——從量身定製的投資建議到有的放矢的促銷活動及定製貸款方案。該等個人化互動滿足了客戶對適切且便捷的金融互動的期望。[50]

促進普及金融：向缺乏傳統身份證明的個人客戶提供金融服務也可發揮關鍵作用，這些人往往生活在發展中國家的偏遠地區或服務不足的地區。

- 擴大覆蓋範圍：透過減低門檻，數碼身份可顯著提高金融環境的包容度，讓更多人參與到數碼經濟中來。
- 政府及商業數碼化：在發展中國家，數碼身份系統對政府款項及物資發放的數碼化至關重要，有助於有需要的人獲得金融服務。

從生物特徵識別技術到基於區塊鏈的解決方案，金融服務業對數碼識別碼的探索正在重塑身份核實的格局。該等技術旨在追求通用性及唯一性，力求減少詐騙及維護交易完整度。儘管構建通用數碼身份系統的道路障礙重重，但業界致力實現互通，這與打造安全包容未來的目標殊途同歸。

數碼身份推動了私隱、安全及監管合規的進步，確定了該等因素在數碼經濟中的重要地位。監管機構正在制定能跟上創新步伐且以消費者安全為先的適配框架，響應金融服務的數碼化。監管舉措聚焦以下方面：[51]

- **標準化**：監管機構旨在透過建立統一的數碼身份核實標準，實現系統兼容，確保交易順暢無縫。
- **合規性**：規定有關資料保護、私隱及盡職審查的最佳做法，保護消費者資料，建立安全的客戶關係。

[50] Global Banking & Finance Review。（日期不詳）。*The impact of digital ID on banking and finance*。https://www.globalbankingandfinance.com/the-impact-of-digital-identity-on-banking-and-finance/
[51] 財務行動特別組織。（2020 年 3 月）。Guidance on Digital ID。https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-ID.pdf.coredownload.pdf

- **問責制**：金融機構有責任保護客戶資料，確保驗證流程的完整性，維護及提高消費者的信任。
- **牌照 / 資格**：應要求數碼身份服務提供商取得證書，以證明其遵守資料私隱及網絡安全標準，並能有效管理潛在利益衝突。

世界各地的金融監管機構正在構建數碼身份框架，以提升互通性、透明度及保護消費者的，這些要素是以可持續方式整合數碼身份的必要條件。數碼身份生態系統要全面投入使用，必須巧妙平衡監管與技術進步。最終目標是利用數碼身份的特徵，營造安全、高效、人人可用的金融環境。

3.2 與金融服務業數碼身份相關的基本資料元素

在金融領域，數碼身份包含對確保交易安全及符合監管要求的關鍵資料元素。數碼身份具有雙重作用，既能提供獲取服務的途徑，又鞏固消費者及金融機構的安全措施。姓名、出生日期及住址等是數碼身份的基本身份識別要素，用於在帳戶管理過程中進行身份核實、反洗錢核查及驗證。歐洲理事會認識到該等資料元素的重要性，發佈制定國家數碼身份框架的指導方針，強調該等基本資料是數碼身份的核心（見圖表 3）。

資料類型	詳細說明
個人資料	民事登記處通常記錄的個人資料： - 出生日期 - 性別
生物特徵識別資料	個人物理識別碼： - 指紋 - 虹膜掃描 - 面部識別 - 其他生理標記
法律身份資料	在法律及國家層面證明合法身份的資料： - 國民身份證號碼 - 社會保障號碼
人口統計資料	人口特徵： - 年齡 - 民族 - 教育 - 職業 - 婚姻狀態

文件資料	以下身份證明文件上的資料： - 身份證 - 護照 - 駕駛執照 - 其他用於表明身份或獲得服務的官方文件
驗證資料	用於核實數碼身份的憑證： - 密碼 - 個人身份識別碼安全問題 - 數碼證書

圖表 3：一般數碼身份的資料類型[52]

要充分發揮數碼身份的潛力，金融服務業不應只關注身份核實，而需著眼更廣泛的資料點。資料範圍可擴大至包含個人的財務背景、投資行為與偏好、風險狀況等。然而，由於該等資料皆屬保密資料，必須按照嚴格的金融監管標準管理。

例如，在歐盟《通用數據保障條例》(GDPR) 框架內，金融機構必須按照嚴格標準處理及保護個人資料，以確保個人金融數碼身份的安全，維護個人私隱權。[53]同樣，澳洲《消費者數據權利規則》（CDR）賦予消費者安全高效地取用個人金融資料的權力，允許他們與認可第三方共享該等資料。金融機構必須遵守這些法規，實施驗證數碼身份及確保數據安全傳輸的系統。[54]這些監管措施推動生態系統中的所有參與者相互信任，確保形成規範的行業格局。

鑒於更詳盡的數碼身份檔案可以全面細緻地呈現個人身份，[55]就金融服務業而言，可考慮在數碼身份中整合或關聯下列額外資料元素。[56、57、58]儘管如此，必須強調的是，整合該等資料元素到數碼身份必須嚴格遵守用戶同意原則。此舉確保個人資料的使用是透明的，並且僅在獲得用戶明確同意的情況下進行：

[52] 歐洲理事會。（2023 年）。*Guidelines on National Digital Identity*。https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-ID.html
[53] 德勤。（2019 年）。*After the dust settles: How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on*。https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf
[54] 澳洲資料專員辦公室 (The Office of the Australian Information Commissioner)。（日期不詳）。*What is the Consumer Data Right?*。https://www.oaic.gov.au/consumer-data-right/information-for-consumers/what-is-the-consumer-data-right#:~:text=The%20Consumer%20Data%20Right%20allows,that%20best%20suits%20your%20needs。
[55] Oliver Wyman & International Banking Federation。（2021 年 12 月）。*Digital Trust: How Banks Can Secure Our Digital Identity*。https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/Digital-Trust-Final.pdf
[56] BIS。（2022 年 6 月）。*Corporate digital ID: no silver bullet, but a silver lining*。https://www.bis.org/publ/bppdf/bispap126.pdf
[57] 經合組織。（2021 年 12 月 16 日）。*Supporting the Digitalisation of Developing Country Tax Administrations*。https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/supporting-the-digitalisation-of-developing-country-tax-administrations.pdf
[58] 經合組織。（2022 年 6 月 22 日）。*Tax Administration 2022: Comparative Information on OECD and other Advanced and Emerging Economies*。https://www.oecd-ilibrary.org/sites/1e797131-en/1/3/3/index.html?itemId=/content/publication/1e797131-en&_csp_=38baa8bc2bc68a4be5b070db809f1650&itemIGO=oecd&itemContentType=book

- **信用資料**：個人信用評分及信用記錄是重要一項。該等資料如同金融認證指紋，提供了解個人信譽及金融行為的途徑。將該等資料嵌入數碼身份，可以令金融機構在處理貸款、信貸服務及風險管理方面作出明智決策。
- **交易資料**：獲取交易記錄本身並非必需，但可以提供有關消費模式、收入穩定性及金融行為作寶貴資訊。該等資料使金融機構能根據個人偏好更有效地客製化產品及服務。
- **稅務記錄**：透過稅務記錄可全面了解個人的過去收入狀況、納稅情況及負債情況。該等資料可證實收入，對評估財務責任及是否遵守稅收法規至關重要。對金融機構而言，獲取稅務相關記錄能為貸款、投資服務及詐騙檢測相關的決策過程提供參考價值。
- **收入及工作經歷：**納入就業資料，包括前任和現任僱主、工作職位及工資詳情，有助於了解個人的財務穩健性及收入潛力，協助評估各種財務承諾的風險。
- **保險單**：獲取有關現時及過往保險單（如人壽保險、健康保險及財產保險）的詳細情況，能了解個人的風險管理策略。金融機構可以利用此類資料定製保險產品，或將保險方面的考量納入財務規劃服務。
- **擁有權的記錄**：財產或車輛等資產的擁有權文件可為信用評估及財務諮詢服務提供資訊，更全面地展現個人財務狀況。

數碼身份在金融領域扮演著重要角色，應用範圍遠不限於交易及合規監管。透過提供全面資料，數碼身份有助改善金融服務及提升整體客戶體驗。

黃金源數據(**Golden source)**在數碼身份系統的討論中，「黃金源數據」的概念至關重要。這一詞指可靠的一手資料儲存庫，是身份資料準確性與完整性的標桿。持份者在籌劃數碼身份舉措時，必須依據黃金源數據的指導原則及標準看齊，確保身份識別框架的一致性與安全性。數碼身份模式中的「黃金源數據」概念是界定持份者在管理、保護及使用身份資料方面的角色及職責的基本要素。這一權威資料庫或資料來源包含經集中核實的可信身份資料，為各種模式的身份識別流程確立標準。它對合規性、營運完整性及用戶私隱亦有重要意義。[59]

在集中模式、半集中模式及去中心化模式中，黃金源數據 e 的特點及持份者在利用黃金源數據中的作用各不相同。

企業數碼身份是實體企業在數碼世界中的代表，包含企業的法律及營運身份。企業數碼身份儲存著各種經核實的資料，包含公司架構、管治、財務狀況及合規記錄。[60]該數碼檔案包括企業內部變化的最新即時動態，如董事職位變動或架構調整，確保企業的數碼形象準確且最新。

[59] World Wide Generation。（2019 年 11 月 26 日）。*In search of the golden source: non-financial data*。https://www.worldwidegeneration.co/news/in-search-of-the-golden-source-non-financial-data
[60] BIS。（2022 年 6 月）。*Corporate digital ID: no silver bullet, but a silver lining*。https://www.bis.org/publ/bppdf/bispap126.pdf

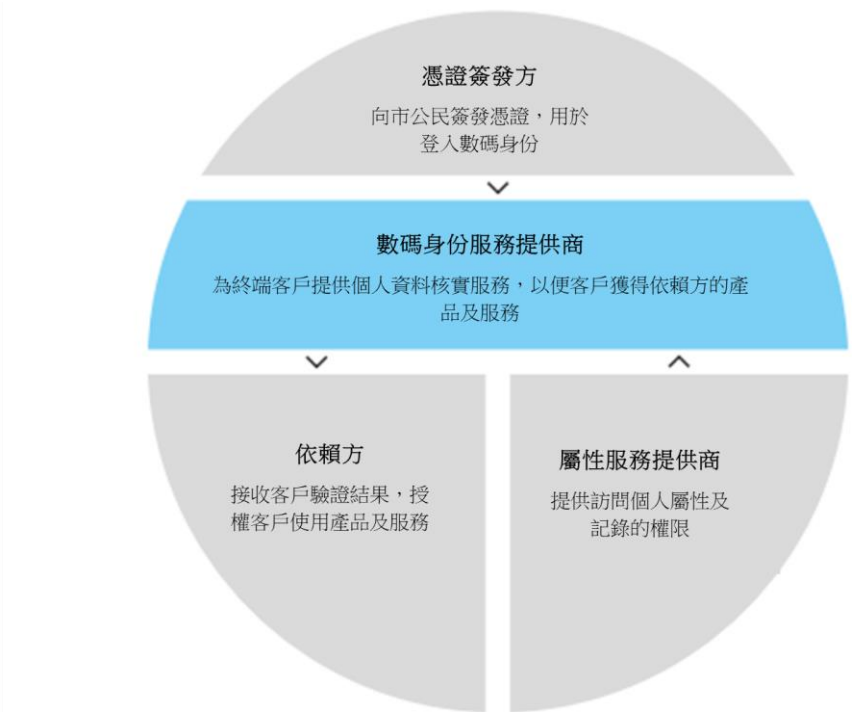
企業數碼身份的應用涵蓋企業營運的多個方面，對於電子交易過程中驗證公司資格、安全獲得金融服務，以及與監管機構保持透明溝通，均至關重要。作為驗證個人或企業的資料中心平台，企業數碼身份有助於在數碼市場中建立信任及促進誠信，同時簡化與供應商、客戶及合作夥伴的互動。

雖然本報告主要關注個人數碼身份，但無可否認，企業數碼身份在業內也有重要作用。本報告後面章節將進一步探討企業數碼身份的意義及功能。

3.3 評估資料模式，整合強大數碼身份

在數碼身份多元應用下，市場上出現各類定製框架以滿足不同場景的特定要求及監管環境。儘管如此，某些持份者始終是數碼身份生態系統中的關鍵支柱。他們的職能或許看似不同，但實際上，一個實體往往同時扮演多種角色，，明數碼身份環境具有高度彈性及相互關聯的性質。

- **憑證簽發方 (Credential issuers)**：這些實體公司負責核實個人身份，並簽發數碼憑證，於未來交易中可驗證個人身份。此項工作通常涉及收集與驗證個人資料和文件，以高度可信的方式來確定身份。
- **身份服務提供商 (ID service providers)**：這些提供商驗證用戶身份，並獲用戶授權與依賴方共享經驗證的身份，使用戶能夠安全地獲得服務或開立帳戶。
- **屬性服務提供商 (Attribute service providers)**：這些實體管理定義用戶屬性的資料。屬性服務提供商在經用戶同意的情況下與依賴方及身份服務提供商共享該等屬性。如果身份服務提供商也處理與屬性相關的服務，則同時履行兩項職責，並遵守對兩種角色的要求。屬性服務提供商負責說明其管理的屬性的質素。
- **依賴方 (Relying parties)**：這些組織使用框架中其他參與者提供的身份及屬性資料，包括航空公司、銀行及零售商等企業。它們依靠身份服務提供商核實用戶身份，依靠屬性服務提供商檢查用戶屬性是否合格。(見圖表 4)



資料來源：奧緯咨詢公司分析

圖表 4 – 各持份者在數碼身份系統中的作用[61]

有效的數碼身份生態系統有賴政府、銀行、科技公司及各種服務提供商等持份者的明確分工與合作。政府設立國民身份框架，確保數碼身份符合法律及監管標準，保護公民私隱及安全。透過公共服務推廣數碼身份，政府可為數碼交易營造可信環境，而數碼交易的成功很大程度上取決於人們對環境的信任程度。

銀行、科技公司及服務提供商等私營機構亦發揮著重要作用。銀行以嚴格的「了解客戶」 (KYC) 流程及信譽著稱，負責核實及保管數碼身份資料。科技公司則構建創新且可擴展的平台及強大的安全架構，為數碼身份提供技術支撐。各行各業的服務提供商將數碼身份整合到消費者交易及服務中。這些持份者必須通力合作，確保打造順暢、以用戶為中心的數碼身份系統，提升系統包容性，促進其廣泛採用。

在金融服務業內整合強大的數碼身份，關鍵在於所用資料模式的架構。該等模式分別採用獨特的數據管理方法，確保安全有效地管理身份資料，共同構成數碼身份生態系統的支柱。(有關持份者在各種身份模式中的詳細作用，請參閱附件 1)。

[61] Oliver Wyman & International Banking Federation。(2021 年 12 月)。*Digital Trust: How Banks Can Secure Our Digital Identity*。https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/Digital-Trust-Final.pdf

3.4 身份核實轉向以用戶為中心— 去中心化身份及自主身份管理

與傳統模式相比，去中心化身份代表身份核實方法朝以用戶為中心的方向轉變。這一模式直接將控制權交到用戶手中，標誌著自主身份的崛起。自主身份框架賦予個人擁有、管理及控制其身份資料的權利。用戶利用數碼身份錢包（安全的儲存庫）收集並儲存由可信機構提供的經核實個人資料，該等可信機構包括政府實體或其他持牌法團。[62]

然而，面對日益突出的資料安全問題，以及公眾對中心化儲存庫的信心不斷降低，這一模式獲得全球關注。市場分析強指出該轉變，預計全球去中心化身份市場將從 2022 年的 2.85 億美元大幅增長至 2027 年的 68 億美元，五年內的複合年均增長率將達到 88.7%。[63]

用戶所有權：去中心化身份與自主身份的核心

以用戶為中心的身份系統的核心在於用戶擁有控制權的原則，即賦予個人控制其身份資料的權利。該原則促進了自主性，是去中心化身份系統的基礎。在該等框架中，自主身份系統強調賦予用戶權利，使個人能夠獨立管理自己的身份。[64]

消費者對個人資料的主權意識不斷提高，近四分之三的受訪者表示對在購買商品及服務時分享個人資料感到不安，此現象體現了賦予用戶權利的趨勢。[65]在此背景下，去中心化身份及自主身份興起，開啟了用戶作主的新時代。

個人設備及安全雲服務將逐漸成為個人資料的保險庫，用戶則承擔起「看門人」的角色。這一轉變不僅賦予個人擁有權，亦降低了與身份盜用及擅自共享資料相關的風險。自主身份減少了對中央核實的依賴，允許用戶按自己的方式驗證憑證，從而保護私隱及促進安全的在線互動。

可核實憑證：在數碼世界建立信任

在去中心化身份框架中，可核實憑證成為關鍵組成部分，增強了數碼互動中的信任與私隱。這些憑證如同數碼證書，包含一系列關於個人的可獨立核實聲明。[66]聲明是實體對自身或他人資料的肯定，包括個人姓名、地址及公共或私營實體發出的識別碼。每項聲明均可單獨核實，為個人身份提供可靠證明。[67]

---

[62] 全球移動通信系統協會。（2022 年）。*Decentralised Identity*。https://www.gsma.com/ID/decentralised-ID
[63] MarketsandMarkets。（2022 年 5 月）。*Decentralized Identity Market by Identity Type, End User, Organization Size, Vertical (BFSI, Government, Healthcare and Life Sciences, Retail and eCommerce, Telecom and IT, Transport and Logistics, Real Estate, Others) and Region - Global forecast to 2027*。 https://www.marketsandmarkets.com/Market-Reports/decentralised-ID-market-59374755.html
[64] Čučko, Š., & Turkanović, M.。（2021 年）。*Decentralized and self-sovereign identity: Systematic mapping study*。IEEE Access, 9, 139009-139027。
[65] Entrust Cybersecurity Institute。（日期不詳）。The Future of ID Report。https://www.entrust.com/cybersecurity-institute/reports/future-of-identity
[66] Brunner, C.、Gallersdörfer, U.、Knirsch, F.、Engel, D. 及 Matthes, F。（2020 年 12 月）。Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust。2020 年第三屆區塊鏈技術與應用國際會議論文集（61-66 頁）。
[67] 萬維網聯盟 (World Wide Web Consortium)。（2019 年 9 月 24 日）。*Verifiable Credentials Use Cases W3C Working Group Note*。https://www.w3.org/TR/vc-use-cases/

例如，可核實憑證可以證實個人的學歷及專業資格。這些由認可機構簽發的憑證可以根據需要無縫整合到電子交易中。這種高效的身份核實方法可簡化流程，提高網上互動的可信度。

可核實憑證的完整性取決於發證實體的加密簽署。[68]該等憑證利用可核實的資料註冊表，即一種安全且能防篡改的分布式分類帳。雖然分佈式分類帳技術因其安全特性而受到青睞，但其他分布式資料庫技術亦可行。作為去中心化資料庫，分佈式分類帳技術可安全記錄交易，防止遭到篡改、駭客攻擊或詐騙，從而確保憑證完好不變。透過採用分佈式分類帳技術，去中心化身份框架防止憑證遭篡改，並為憑證的簽發及核實提供透明的稽查線索，從而營造值得信賴的數碼身份生態系統。

去中心化識別碼：重塑身份概念

萬維網聯盟正視為去中心化的識別碼為重要的標準，是強大的自主身份模式中的另一基本元素。[69]該等識別碼使個人能創建可核實的獨立數碼身份，擺脫傳統集中式且受領域局限的識別方式。這一轉變或會徹底改變數碼身份管理方式。[70]

去中心化識別碼利用加密技術，提供持久、無形而可移植及可廣泛核實身份的方式，適用於多種平台與服務。該方法取代傳統身份驗證方式，簡化流程、增強私隱保護，同時大幅減低資料洩露風險，從而促進網上互動的安全性與完整性。[71]在承認加密技術好處的同時，本報告後續章節將進一步探討實施去中心化識別碼方面的考慮要素。

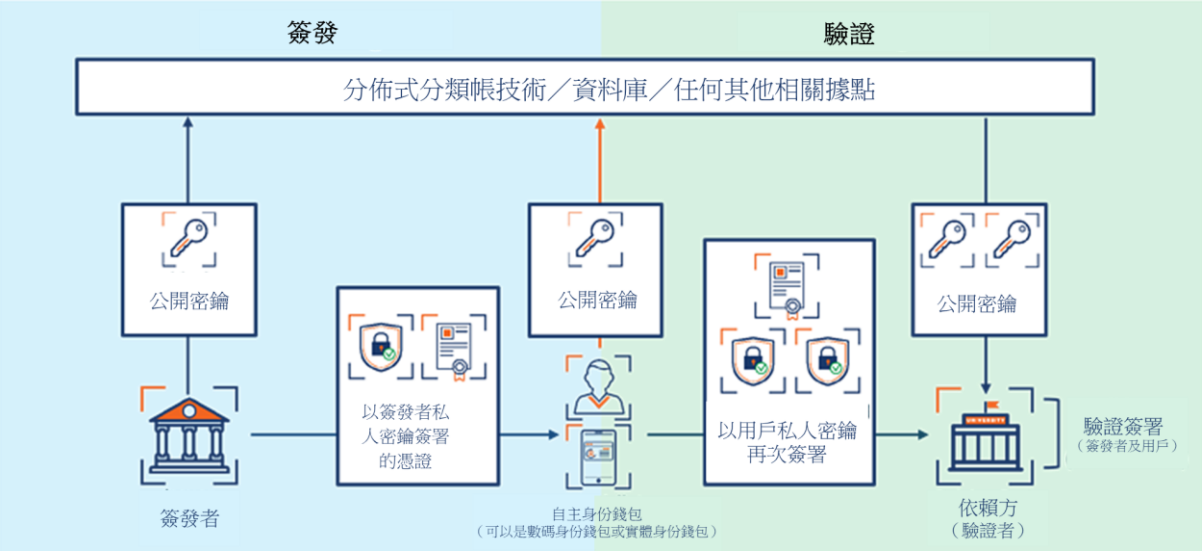
引入去中心化識別碼將為各界持份者帶來廣泛的益處：

- **對於組織而言**，該方法簡化了憑證的安全驗證流程，在提高客戶開戶效率與成本效益的同時，亦減輕了行政負擔。
- **對於個人而言**，該方法帶來前所未有的個人資料控制權，保障個人私隱並預防未經授權的追蹤與數據取用。
- **對於開發人員而言**，該方法鼓勵構建將用戶私隱置於首位的架構系統，摒棄以密碼為中心的傳統安全模式。

於簽發與驗證此類去中心化識別碼的過程中，如政府、教育機構或私營機構等簽發者會建立與用戶公開密鑰（去中心化身份）掛鉤的憑證，隨後存於用戶的數碼或實體自主身份錢包。用戶在需要驗證身

[68] Camilleri, A.、Muramatsu, B. 及 Schmidt, P。（2022 年）。Credentials to Employment: The Last Mile。Digital Credentials Consortium Report。
[69] 萬維網聯盟 (World Wide Web Consortium)。（2022 年 7 月 19 日）。*Decentralized identifiers (DIDs) v1.0*。*W3C Recommendation*。https://www.w3.org/TR/did-core/
[70] Truvity。（日期不詳）。*What is Self-Sovereign Identity?*。https://www.truvity.com/ssi-guide/what-is-self-sovereign-identity#:~:text=Self%2DSovereign%20Identity%20(SSI),on%20centralised%20authorities%20or%20intermediaries。
[71] 納斯達克。（2023 年 9 月 12 日）。*What Are Decentralised Identifiers (DID) And How Will They Boost Web3?*。https://www.nasdaq.com/articles/what-are-decentralized-identifiers-did-and-how-will-they-boost-web3#:~:text=In%20the%20Web3%20paradigm%2C%20individuals,and%20manage%20their%20unique%20identifiers。

份時向驗證者出示用私人密鑰簽署的憑證，而驗證人則對照分布式分類帳或資料庫查核公開密鑰，確認簽署的真偽。(見圖表 5)



資料來源：奧緯咨詢公司, International Banking Federation

圖表 5：*識別碼及其在分布式分類帳技術中的應用*[72]

不同於依賴社交網絡提供商的集中式識別碼或其他自證身份類型，去中心化識別碼由用戶創建並控制，天然具備防跟蹤與分析功能。該等識別碼方便進行安全保密的點對點互動，為建立以信任、私隱及用戶賦權為主的數碼身份生態系統奠定基礎。

去中心化識別碼的適應性遠不止單純的身份識別，亦可用於保障交易安全、加密通訊，以及促進以同意為基礎的資料共享，從而打造更可靠的數碼經濟。隨著去中心化識別碼的潛力在各行各業逐漸顯現，數碼身份有望從功能性組件發展成數碼權利與自主權的重要一環。

國際航空運輸協會的「One ID」項目即為實例。該項目展示了去中心化識別碼在航空旅行體驗中的實際應用，證明效率與安全均有重大提升。[73]該舉措為乘客提供簡化的非接觸式體驗，同時只在徵得用戶同意的情況下取得基本資訊，加強數據私隱。該案例對去中心化識別碼框架的應用，突顯了重塑各行各業互動方式的變革潛力，印證構建更加以用戶主導權和私隱保護為核心的網上交互環境的趨勢。

透過回顧文獻及與業界人士的討論，我們從全球不同市場採用與實施數碼身份的案例中汲取了深刻見解。附件 2 詳細介紹了一些關鍵考慮因素，如全球數碼身份發展背後的驅動力，以及重點介紹選定市場開發與應用數碼身份解決方案的研究案例。

[72] 歐洲理事會。(2023 年)。*Guidelines on National Digital Identity*。https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-ID.html
[73] 國際航空運輸協會 (IATA)。(日期不詳)。*One ID*。https://www.iata.org/en/programs/passenger/one-id/

採用數碼身份的風險與挑戰

數碼身份為金融服務業帶來變革潛力，有望顯著提高安全性、簡化營運及改善客戶關係。然而，要釋放這一潛力，需要把握錯綜複雜的監管格局，有效解決複雜的技術難題。數碼身份的順利整合，需要金融機構、監管機構、技術提供商及消費者等主要持份者深思遠慮、通力合作。

4.1 實施數碼身份解決方案的關鍵考慮因素

金融機構部署數碼身份系統需同時解決機構與監管方面的複雜難題。中央化或半中央化系統面臨的情況尤為複雜，因該等系統須遵循國際法律與統一的全球框架。監管、標準化與網絡安全之間的密切關係至關重要。因為它們共同影響數碼身份解決方案的安全、效率與可靠性。金融機構在實施數碼身份系統時，須隨時掌握該等動態因素，以便在創新與風險管理之間達到平衡。

監管複雜性

駕馭數碼身份的監管環境是金融機構的一項重要任務。除遵循現行法律外，，主動順應監管規例的發展變化是確保未來長期發展的關鍵。金融機構須努力創建能夠隨機應變的合規框架，以滿足當前及未來的監管需求，從而維繫營運完整性及客戶信心。例如《通用數據保障條例》等國際規例為數據保護訂下高標準，一旦要納入考慮，情況會愈發複雜。鑒於金融具有全球性特點，金融機構須採取周全方法，與各種區域法律接軌，以緩減合規差異風險。若要在全球範圍實現監管協調，須制定能隨機應變的策略政策。

增強互通性與標準化

根據世界銀行的身份識別促發展計劃（ID4D），互通性對不同數碼身份系統之間的通信至關重要。互通性要求各身份平台之間實現同步，並與國內外標準進行協調。[74]

金融服務業對全球標準與無縫互通的需求，在數碼身份背景下顯得尤為關鍵。該等標準是促進跨境交易順利進行及國際銀行業務有效運作的根本所在。然而，當前的金融機構因系統無法兼容而面臨重重挑戰，不但拖累業務營運節奏，也同時降低客戶體驗。因此，互通性不僅是一項便利功能，對於旨在擴大市場覆蓋率、整合多元金融體系及確立全球領先地位的機構而言，亦是一項策略要務。

[74] 世界銀行「身份識別促發展」項目 (ID4D)。（日期不詳）。*Interoperability*。https://id4d.worldbank.org/guide/interoperability

在數碼時代，需要跨越領域、行業及邊界的互通性。金融機構須致力實現各種系統及流程的無縫整合，這需要統一技術協議、數據格式及安全框架。雙重認證或高級生物特徵認證等身份驗證方法上的差異，或會影響用戶體驗，放大安全擔憂。[75]

再者，不同司法管轄區的地方規例及私隱法律的差異，不僅使金融實體的營運環境更複雜，更可能導致體驗不一致及安全風險增加。目前業內對推動互通性的支持還不充份。金融機構須積極參與制定跨行業標準，以提升營運效率，及加強安全與私隱保護措施。透過採取積極主動的態度，金融機構能夠為創建更具協作性與安全性的全球市場獻一己之力。滿足全球經濟互聯互通的需求，確保金融業用戶進行順暢安全的互動，這一承諾必不可少。[76]

網絡安全與資料保護

採用數碼身份管理，使網絡安全成為金融機構關注的焦點。資料洩露不僅會帶來巨大經濟損失，更會給聲譽造成不可恢復的傷害。因此，制定全面的安全策略至關重要，其中須涵蓋先進的加密技術、持續監控、高級威脅檢測及穩健的事件應急響應機制，以抵禦持續演變的網絡威脅。

網絡安全措施的有效性並非完全依賴技術，亦取決於個人警惕性與程序嚴密性。金融機構須培育網絡安全意識文化，實施嚴格的取用管控措施及持續的安全稽查，以保護數碼身份。

資料保護必須是數碼身份系統不可或缺的一部分。「貫徹私隱設計」方法確保將私隱考量融入每個開發階段，這對遏制網絡攻擊至關重要。該方法有助於打擊針對系統漏洞及人為因素的複雜網絡攻擊。隨著雲解決方案日漸普及，資料著色、運用公鑰基建、數碼指紋及水印等創新技術帶來額外安全保障。該等方法對於從開始直至儲存處理全程保護身份資料必不可少。

總括來說，保護數碼身份系統的安全，需要採用集尖端技術、持續教育及嚴密程序為一體的綜合方法。積極主動的防禦策略對於為金融服務業維繫安全可信的數碼身份環境不可或缺。

量子威脅與挑戰

量子計算的興起對保護身份解決方案的既有安全加密系統構成嚴峻挑戰，而身份解決方案對於保護金融、政府及個人資料的安全至關重要。[77]量子計算已從理論概念發展到實際應用，能夠透過 秀爾演算法(Shor's Algorithm) 等算法破解傳統加密協議，如 Rivest-Shamir-Adleman (RSA)與橢圓曲線密碼

[75] Wang, C.、Wang, Y.、Chen, Y.、Liu, H.及 Liu, J。(2020 年)。User authentication on mobile devices: Approaches, threats and trends。Computer Networks, 170, 107118。
[76] ENISA。(2023 年 7 月 3 日)。*Digital ID Standards*。https://www.enisa.europa.eu/publications/digital-ID-standards
[77] 安永。(2023 年 8 月)。Quantum Power Play: Navigating the New Landscape of Cybersecurity and Defence。
https://www.ey.com/en_au/cybersecurity/quantum-power-play-navigating-the-new-landscape-of-cybersecurity-and-defence

學 (ECC) 等加密系統。[78]由於穩健的資料保護對該等行業至為重要，這對於金融業等行業而言帶來重大隱患。

有見及此，加密系統需迅速過渡至抗量子加密 (QRC) 。隨著量子計算的不斷進步，既有加密系統的漏洞增加，故有必要立即改用抗量子算法。這一轉變涉及複雜的基建更新、新加密標準的採用及全面的系統測試，以確保在維繫既有系統兼容性的同時，實現抵禦量子攻擊的韌性。

全球正在採取積極主動的措施。例如，美國已發佈第 10 號《國家安全備忘錄》[79]，授權政府機構採用抗量子加密技術。這顯示了全球協調行動以有效緩減量子風險的必要性。金融行業宜與政府機構攜手，優先考慮制定並實施能夠抵禦潛在量子干擾的安全技術。這對於在後量子世界維繫數碼身份的保密性與完整性實屬關鍵。

當前，將生物特徵識別技術融入身份框架的做法，為抗量子安全增加了一重保障。指紋及虹膜掃描等獨一無二的識別碼，即便是最為先進的量子計算也難以複製或解碼，故可提高數據的安全性及可核實性。融合該等技術加強了數碼生態系統抵禦潛在安全風險的能力，亦提高了用戶在數碼互動中的信任度與可靠性。

可擴展性與技術運用

數碼身份系統須具可擴展性，以配合日益增長的用戶數量與交易量，同時又不影響性能或安全。從投資穩健的雲端基建、模塊化設計及人工智能等科技，可實現高效的可擴展性。此外，還需採取措施確保各個社會群體都可以公平使用數碼身份系統，包括無銀行帳戶的人群及弱勢群體。消除數碼鴻溝需要制定配合社會各階層需求的技術解決方案同時該舉措能提升數碼素養。金融機構有責任提供共融服務，通過對用戶的宣傳教育以實現數碼生態系統普及化。

法律與道德複雜性

作為跨國運營的金融機構，需處理錯綜複雜的法律與道德問題。它們須遵守很多有關跨境數據流與主權的法律規定，同時亦要堅守道德原則，以確保通過公平的數碼身份得到金融服務，並在徵得明確同意的基礎上合理地使用數據。

在推動創新與卓越服務的同時，機構須兼顧道德判斷。高效部署數碼身份取決需通過深思熟慮的方法來應對該等重大挑戰。

[78] Arel, R。(2023 年 5 月 12 日)。*Explore the impact of quantum computing on cryptography*。*TechTarget*。https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography
[79] 白宮。(2022 年 5 月 4 日)。*National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*。https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

歸根結底，金融機構的策略方向涉及採取協同方針、共同構建統一的監管環境、倡導創建全面的全球互通性標準、把網絡安全放在首位、確保技術解決方案的可擴展性、以及嚴格遵循既有法律與道德準則。此種策略將成為數碼身份的基石，推動金融服務業重塑格局。

數據濫用

數據濫用已成為影響深遠但又難以防範的風險。不僅破壞用戶私隱，也會嚴重損害公眾對機構的信任。這種現象涉及透過有違道德的方式擅自收集與使用數碼身份資料。從共享敏感數據到擅自利用個人身份謀利，其負面影響尤為嚴重。除侵犯個人私隱外，它還造成系統性漏洞，進而影響整個金融服務架構的運行。

隨著金融機構將數碼身份融入業務中，數據利用的風險也在擴大。面對此形勢，需要及時的監管與嚴格的控制。世界經濟論壇指出，某些形式的數碼身份或會成為數據利用的潛在入口。應對數據利用相關風險，既需監管約束，亦需科技設防。政府與金融機構須通力合作，確保該等數碼身份得到安全且合乎道德的管理。融合先進網絡安全措施與健全私隱政策及透明實踐的綜合方法至關重要。各方面協調行動對於緩減數據利用風險及促進消費者與持份者之間的持久信任十分必要。

金融機構須秉承「貫徹私隱設計」原則，主動預測及防範安全漏洞。這一承諾包括部署精密的加密技術、實施嚴格的取用控制措施，以及在整個組織內灌輸網絡安全意識文化。此外，堅持知情同意原則亦至關重要，它能確保個人對自身數據及使用情況的控制權。

4.2 應對去中心化身份的複雜局面：潛力與挑戰

如前所述，去中心化身份系統代表網上個人身份管理的開創性方法。要理解去中心化身份系統的繁雜之處，需要關注該創新方法的科技基礎。本節將深入探討分布式分類帳技術的作用、去中心化網絡內的具體互通性協議，以及與採用這一新型技術框架相關的內在用戶體驗難題。

互通性

實現互通性是發展去中心化身份系統的核心難題。與傳統數碼身份不同,去中心化身份需要與大量平台和服務無縫整合,以創造一致的用戶體驗。當前格局透過碎片化管理來實現用戶體驗的一致性，其特點是多種專有系統與標準共存，有礙身份憑證在不同生態系統之間的順暢交換。消除該等壁壘需要全行業展開合作，採用通用協議與標準。這種合作方式在去中心化系統中尤為重要，因為分布式分類帳技

術型平台架構的迥異會產生額外的整合互通性要求，從而促進不同分布式分類帳技術型網絡之間的協作。透過實現無縫交互，該等標準便可提升用戶體驗，擴展去中心化身份解決方案的覆蓋率。[80]

用戶接受度與去中心化身份

去中心化身份系統的廣泛採用有賴於培養用戶接受度，從而建立信任。去中心化系統具有更高的安全性、私隱性及用戶控制權，而該等優勢須作出有效宣傳。此項工作的核心是簡化用戶界面，推進從傳統系統到去中心化系統過渡。此外，圍繞去中心化身份的運作及優勢展開公眾教育亦必不可少。教育工作應包括公開討論數據處理與保護措施，同時展示去中心化系統能夠提供的實際優勢，比如使交易更快捷安全。

可擴展性與技術局限

可擴展性依然是去中心化身份系統面臨的多元挑戰，因為該等系統須在維持效率與經濟效益的同時，適應持續擴大的用戶群與交易量。作為常用基礎架構，分布式分類帳技術型平台頻繁遭遇擴展性問題，例如交易速度變慢及成本攀升。要應對這些挑戰，技術創新是關鍵所在。這包括開發第二層解決方案、改善共識機制，以及採納更可持續的技術—這些都對獲得公眾認可及促進去中心化身份在日常交易中的實際應用至關重要。金發局於 2024 年 3 月發佈一份有關金融服務業利用分布式分類帳技術的情況報告。該報告分析了分布式分類帳技術所帶來的風險與挑戰，並為其廣泛採用提出建議。

法律、私隱、安全及管治問題

去中心化身份系統為個人資料控制權帶來範式轉變，這對傳統的隱私保護規範如《通用數據保障條例》等框架帶來挑戰。要在分佈式環境中管理數據擁有權、同意權與刪除權，就必須通力合作，構建契合去中心化模式的新型監管框架，確保對系統操作性實施統一的國際監管。

去中心化身份系統的私隱與安全功能，取決於強大的技術與安全組件，例如智能合約。為維護系統完整性，定期進行安全稽查與主動實施漏洞管理是關鍵。[81]此外，公共分類帳可能有暴露個人資料的潛在風險，需要求整合私隱保護技術如零知識證明，並需仔細審視其法律含義。

再者，有效的密鑰管理亦是確保去中心化身份系統安全的重要一環。透過密鑰輪換定期更新加密密鑰，可防止未經授權的取用及減緩密鑰洩露的影響。[82]可是，在去中心化環境中管理密鑰輪換是一項

[80] 歐盟區塊鏈觀察與論壇 (EU Blockchain Observatory and Forum)。（2023 年 11 月 29 日）。*The current state of interoperability between blockchain networks*。https://blockchain-observatory.ec.europa.eu/news/press-release-eu-blockchain-observatory-and-forum-announces-release-landmark-report-blockchain-2023-11-29_en
[81] Dock。（2024 年 1 月 11 日）。*Decentralised ID: The Ultimate Guide 2024*。https://www.dock.io/post/decentralised-ID
[82] Smith, S. M。（日期不詳）。*Key Management for Self-Sovereign Identity*。
https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/10-ssi-key-management.pdf

重大挑戰，需要有安全機制來更新、撤銷並在整個網絡中精準傳遞該等變更。[83]如若未能有效管理該流程，會給系統留下漏洞，從而可能使用過期或已遭洩露的密鑰，損害系統整體安全性。

去中心化系統內的管治需要從集權模式轉為分散模式，分別對更新、爭議解決與監管合規方面進行監督。[84]該等模式須在參與者自治與集體管治之間取得平衡，確保在不同法律與監管環境中實現公平決策。此外，有效管治須能夠促進在不同司法管轄區持續合規，並持平地解決衝突。制定尊重文化、法律及道德差異的管治框架對獲得廣泛接受至關重要。

雖然部分國家在制定相關框架方面已取得進展,但專門針對去中心化身份的全球性綜合法律與管治方法仍處於萌芽階段。中國內地推出的實名身份認證 DID 計劃代表了朝這個方向邁出的重要一步, 其深遠影響將在本報告後續章節中詳細討論。

[83] Smith, S. M。(日期不詳)。*Key Management for Self-Sovereign Identity*。
https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/10-ssi-key-management.pdf
[84] Rikken, O.、Janssen, M. 及 Kwee, Z。(2019 年)。Governance challenges of blockchain and decentralized autonomous organizations。Information Polity, 24(4), 397-417。

政策建議

數碼身份已成為數碼轉型領域的基本要素，對金融服務業而言尤為重要。它在緊跟快速數碼化節奏與配合持續升級的客戶期望方面扮演關鍵角色。

香港在強化數碼身份與數據共享能力方面已取得長足進展，反映公私營部門的通力合作。「智方便」平台自 2020 年推出以來，簡化了身份核實流程，提升了客戶開戶體驗。該系統提供了一個集成的數碼服務中心，融合了身份驗證、表單填寫、個人化通知以及電子簽名等功能，促進了市民、公共服務機構和私營企業之間的無縫數碼化互動。

於企業層面，2022 年推出的商業數據通 (CDI)，展示數據交互在安全性和便捷性方面取得的發展。作為資料提供者和金融機構之間的接口，CDI 簡化了信用評估流程並推動了對中小企業的金融包容性。此外，2024-25 年度預算案宣布開發「數位企業 ID」，即「智方便」的商業版本。[85]目標是於 2026 年推出，將 180 萬家本地企業納入該企業平台。

此外，法律實體識別編碼 (LEI) 的持續融合，提升了交易透明度和信任度，尤其是在跨境交易中發揮了重要作用。在。該等舉措在銀行、證券、保險等金融界別均取得良好發展勢頭。附件 中會詳細介紹了上述舉措。

在該等成就的基礎之上，香港政府透過數字化經濟發展委員會的工作，展現持續改進的決心。數字化經濟發展委員會近期呈遞的提案旨在加強香港數碼政策框架與基建。該等提案包括完善管治框架、優化政策的制定與實施，從而構建統一的企業數碼身份，並在更多界別推廣商業數據通及「授權數據交換閘」。[86][87]

奠定此基礎後，下一關鍵任務便是發展成熟的數碼身份生態系統。此生態系統須促進數碼身份解決方案的快速發展，並解決安全、私隱、監管合規及維護用戶信任方面的問題。

本節概述的政策建議闡明了一項策略方針，即善用香港既有基建及支援，在構建穩健數碼身份生態系統的同時，填補現有差距。目標是創建一個具有韌性、以用戶為中心，並能與全球框架接軌的數碼身份解決方案，進而推動經濟發展與創新，提高公信力。

[85] 2024-25 年度財政預算案。 https://www.budget.gov.hk/2024/eng/pdf/e_budget_speech_2024-25.pdf
[86] 「授權數據交換閘」正建構中，讓市民可選擇授 權 相 關政府部門透過系統及數據互通的方式交換其個人資料，並以單一數碼身份認證進行政府和商業網上交易。立法會。 (2024 年 5 月 13 日)。 資訊科技及廣播事務委員會 (會議議程) – 有關“數碼企業身份”平台的背景資料簡介。https://www.legco.gov.hk/yr2024/english/panels/itb/papers/itb20240513cb1-552-3-e.pdf
[87] 香港特區政府數字化經濟發展委員會。(2024 年 2 月)。*《數字化經濟發展委員會核心建議》*。香港特區政府。 https://www.itib.gov.hk/assets/files/DEDC_Core_Recommendations_Eng_issued.pdf

該等建議旨在為未來設定方向，使數碼身份能夠促進而非阻礙數碼世界的增長與活力，特別是對金融服務業而言。

建議 1：公私協同 — 探索「智方便」計劃更全面貫通實施，並賦能私營數碼身份錢包的發展

個人對自身的資料控制權已成為現代數碼經濟的核心要點。在數據洩露頻頻發生的環境下，個人逐步尋求對自身數據的自主權，以確保個人資料的安全與隱私得到保護。數碼身份錢包以變革性解決方案的姿態出現，開創全新的個人資料儲存、管理及共享範式。此方法以用戶為中心，以「使用者同意」為先的概念，近期受到全球廣泛關注。

全面施行「智方便」

「智方便」平台在推動香港數碼身份環境的發展方面發揮著重要作用。作為集中式平台，「智方便」與數碼身份錢包的功能類似，具多種職能，包括簽發憑證、提供數碼身份服務以及作為可信實體提供核實與屬性。「智方便」在身份核實方面發揮主要作用，善用對政府數據的取用權限充當可靠「黃金資料源」，正如前文所述，簡化市民使用各種公私營服務的流程。

不過，為充份發揮潛能，「智方便」必須與時俱進，配合用戶與服務提供商持續變化的需求，努力深化與更廣泛的生態系統的整合，這對需要增強互通性的金融服務業而言尤為重要。

雖然現時「智方便」系統已實現與多個政府部門的數據同步共享，但要進一步擴大同步範圍及與公共服務的整合，對廣泛採納與使用該系統十分重要。有鑑於此，政府資訊科技總監辦公室(OGCIO) 現正構建「授權數據交換閘」(CDEG)，計劃於 2024 年底正式推出。「授權數據交換閘」旨在為促進政府與金融機構的數據共享，彌合政府持有的數據與金融實體之間的差距，促進更加一體化的數位生態系統。

為優化生態系統，政府部門必須增加協作，特別是針對某些受法律限制而無法納入系統的數據。例如，受《稅務條例》約束的稅務資料無法共享等情況。可在政府高層討論與策略指導中探索對該等規例進行修改，以便建立更為全面的數碼檔案，促進個人與企業的採用。

私營數碼身份錢包的作用及其與「智方便」的共存

構建強大的數碼身份生態系統不僅需要政府同心協力，更需要公共機構與私營部門攜手合作。「智方便」作為互聯為基礎的一個數碼身份認證平台，為政府、公共和私營組織提供線上身份認證的服務，體現了個人數碼身份錢包的概念。然而，但蓬勃發展的數碼經濟需要私營部門的相應數據與服務同行。

私營部門每天會產生大量數碼身份，提供單獨、私營專用的數碼身份錢包。[88]法律認證服務提供商依據政府界定的信任框架營運，其支援將有利於該等私營數碼身份錢包。這種方法鼓勵用戶選擇，並促進私營數碼身份錢包在生態系統中的發展。

同時，「智方便」也是私營數位身份解決方案的「黃金資料源」。通過「智方便」，資料擁有者可以在獲得使用者授權的前提下，即時核查必要的資訊和狀態，而無需向對方透露任何額外的個人隱私數據。這種安排將鼓勵以市場為導向的快速應變與創新，使私營數碼身份錢包在政府以外的領域發揮作用。該等措施最終會促進經濟擴張，亦可能將服務範圍擴大至國際用戶。

政府主導的數碼身份錢包與私營數碼身份錢包共存，在未來有望形成共生生態系統，推動循序發展與創新。「智方便」已邀請私營企業參與沙盒計劃，共同開發與該平台兼容的服務，利用其數據與身份憑證實現各種功能，例如身份核實與遙距開戶。雖然基礎概念已經明確，但有必要制定更為詳細的路線圖或解釋框架，以促進該部門的動態發展。

總而言之，香港數碼身份的未來有賴於在確保用戶自主權與促進技術創新之間實現巧妙平衡。隨著「智方便」的持續發展，其與政府及私營數碼錢包的整合將開創一個安全、高效及以用戶為中心的身份管理新時代，使香港走在全球數碼經濟的前列。

建議 2：為數碼身份生態系統制定數位身份信任框架[89]

隨著數碼版圖的擴大，對強大身份核實以及安全網上互動的需求愈發明顯。在此背景下，有必要制定數位身份信任框，確保數碼經濟的健全。該框架有望打造一個更具凝聚力的數碼環境，讓用戶可以放心交易，機構可以大膽創新，同時不會損害安全與私隱。香港可從澳洲、加拿大、瑞士及英國等國家提出的類似框架中汲取寶貴經驗。

當組織在各自獨立的情況下運作，缺乏在創建和管理數字身份方面的共同基礎時，就會面臨挑戰。這種碎片化使得建立信任變得困難。為應對這一問題，與數字身份信任框架保持一致，代表了組織對維護嚴格數據保護和隱私標準的承諾。通過提供立法、標準和良好實踐指南等共同方向和共同理解，該框架建立了一種統一的方法來處理包容性、隱私、數據保護、欺詐管理和安全性。這種統一性促進了數字身份及屬性的統一描述，從而建立了一個信息共享既簡化又安全的網絡。

[88] Open Identity Exchange。（2023 年 10 月）。*Governments and Digital Wallet*。https://openidentityexchange.org/user_assets/706.pdf
[89] 英國政府。（2023 年 1 月）。*Policy paper UK digital identity and attributes trust framework alpha v1 (0.1)*。https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

為了增強可訪問性和理解力，該框架應包括詳細的使用案例，說明其在各個行業中的實際應用，展示其如何增強安全性、隱私和用戶體驗。該框架可以基於現有的安全程序，進一步提升採用「智方便」的線上服務提供商所需的這些標準。

所有相關文件可以整合並展示在一個資料庫網站上，包括政府的願景、路線圖和相關倡議。這提供了一個數字身份領域戰略方向和持續努力的透明視角。建議定期進行行業諮詢，以制定全面的數字化戰略和路線圖，這在金發局於 2024 年 3 月發佈的一份關於區塊鏈技術在推動香港金融服務業的潛力報告中有所強調。此外，可以在這一框架內設立一個專門的工作小組，監控全球密碼學標準的演變，確保香港在應對包括量子計算在內的新興威脅時保持韌性。

隨著生態系統的不斷演變，可以引入數字身份解決方案提供商的認證計劃，以進一步增強框架的穩健性。這種認證確保了共享信息的準確性和可靠性，經認證的組織將在框架網站上展示以供參考。遵守這些基於結果的規則可以保證實現特定目標，而不要求使用特定技術或流程。這種方法支持創新，賦予服務提供商靈活性來開發和定制其產品，以最好地服務其用戶，同時保持互操作性並遵守開放技術標準。

建議 3：雙管齊下促互通：改善基建及法律框架提升數位身份的互聯互通能力

數碼身份的無縫使用及相關資料在公司、部門與行業之間的交換，包括政府數碼身份錢包與私營數碼身份錢包之間的交互，均至關重要。我們的願景是跨越國界，制定能便捷聯通世界的數碼身份解決方案。

一個健全且廣獲認可的數碼身份取決於可互通的基建與穩健的法律框架這兩大支柱。同時解決這兩大議題關乎解決方案的成功。互通性須納入數碼身份系統架構，以便實現不同平台與網絡之間的無縫連接與通信。在技術規範中達成此共識是減少用戶與服務供應商摩擦的關鍵。

此外，各組織與行業須在共同標準與協議方面團結一致。要在金融服務中高效部署數碼身份，務必提高互通性標準。為此，主要監管機構與私營部門攜手合作是關鍵。此策略不但能促進順暢整合，擴大應用範圍，尤其是在國際上推廣而且能契合監管規定與實際行業需求。這對支援全球金融業務及提高工作成效相當重要。於 2021 年 4 月發佈的數碼身份指南特別強調審慎管理數碼身份的重要性。[90]

[90] 香港電腦保安事故協調中心。（2021 年 4 月）。保護你的數碼身分。https://www.cybersecurity.hk/images/resources/digitalidentity_en.pdf

此外，還需制定平衡且值得信賴的法律框架作為輔助。在《個人資料（私隱）條例》等既有框架中納入具體標準或認證計劃，將能提供必要管治，確保數碼身份管理中的安全性、私隱性及合規性。此舉可推動其他數碼身份服務提供商的發展。當用戶與企業的數碼身份在數碼世界的複雜網絡中穿梭時，法律框架能提供他們所需的保障。法律框架是支援技術基建的信任支柱，確保數碼身份生態系統的凝聚力與安全性。

在金融服務業整合數碼身份解決方案時，須優先考慮互通性，同時保護敏感數據及遵循嚴格的核實與監管規定。金融服務業本就複雜，存在詐騙風險，且受嚴格的反洗錢及「了解客戶」規定約束，理應制定專門的標準框架。這種框架將為金融機構提供精準指導，促進合規及緩減風險。

數碼港與政府資訊科技總監辦公室於「智方便」平台上推出的監管沙盒計劃，在橋接監管合規與創新方面發揮著重要作用。該平台在可控環境中對金融科技解決方案（包括數碼身份相關金融科技解決方案）進行測試，推動創新。為充份實現沙盒潛力，迫切需要追加投資及擴大沙盒。確保政府資訊科技總監辦公室轄下的專責小組擁有充足的資源至關重要，這可以通過從相關部門抽調專家及引進專業知識來實現。該小組在管理沙盒運作以及促進與各監管機構的協調工作方面發揮著關鍵作用。該專責小組將提供必要協調與支援，讓創新人員充分利用「智方便」的基建來開發符合金融業特殊需求的解決方案。該等精準策略支援將助力金融業在數碼時代大放異彩。

建議 4：協調數碼身份認證標準，實現跨境身份認證機制的無縫對接

香港正透過建設數碼身份基建，力求促進本地交易，實現在大灣區內的無縫互動，進而提高其在全球經濟中的地位。此舉的核心在於納入「大灣區數據傳輸標準合同」作為穩健框架，確保個人資料跨境傳輸的標準化與安全性。這一框架不僅對於強化數碼身份的功能至關重要，對於在國際交易與數據交換中建立信任亦是如此。[91]

兼容性或互通性原則可確保香港簽發的數碼身份能夠在不同服務、行業與地區獲得廣泛認可與接受，亦為此類數碼身份在大灣區獲得承認創造條件，從而推動安全、高效交易與數據交換。此互通性有望擴大範圍，為香港數碼身份獲得全球認可奠定基礎，進而為國際貿易鋪路，並為全球數碼身份協定訂立基準。

[91] 政府資訊科技總監辦公室。（2023 年）。*促進粵港澳大灣區數據跨境流動。香港特別行政區政府。*
https://www.ogcio.gov.hk/en/our_work/business/cross-boundary_data_flow/

互通性與標準數據合同具有深遠的連鎖效應。它們簡化國際交易流程，鞏固貿易產業，亦有可能為全球數碼身份協定訂立新的基準。實現這一願景需要與大灣區及國際監管實體的監管人士協作，根據全球最佳實踐協調數碼身份標準及數據傳輸協議。[92]

香港應完善法律框架，大力支援數碼身份，透過徵詢公眾意見及制定明確、全面的指引，確保數據交換的私隱與安全。這涉及實施先進的技術基建，並採取可靠的安全措施，來應對網絡威脅，尤其是跨境活動涉及的網絡威脅。與領先科技公司及國際機構建立策略夥伴關係，將擴大數碼身份倡議的影響力與可信度。邀請公私營部門持份者參與，對數碼身份的實際應用與廣泛採用至關重要。

香港致力構建全球認可的數碼身份系統，彰顯其追求創新與國際合作的決心。透過促進數碼身份互認，香港市民可在全球使用自己的數碼身份，而企業可接受其他司法管轄區的數碼身份，進而鞏固香港在數碼經濟中的關鍵地位。

建議 5：增強對可信數碼身份採用的教育宣傳和推動社會賦權

推出激勵措施，實施分階段推廣策略

「智方便」等數碼身份平台的成功部署依賴於公眾信任與理解。教育宣傳及建立信任的舉措至關重要，特別是對金融服務等私營敏感性行業而言。透過闡明數碼身份的優點與保障措施，我們可以營造推動數碼身份獲廣泛接納的有利環境。

制定周詳的政策框架對鼓勵採用數碼身份解決方案至關重要。此外，提供財務和技術激勵可以減輕企業整合數碼身份的成本。再者，為了展示機構對中央數碼身份系統的廣泛訪問，我們應參考香港在銀行、支付和電子錢包營運商之間成功實施快速支付系統的經驗。營造支持初創企業的環境也可以帶來數碼身份創新方法的激增。公私合作夥伴關係在這方面發揮關鍵作用，創造既易用又經濟實惠的數碼身份解決方案，彌合公眾需求與市場機遇之間的差距。

個人採用的關鍵在於使數碼身份流程簡單、包容且安全。強大的個人資料保護和透明的數據管理可以建立信任。簡化數碼身份的獲取和使用可以鼓勵不同人群廣泛使用。引入選擇加入/退出機制可以讓居民根據自身需求和舒適度選擇是否使用「智方便」作為其數碼身份。

[92] 香港政府。（2023 年 10 月 25 日）。*《行政長官 2023 年施政報告》*。https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

分階段實施方法可以確保平穩過渡。從非關鍵政府服務開始，讓個人逐漸適應數碼身份生態系統。隨著社區對技術越來越適應，範圍可以擴展到更多基本服務。在這個過渡期間，確保提供替代服務獲取方式為關鍵，以防止數碼排斥。

「智方便」的建立體現了部署數碼身份解決方案的分階段策略方法。截至 2024 年 5 月，已有超過 270 萬註冊用戶，以及來自政府、公共和私營機構的 370 多項在線服務已在「智方便」上提供。這種分階段推出確保了以可管理的方式引入更多基本服務，最終目標是提供一站式個人化數碼服務平台。通過全面採用「智方便」，香港希望到 2025 年實現「政府網上服務單一門戶」的願景。

隨著政府服務越來越多地整合「智方便」，市民對其使用也越來越熟練，私營部門可能會認識到其優勢。這種認識可以激發企業開發兼容平台，創造一個協同生態系統，政府倡議和私營部門創新相互促進採用。結果是形成一個凝聚力強、不斷擴大的數碼身份使用網絡，為持續增長和創新奠定基礎。

展開宣傳教育，提高公眾意識

「智方便」等數碼身份系統的成功實施與廣泛應用在相當大程度上取決於公眾信任與意識。有見及此，我們迫切需要大力展開提升公眾意識的宣傳教育活動，闡明數碼身份的優勢與機制，消除誤解，並展示數碼身份的實際效用，尤其是在金融服務業。

政府資訊科技總監辦公室一直積極組織各行各業參與活動，務必再接再厲，尤其是在金融領域。目標明確的教育活動對建立信任及推動「智方便」的採用而言必不可少。向數碼身份轉型有望重塑金融服務的格局，帶來前所未有的高效、安全與用戶便利。然而，要獲得該等優勢，行業須全面了解並熟練應用該等技術。

為此，擬定策略提倡從多個維度展開針對性教育活動，以配合企業與金融界的不同要求與顧慮。該等活動宜專注於展現「智方便」及潛在私營數碼身份錢包帶來的營運效益與競爭優勢。諸如工作坊與研討會等互動式學習單元，可讓參與者深刻理解數碼身份如何與既有基建無縫整合。這包括改善客戶服務、減少詐騙，及掃除監管合規障礙。

該等舉措須具包容性，面向金融業務的各個層面，培育數碼素養文化。量身定製的訓練單元將為員工裝備技能，以協助客戶採用「智方便」系統，優化客戶體驗及增強他們對數碼身份系統的信任。

此外，該等教育活動可擴展至金融機構以外範疇，邀請更廣泛的商業生態系統參與其中。透過在活動中展示「智方便」及潛在私營數碼身份錢包在從貸款融通到資產管理的各種金融交易中的廣泛應用，採用數碼身份帶來的實際價值及策略優勢不言自明。闡明數碼身份如何催生創新業務模式與新型營收渠道，從而在金融服務業培育進取及創新文化，這點非常重要。

同舟共濟：廣納行業觀點，實現統一進展

有效協調所有利益相關者的努力，需要採取協調一致的多邊方法。如十月發佈的《2023 年施政報告》所述，政府計劃成立數字政策辦公室，負責督導政府數碼策略、數據管治及資訊科技。[93]

鑒於數碼身份對企業和個人的重要性，建議在這個新辦公室內設立專門的數碼身份工作組或指導小組，專注於金融領域，這是一個策略性舉措。該工作組由金融機構和金融科技公司的代表組成，將成為連接不同領域的橋樑。其首要目標是制定詳細策略，明確金融服務業內各實體的角色和責任。此外，它將指導行業發展，確保各項舉措與更廣泛的策略目標保持一致。

工作組的職責包括建立持續對話、意見交流和反饋的平台，以確保數碼身份基礎設施滿足金融業的獨特需求。為促進開放溝通並分享最佳實踐和行業特定見解，召開定期的利益相關者會議和工作坊至關重要。這些互動為利益相關者提供機會，以建立夥伴關係、同步努力，並使活動與數碼身份倡議的總體目標保持一致。這種協作努力至關重要，因為它們確保邁向數碼未來的進程是由集體努力和共同願景驅動的。

[93] 香港政府。（2023 年 10 月 25 日）。*《行政長官 2023 年施政報告》*。https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

結語

數碼身份的發展與金融服務乃至整體經濟正在經歷的數碼轉型密不可分。這些系統通過利用生物識別和密碼學等先進技術，重新定義了可及性、安全性和效率。因此，數碼身份已成為日常運營不可或缺的一部分，在防範網絡威脅的同時，促進快速、無縫的交易。其在維護消費者信任和確保全球市場競爭優勢方面的關鍵作用不容忽視。

香港通過策略性實施「智方便」等舉措及相關措施，為蓬勃發展的數碼身份生態系統奠定了堅實基礎。通過進一步整合多元化的私人身份解決方案，並在共同商定的信任框架內運作，香港可以加速數碼身份的發展和採用，使自己成為全球數碼創新和金融治理的領先者。這個包容性框架賦予利益相關者提升運營能力、使技術解決方案與戰略目標保持一致，並促進跨部門協作的能力。此外，它提供了獲取關鍵資源的途徑，並協助應對監管複雜性，最終推動數碼化轉型的重大成果。

為充份發揮此潛力，香港應繼續完善及擴展其數碼身份基建。優先考慮互操作性、基礎設施改進和標準協調將強化數碼生態系統，確保其能夠持續回應金融業不斷變化的需求，並催化更廣泛的經濟效益，包括創新商業模式的湧現和各行業數碼化轉型的加速。

通過建立完善且有效部署的數碼身份生態系統，香港不僅鞏固了其作為數碼創新領導者的地位，還提升了國際合作和連通性的能力。通過展示金融治理方面有效的國際合作，香港鞏固了其作為全球金融中心的地位，並在國際市場中保持競爭優勢。因此，在這個快速演進的數碼時代，擁抱數碼身份系統的變革潛力對於香港持續成為國際金融中心和科技創新樞紐至關重要。

附件 1：持份者在各種數碼身份模式中的作用

集中模式：在以政府為中心的集中式系統中，政府是主要持份者，是「黃金資料源」儲存庫的保管人。政府負責按照反洗錢法及「了解客戶」等國家規例及標準創建、更新及維繫該權威性資料庫。政府的關鍵作用在於建立可信可靠的黃金資料源，供金融機構及其他持份者進行精準核實及身份管理。

半集中模式：[94]聯合模式或半集中模式引入更為多元的持份者生態系統。雖然中央機構或聯合會可能會維繫黃金資料源的總體標準及協議，但銀行、信貸機構及服務提供商等各類認可機構亦可充當管理人，在各自領域簽發並管理數碼身份。該等持份者通力合作，確保黃金資料源保持最新與可靠，在分佈式控制與標準化及互通性需求之間取得平衡。[95]

去中心化模式：去中心化模式中通常由分布式分類帳技術支持，維持黃金資料源的責任分散至持份者網絡中。該模式不依賴單一實體，而是由多個參與者（包括用戶、金融服務提供商及科技專家）共同驗證與核實身份數據，形成作為黃金資料源的分佈式分類帳。該共同承擔責任的方式，確保身份數據的準確、安全及私隱，每個持份者都是系統完整性的既得受益人。

自主身份模式：在自主身份模式中，個人用戶是關鍵持份者，亦是自身身份數據的負責人，佔據中心位置，對集中式黃金資料源的傳統概念提出挑戰。用戶對自己的個人資料享有擁有權及控制權，可以自主選擇與可信實體共享部分個人資料，而該等可信實體反過來又促成一個去中心化黃金資料源。此模式要求用戶與服務提供商協作，在身份資料的易用性、安全性及可核實性之間取得平衡。

無論哪種模式，黃金資料源皆是需要精心管理與保護的關鍵資產。包括政府和個人在內的相關持份者須處理好安全、私隱、合規及用戶便利之間複雜的相互作用，確保黃金資料源能夠發揮預期作用，充當可信數碼身份核實的基石。

[94] Centre for European Policy Studies。（2020 年）。*Europe's Digital ID Opportunity*。https://theblockchaintest.com/uploads/resources/CEPS%20-%20Europes%20Digital%20ID%20Opportunity%20-%202020.pdf
[95] Landau, S.、Le Van Gong, H. 及 Wilton, R。（2009 年）。Achieving privacy in a federated identity management system。In Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009。Revised Selected Papers 13 (pp. 51-70)。Springer Berlin Heidelberg。

附件 2：全球數碼身份發展的關鍵考慮因素：驅動力與案例研究

全球數碼身份發展的驅動力

受對健全身份核實系統的迫切需求推動，金融服務業採用數碼身份科技的步伐加快。市場分析特別指出這一趨勢，預測全球數碼身份解決方案市場將從 2023 年的 345 億美元擴大至 2028 年的 832 億美元，複合年均增長率達 19.3%。[96]這一增長部分來自於政府與私營部門的協作努力，強調了數碼身份在安全、營運效率及普及金融方面的變革性影響。此外，持續演變的國際標準亦在推動這一勢頭方面發揮關鍵作用，確保數碼身份解決方案符合全球互通性要求。

這一領域的主要推動因素包括全球範圍內由政府牽頭的國家身份計劃，旨在加強服務的提供與安全，以及私營部門優先考慮客戶體驗並嚴格遵守規例的各項舉措。該等策略工作涵蓋一系列活動，從資助創新科技初創企業到與業內成熟企業建立合作夥伴關係，不一而足。政府的支援及國際對基建發展的援助，進一步促進該等舉措。

在科技快速進步與金融服務格局變化的推動下，創建可互通及可普遍取用的數碼身份生態系統之勢頭愈發強勁。隨著網上銀行與虛擬銀行的崛起，人們對能夠實現跨平台與法律框架無縫運行的數碼身份解決方案之需求亦水漲船高。與此同時，Web3 與虛擬資產的出現推高對穩健數碼身份框架的需求。隨著經濟進一步向去中心化與分佈式分類帳技術發展，安全且可核實的數碼身份已成為在該等不斷發展的領域中促進信任與確保監管合規密不可分的一部分。

為應對該等多方面挑戰，金融業正率先倡導數碼身份架構的標準化。這一努力旨在透過減少繁雜的身份核實程序與推動監管合規，簡化用戶體驗。不過，這一轉型的推動力並非僅限於傳統銀行，電訊與金融科技實體亦發揮重大作用。該等實體善用自己在管理龐大數碼身份記錄與消費者數據方面的專業知識，在強化數碼身份框架方面作出巨大貢獻。

此外，國際合作亦為這一動態格局獻出一己之力，因為正是各國合作同步各自的數碼身份策略，推動了跨界交易與個人流動性。與此同時，發達經濟體正運用生物特徵識別與區塊鏈等尖端技術完善內部錯綜複雜的系統，而新興國家則運用數碼身份來克服傳統基建局限，從而讓數百萬人進入正式的金融服務業。

流動技術的廣泛應用為數碼身份實施帶來革命性變化，它超越地理位置上的屏障，為人們提供無與倫比的金融服務。不過，雖然數碼身份系統的普及意味著在金融普及與安全方面的重大進展，但也引發

[96] MarketsandMarkets。（2023 年）。*Digital identity solutions market by offering (solutions, services), software, solution type (identity verification, authentication), authentication type, identity type, organization size, vertical and region - Global forecast to 2028*。https://www.marketsandmarkets.com/Market-Reports/digital-ID-solutions-market-247527694.html?utm_source=GlobeNewsWire&utm_medium=referral&utm_campaign=paidpr

對私隱、數據保護及社會排斥風險的擔憂。為應對該等挑戰，持續進行國際合作與投資勢在必行，以確保公平使用原則及道德標準成為數碼身份發展的基礎。

數碼身份發展與應用案例研究

中國內地

於 2022 年 3 月召開的中國全國人民代表大會期間，國家總理李克強透露了在全國範圍內推廣數碼身份證的計劃。這一舉措旨在讓個人能夠在流動設備上儲存個人身份資料，從而簡化中國日益增長的流動人口取用跨省服務的過程。公安部大刀闊斧地進行了這項數碼轉型工作，由此用戶只需掃描手機上的碼，即可取用服務。

網絡可信身份認證平台

於 2020 年世界互聯網大會 (WIC) 上，公安部第一研究所透過「互聯網+」可信身份認證平台 (CTID) 引入權威性網絡身份證明。[97]在傳統身份核實過程中，需要出示及複印實體身份證，上述平台旨在減低該過程中的個人資料洩露風險。[98]「無卡式」電子身份核實系統透過商業流動應用程式運作，於後台警方核實用戶身份後生成加密認證，同時在用戶手機上生成動態二維碼。[99]CTID 已在廣東、福建等城市進行先導試驗，並正在與其他實體進行互聯互通，如於 2022 年 5 月與中國電信訂立互通性安排。當前，CTID 平台已成為諸多地區與行業公認的可信身份驗證基建設施。其並行能力達每秒 20,000 宗交易，平均應答時間僅 0.5 秒，能處理高達 50 億單位的海量數據。[100]

公民網絡身份識別系統（「eID」）

2015 年，公安部第三研究所開發的「公民網絡身份識別系統」順利通過國家密碼管理局的安全審查，開始向公民發放電子身份證。該系統擁有三大特點：(i) 手機兼容性（僅限指定類型）；(ii) SIMeID 貼膜；以及 (iii) NFC-IC 卡通信。eID 支持網上身份驗證、簽署核實及離線身份驗證。該等功能可精準識別自然人的身份，同時保護公民的個人資料，尤其是在銀行帳戶開立及其他日常付款交易過程中，例如航空旅行服務與酒店住宿。

[97] 陳進安。（2020 年 11 月 25 日）。內地全新證件「網證」曝光：官方：代替身份信息認證保護私隱。香港 01。https://www.hk01.com/即時中國/553869/
[98] Liu, A。（2018 年 11 月 18 日）。A smart future for identity verification。Keesing Platform。https://platform.keesingtechnologies.com/a-smart-future-for-identify-verification/#:~:text=Cyber%20Trusted%20Identification%2C%20or%20CTID,verification%20and%20ID%20card%20verification。
[99] Liu, A。（2018 年 11 月 18 日）。A smart future for identity verification。Keesing Platform。https://platform.keesingtechnologies.com/a-smart-future-for-identify-verification/#:~:text=Cyber%20Trusted%20Identification%2C%20or%20CTID,verification%20and%20ID%20card%20verification。
[100] 邢開允。（2022 年 3 月 15 日）。*數字身份行業專題：數字身份引領數字經濟新時代*。https://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rptid/700688401898/index.phtml

實名去中心化身份

2023 年，中國宣佈一項名為「實名去中心化身份 (實名 DID)」的計劃，面向 14 億龐大人口。這一開創性項目由公安部與中國區塊鏈服務網絡 (BSN) 攜手推進，並得到中國移動與中國銀聯等科技巨頭的大力支援。[101]實名 DID 計劃旨在提供一整套服務，涵蓋個人實名驗證、數據加密、安全登入程序及企業身份驗證。實名 DID 最顯著的一大特點是允許公民在保護其私隱的情況下註冊並與網上平台互動。

實名 DID 系統建立於 CTID 數碼身份鏈之上，為具可核實實名憑證的數碼身份創建分佈式分類帳。這一開創性國家級系統標誌著該領域的一個重要里程碑，有望得到多種應用，從社交媒體核實到安全數據傳輸與個人身份認證，造福公民。[102]該身份框架的引入契合中國內地數碼環境中分佈式分類帳技術的快速發展。BSN 的倡議是更廣泛的全球趨勢的一部分，旨在賦予個人對個人資料的更多控制權，讓他們自主決定與誰共享哪些數據。[103]

新加坡

國民數碼身份證、MyInfo Profile、SingPass 與 CorpPass

新加坡已推出國民數碼身份證 (NDI)，使居民與企業能夠安全便捷地在公私部門進行數碼交易。國民數碼身份證是一種中心化數碼身份管理系統，依賴公鑰基建加密安全技術。該系統最初於 2017 年推出，如今已經歷多輪改進。國民數碼身份證框架建立在身份驗證系統「SingPass」之上，後者於 2003 年推出，供新加坡居民用於取用政府電子服務。此外，所有「SingPass」用戶自動有權取用自己的 MyInfo Profile。該檔案涵蓋逾 100 項從不同政府機構檢索所得並經政府核實的個人資料項目。另一方面，企業可申請「CorpPass」來取用 130 多種政府服務並管理對員工的授權。

2019 年，新加坡啟動「MyInfo Business 先導計劃」，透過「CorpPass」運作。該計劃允許企業透過該平台共享經政府核實的數據，例如企業檔案、財務業績及擁有權資料。該服務還在當地部分銀行進行試驗，以期促進企業公用事業帳戶開立及申請中小企業貸款等流程。

[101] 區塊鏈服務網絡。(2023 年)。*BSN 實名 DID 服務發佈會將在北京召開*。
https://mp.weixin.qq.com/s?__biz=MzI3MzU0NTY0OA==&mid=2247505468&idx=1&sn=7ee52697474d2d38233efa56e0e36603&chksm=eb2336e3dc54bff55c1c0021aed8f17eeda4acbc5a7f58cc1b3b74e918946362428cfc7e442c&token=1602819206&lang=zh_CN#rd
[102] CoinDesk。(2023 年 12 月 12 日)。*China's Ministry of Public Security launches blockchain-based real-name decentralised identifier system*。
https://www.coindesk.com/policy/2023/12/12/chinas-ministry-of-public-security-launches-blockchain-based-real-name-decentralised-identifier-system/
[103] Fintech News Hong Kong。(2023 年 12 月 13 日)。*China to introduce blockchain-based identity verification*。
https://fintechnews.hk/24517/fintechchina/china-to-introduce-blockchain-based-ID-verification/

在國民數碼身份證框架下，可信身份層乃使用政府提供的官方核證數據建立，推動形成一個開放聯合式的身份驗證與數碼簽署服務生態系統。其中一個身份驗證服務提供商由新加坡政府營運，而 MyInfo 檔案則充當國民數碼身份證的可信身份資料庫。在該框架內，用戶只需向政府提供一次個人資料，而不必在每次進行網上交易時提供。金融機構可善用 MyInfo 資料庫優化客戶開戶流程並提高營運效率，尤其是銀行帳戶開立程序。截至 2020 年，逾 60 家金融機構運用 MyInfo 提供 220 項數碼服務，簡化了開戶及客戶盡職審查程序。

新加坡積極尋求與其他司法管轄區建立夥伴關係，以期優化數碼身份的互通性。2020 年，新加坡與澳洲簽訂一份諒解備忘錄，探討在跨境應用方面實現數碼身份互認，其中包括加快銀行開戶流程與簽證申請。該協作有望加強兩國之間的貿易活動。隨後，新加坡還建立了具有類似目標的其他夥伴關係，例如與智利和新西蘭訂立的《數碼經濟夥伴關係協議》。另外，新加坡於 2021 年與英國簽訂另一份諒解備忘錄。

印度

印度資產證券化重組及擔保權益中央登記處

印度資產證券化重組及擔保權益中央登記處 (CERSAI) 成立於 2015 年，以《2013 年公司法》項下的持牌公司身份運作。其中印度政府持有 51% 的股權，餘下股權則由幾家公共部門銀行與國家住房銀行持有。該公司的主要目標是作為印度擔保物權的登記處，管理登記系統。據 2002 年《金融資產證券化和重組及擔保權益執行法案》(《SARFAESI 法案》) 的規定，該登記處為證券化、資產重組及擔保權益相關交易的登記提供便利。

印度 Stack 及 Aadhaar 計劃

2010 年，由印度中央政府成立的印度唯一身份識別管理局 (UIDAI) 開始透過「Aadhaar 計劃」向印度公民發放唯一身份證（UID 或 Aadhaar 號碼）。UID 建立於最低限度的個人資料與生物特徵識別資料（包括指紋與虹膜掃描）基礎上，可用於進行身份驗證。基於 Aadhaar 的電子化「了解客戶」使用戶可透過電子方式向金融機構提供個人資料，而服務提供商可透過平台即時核實與驗證身份資料，從而大大減少文書工作與處理時間。

為進一步加強 Aadhaar 號碼持有人的私隱與安全，UIDAI 於 2018 年推出並實施虛擬 ID、UID 令牌及有限「了解客戶」系統，具體如下：

(i) 虛擬 ID 的引入使得用戶可獨立生成無數個 ID。透過該功能，用戶可在身份驗證過程中選擇不提供 Aadhaar 號碼，從而解決了潛在的安全擔憂，因為 Aadhaar 號碼與用戶完整的人口資料掛鉤。

(ii) 實施有限「了解客戶」服務，以限制對 Aadhaar 號碼的取用。身份驗證用戶機構 (AUA) 分為全球 AUA 與本地 AUA。諸如銀行與稅務等全球 AUA 可不受限制地取用用戶資料。與此相反，本地 AUA 的權限有限，並獲分配一個「機構特定」的令牌化號碼（UID 令牌），用於身份匹配與核實。如此一來，本地 AUA 在進行「了解客戶」流程時無需儲存唯一 Aadhaar 號碼。

印度於 2020 年 7 月 13 日發佈了《非個人資料 (NPD) 治理框架》初稿，以徵求公眾意見。該框架旨在構建一個數據共享架構，以實現將社區數據用於創造社會、公共及經濟價值。不過，政府收到一些反對意見：

(i) 大多數中小微企業及初創企業發聲反對政府現行的非個人資料政策框架。他們認為，允許大企業出售其綜合數據不會造福大多數小企業。

(ii) 亞馬遜、Facebook 及谷歌亦表示反對該項命令，稱其有損公司在處理與收集此類資料方面的投資。

澳洲

數碼化轉型局 (DTA) 一直在開發一個名為「信任數碼身份框架」(TDIF) 的國家數碼身份框架。該框架為聯合身份模式訂立規則與標準。聯合身份模式即多個經認證的身份服務提供商提供數碼身份服務，可用於獲取政府與私營部門的服務。

myGovID

myGovID 是澳洲數碼身份系統的重要組成部分。這是一款應用程式，旨在提供安全的網上身份核實方法。有別於傳統的身份形式，myGovID 可透過智能手機取用，提供了以數碼方式獲取政府服務的便捷方式。這一舉措是更為廣泛的數碼身份計劃不可或缺的一部分，該計劃旨在為澳洲人創造更加順暢且安全的方法，在網上獲取政府服務，其中強調私隱、安全及選擇的原則。

此外，澳洲一直積極參與有關數碼身份認可的國家討論，與新加坡簽署的 2020 年諒解備忘錄便是例證。該舉措旨在建立連接，實現雙方數碼身份系統互認，從而簡化兩國之間的國際交易及旅行。

新南威爾士州 — ServiceNSW

縱觀各州，新南威爾士州因成功推出數碼身份計劃脫穎而出。Service NSW 應用程式由州政府營運，在該州人口中的普及率幾乎達到百分之百，是實施數碼身份計劃的典範。這一高采用率相當大程度歸功於該應用程式對 2019 年冠狀病毒病安全簽到功能的整合，以及提供數碼駕駛執照功能，這對許多居民而言幾乎必不可少。

以此為基礎進行擴展，用戶可選擇在自己的 MyServiceNSW 帳戶內創建數碼身份證，從而使用政府頒發的既有實體證件進行不同程度的身份核實。用戶可將該等證件的數碼版本加載至個人帳戶，連同其他經核實的個人資料，例如手機號碼、出生日期及電子郵箱地址。該等基礎步驟為納入更高級的可核實憑證鋪平道路，其中包括新南威爾士州出生、死亡及婚姻登記處頒發的憑證。可透過 ServiceNSW 應用程式或登記處提供的專用應用程式出示憑證。

同樣，香港的「安心出行」流動應用程式在疫情期間亦發揮重要作用。不過，有別於新南威爾士州已將數碼身份擴展至包括多種功能與憑證，香港在後疫情時代未有在日常生活中廣泛採用數碼身份。

歐盟

歐洲數碼身份（電子身份）[104]

此前，歐盟不同國家分別頒發了電子身份，這種身份系統缺乏與其他司法管轄區或部門同步所需的互通性，阻礙了用戶獲取跨境公共與商業服務。為克服這一挑戰，歐盟於 2021 年 6 月提出新的電子身份框架。此框架旨在解決有關內部市場電子交易的電子身份識別與信任服務 (eIDAS) 條例的局限性與不足。

修訂後的電子身份框架將確保持有國家身份證的全體歐盟公民與居民能夠實現無縫身份核實。此項改進使得他們能夠在整個歐盟境內以網上及網下方式獲取公共及商業服務。此高級功能已添加至個人數碼錢包——一個可在各種電子設備上使用的應用程式。

數碼錢包可及性廣，任何歐盟公民、居民或企業均可使用。作為身份核實的流動數碼儲存庫，數碼錢包賦予用戶放心、透明地管理自身資料的權利，無論身在歐盟何處。這一創新技術直接消除人們對在網上共享個人資料的擔憂。

[104] 歐盟委員會。（日期不詳）。*A Europe fit for the digital age*。 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

歐盟委員會致力確保歐洲電子身份的安全，是對該等關注點的直接回應。它為全體公民構想了一個可信、適應性強的解決方案，可用於從行政任務到日常便利等一系列活動。

eIDAS 條例[105]

eIDAS 條例頒佈於 2014 年，自 2016 年 7 月起生效，對塑造歐盟的數碼格局非常重要。它為區內公私部門的電子互動建立統一框架，實現無縫使用國家電子身份獲取跨境公共服務。此外，該條例統一電子簽署、電子蓋章及時間戳等信任服務，從而使該等數碼措施具有與實體措施相同的法律地位，進而提升市場效率。

在 eIDAS 條例所推動的基建改進的基礎上，歐盟數碼身份的引入志在進一步縮小數碼服務可及性方面的差距。該舉措是為了解決此前跨境身份驗證能力有限的問題，有能力處理此類互動的公共服務提供商比例較低便是證明。

在歐盟的銀行與金融領域，eIDAS 框架正顯著提高客戶參與度。它簡化了身份核實、合規、合約簽立及安全協議敲定等流程。採納 eIDAS 規定的金融機構不僅減少了行政開支，還改善了客戶體驗。有可靠且安全的身份識別基礎作為支援，該框架在使該等實體能夠在歐盟範圍內有效擴展其服務方面發揮關鍵作用。

《數據治理法案》

2020 年，歐盟委員會提出「歐洲數據治理條例 (《數據治理法案》)」，這是一套旨在加強數據交換與支援歐盟數據空間的治理措施。這份文書的重點是透過處理各種場景來促進數據交換，其中包括：

(i) 促進公共部門重用數據。

(ii) 促進企業間的數據共享。

(iii) 根據《通用數據保障條例》，引入額外的中介層，以保障個人權益。

(iv) 允許出於公益目的使用數據。

委員會在這一框架內，提出建立自願機制，允許參與數據公益[106]的組織註冊為「歐盟認可的數據公益組織」。該機制旨在為跨境數據儲存庫的建立提供便利。經認可的數據公益組織可以出於造福社會的

[105] 歐盟委員會。(日期不詳)。*Discover eIDAS | Shaping Europe's digital future*。*Shaping Europe's Digital Future*。https://digital-strategy.ec.europa.eu/en/policies/discover-eidas

[106] 數據公益指個人及公司自願同意或允許免費提供其生成的數據，用於公益事業。(引自歐盟委員會《數據治理法案》詮釋，https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#:~:text=Data%20altruism%20is%20about%20individuals,used%20in%20the%20public%20interest)

目的，收集個人資料或處理數據。此外，該提案還包括引入新的數據中介層。該等獨立數據共享實體將透過促進負責任的數據匯總與交換，捍衛公眾權益，並維護數據私隱。[107]

[107] 歐盟委員會。（日期不詳）。《數據治理法案》詮釋。Shaping Europe's digital future。https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#ecl-inpage-l4ihlqt9

附件 3：評估香港的數碼身份生態系統及其實施準備情況

香港正在構建數碼身份框架，以配合全社會日益增加的互聯互通需求。這一轉型核心在於政府推出的「智方便」計劃，促進市民、公共服務及私營企業之間的無縫數碼互動。這項計劃開闢一條新的增長途徑，尤其是對私營數碼身份解決方案提供商而言，他們可以藉此機會，提升用戶體驗。香港的監管機構、金融機構及科技創新者通力協作，努力創造更具凝聚力與效率的數碼基建，並成功構建數碼身份框架。不過，儘管該等持續發展彰顯香港不斷進取的決心，然尚需採取後續行動來推動生態系統的全面成熟。接下來的關鍵措施包括完善政策、加強安全措施，以及在保護私隱的同時維繫有利於創新的環境。採用系統性的方法處理該等範疇的問題，對於香港數碼身份格局的發展至關重要，而我們的最終目標是打造以用戶為中心的強大數碼社會。

1. 香港格局

政府牽頭計劃 —「智方便」

「智方便」前稱「數碼個人身份」，是一個於 2020 年推出的綜合數碼服務平台。它為香港居民提供數碼電子身份，方便他們使用各種公共服務、簡化網上商業交易。作為個人身份的權威資料源（或黃金資料源），「智方便」已擴展至私營部門，涵蓋銀行、保險及公用事業（包括電力與煤氣公司）等行業。該平台的構建基於四大核心功能：[108、109]

- 身份驗證：於登記過程中對用戶香港身份進行核實後，用戶可使用生物特徵或一組安全密鑰進行身份驗證，登入以使用各種網上服務，從而減少使用不同服務所需的程序及時間。
- 填表通：平台儲存經驗證的個人化數據，於獲得用戶同意後可自動填寫表格。
- 個人化提示：「智方便」會向用戶發送提示，確保用戶隨時了解有關政府服務與個人任務的最新資訊。
- 數碼簽署：用戶可使用具法律約束力的數碼簽署功能處理法律文件及程序，受《電子交易條例》支持。

該計劃的精髓在於其綜合數碼服務中心「智方便」流動應用程式，可提供個人化用戶體驗。該平台對安全的承諾在基礎設計中體現得淋漓盡致。它嚴格遵循政府的資訊科技保安政策及指引，以及 ISO 27001 與 ISO 27701 標準，確保用戶數據的完整性與保密性。於該平台推出前，政府遵循《個人資

[108] 政府資訊科技總監辦公室。（日期不詳）。*「智方便」*。https://www.ogcio.gov.hk/en/our_work/community/iam_smart/
[109]「智方便」。https://www.iamsmart.gov.hk/en/ /

料（私隱）條例》(PDPO) 的規定，主動完成透徹的私隱影響評估，加強對用戶信任與私隱的承諾。[110]

截至 2020 年底，香港金融管理局（金管局）、證券及期貨事務監管委員會（證監會）、保險業監管局（保監局）及強制性公積金計劃管理局（積金局）已分別向各自的受監管實體發佈通告，認可「智方便」作為促進香港金融科技生態系統發展的重要平台。他們提倡將「智方便」整合到金融機構提供的網上服務中，如遙距開戶、帳戶登入身份驗證及數碼文件簽署，以期為客戶提供精簡高效的體驗，同時確保符合法定及監管要求。鑒於「智方便」可對香港居民的身份進行可靠、獨立核實，監管機構已認可它的能力，即能夠進行可靠的客戶身份核實，並用於開戶過程中的數碼簽署。我們鼓勵擬將「智方便」用於生產的機構參加沙盒計劃。關鍵一點，「智方便」的採用遵循自願原則。

自 2020 年推出以來，「智方便」已獲約 270 萬用戶登記。[111]該計劃的側重點已不僅僅是增加登記用戶數量，還要提高平台的年度使用量。確切而言，目標是到 2025 年，將年度交易總量從 2021 年的 500 萬筆提升至 1,750 萬筆。[112]推動金融服務採用該平台的一大因素在於，平台能夠提供卓越的用戶體驗。如若「智方便」在無縫銜接與用戶友好方面的表現比現有方案更為出色，自然會獲得用戶的青睞。

為中小企業提供支援的金融基建

如《2024 年度財政預算案》所述，香港政府已計劃建立一個為企業量身定製的數碼身份框架。[113]該策略舉措涉及將 180 萬家本地企業納入企業版「智方便」平台，該平台預計將於 2026 年推出。[114]該平台旨在透過為數碼文件的簽署提供便利及實現政府服務的電子支付，簡化企業營運。一旦推出，將為企業提供強大的數碼身份核實功能，從而透過自動填充表格及安全儲存電子憑證等功能提高營運效率。

商業數據通[115]

商業數據通 (CDI) 是企業銀行業務的一大進步，為金融及商業數據的安全快捷交換提供強大平台。該平台連接數據提供商與金融機構，打造更為高效、透明的金融生態環境。

---

[110]「智方便」。（日期不詳）。*「智方便」沙盒計劃簡介*。https://www.hklawsoc.org.hk/-/media/HKLS/Home/Support-Member/Professional-Support/AML/AML-Template/iAM-Smart-Information-Pack.pdf
[111]「智方便」。https://www.iamsmart.gov.hk/en/
[112] 香港特區政府。（2023 年 2 月 22 日）。*立法會二題：推動數碼個人身份的發展*。https://www.info.gov.hk/gia/general/202302/22/P2023022200263.htm
[113] 香港特區政府《2024 年度財政預算案》。https://www.budget.gov.hk/2024/eng/pdf/e_budget_speech_2024-25.pdf
[114] 南華早報。（2024 年 4 月）。Hong Kong finance chief Paul Chan vows to help 1.8 million firms make payments, use services on enterprise version of iAM Smart。南華早報。https://www.scmp.com/news/hong-kong/hong-kong-economy/article/3258949/hong-kong-finance-chief-paul-chan-vows-help-18-million-firms-make-payments-use-services-enterprise
[115] 香港金融管理局。（2022 年 10 月 24 日）。*金管局正式推出「商業數據通」*。https://www.hkma.gov.hk/eng/news-and-media/press-releases/2022/10/20221024-3/

2020 年，金管局攜手多家銀行合作夥伴，成功進行「概念驗證」(PoC)，以完善中小企業融資的信用評估流程。該計劃證實，商業數據通有望善用大量貿易相關數據，徹底改變貿易融資申請程序。基於這一成果，商業數據通將在下一發展階段整合各種商業資料源，加強銀行的替代信用評估能力。此外，公司註冊處作為數據提供商的加入，有望在商業數據通豐富數據儲備的推動下，實現創新的「了解客戶」應用。

2022 年是另一重要里程碑，金管局正式推出商業數據通，將其定位為「金融科技 2025」策略的基石。商業數據通計劃的成效於先導階段已得到證實，在銀行及數據提供商的廣泛參與下，該計劃共批核了逾 16 億港元的中小企業貸款。有見及此，確保數據安全交換勢在必行。中小企業將從商業數據通中受惠良多，我們鼓勵所有持份者探索該平台帶來的商機。透過邀請銀行加入並探索商業數據通網上門戶，企業可使用全套的服務，從而提高他們的金融普及性及成長性。

隨著金融業持續發展，商業數據通的重要地位日益凸顯，而精簡式數據交換的優勢也不言自明。不過，唯有數碼身份框架的全面應用與完善方會切實推動金融科技行業發展。雖然商業數據通與數碼身份系統獨立運作，卻相輔相成，形成充滿信任與創新的健全基建設施。這種協同關係將推動金融服務業再創新高，形成一個不僅能維繫銀行服務既有範疇，又能刺激創造以消費者為核心的新型金融產品的生態系統。要營造一個有利於金融科技發展的安全可靠環境，須採取一致行動來開發數碼身份協議並使之標準化。這樣一種環境有望開創金融服務新紀元，不僅可及性與定製化程度高，還能滿足精通數碼技術的客戶群的期望。

銀行同業帳戶數據共享[116]

與此同時，金管局擬於 2024 年 1 月 1 日啟動「銀行同業帳戶數據共享」先導計劃。這一開創性項目將允許客戶在知情同意的情況下，以安全方式與其他銀行共享自己的銀行數據。

「銀行同業帳戶數據共享」計劃由金管局金融科技促進辦公室聯同香港銀行公會及其他業界人士制定，源自金管局金融科技促進辦公室的全面研究。該等研究表明，共享客戶銀行帳戶數據可大大改善銀行業務營運水平、加強風險管理，以及提升整體客戶體驗。「銀行同業帳戶數據共享」先導計劃涵蓋零售、企業及中小企業，將納入存款帳戶資料，包括可用性、狀態、餘額及交易記錄。

在 28 家銀行的參與下，「銀行同業帳戶數據共享」先導計劃有望帶來創新的銀行業務服務，促進貸款流程簡化以及個人化數據驅動解決方案。金管局將密切關注先導計劃進展，評估市場反應，為潛在全面實施策略提供參考。於當前以快速數碼轉型為標誌的時代——疫情進一步加快這一進程——香港已展現出靈活的適應能力。客戶對數碼參與的期望顯著提高，對快速獲得各種公共與商業服務的需求

[116] 香港金融管理局。(2023 年 12 月 21 日)。*「銀行同業帳戶數據共享」先導計劃*。
https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/12/20231221-3/

亦隨之增加，尤其是透過網上身份核實來實現的服務。此外，金融服務業如今已認識到遙距客戶開戶的重要性。

因應這一數碼轉變，監管機構已發佈通告並倡導最佳實踐來駕馭持續變化的格局。與此同時，行業協會亦積極實施支援性措施來推動該等進步。全體一心的舉動彰顯我們的承諾，即緊貼數碼金融的發展、塑造數碼金融的未來，確保「銀行同業帳戶數據共享」等創新計劃能夠無縫融入以安全、效率及客戶滿意度為先的生態系統。

私營機構的進展

在數碼經濟快速擴展的背景下，網上交易已然成為常態，而私營部門正發展為推動身份驗證格局重塑的中堅力量。該領域的重大進展包括，滙豐銀行實驗室在零售層面探索去中心化身份解決方案。

去中心化身份技術代表著從傳統身份核實向以安全與用戶控制權為先的系統的轉變。滙豐銀行實驗室的實驗運用公共與私營數碼分類帳協議（亦稱區塊鏈）開發原型，可簡化內部帳戶開立流程，同時維護高水準的數據私隱與「了解客戶」控制措施。此系統允許客戶在各種銀行業務及產品中直接使用滙豐銀行的經核實數碼憑證，從而提高便利性與效率。滙豐銀行實驗室開發的去中心化身份平台旨在管理銀行業務憑證，專為認證與保護來自政府機構及信用局等一系列憑證簽發人的數據而設計。這種互通性對於發展信任與簡化不同交易及帳戶設置的核實流程至關重要。

滙豐銀行的計劃追求透過去除傳統身份驗證中的重複環節，提升整體客戶體驗。無密碼身份驗證的引入，以及未來建立個人身份檔案的能力，有助於提供更加順暢的用戶體驗。滙豐銀行對去中心化身份技術的探索反映了金融服務業的一大趨勢，即採用更加安全、高效、以用戶為中心的系統。去中心化身份系統在管理「了解客戶」及其他身份相關程序方面的效率表明，該系統有望完善營運流程並提升數碼信任。私營部門實體在數碼身份方面取得的進步標誌著向精簡型數碼經濟邁進的重要一步。金融服務正邁向新紀元，實現個人憑證的安全管理及按需共享，從而提升用戶體驗與互聯互通。

銀行業的其他進展

隨著銀行業對技術進步的接納，服務的交付不再局限於傳統方式。自 2018 年金管局頒發首張虛擬銀行牌照以來，香港已有八家虛擬銀行。位於香港虛擬銀行格局中心的是運用「身份驗證與比對」的電子化「了解客戶」框架。該系統依賴以數碼化方式呈遞的身份證件，並結合有效性檢測與人臉比對技術，對新客戶的開戶流程至關重要。

為提高營運效率與客戶滿意度，傳統銀行正在重構方法。自 2019 年以來，諸多此類機構已採用流動帳戶開立服務，部分還將此類服務擴展至國際範圍，以便定居國外的香港居民開立帳戶。儘管如此，由於缺乏統一的電子化「了解客戶」平台，整個行業的做法五花八門，迫使金融實體精心打磨切合自身需求的電子化「了解客戶」解決方案。

隨著零售銀行越來越多地在「了解客戶」流程中融入技術，部分機構正將其網上服務擴展至商業及企業客戶，尤其是中小企業。所需文件乃專門定製，以配合具體行業與業務性質需求，其中或會涵蓋買方發票、租賃協議或業務計劃等項目。

在 2019 冠狀病毒病的推動下，港內銀行加速轉向遙距客戶開戶，為此，金管局發佈了一系列通函。該等文件為實施「打擊洗錢及恐怖分子資金籌集」控制措施指明方向。

- 2019 年 2 月，金管局發佈一份文件，概述對個人客戶遙距開戶的監管期望。[117]根據該文件，授權機構宜採用先進程度「*至少與客戶面對員工時所運用技術解決方案相當*」的技術解決方案，緩減識別及核實個人客戶身份相關的風險。[118]

- 金管局於 2020 年 6 月發佈題為「*近期專題審查遙距開戶程序的打擊洗錢及恐怖分子資金籌集管控措施所得結果*」通告，分享了金管局在打擊洗錢及恐怖分子資金籌集管控措施的主要觀察結果及良好做法。[119]

- 隨後，金管局於 2020 年 9 月發佈「公司客戶遙距開戶」通告。[120]該通告重申，有必要在客戶盡職審查過程中採用風險為本方法，同時確認無論當中採用傳統方法或是科技手段，須遵循的監管要求是一致的。該通函確認，客戶盡職審查步驟可：(i) 透過電話會議或視像會議或獨立且合適的中介人與客戶互動的方式進行，但採用的渠道須與評估的洗錢及恐怖分子資金籌集風險相稱，以及 (ii) 運用可靠技術解決方案核實公司代表與所有者的身份。[121]

[117] 香港金融管理局。(2019 年 2 月 1 日)。*個人客戶遙距開戶*。https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf
[118] 香港金融管理局。(2019 年 2 月 1 日)。*個人客戶遙距開戶*。https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf
[119] 香港金融管理局。(2020 年 6 月 3 日)。*近期專題審查遙距開戶程序的打擊洗錢及恐怖分子資金籌集管控措施所得結果*。https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200603e1.pdf
[120] 香港金融管理局。(2020 年 9 月 24 日)。*公司客戶遙距開戶*。https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200924e1.pdf
[121] 的近律師行。(2020 年 11 月 26 日)。*Hong Kong Monetary Authority (HKMA)'s expectations on remote on-boarding of corporate customers*。https://www.deacons.com/news-and-insights/publications/hong-kong-monetary-authority-(hkma)%E2%80%99s-expectations-on-remote-on-boarding-of-corporate.html

- 2021 年 5 月，金管局鼓勵採用「智方便」完成遙距開戶，與特別組織的準則及其於 2020 年 3 月發佈的數碼身份指南保持一致。[122]其指明，「智方便」的使用符合打擊洗錢及恐怖分子資金籌集要求，例如透過 API 數據保存記錄，無需提供額外文件。金管局始終讚成善用科技提升客戶盡職審查效率與客戶體驗。

證券業的其他進展

據投資者及理財教育委員會展開的《2023 年零售投資者研究》，八成股票投資者主要透過網上渠道進行交易，其中流動應用程式是最受歡迎的交易方式。[123]該趨勢推動網上經紀商的誕生，它們與投資者的動態偏好與行為保持一致，極大顛覆了傳統證券公司。與實體經紀商相比，網上經紀商能夠提供更具效率與成本效益的服務，因此搶佔了零售市場的大部分份額。其中許多經紀商已在競爭激烈的金融領域嶄露頭角。雖然它們採用的科技可能各不相同，但存在一個共同點，即採用標準網上帳戶開立程序，通常需要一到兩周來完成。

因應該數碼轉變，傳統銀行及證券公司紛紛加入提升網上服務的隊伍。在當今數碼時代，擁有強大的數碼身份基建至關重要——它可以快速、安全地核實客戶身份，從而簡化開戶流程，這與提升客戶體驗及保護金融系統的完整性密不可分。

依據《證券及期貨事務監察委員會持牌人或註冊人操守準則》(《操守準則》)，[124]如若在帳戶開立過程中採取非面對面方式，持牌或註冊實體有責任採取一切合理手段核實客戶身份。證券及期貨事務監察委員會（證監會）已列示五大可接受的開立帳戶方式，只需遵循特定的程序步驟，即可實現網上客戶開戶，包括：(i) 取得客戶協議的電子簽署，連同一份身份證件副本；(ii) 從指明銀行帳戶向中介機構銀行帳戶轉入一筆 10,000 港元或以上金額的初始保證金；(iii) 使用指明銀行帳戶作為期貨交易的唯一交易帳戶；以及 (iv) 備存對開立帳戶流程的妥善記錄。2019 年的更新將可接受方式擴展至涵蓋遙距程序步驟，包括但不限於身份核實、身份證件驗證及電子協議簽署。該通告明確界定網上帳戶開立流程，促進了該領域的發展。

[122] 香港金融管理局。（2021 年 5 月 24 日）。*遙距開戶及「智方便」*。https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210524e1.pdf
[123] 投資者及理財教育委員會。（2023 年）。*2023 年《零售投資者研究》*。https://www.ifec.org.hk/web/common/pdf/about-ifec/retail-investor-study-2023.pdf
[124] 證券及期貨事務監察委員會。（2024 年）。*《證券及期貨事務監察委員會持牌人或註冊人操守準則》2024 年 1 月最新帶標記版*。https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/codes/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/Code_of_conduct-Jan-2024_Eng-Final-with-Bookmark_20240119.pdf?rev=58cb723ff0494f168d908fc5e061b9d5

保險業的其他進展

香港保險業監管局（保監局）歷來率先擁抱金融科技創新，於 2017 年推出「快速通道」計劃，為專門的數碼分銷渠道的發展提速，並推動保險科技的發展。繼 2019 年授權成立首家虛擬保險公司後，保險領域飛速發展，到 2021 年已有五家數碼保險公司獲得授權。

保險業協同香港保險業聯會等協會，迅速應對疫情帶來的挑戰，並與保監局攜手，推出香港首個虛擬投保平台。該舉措有助於遙距分銷長期保險產品，能提供視像會議諮詢，在這前所未有的特殊時刻，拉近保險公司與消費者的距離。[125]同年，保險科技沙盒推出，為保險業人士提供可控測試環境，於完善創新應用的同時，確保符合監管標準及處理潛在風險與網絡安全憂慮。這使得傳統保險公司也能採用符合保監局規定的非面對面新式銷售流程。[126]

2020 年，保監局發佈《關於保險公司對虛擬客戶投保採取的打擊洗錢及恐怖分子資金籌集管控措施的主要觀察結果》，[127]以加深業界對《打擊洗錢及恐怖分子資金籌集條例》及《打擊洗錢及恐怖分子資金籌集指引》(「指引 3」) 所列若干規定的理解。為推廣普及金融及維繫公平競爭環境，保監局指出，他們的長期目標是為不同保險公司，尤其是缺乏必要資源來開發自己專有平台的中小型保險公司，建立共用虛擬投保平台。[128]

數碼身份已成為保險業發展的基本組成部分，對保險公司及保單持有人具重要意義。強大的數碼身份基建將徹底改變保險流程，從最初的保單購買到理賠管理及結算。這樣一個系統需要簡化對醫療記錄的核實流程、提升理賠流程的流暢度，以及加強個人資料的安全性。

一旦有效施行，全面的數碼身份框架可為保單交易及付款提供卓越的效率與安全。該進步有望大大減低詐騙與行政開支，為所有持份者營造統一而又安全的環境。隨著行業不斷發展，數碼身份解決方案的關鍵作用日益凸顯。該等方案並非單純的附加功能，而是香港保險業邁向更便捷、更安全未來的根本性飛躍。

[125] 保險業監管局。（日期不詳）。數碼投保。https://www.ia.org.hk/en/digital_onboarding/index.html
[126] 星展銀行。（2021 年 6 月 21 日）。*星展香港推出電子遙距投保服務*。https://www.dbs.com/NewsPrinter.page?newsId=kq2bdwid&locale=en
[127] 保險業監管局。（2020 年 12 月 4 日）。*關於保險公司對虛擬客戶投保採取的打擊洗錢及恐怖分子資金籌集管控措施的主要觀察結果*。https://www.ia.org.hk/en/supervision/antimoney_laundering/files/AML_Online_Sharing_Session_20201204_Presentation.pdf
[128] 保險業監管局。（日期不詳）。*保險數碼投保*。https://www.ia.org.hk/en/digital_onboarding/promotion_of_insurtech_development.html

2. 協作計劃：公共部門合作制定「智方便」沙盒計劃

數碼港與政府資訊科技總監辦公室攜手合作，於 2020 年推出「智方便」沙盒先導計劃。這一夥伴關係體現一項承諾，即攜手不同公共組織推動香港的數碼賦能，創建數碼共融型社會。該計劃強調協作對完善香港數碼生態系統的重要性，旨在推動「智方便」平台的廣泛應用與創新使用。[129]

沙盒計劃的初衷是成為探索數碼創新的測試平台，為運用「智方便」基建測試 API 功能及進行「概念驗證」提供安全環境。自推出以來，該計劃已取得長足進步，吸引逾 330 家組織參與「智方便」相關的測試與開發。此外，10 多家公私營實體已成功將「智方便」整合到自身服務產品中，證明該計劃對數碼格局的影響持續擴大。[130]

該計劃充當一座橋樑，帶領實體邁向一個政府認可的數碼身份框架。透過提供一系列支援服務（包括專職求助台、專業訓練工作坊，以及測試協助），該計劃可確保各組織順利實現從概念到應用的過渡，有效地將「智方便」功能整合到各自的服務中。[131]

參與者在該計劃內開啟了結構化的兩階段開發之旅。第一階段側重於初始測試及服務完善，而第二階段則善用整合測試環境模擬生產環境。[132]該環境對服務於公開發佈前的細緻調整非常重要。順利完成該兩個階段能為參與者提供必要工具與信心，方便將「智方便」功能整合到各自的網上服務中，繼而推出供用戶使用。

該計劃遵循共融方針，面向銀行、保險及投資等金融服務界別的實體，並為包括資訊及通訊科技、電訊、醫療、運輸、物流在內的廣大行業組織提供支援。[133]這一方針彰顯了該計劃的承諾，即開發一個靈活、全面的數碼身份生態系統，配合各行各業的需求。

這一共融策略的總體目標是建立一個全能型數碼身份框架，能夠適用各行各業持續發展的數碼服務。展望未來，該計劃旨在拓寬參與範疇，邀請更多部門運用「智方便」平台。如此一來，該計劃可充分發揮數碼身份的變革力量。持份者持續專注於發展一個不僅科技精湛而且符合監管標準、優化用戶參與及有利於跨行業協作的數碼生態環境，正是該計劃不斷發展的最佳證明。得益於各方面的協作，一個兼具韌性與用戶友好性的數碼身份框架正在形成，將滿足香港不同經濟領域的動態需求。

---

[129] 政府資訊科技總監辦公室。（日期不詳）。*公私營機構採用「智方便」。*
https://www.ogcio.gov.hk/en/our_work/business/i_am_smart_adoption/
[130] 香港特別行政區立法會。（2022 年 10 月 10 日）。*資訊科技及廣播事務委員會。（2022 年 10 月 10 日）。推行「智方便」平台及電子政府服務的進展（立法會 CB(1)654/2022(02) 號文件）。*https://www.legco.gov.hk/yr2022/english/panels/itb/papers/itb20221010cb1-654-2-e.pdf
[131]「智方便」。（日期不詳）。*「智方便」沙盒計劃簡介。*https://www.hklawsoc.org.hk/-/media/HKLS/Home/Support-Member/Professional-Support/AML/AML-Template/iAM-Smart-Information-Pack.pdf
[132] 保險業監管局。（2020 年 9 月 30 日）。*iAM Smart Pilot Sandbox Programme - Phase 2 [通函]。*
https://www.ia.org.hk/en/legislative_framework/circulars/reg_matters/files/Circulars_iAM_Smart_Pilot_Sandbox_Programme__Phase_2.pdf
[133] 政府資訊科技總監辦公室。（日期不詳）。*公私營機構採用「智方便」。*
https://www.ogcio.gov.hk/en/our_work/business/i_am_smart_adoption/

3. 香港在推進全球商業數碼身份標準方面的作用

企業數碼身份與個人數碼身份同等重要，為數碼經濟構建信任基礎，能夠促進交易、監管合規及可信度。企業數碼身份可以記錄公司的法律地位、監管合規及財務活動，對於確保營商環境的透明度與可及性非常重要。[134]

香港憑藉強大的金融業及對科技創新的承諾，率先在經濟基建中納入企業數碼身份。該策略舉措的意圖不僅在於優化本地業務，亦在於對國際數碼身份標準的建立施加影響。

在香港，採用企業數碼身份有望簡化行政流程、加強盡職審查，以及提升商業交易中的透明度，從而支援監管工作，打擊金融瀆職行為、維護市場誠信。諸如金管局的開放式應用程式接口 (API) 框架[135]等舉措在香港金融服務現代化中發揮關鍵作用。採用法律實體識別編碼 (LEI) 亦同等重要，香港交易資料儲存庫建議將其作為識別交易當事方的首要任務。[136]中國人民銀行採用法律實體識別編碼的策略路線圖[137]，連同銀聯納入該系統的舉措[138]，進一步凸顯香港對這一舉措的重視。

成熟的市場機制及充滿活力的科技應用，對於駕馭複雜的數碼身份整合局勢至關重要。香港在網絡安全、數據分析及金融科技專業發展方面的投資，體現了香港對這一轉型的決心。然而，前方的道路依然充滿荊棘。如何保障私隱、保護數據安全及實現系統互通性，是需要政府機構、金融機構、科技公司及民間社會齊心協力來解決的首要議題。隨著對數碼身份解決方案的探索，香港正站在十字路口。城市對法律實體識別編碼的引入，暗示著重塑營商及金融格局的潛力，是對更加健全及共融的未來的追求。諸如全球法人機構識別編碼基金會等組織以及香港公匙基建論壇等本地計劃的支援對於取得這一進步相當關鍵。香港數碼身份策略有望完善企業營運、促進全球貿易，並改善金融服務的可及性，從而提振經濟增長。在此背景下，企業數碼身份不僅意味著效率，亦是全球經濟互聯互通的重要基建。

[134] BIS。(2022 年 6 月)。*Corporate digital identity: No silver bullet, but a silver lining*。https://www.bis.org/publ/bppdf/bispap126.pdf
[135] 香港金融管理局。(日期不詳)。銀行業開放應用程式介面（開放 API）。https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/
[136] 香港交易資料儲存庫。(2019 年 3 月 14 日)。*實體身份*。https://hktr.hkma.gov.hk/ContentDetail.aspx?pageName=Identifiers-for-Entities
[137] 中國人民銀行。(2020 年 12 月 11 日)。*發佈《全球法人識別編碼應用實施路線圖（2020-2022 年）》*。https://www.gov.cn/xinwen/2020-12/11/content_5568976.htm
[138] 銀聯國際。(2022 年 6 月 3 日)。UnionPay's LEI safeguards cross-border payments, boosting innovation in digital payment。https://www.unionpayintl.com/en/mediaCenter/newsCenter/marketUpdate/3015078.shtml

鳴謝

金發局感謝以下工作小組成員的寶貴意見：

鄭志剛博士

Douglas Arner 教授

區偉權先生

陳磊明先生

趙必立先生

何志恒先生

許穗華女士

劉彥奇先生

呂志宏先生

潘宏烽先生

Benjamin Quinlan 先生

黃凱榮先生

金發局亦衷心感謝中國信息通信研究院為此報告提供的協助。

金發局的運作由行政總監領導：

區景麟博士

行政總監

此報告由金發局的政策研究團隊妥為準備：

董一岳博士

總監 · 政策研究主管

陸浩賢女士

高級經理

李恩如女士

高級經理

梁雋邦先生

經理

陳晴臻女士

經理

鍾曦文女士

經理

施凱凝女士

分析師

金發局網頁連結

香港金融發展局

關於香港金融發展局

香港金融發展局於二零一三年一月由特區政府宣布成立，為高層和跨界別 的平台，就如何推動香港金融業的更大發展及金融產業策略性發展路向， 徵詢業界並向政府提出建議。金融發展局會集中研究如何進一步發展 香港金融業，促進金融業多元化，提升香港國際金融中心在國家和地區中 的地位和作用，並背靠國家優勢、把握環球機遇，以鞏固本港的競爭力。

聯絡我們

電郵：enquiry@fsdc.org.hk

電話：(852) 2493 1313

網頁：www.fsdc.org.hk