FINANCIAL SERVICES DEVELOPMENT COUNCIL
香港金融發展局

June 2024

FSDC Paper No. 64

Embracing Digital ID:

Accelerating Digital Transformation in Hong Kong's Financial Services Industry

Table of Contents

Table of Contents

Executive summary

Executive summary

In today's dynamic global market, technological advancements are fundamentally reshaping business operations and economic landscapes. Embracing this evolution is vital for enhancing a city's competitiveness, especially in the dynamic financial sector. Hong Kong is strategically leveraging these advancements to reinforce its role as a leading international financial centre and a technological innovation hub.

The rapid growth of the digital economy, particularly in the post-pandemic era, is marked by a significant increase in acceptance and usage of digital channels by consumers. At the core of this expansion are digital identity (digital ID) systems, which play a crucial role in supporting Hong Kong's burgeoning digital economy.[1] These systems are transforming the financial services industry by enhancing transaction security and efficiency, broadening access to financial services, fostering inclusivity, and driving the development of new business models and service delivery mechanisms.

Digital IDs address critical needs in the financial sector, such as mitigating cyber threats and meeting stringent data protection requirements. Moreover, they facilitate more efficient and secure online transactions, which is essential for maintaining customer trust and market competitiveness. By employing advanced technologies such as biometrics and cryptography, these systems enhance customer verification processes and ensure regulatory compliance. Additionally, digital IDs streamline onboarding processes, reduce operational costs, and enhance customer experience by offering more personalised and accessible services, driving financial inclusion and sectoral innovation.

In Hong Kong, initiatives like iAM Smart exemplify its commitment to embracing digital ID concepts. It aligns with the broader goals of digital IDs by enhancing online security, streamlining transactions, and providing easier access to public and commercial services. The 2023 Policy Address and the subsequent recommendations from the Digital Economy Development Committee (DEDC) released in February 2024 collectively highlight Hong Kong's strategic approach to advancing its digital economy. These initiatives focus on key areas such as strengthening digital infrastructure, enabling cross-border data flow, supporting enterprise digital transformation, and improving digital governance and policies.[2,3] Some of these measures are interlinked with the digital ID system, emphasising the need for a cohesive strategy to maximise economic and operational benefits.

While acknowledging the Hong Kong SAR Government's efforts to transition into a digital economy, it is crucial to focus on digital ID opportunities and identify areas for improvement, particularly in digital infrastructure and regulatory frameworks. To this end, the Financial Services Development Council (FSDC) has established a Working Group comprised of industry experts. This group aims to identify and address challenges in developing and applying digital ID systems within the financial services industry and to formulate structured policy recommendations for the Government and other public stakeholders' considerations. Our key recommendations include:

i) To explore full-fledged implementation of the iAM Smart and enable the development of private digital ID wallets;

ii) To establish a trust framework for the digital ID ecosystem;

iii) To facilitate interoperability through enhanced infrastructure and legal frameworks;

iv) To harmonise digital ID standards for seamless cross-boundary/border interactions; and

v) To promote trusted digital ID adoption and enhance educational engagement.

1 In this paper, the term "digital ID" primarily refers to personal identities linked to an individual's official or legal identification and recognised by the government for official purposes. Any reference to digital identities related to businesses or corporations will be explicitly stated

2 HKSAR. (2023, October 25). The Chief Executive's 2023 Policy Address. https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

3 HKSAR Government Digital Economy Development Committee. (2024, February). Core recommendations of the Digital Economy Development Committee. Hong Kong SAR Government. https://www.itib.gov.hk/assets/files/DEDC_Core_Recommendations_Eng_issued.pdf

1. Introduction

1. Introduction

The digital economy is steering a paradigm shift towards digital marketplaces, reshaping business operations and societal interactions globally. The proliferation of digital platforms has cultivated a vast interconnected ecosystem that enhances the efficiency of services and transactions. Within this digital ecosystem, communication happens in various digital forms, connecting users through a high-speed global network.

Digital ID solutions are at the core of this expansion, facilitating secure and efficient online engagements. It offers a reliable framework for authenticating the online presence of individuals and business entities. Digital ID is more than an electronic credential; it has the potential to function like a virtual passport, guiding users through the complexities of the digital landscape with confidence.

This report aims to highlight the importance of digital ID in the digital economy, with a specific focus on its impact on the financial services industry. The analysis will explore the importance of nurturing a conducive ecosystem for the robust development of digital IDs. It will also examine how digital ID plays a fundamental role in promoting inclusivity, enabling access to services, and catalysing advancement within the broader economy and, more specifically, the financial sector.

1.1 Navigating the future with digital ID in an expanding digital economy

In the rapidly evolving digital economy, establishing a secure and reliable digital ID is imperative, particularly within the dynamic financial services industry. This sector stands on the cusp of transformative change spurred by digital innovations that are disrupting traditional models and businesses. Industry research has pointed to this shift; a study conducted by KPMG revealed that almost half of the financial service providers surveyed were preparing for a radical digital transformation within the next three years.[4] This sentiment is echoed by another market study, where 90% of surveyed experts, consisting of business executives, managers, and analysts from global organisations, agreed that digital innovations are reshaping the financial landscape.[5]

A working paper from the International Monetary Fund (IMF) defines the digital economy as encompassing a broad spectrum of economic activities that rely on digitised information and knowledge as the principal production factors. These activities hinge on advanced communication networks and leverage information technology as a catalyst for growth.[6] While the intersection of technology and finance has long-standing origins, innovation has accelerated in recent years, driven by a surge in technology investment. For instance, the MSCI ACWI IMI Fintech Innovation Index, a benchmark of the global fintech sector's performance, has almost quintupled over the past decade, reaching a value of 491.94 by April 2024.[7] Moreover, fintech industry revenues are projected to triple that of traditional banking from 2022 to 2028,[8] propelled by the financial sector's adoption of technologies like artificial intelligence, Distributed ledger technology (DLT), cloud computing, and data analytics. These tools are reshaping operational and customer engagement models, enabling new players to challenge long-standing industry norms.

During this transformation period, the global pandemic catalysed the digital evolution of the financial services industry as the demand for digital services intensified amidst lockdowns and social distancing measures. A study by the World Bank validates this shift, particularly in developing countries, where there has been a noticeable surge in financial account ownership and digital transactions.[9] Currently, two-thirds of adults worldwide utilise digital payment methods. However, it is noteworthy that the pandemic has significantly influenced the adoption of these digital methods among individuals in developing nations. Approximately 40% of adults in these nations, excluding China, have embraced digital payments for the first time due to the pandemic's impact.[10] This transition highlights the critical role of integrated systems capable of handling

4 KPMG.(2020, September). Digitalisation in banking beyond COVID-19. https://assets.kpmg.com/content/dam/kpmg/be/pdf/2021/Digitalization-in-banking-beyond-Covid-19.pdf

5 Deloitte. (2017). Digital transformation in financial services. https://www2.deloitte.com/tr/en/pages/financial-services/articles/digital-transformation-in-financial-services.html

6 International Monetary Fund. (2022, September 29). 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 MSCI. (2024). MSCI ACWI IMI Fintech Innovation Index (USD) Net [Factsheet]. https://www.msci.com/documents/10199/97543aa0-0ade-1dd6-1f12-fd2320479433

8 McKinsey & Company. (2023, October 24). Fintechs: A new paradigm of growth. https://www.mckinsey.com/industries/financial-services/our-insights/fintechs-a-new-paradigm-of-growth

9 The World Bank. (2022, July 21). 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 The World Bank. (2022, July 21). 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

digital identification and payments securely and efficiently. Such systems are vital for expanding access to financial services, especially for those previously underserved, and for connecting communities to new economic opportunities.

In terms of trade, digital transactions of goods and services in 2022 amounted to US$3.82 trillion, representing over half of the global services trade.[11] The growing involvement of businesses and consumers in the digital marketplace underscores the necessity for reliable digital ID solutions. Digital ID refers to unique online data "*linked to a person's / corporate's "official" or "legal" ID and is recognised by the government for official purposes*".[12] It empowers individuals to conduct secure digital interactions and transactions. For businesses, robust digital ID systems are essential in establishing trust and securing a competitive edge in the financial arena.

The concept of digital ID transcends mere authentication; it serves as the foundation for promoting inclusivity and orchestrating interactions as digital and physical realms converge, unveiling fresh opportunities. Recognising this convergence is crucial as digital engagements increasingly permeate daily existence, fostering the emergence of global digital citizenship.

In this context, adopting a forward-looking approach towards digital ID infrastructure and regulatory framework is crucial. These systems require agility to address current demands while remaining adaptable to future technological advancements. In an innovation-driven digital economy where trust is fundamental, resilient digital ID solutions are essential for individuals and businesses to navigate the emerging economic landscape effectively.

Hong Kong recognises the potential of the digital economy as a catalyst for high-quality development. The 2023 Policy Address has outlined initiatives aimed at nurturing this growth. These initiatives include enhancing digital infrastructure, promoting cross-border data flows, facilitating enterprise transformation, and strengthening human capital, all under the guidance of the DEDC.[13] While Hong Kong has developed its digital capabilities, there is a crucial need to intensify its efforts further. Cultivating an ecosystem conducive to the development and adoption of digital ID is pressing. Prioritising the establishment of digital ID systems is not merely an optional upgrade but a fundamental step towards maintaining a competitive edge in the digital revolution, ensuring the city's economic vibrancy, and fostering global connectivity for its citizens.

1.2 Unlocking economic value and pathways to growth through digital ID integration

Digital ID systems are essential for adapting to the digital economy and catalysing economic growth. The McKinsey Global Institute highlights the potential impact of digital ID, projecting that the widespread adoption of universal digital ID could unlock the economic value equivalent to 3–13% of GDP by 2030.[14] Moreover, according to PwC's consulting team, the global digital ID market is expanding rapidly, anticipated to double from US$16 billion in 2020 to US$33 billion by 2025, with a compound annual growth rate (CAGR) of 16%.[15]

These forecasts highlight the transformative potential of digital ID in enabling economic activities beyond traditional boundaries. By eliminating barriers such as manual or operationally onerous Know Your Customer (KYC) regulations, the absence of universally recognised credit records across jurisdictions, and high operational costs, digital ID has the potential to bridge the gap. This fosters more inclusive participation and empowerment in the digital economy, particularly in developing regions. Integration of digital ID can streamline operations for financial institutions, resulting in cost savings, risk reduction, and market expansion opportunities.

The anticipated economic benefits of digital ID are extensive. They can reclaim up to 110 billion hours of work for public services, reduce business onboarding costs by up to 90%, and lead to substantial savings in payroll fraud – potentially amounting to US$1.6 trillion annually.[16] Additionally, advancements in biometric solutions, increasingly incorporated into digital ID solutions, are expected to expedite digital onboarding to near real-time

11 International Monetary Fund. (2023, December 13). Why Digital Trade Should Remain Open. https://www.imf.org/en/Blogs/Articles/2023/12/13/why-digital-trade-should-remain-open

12 Alliance for Financial Inclusion. (2021, September 9). 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 HKSAR. (2023, October 25). The Chief Executive's 2023 Policy Address. https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

14 McKinsey Global Institute. (2019, April 17). 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 Strategy&. (2021). 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 McKinsey & Company. (2023, October 24). Fintechs: A new paradigm of growth. https://www.mckinsey.com/industries/financial-services/our-insights/fintechs-a-new-paradigm-of-growth

verification, significantly enhancing user experience and operation efficiency.[17] Digital ID solutions thus form the foundation for a more interconnected and prosperous economic future.

The role of digtial ID in fostering digital trust

In a digital economy, trust is a cornerstone that supports growth, innovation, and interaction. Digital ID is critical in establishing the trust necessary for economic resilience and societal inclusion. Both government entities and private organisations acknowledge the persistent challenge of maintaining trust among consumers and citizens.

As cybersecurity threats advance in complexity, a research study by Gartner highlighted concerns that conventional ID verification methods are nearing obsolescence. By 2026, approximately one-third of enterprises would find these solutions no longer reliable.[18] Supporting this view, the Canadian Centre for Cyber Security emphasises the urgency of these concerns, pointing out the increasing prevalence of sophisticated threats such as phishing, malware, and social engineering, all aimed at compromising personal data.[19] In addition, the growing incidence of biometric data breaches and system vulnerabilities highlights the urgency of robust data protection measures. In 2022, one in every four banks reported over 100 ID fraud incidents, with common offences including document forgery and physical ID tampering, each incident resulting in an industry average cost exceeding US$310,000.[20]

These concerns transcend geographical and sectoral boundaries, as evidenced by a report in 2023 indicating an 18.3% suspected digital fraud attempts rate - the highest among all studied markets.[21] The sophistication of cyberattacks is escalating due to technological advancements and the increased data accessibility. An example of this was an incident where an international corporation suffered a loss of HK$200 million. Fraudsters manipulated video and audio to mimic their senior management during a video conference, leading to fraudulent financial transactions.[22]

Amidst the escalating complexity and frequency of cybersecurity threats, the implementation of well-designed digital ID solutions may provide critical protection. Regular scrutiny is also essential to pre-empt potential vulnerabilities. A robust digital ID system incorporates secure biometric identification while prioritising privacy, adhering to the guidance of the International Association for Privacy Professionals (IAPP).[23] Digital ID is pivotal not only for consumer transactions but also for employees, business partners, and networked devices, making ID management a strategic corporate priority. In the financial services industry, identity verification is crucial to prevent fraud and enhance the customer experience, in alignment with the guidelines of the Financial Action Task Force (FATF). The adoption of global standards could be considered to bolster the security and efficacy of digital IDs, providing a more unified and resilient framework for combating digital fraud worldwid.

In addition, integrating technologies such as artificial intelligence (AI) and machine learning is transforming the landscape of digital ID management. These tools facilitate the automation and scalability of ID management systems, providing adaptable solutions to address the evolving cybersecurity requirements and ID verification needs.[24]

Social inclusion and empowerment through digital ID integration

The implementation of digital ID systems holds significant implications for both economic and social inclusion. These systems transform how individuals engage with government entities, access public services, and participate in the global marketplace.

17 Innovatrics. (n.d.). Traditional versus digital onboarding in banking. https://innovatrics.com/trustreport/traditional-versus-digital-onboarding-in-banking/
18 Gartner. (2024, February 1). 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 Canadian Centre for Cyber Security. (2022). An Introduction to the Cyber Threat Environment. https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment
20 Regula. (2023, March 29). 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 TransUnion. (2023, October 4). 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 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 CNN. (2024, February 4). 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 International Association of Privacy Professionals:. (n.d). Biometrics. https://iapp.org/resources/article/biometrics/
24 MarketsandMarkets. (2024). Global identity verification market size, trends, growth rate & industry share 2030. https://www.marketsandmarkets.com/Market-Reports/ID-verification-market-178660742.html

Despite notable advancements in service digitisation by the private sector in Europe, inadequate digital ID frameworks have hindered public sector progress. A robust digital ID system is essential for facilitating more streamlined interactions between governments and their citizens, particularly through mobile technology and DLT, ensuring secure digital ID solutions.[25] Such systems empower individuals with greater control over their data and support applications like electronic voting and digital health services.[26]

Universal access to government services is key to advancing social and financial inclusion. Initiatives aimed at establishing a globally recognised digital ID framework correspond with the United Nations' 2030 Agenda for Sustainable Development, particularly the goal of providing legal identification for all. Considering the significant number of individuals without official identification, digital strategies are essential for mitigating this disparity.[27]

Digital ID serves as gateway to opportunities for diverse societal segments. When paired with robust governance frameworks, they possess the potential to function as formidable instruments of inclusion, transforming citizen-government relations and fostering empowerment on a global scale.

25 IBM. (2022, September 2022). 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. (n.d.) Building trust and social inclusion with digital identities. https://innovationinpolitics.eu/showroom/project/building-trust-and-social-inclusion-with-digital-identities/
27 UNCTAD. (2023, September 14). UNCTAD supports small island nations to harness digital ID for inclusion. https://unctad.org/news/unctad-supports-small-island-nations-harness-digital-id-inclusion

2. Foundation of digital ID

2.1 Core principles and technologies underpinning digital ID

Digital ID systems are grounded on fundamental principles and technologies that ensure their functionality, integrity, and security. A digital ID acts as an electronic record of an individual's physical ID, facilitating secure and efficient interactions across various digital platforms by authenticating the user's ID.[28] It represents a person's unique digital profile, incorporating various personal credentials and attributes. This digital footprint forms the foundation of modern identification practices, enabling individuals to establish their online presence with a level of trust and assurance akin to their physical ID.

As digital interactions become increasingly prevalent, digital ID systems are evolving to meet the demand for reliable identity verification. These systems seamlessly combine convenience with robust security measures, enabling smooth participation in the digital world. Organisations like the World Bank have established comprehensive standards to govern the ethical and practical use of digital IDs. These standards aim to foster inclusive, secure, and mutually beneficial systems for all stakeholders, including the public and private sectors.[29]

Governments play a pivotal role in shaping the digital ID ecosystem by establishing core principles. For instance, the United Kingdom's Digital ID Strategy Board outlined six guiding principles in 2020 that steer the development of digital ID frameworks. These principles provide detailed recommendations covering a broader classification of digital ID fundamentals.[30] Similarly, in September 2023, the Australian Federal Government released an exposure draft of legislation for a comprehensive digital ID system, proposing four comparable principles.[31] These governments' perspectives, along with insights from academic and industry research,[32] can be broadly categorised into three overarching principles critical for designing a digital ID system:

- **Inclusion:** A well-designed digital ID framework should strive for universal accessibility, ensuring equitable access for all individuals. The goal is to create a system that does not discriminate based on factors such as socioeconomic status or geographic location. By achieving this, it fosters an environment where every user can fully participate in the digital economy, bridging the gap between the underserved and the well-connected.
- **Trust:** Trust serves as the foundation upon which user confidence is built. Establishing a robust digital ID system requires ironclad security measures to safeguard personal data against breaches and unauthorised access. Equally important is the clarity of the managing processes and the accountability of those responsible for overseeing these systems. When users have confidence in the system's integrity and believe that their data is protected and their privacy respected, trust naturally follows.
- **Utility:** This emphasises the practical benefits of digital ID. The system should streamline users' interactions with the public and private sectors, facilitating smoother transactions and more efficient service delivery. An effective digital ID goes beyond mere functionality; it enhances user experience, driving increased adoption and satisfaction.

Digital ID solutions could be complex networks that integrate diverse data points and digital interactions. Key elements such as passwords, birthdates, and biometric data are complemented by e-passports, digital wallets, and mobile IDs, creating a comprehensive digital profile tailored to individual preferences and requirements.[33]

Safeguarding personal data is also critical, necessitating robust security and privacy infrastructure. Achieving the optimal balance between personalisation and privacy protection is essential for building trust in digital ID solutions. A secure and user-centric digital ID system emerges from the convergence of advanced technologies, including but not limited to the following: [34,35,36]

28 McKinsey Global Institute. (2019, April 17). Digital identification: A key to inclusive growth. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20

29 World Bank ID4D. (n.d). 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 UK Government. (2020, September 1). 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 The Parliament of the Commonwealth of Australia. (2023, September). 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.pd

32 The Sorvin Foundation. (2022, September). Principles of SSI V3. https://sovrin.org/principles-of-ssi/

33 Aratek. (2023, May 30). 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 Aratek. (2023, May 30). 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). The next evolution of digital identity: Scalable, secure, and trusted digital credentials. https://www.ibm.com/downloads/cas/PEZANJ1N

36 Thales Group. (n.d.). Trusted digital identity by Thales. https://www.thalesgroup.com/en/markets/digital-ID-and-security/government/ID/digital-ID-services/trends

- **Cryptography:** Utilises technologies like public key infrastructure to ensure secure electronic identities, digital signatures to authenticate documents, and hashing to maintain data integrity and confidentiality.
- **Biometric authentication:** Utilises distinctive physical or behavioural traits for verification, such as fingerprint scans, facial recognition, voice authentication, and iris scans.
- **DLT:** Provides immutable transaction records and supports self-sovereign ID (SSI) models, allowing individuals to control their digital identities independently individuals on a public and immutable distributed ledger.
- **Artificial intelligence and machine learning:** Enhances security protocols through the detection of fraudulent patterns and improves biometric systems with advanced liveness detection capabilities.
- **Mobile ID wallets:** Provides secure storage for smartphone digital credentials, featuring selective disclosure functionalities for privacy protection.
- **Advanced encryption standards:** Protects stored data with strong encryption, rendering it unreadable to unauthorised users.
- **Zero-knowledge proofs:** Validates the authenticity of information without disclosing the underlying data, ensuring privacy and fostering trust.
- **Federated ID management:** Facilitates ID portability across various systems and services, promoting interoperability and user convenience.

By integrating these technologies, digital ID systems mitigate the risks of identity theft and fraud while ensuring a seamless user experience. They are poised to revolutionise the field of ID verification by delivering an ideal balance of security and user convenience.

However, the success of digital ID systems hinges not solely on technological advancements but also on the establishment of robust policies, effective governance, and a keen emphasis on user-centric design. A well-rounded approach to digital ID encompasses both technological innovation and societal considerations, striving for active user engagement and broad societal acceptance.

2.2 The digital ID landscape: different approaches to digital ID

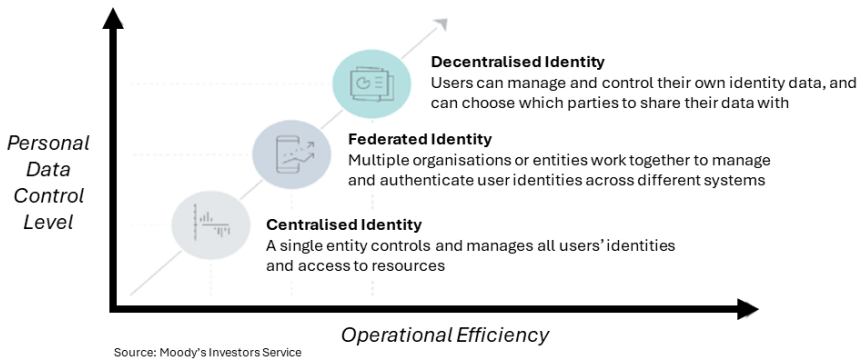
Digital IDs are integral to online transactions, capturing unique personal attributes for digital identification. The table below provides a brief overview of the evolving landscape of digital ID management, presenting a spectrum of models tailored to meet the demands of the digital era. These approaches span from the centralised model, known for its efficient process and centralised control, to the decentralised model, which grants data sovereignty to users. Each framework presents distinct benefits and considerations (Figure 1).

Figure 1: Types of Digital ID [37,38,39]

Types of Digital ID	Details	Ownership
Government-driven centralised approach	A comprehensive system where the government retains full oversight and control over ID verification, management, and authentication processes. Common applications include official functions such as taxation, healthcare, voting, etc.	Government-owned and controlled. The model designates the state as the exclusive authority on data collection, digital ID issuance, and user authentication.
Semi-centralised, federated approach	An interconnected system enabling users to generate a digital ID through multiple accredited providers. This ID is universally applicable across diverse services, promoting interoperability while maintaining a level of centralised oversight.	Managed through a central hub that coordinates multiple ID providers, offering user flexibility within a trusted framework.
Decentralised, open ID market	A marketplace-oriented approach where ID verification and management are decentralised, enabling users to maintain multiple identities for distinct purposes. This model adapts to emerging technologies like DLT for heightened security and privacy.	ID data is owned by individuals and distributed across the network without a central authority. Participants adhere to a standard set of rules or protocols within a self-regulated market.
Self-asserted digital ID	A user-centric model where individuals assert their ID attributes is commonly found in environments prioritising ease of access over rigorous ID verification, such as social networks and e-commerce platforms.	Individuals retain autonomy over their digital presence, with minimal oversight from external verifying bodies

Digital ID management models encompass centralised and decentralised systems, each carrying distinct operational implications. Decentralised systems often yield higher operational efficiency by distributing control and data robustly. This efficiency arises from granting users autonomy over their data, and expediting and securing ID verification, especially when leveraging DLT. Conversely, centralised models, through potentially more straightforward structures, may suffer from reduced agility due to bureaucratic processes (Figure 2). The choice between these models holds significant consequences for user trust and engagement. Decision-makers face the challenge of balancing the benefits of decentralised systems—efficiency and user empowerment—with the need for a system that is intuitive and accessible to all users.

Figure 2: Digital ID systems and their degree of centralisation[40]



37 International Telecommunication Union. (2018). 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 Strategy&. (2021). 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 World Bank ID4D. (n.d). Types of ID systems. https://id4d.worldbank.org/guide/types-id-systems
40 Moody's Investors Service (2023, September 21). 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

2.3 Empowering individuals - a hybrid decentralised approach

Centralised digital ID management systems, which draw from government demographic databases, streamline organisational processes and offer reliable ID verification. However, there is a global shift towards prioritising privacy, personal control, and data autonomy in ID management. This trend is reflected in various digital ID models, such as Estonia's, which integrates private digital ID providers into its centralised system, and Israel's, which adopts a central ID approach with differing levels of centralisation.[41] Despite their distinctions, both models share a commitment to empowering individuals to manage their digital identities.

The emergence of a decentralised ID management system marks a notable shift in the landscape, placing control with individuals as the custodians of their own digital IDs.[42] Through digital wallets, users can securely manage credentials, adopting a self-sovereign ID (SSI) model that reduces reliance on central authorities. This approach mitigates risks associated with centralised data storage, such as significant breaches.[43]

Corporations also benefit from the adoption of decentralised ID systems. These systems streamline customer data verification, providing a more efficient and enhanced user experience. Additionally, they assist companies in meeting data protection standards, such as those mandated by the General Data Protection Regulation (GDPR), by sharing only the necessary data for specific interactions.[44] While federated ID systems offer similar benefits, decentralised models stand out for their ability to minimise data collection and enhance individual control over personal information.[45]

With the increasing prevalence of digital wallets for credential management, standardised regulatory frameworks and protocols become imperative to ensure cross-platform interoperability. Although decentralisation may imply limited government oversight, strategic government involvement can strengthen the digital ID infrastructure, improving verification and authentication processes.

Integrating verifiable credentials from a "golden source" combines user control with centralised trust (the concept of "golden source" will be explored further in subsequent sections of this paper). These credentials, authenticated against a central database and digitally signed, are stored in digital wallets and generated on demand, eliminating the need for constant central checks. The cryptographic signature of the credentials confirms their authenticity.[46] However, despite its potential, decentralised ID encounters obstacles, including technical complexity, security risks, compatibility concerns, and potential data misuse.[47] Without overcoming these challenges, decentralised IDs may struggle to attain global adoption and widespread acceptance.

To address these hurdles, hybrid models emerge as a solution, offering a balanced solution that combines enhanced security with user empowerment. These models blend the benefits of centralised and decentralised systems, streamlining technology, enhancing access, and lowering entry barriers. By integrating centralised security measures with decentralised encryption, hybrid models can bolster trust. Collaborative efforts between governments and private entities are crucial for developing standardised frameworks, ensuring smooth interoperability, and upholding accountability. Countries like Australia, Canada, and Finland illustrate such collaborative ecosystems, leveraging regulatory precision and private-sector innovation to craft a secure, user-friendly, and adaptable digital infrastructure.[48]

41 Digital Government Exchange. (2022). 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. (n.d.). What is decentralised ID?. https://proofid.com/what-is-decentralised-ID/
43 Allen, C. (2020, April 25). The path to self-sovereign ID. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-ID/
44 ENISA. (2021). 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 Moody's Investors Service. (2023, September 21). 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 Citi. (2023, March). 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 Moody's Investors Service. (2023, September 21). 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). 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

3. Functions of digital ID and its adoption in the financial services industry

3.1 The role and characteristics of digital ID in financial services

In the financial services industry, it is crucial to navigate a landscape that demands stringent data integrity and advanced protection measures. With the proliferation of cyber threats, safeguarding sensitive personal and financial data requires top-tier security protocols. As the industry progresses towards more secure online transactions, there is an essential shift in security practices. Simultaneously, there is a growing consumer expectation for swift and convenient remote banking services. Balancing the need for expedited transaction processing with robust security is a challenge digital ID solutions are poised to meet.

The implementation of digital ID systems aims to address these challenges, offering benefits such as operational efficiency, fortified security, and increased service accessibility to a diverse clientele. The adoption is driving transformative changes within the core functions of financial services, notably:

Strengthening customer due diligence: Digital IDs elevate the effectiveness of customer identification and verification during onboarding, as well as the authentication of customer identities for account access.

- **Streamlined verification process:** By leveraging advanced digital technologies, including biometric data and cryptographic methods, the verification process is refined. These technologies strengthen the authenticity checks of ID documents and the individuals presenting them, thereby reducing fraud and identity theft incidences.
- **Ongoing due diligence:** Digital ID systems assist financial institutions in their continuous monitoring efforts by facilitating regular customer information updates. This ensures that observed financial behaviour aligns with the customer's profile and expected activities. Such ongoing diligence is vital for upholding the integrity of the financial system and complying with regulatory standards.

Reducing human error in control: Traditional identification methods frequently rely on the subjective judgment of financial institution officers, who may lack the tools and expertise to detect fraudulent documents.

- **Specialised verification:** Digital ID verification processes, when integrated with advanced automated systems, are adept at identifying falsified or modified documents with high accuracy. This reliance on technology diminishes the necessity for human intervention in document authentication. In addition, it ensures a uniform and dependable approach for verifying identities during account access.

Cost efficiency and transaction monitoring:

- **Cost reduction:** Streamlining the digital verification process can result in substantial cost savings in customer onboarding.[49] With potential reductions in onboarding expenses, financial institutions can reallocate resources to other compliance functions and expand services to underserved populations.
- **Transaction monitoring:** Real-time verification assists in identifying and reporting suspicious activities. Furthermore, integrating additional data points such as geolocation and device ID aids in creating detailed customer profiles and identifying unusual transaction patterns, thus enhancing the institution's anti-fraud and anti-money laundering efforts.

Enhancing customer experience:

- **Streamlined customer onboarding experience:** The onboarding experience is streamlined by eliminating the need for in-person branch visits and the associated wait times. This enhanced process accelerates service delivery and improves customer satisfaction, fostering stronger loyalty in the competitive financial landscape.
- **Tailored financial products and services:** The strategic use of digital ID also enables financial institutions to collect and analyse customer-specific data, gaining deeper insights into consumer behaviours and needs. This data-driven approach empowers banks and fintech firms to develop personalised financial products and services — from tailored investment advice

49 McKinsey Global Institute. (2019, April 17). Digital identification: A key to inclusive growth. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20

to targeted promotions and customised lending solutions. Such personalised engagement meets customers' expectations for relevance and convenience in their financial interactions.[50]

Promoting financial inclusion: A crucial role in extending financial services to individuals lacking traditional identification, often in remote or underserved regions of developing countries.

- **Greater reach:** By removing barriers to entry, digital IDs can notably broaden financial inclusivity, allowing more individuals to participate in the digital economy.
- **Government and commercial digitalisation:** In developing countries, digital ID systems are crucial for digitising government-to-person payments and aid distribution, facilitating access to financial services for those in need.

The financial services industry's exploration of digital identifiers, ranging from biometrics to blockchain-based solutions, is reshaping the landscape of ID verification. These technologies are designed to be universal and unique, aiming to reduce fraud and maintain transactional integrity. Despite the hurdles in creating a universal digital ID system, the industry's commitment to interoperability aligns with goals for a secure and inclusive financial future.

Digital IDs are propelling advancement in privacy, security, and regulatory compliance, establishing their importance within the digital economy. Regulators are responding to the digitisation of financial services by crafting adaptive frameworks that keep pace with innovation and prioritise consumer safety. Regulatory initiatives concentrate on: [51]

- **Standardisation:** Regulators aim to ensure smooth and seamless transactions by establishing consistent digital ID verification standards, enabling compatible systems.
- **Compliance:** Mandating best practices in data protection, privacy, and due diligence to safeguard consumer information and cultivate secure customer relationships.
- **Accountability:** Financial institutions are responsible for safeguarding customer data and ensuring the integrity of authentication processes to uphold and enhance consumer trust.
- **Licensing/Qualification:** Digital ID service providers should be required to obtain certification verifying their adherence to data privacy and cybersecurity standards, as well as their ability to effectively manage potential conflicts of interest.

Financial regulatory authorities worldwide are currently in the process of establishing frameworks that promote interoperability, transparency, and consumer protection — all essential qualities for the sustainable integration of digital IDs. Achieving a fully operational digital ID ecosystem necessitates striking a delicate equilibrium between regulation and technological progress. The ultimate objective is leveraging digital ID features to promote a financial environment that is secure, efficient, and accessible to all.

50 Global Banking & Finance Review. (n.d.). The impact of digital ID on banking and finance. https://www.globalbankingandfinance.com/the-impact-of-digital-identity-on-banking-and-finance/

51 The Financial Action Task Force. (March 2020). Guidance on Digital ID. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-ID.pdf.coredownload.pdf

3.2 Essential data elements associated with digital ID in the financial services industry

In the financial sector, a digital ID encompasses critical data elements vital for ensuring secure transactions and regulatory compliance. Serving a dual purpose, a digital ID provides access to services while enhancing security measures for both consumers and financial institutions. Its foundation lies essential identification components — such as name, date of birth, and residential address — utilised for ID verification, anti-money laundering (AML) checks and authentication during account management. Recognising the significance of these data components, the Council of Europe has issued guidelines for the development of national digital ID frameworks, emphasising the essential data at the core of a digital ID (Figure 3).

Figure 3: Types of data for a national digital ID[52]

Types of data	Details
Biographical data	Personal information typically recorded in civil registries: Date of birth, gender, etc.
Biometric data	Unique physical identifiers: Fingerprints, iris scans, facial recognition, and other physiological markers.
Legal ID data	Information certifying legal ID before the law and vis-à-vis the state: National ID numbers, social security numbers, etc.
Demographic data	Population characteristics: Age, ethnicity, education, employment, marital status, etc.
Documentary data	Information found on ID documents: ID cards, passports, driver's licenses, and other official documents used to assert ID or access services.
Authentication data	Credentials for digital ID verification: Passwords, PINs, security questions, digital certificates, etc.

To fully harness the potential of digital ID, the financial services industry must look beyond mere ID verification and embrace a broader spectrum of data points. This expansion could encompass an individual's financial background, investment behaviour and preferences, risk profiles, and more. However, due to the confidentiality of these metrics, its management must adhere to rigorous financial regulatory standards.

For instance, within the European Union's GDPR framework, financial institutions must comply with strict standards for processing and safeguarding personal data, ensuring the protection of an individual's financial digital ID and upholding their privacy rights.[53] Similarly, Australia's Consumer Data Right (CDR) grants consumers the power to access their financial information securely and efficiently, allowing them to share this data with accredited third parties. Financial institutions are required to comply with these regulations, implementing systems that validate digital IDs and ensure the secure transmission of data.[54] Such regulatory measures foster trust among all participants in the ecosystem, ensuring a regulated landscape.

Considering that a more expansive digital ID profile could provide a nuanced and complete representation of an individual's ID,[55] the following additional data elements could be regarded as for integration into or linkage with a digital ID for the financial services industry:[56,57,58] That said, it is crucial to emphasise that the integration of these data elements into digital IDs must strictly adhere to the principles of user consent:

- **Credit information:** An individual's credit score and history are crucial components. This data acts as a financial fingerprint, providing insight into an individual's creditworthiness and financial behaviour. Embedding this information within the digital ID allows financial institutions to make informed decisions regarding lending, credit offerings, and risk management.
- **Transaction data:** Whilst not inherently essential, access to transactional records can provide valuable insights into spending patterns, income stability, and financial behaviours. This data enables financial institutions to tailor product and service offerings more effectively to individual needs.
- **Tax records:** Tax records offer a comprehensive view of an individual's earning history, tax payments, and liabilities. This information verifies income and is crucial in assessing fiscal

52 The Council of Europe. (2023). Guidelines on National Digital Identity. https://edoc.coe.int/en/data-protection/11578-guidelines-on-national-digital-ID.html
53 Deloitte. (2019). 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 The Office of the Australian Information Commissioner. (n.d.). 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, December). 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, June). Corporate digital ID: no silver bullet, but a silver lining. https://www.bis.org/publ/bppdf/bispap126.pdf
57 OECD. (2021, December 16). 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 OECD. (2022, June 22). 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

responsibility and compliance with tax regulations. For financial institutions, access to tax-related data can significantly impact decision-making processes related to loans, investment services, and fraud detection.

- **Income and employment history:** Incorporating employment data, including past and current employers, job positions, and salary details, enhances the understanding of an individual's financial stability and earning potential. This information assists in assessing risk for various financial commitments.
- **Insurance policies:** Access to details regarding current and past insurance policies, such as life, health, and property insurance, provides insights into an individual's risk management strategies. Financial institutions can use this information to tailor insurance products or integrate insurance considerations into their financial planning services.
- **Ownership records:** Documentation of ownership for assets like property or vehicles informs credit assessments and financial advisory services, offering a more comprehensive picture of an individual's financial situation.

Digital IDs play a significant role in the financial sector, extending far beyond mere transactions and regulatory compliance. They are instrumental in enhancing financial services and elevating the overall customer experience by leveraging the comprehensive data they provide.

Golden source

The concept of a 'golden source' is pivotal in discussions surrounding digital ID systems. This term refers to a primary, reliable data repository that serves as the benchmark for accuracy and integrity in ID information. Stakeholders must align their digital ID initiatives with the principles and standards guiding the golden source to ensure a consistent and secure ID framework. The notion of the "golden source" in digital ID models constitutes a foundational element that delineates the roles and responsibilities of stakeholders in managing, safeguarding, and utilising ID data. This authoritative database or source contains centralised verified and trusted ID data, establishing the standard for identification processes across various models. Its significance extends to compliance, operational integrity, and user privacy.[59]

The character of the golden source and the role of stakeholders in its utilisation vary across centralised, semi-centralised, and decentralised models.

A corporate digital ID functions as the digital representation of a business entity, encapsulating its legal and operational identity within the digital realm. It is a repository of verified data encompassing corporate structure, governance, financial status, and compliance records.[60] This digital profile includes real-time updates on changes within the corporation, such as shifts in directorship or structural adjustments, ensuring that the entity's digital representation is accurate and up to date.

The utility of a corporate digital ID extends across various facets of business operations. It is critical for authenticating a company's credentials during electronic transactions, securing access to financial services, and maintaining transparent communication with regulatory authorities. As a hub of verified information, it fosters trust and integrity within the digital marketplace, streamlining interactions with suppliers, customers, and partners.

While this paper primarily focuses on individual digital IDs, it acknowledges the critical role of corporate digital IDs in the industry. The significance and functions of corporate digital ID will be briefly discussed in later sections of this paper.

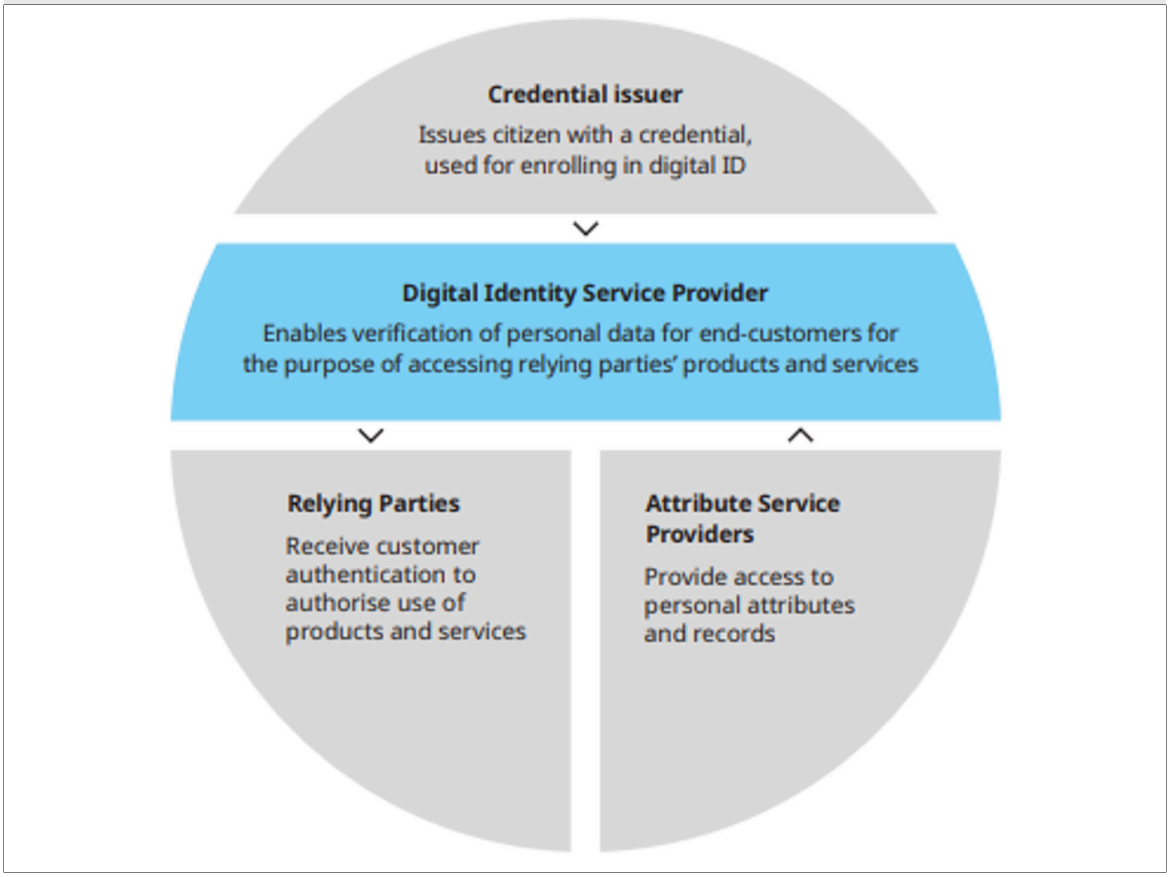
59 World Wide Generation. (2019, November 26). In search of the golden source: non-financial data. https://www.worldwidegeneration.co/news/in-search-of-the-golden-source-non-financial-data
60 BIS. (2022, June). Corporate digital ID: no silver bullet, but a silver lining. https://www.bis.org/publ/bppdf/bispap126.pdf

3.3 Assessing data models for robust digital ID integration

In the diverse landscape of digital ID, various frameworks are designed to meet the specific requirements and regulatory environments of different contexts. Despite this diversity, certain stakeholders consistently emerge as the critical pillars within any digital ID ecosystem. While their functions may appear distinct, it is common for an entity to fulfil multiple roles, illustrating the adaptability and interconnected nature of the digital ID environment (Figure 4).

- **Credential Issuers (CIs):** These entities are responsible for verifying individuals' identities and issuing a digital credential that authenticates those identities for future transactions. This typically involves collecting and validating personal information and documentation to establish the identity with a high level of confidence.
- **ID Service Providers (ISPs):** These providers verify users' identities and are authorised by users to share verified identities with relying parties. This enables users to access services or create accounts securely.
- **Attribute Service Providers (ASPs):** These entities manage information that defines user attributes. With user consent, ASPs share these attributes with relying parties and ISPs. In cases where ISPs also handle attribute-related services, they fulfil the role of ASPs, adhering to the requirements of both roles. ASPs are responsible for describing the quality of the attributes they manage.
- **Relying Parties (RPs):** These organisations utilise ID and attribute information provided by other participants in the framework. They include businesses such as airlines, banks, and retailers, which rely on ISPs for user ID verification and ASPs for eligibility checks based on user attributes without conducting the checks themselves.

Figure 4: The roles of stakeholders in a digital ID ecosystem[61]



Source: Oliver Wyman analysis

61 Oliver Wyman & International Banking Federation. (2021, December). 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

An effective digital ID ecosystem relies on the precise definition and collaboration of stakeholders, including governments, banks, technology firms, and various service providers. Governments establish national ID frameworks to ensure digital IDs adhere to legal and regulatory standards, protecting citizen privacy and security. They promote digital ID adoption through public services, fostering a trusted environment for digital transactions, whose success depends on perceived reliability.

Private sector entities, including banks, technology firms, and service providers, also play a significant role. Banks, known for their stringent KYC processes and customer trust, serve as verifiers and custodians of digital ID data. Technology companies contribute innovative and scalable platforms and robust security infrastructure supporting digital identities. Service providers across industries integrate digital IDs into consumer transactions and services. These stakeholders must collaborate to ensure seamless, user-centric, and universally accessible digital ID systems, thus promoting broad inclusion and adoption.

The integration of robust digital IDs within the financial services industry hinges on the architecture of the employed data models. These models form the backbone of the digital ID ecosystem, each with its unique approach to data governance, ensuring the secure and efficient management of ID information. (Refer to Annex 1 for detailed stakeholder roles in each ID model)

3.4 A shift towards user-centric verification – decentralised ID and Self-sovereign ID (SSI)

In contrast to traditional models, decentralised ID represents a paradigm shift towards a more user-centric approach to ID verification. This model places control directly in the hands of the user, signalling the rise of SSI, a framework empowering individuals to own, manage, and control their ID data. Users leverage a digital ID wallet—a secure repository—to collect and store verified personal information from trusted authorities, including government entities or licensed corporations.[62]

This model is gaining global traction amid heightened data security concerns and diminishing confidence in centralised repositories. Market analysis highlights this shift, projecting significant expansion in the global decentralised ID market from US$285 million in 2022 to over US$6.8 billion in revenue by 2027, reflecting a notable CAGR of 88.7% over five years.[63]

User ownership: the core of decentralised ID and SSI

At the core of a user-centric ID system lies the principle of user ownership, granting individuals control over their ID data. This principle fosters autonomy and serves as the foundation of decentralised identification systems. Within these frameworks, SSI emerges as a subset that emphasises user empowerment, enabling individuals to manage their identities independently.[64] This empowerment is reflected in the growing consumer awareness surrounding personal data sovereignty, with nearly three-quarters of surveyed participants expressing discomfort at sharing personal information for goods and services.[65] Against this backdrop, the ascent of decentralised IDs and SSI ushers in a new era of user sovereignty.

Personal devices and secure cloud services are evolving into personal data vaults, with users assuming the role of gatekeepers. This transition vests ownership upon individuals and mitigates risks associated with ID theft and unauthorised data sharing. SSI reduces dependence on central verification, allowing users to authenticate credentials on their terms, thereby safeguarding privacy and facilitating secure online interactions.

Verifiable credentials: establishing trust in the digital realm

Within the decentralised ID framework, verifiable credentials emerge as a pivotal component, enhancing trust and privacy in digital interactions. These credentials resemble digital certificates, carrying a set of independently verifiable claims about an individual.[66] A claim constitutes a piece of information asserted by an entity about

62 GSMA. (2022). Decentralised Identity. https://www.gsma.com/ID/decentralised-ID

63 MarketsandMarkets. (2022, May). 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 Cucko, Š., & Turkanovic, M. (2021). Decentralized and self-sovereign identity: Systematic mapping study. IEEE Access, 9, 139009-139027.

65 Entrust Cybersecurity Institute. (n.d.) The Future of ID Report. https://www.entrust.com/cybersecurity-institute/reports/future-of-identity

66 Brunner, C., Gallersdörfer, U., Knirsch, F., Engel, D., & Matthes, F. (2020, December). Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust. In Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications (pp. 61-66)..

itself or another, ranging from an individual's name and address to identifiers issued by public or private entities. Each claim is independently verifiable, offering a robust testament to an individual's ID.[67]

For instance, a verifiable credential could confirm an individual's academic and professional qualifications. These credentials, issued by recognised authorities, can be seamlessly integrated into electronic transactions as required. This efficient approach to ID verification streamlines processes and enhances the credibility of online interactions.

The integrity of verifiable credentials hinges on cryptographic signatures from the issuing entities.[68] These credentials leverage a verifiable data registry—a secure, distributed ledger resistant to tampering. While DLT is preferred for its security features, other distributed database technologies are also viable. DLT serves as a decentralised database, securely documenting transactions to prevent alteration, hacking, or fraud, thereby ensuring the immutability and integrity of the credentials. By employing DLT, decentralised ID frameworks inhibit unauthorised credential modification and provide a transparent audit trail for issuing and verifying credentials, nurturing a trustworthy digital ID ecosystem.

Decentralised identifiers: reframing the concept of ID

Decentralised identifiers, acknowledged by the World Wide Web Consortium (W3C) as a critical standard, represent another fundamental component within a robust SSI model.[69] These identifiers empower individuals to establish a verifiable, independent digital ID, departing from traditional, centralised, and domain-specific identification methods. This shift holds the potential to revolutionise digital ID management.[70]

By utilising cryptographic technology, decentralised identifiers offer a persistent, portable, and universally verifiable ID that functions across multiple platforms and services. This approach replaces traditional authentication methods, streamlining access, enhancing privacy, and significantly reducing the risk of data breaches, thereby bolstering the security and integrity of online interactions.[71] While acknowledging the benefits of cryptographic technology, the key considerations regarding the implementation of decentralised identifiers will be further explored in subsequent sections of this paper.

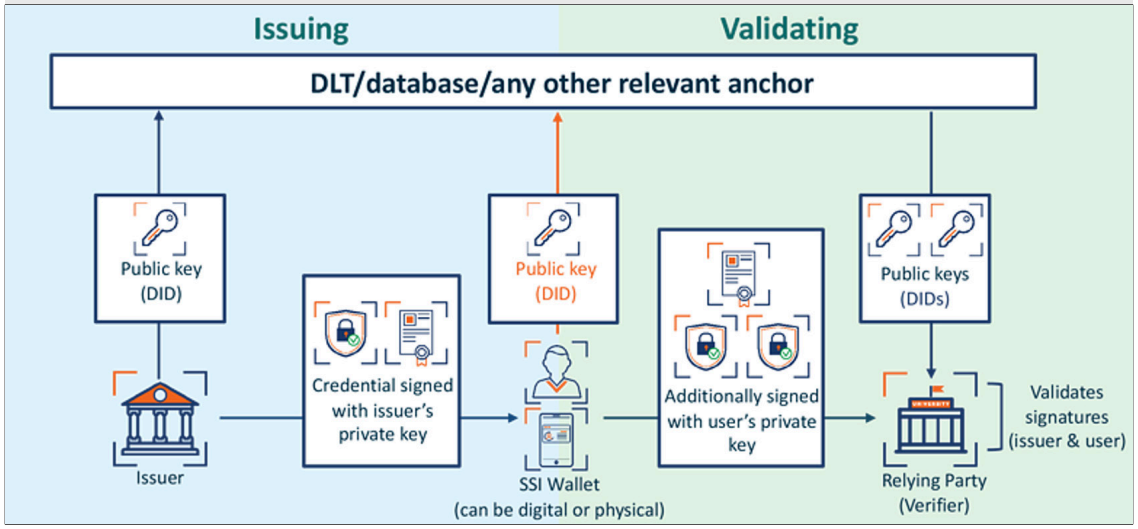
The introduction of decentralised IDs offers extensive benefits across various stakeholders:

- **For organisations**, it streamlines the secure verification of credentials, making customer onboarding more efficient and cost-effective while reducing the administrative burden.
- **For individuals**, it delivers unprecedented control over personal data, safeguarding privacy and preventing unauthorised tracking and data access.
- **For developers**, it encourages the creation of architect systems that place user privacy at the forefront, moving beyond the conventional password-centric security models.

During the issuance and validation of these decentralised identifiers, an issuer, such as a government, educational institution or private institution, generates a credential linked to the user's public key (Decentralised ID), which is then stored in the user's digital or physical SSI wallet. When validation is required, the user presents their credential, signed with their private key, to a verifier who, in turn, checks the public key against a decentralised ledger or database to confirm the authenticity of the signatures (Figure 5).

67 World Wide Web Consortium. (2019, September 24). Verifiable Credentials Use Cases W3C Working Group Note. https://www.w3.org/TR/vc-use-cases/
68 Camilleri, A., Muramatsu, B., & Schmidt, P. (2022). Credentials to Employment: The Last Mile. Digital Credentials Consortium Report.
69 World Wide Web Consortium. (2022, July 19). Decentralized identifiers (DIDs) v1.0. W3C Recommendation. https://www.w3.org/TR/did-core/
70 Truvity. (n.d.). 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 Nasdaq. (2023, September 12).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.

Figure 5: Identifiers and their application in DLT [72]



Source: Oliver Wyman, International Banking Federation

Unlike centralised identifiers or other self-asserted types of identities, which rely on social network providers, decentralised identifiers are created and controlled by the user, rendering them naturally resistant to tracking and profiling. These identifiers facilitate secure and confidential peer-to-peer interactions, laying the groundwork for a digital ID ecosystem founded on trust, privacy, and user empowerment.

The adaptability of decentralised identifiers extends far beyond mere identification. They can be used to secure transactions, encrypt communications, and facilitate consent-based data sharing, thereby contributing to a more reliable digital economy. As the potential of decentralised identifiers becomes increasingly apparent across industries, the digital ID landscape is expected to evolve from a functional component to a crucial aspect of digital rights and autonomy.

The International Air Transport Association's (IATA) One ID project serves as a tangible example of how decentralised identifiers are practically implemented in air travel, demonstrating significant enhancements in efficiency and security.[73] This initiative provides passengers with a streamlined, contactless experience while reinforcing data privacy by selecting essential information with user consent. Such applications of decentralised identifier frameworks highlight the transformative potential in redefining interactions across diverse sectors, indicating a shift towards a more privacy-conscious, user-governed online environment.

Drawing from our literature review and discussion with industry practitioners, we have gleaned insights from cases involving the adoption and implementation of digital ID in diverse global markets. Key considerations such as the driving forces behind the global evolution of digital ID, along with case studies highlighting the development and adoption of digital ID solutions in selected markets are detailed in Annex 2.

72 Oliver Wyman & International Banking Federation. (2021, December). 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
73 IATA. (n.d.). One ID. https://www.iata.org/en/programs/passenger/one-id/

4. Risks and challenges in digital ID adoption

Digital IDs hold transformative potential for the financial services industry, promising to enhance security, streamline operations, and improve customer relations significantly. However, unlocking this potential requires navigating intricate regulatory landscapes and addressing sophisticated technical challenges effectively. Successful integration of digital ID demands a strategic, collaborative effort involving key stakeholders such as financial institutions, regulators, technology providers, and consumers.

4.1 Key considerations for implementing digital ID solutions

The deployment of digital ID systems by financial institutions involves navigating a complex mix of institutional and regulatory challenges. This complexity is particularly notable in centralised or semi-centralised systems, which must comply with international laws and a coordinated global framework. The interplay between regulation, standardisation, and cybersecurity is critical, as they collectively influence the security, effectiveness, and reliability of digital ID solutions. Financial institutions must understand these dynamics to balance innovation and risk management when implementing digital ID systems.

Regulatory complexities

Navigating the regulatory landscape for digital IDs is critical for financial institutions. Compliance with existing laws is a baseline requirement, while proactive engagement with evolving regulations ensures future viability. Institutions must strive for adaptable compliance frameworks to meet both present and future regulatory demands, thus maintaining operational integrity and customer confidence. The complexity is compounded when considering international regulations such as the GDPR, which set high standards for data protection. The global nature of finance necessitates a thoughtful approach to align various regional laws, mitigating the risk of compliance discrepancies. Achieving regulatory harmonisation on a global scale requires a strategic yet adaptable policy.

Enhanced interoperability and standardisation

Interoperability, as defined by the World Bank's ID4D Initiative, is crucial for the communication between different digital ID systems. It requires synchronisation across ID platforms and coordination with domestic and international standards.[74]

In the financial sector, the call for global standards and effortless interoperability is particularly crucial in the context of digital IDs. These standards are foundational, facilitating smooth cross-border transactions and effective operation of international banking. Currently, financial institutions face significant challenges due to incompatible systems, leading to operational delays and a diminished customer experience. Interoperability is thus not merely a convenience but a strategic imperative for organisations aiming to expand their market reach, integrate diverse financial systems, and establish a competitive global stance.

The digital era demands interoperability that transcends sectors, industries, and borders. Financial institutions must strive to integrate various systems and processes seamlessly. This requires harmonising technical protocols, data formats, and security frameworks. Disparities in authentication methods, such as two-factor or advanced biometric verifications, can potentially disrupt user experiences and amplify security concerns.[75]

Furthermore, local regulations and privacy laws vary across jurisdictions, complicating the operational landscape for financial entities and potentially resulting in inconsistent experiences and heightened security threats. Passive support for interoperability within the industry is inadequate. The financial services industry must actively engage in the development of cross-industry standards to enhance operational efficiency and strengthen security and privacy protections. By adopting a proactive approach, financial institutions can contribute to forging a more collaborative and secure global marketplace. This commitment is necessary to meet the demands of an interconnected global economy and to ensure smooth, secure user interactions in the financial sector.[76]

74 The World Bank Group's Identification for Development (ID4D). (n.d.). Interoperability. https://id4d.worldbank.org/guide/interoperability
75 Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118.
76 ENISA. (2023, July 3). Digital ID Standards. https://www.enisa.europa.eu/publications/digital-ID-standards

Cybersecurity and data protection

The adoption of digital ID management has placed cybersecurity at the forefront of financial institutions' concerns. Data breaches pose a significant financial risk and can inflict lasting damage to reputations. Therefore, a comprehensive security strategy is critical, encompassing state-of-the-art encryption, continuous monitoring, advanced threat detection, and robust incident response frameworks to guard against evolving cyber threats.

The efficacy of cybersecurity measures does not rely solely on technology; it also hinges on human vigilance and procedural rigour. Financial organisations must cultivate a culture of cybersecurity awareness and implement stringent access controls and ongoing security audits to protect digital IDs.

Data protection must be an integral part of digital ID systems. The "privacy by design" approach ensures privacy considerations at every development stage, which is vital in deterring cyberattacks. This approach could help combat sophisticated cyberattacks targeting system vulnerabilities and human factors alike. As cloud-based solutions gain prevalent, innovative techniques like Data Colouring, employing Public Key Infrastructure (PKI), digital fingerprints, and watermarking provide additional layers of security. These methods are essential for protecting ID data from inception through storage processing.

In conclusion, securing digital ID systems requires an integrated approach that combines cutting-edge technology, continuous education, and strict procedures. A proactive defence strategy is essential for maintaining a secure and trustworthy digital ID landscape in the financial services industry.

Quantum threats and challenges

The rise of quantum computing presents a formidable challenge to current cryptographic systems that safeguard identity solutions, which are crucial for securing financial, governmental, and personal data.[77] Quantum computing has evolved from being a theoretical concept to a practical reality, capable of compromising traditional encryption protocols such as the Rivest-Shamir-Adleman (RSA) and Elliptic-curve cryptography (ECC) through algorithms like Shor's algorithm.[78] This poses a significant risk to sectors like finance, where robust data protection is paramount.

Given this scenario, the urgency of transitioning to Quantum-Resistant Cryptography (QRC) cannot be overstated. As quantum computing advances, the vulnerability of existing cryptographic systems grows, necessitating an immediate shift towards quantum-resistant algorithms. This transition involves complex updates to infrastructure, the adoption of new cryptographic standards, and extensive system testing to ensure resilience against quantum attacks while maintaining compatibility with existing systems.

Globally, proactive steps are underway. For instance, the United States has issued National Security Memorandum 10,[79] mandating government agencies to adopt quantum-resistant cryptography. This highlights the need for a coordinated global approach to effectively mitigate the quantum threat. The financial sector, in collaboration with governmental bodies, should prioritise the development and implementation of secure technologies capable of withstanding potential quantum disruptions. This is crucial to maintaining the confidentiality and integrity of digital IDs in a post-quantum world.

Currently, the integration of biometric technologies into identity frameworks offers an additional layer of quantum-resistant security. Unique identifiers such as fingerprints and iris scans, which are difficult to replicate or decode even with advanced quantum computing, could enhance data security and verifiability. This integration strengthens digital ecosystems against potential vulnerabilities and boosts user trust and reliability in digital interactions.

Scalability and technological adoption

Digital ID systems must be scalable to accommodate increasing users and transaction volumes without compromising performance or security. Achieving this requires investment in robust cloud infrastructure, modular design, and technologies like AI for efficient scalability. Ensuring that digital ID systems are accessible

77 EY. (Aug 2023). 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-defenc

78 Arel, R. (2023, May 12). Explore the impact of quantum computing on cryptography. TechTarget. https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography

79 The White House. (2022, May 4). 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/

to all, including those who are unbanked or from underprivileged backgrounds, is equally important. Bridging the digital divide requires technology solutions that cater to a diverse spectrum of society alongside initiatives aimed at enhancing digital literacy. Financial institutions bear the responsibility to offer inclusive services and to support the education of all users in the digital ecosystem.

Legal and ethical complexities

Financial institutions navigate a sophisticated matrix of legal and ethical considerations, particularly given their global operations. They are subject to numerous legal requirements concerning cross-border data flow and sovereignty while upholding ethical principles to ensure equitable digital ID access for financial services and ethical use of data through explicit consent.

The drive for innovation and service excellence must be balanced with ethical discernment. The effective deployment of digital IDs hinges on a thoughtful approach to these significant challenges.

Ultimately, the strategic direction for financial institutions involves orchestrating a coordinated approach to establish a harmonious regulatory landscape, advocating for the creation of comprehensive global interoperability standards, prioritising cybersecurity, ensuring technological solutions' scalability, and rigorously complying with established legal and ethical standards. Such a strategy will serve as the cornerstone for digital IDs to emerge as a catalyst in reshaping the financial sector.

Data exploitation

Data exploitation has emerged as a subtle yet pernicious threat, undermining user privacy and eroding trust. This phenomenon involves the unauthorised and unethical collection and use of digital ID information. Ranging from the covert sharing of sensitive data to the unauthorised commercial exploitation of personal identities, data exploitation has far-reaching consequences. Beyond individual privacy violations, it creates systemic vulnerabilities capable of compromising entire financial systems.

As financial institutions increasingly integrate digital IDs into their operations, the risk of data exploitation intensifies, demanding vigilant oversight and rigorous controls to prevent unlawful data usage. According to the World Economic Forum, it states that certain forms of digital ID are potential gateways to data exploitation. Confronting the risks associated with data exploitation requires both regulatory mandates and technical fortification. Governments and financial institutions must collaborate to secure and ethically manage these digital IDs. An integrated approach, combining advanced cybersecurity measures with robust privacy policies and transparent practices, is crucial. Such alignment is essential for mitigating the risks of data exploitation and nurturing lasting trust among consumers and stakeholders.

Financial institutions must champion privacy-by-design principles, proactively anticipating and preventing security breaches. This commitment involves deploying sophisticated encryption technologies, enforcing strict access controls, and instilling a culture of cybersecurity awareness across the organisation. Moreover, upholding the principle of informed consent is important, ensuring individuals maintain control over their data and its utilisation.

4.2 Navigating the complex landscape of decentralised ID: potential and challenges

As previously outlined, decentralised ID systems represent a groundbreaking approach to online personal identity management. Understanding the intricacies of decentralised ID systems requires a focus on the technical foundations of this innovative approach. This exploration delves into the role of DLT, specific protocols for interoperability within decentralised networks, and the inherent user experience challenges associated with adopting this new technological framework.

Interoperability

Achieving interoperability is a central challenge in the development of decentralised ID systems akin to other types of digital IDs. Unlike traditional digital ID, decentralised ID must seamlessly integrate across a myriad of platforms and services, which is crucial for creating a consistent user experience. However, the current landscape is fragmented, characterised by various proprietary systems and standards that prevent the fluid exchange of ID credentials across ecosystems. Overcoming these barriers necessitates the adoption of

common protocols and standards forged through industry-wide collaboration. This cooperative approach is particularly vital in decentralised systems, where the disparate architectures of DLT-based platforms can pose additional integration interoperability, facilitating collaboration among diverse DLT-based networks. By enabling seamless interaction, these standards enhance user experiences and broaden the reach of decentralised ID solutions.[80]

User acceptance and decentralised IDs

Securing widespread adoption of decentralised ID systems hinges on cultivating user acceptance. This requires establishing trust in a system that appears complex and unfamiliar to the users. Decentralised systems promise enhanced security, privacy, and user control – benefits that must be effectively communicated. Central to this effort is simplifying the user interface to facilitate a smooth transition from traditional to decentralised systems. Moreover, public education about the operation and benefits of decentralised identities is essential. This includes transparently discussing data handling and protective measures while showcasing the practical advantages of decentralised systems, such as faster and more secure transactions.

Scalability and technical limitations

Scalability remains a multifaceted challenge within decentralised ID systems, as they must accommodate an expanding user base and transaction volume while maintaining efficiency and affordability. DLT-based platforms, commonly utilised as the foundation for these systems, often encounter scalability issues such as slow transaction speed and rising costs. Addressing these challenges requires continuous technological innovation. This includes the development of second-layer solutions, improved consensus mechanisms, and the adoption of more sustainable technologies — all vital for garnering public acceptance and facilitating the practical application of decentralised IDs in everyday transactions. FSDC published a report in March 2024 on blockchain/ DLT adoption in the financial services industry.[81] The report offers an analysis of the risks and challenges associated with the technology and provides recommendations for its broader adoption.

Legal, privacy, security, and governance concerns

Decentralised ID systems present a paradigm shift in personal data control, challenging traditional regulatory compliance frameworks such as the GDPR. Managing data ownership, consent, and erasure in a distributed landscape necessitates collaborative efforts to establish new regulatory frameworks that align with the decentralised model, ensuring international regulatory coherence for systems operability.

Privacy and security features in decentralised ID systems rely on robust technology and secure components, such as smart contracts. To uphold system integrity, regular security audits and proactive vulnerability management are essential.[82] Moreover, the potential exposure of personal data on public ledgers mandates the integration of privacy-preserving technologies, like zero-knowledge proofs, while carefully considering their legal implications.

Furthermore, effective key management is crucial for the security of decentralised ID systems. Regularly updating cryptographic keys through key rotation is pivotal to preventing unauthorised access and mitigating impact of key compromises.[83] Managing key rotation in decentralised settings presents significant challenges, necessitating secure mechanisms to update, revoke, and accurately propagate these changes across the network.[84] Failure to effectively manage this process can leave the system vulnerable, potentially exploiting outdated or compromised keys and compromising overall security.

Governance within decentralised systems demands a shift from centralised authority to distributed models that oversee updates, dispute resolution, and regulatory compliance.[85] These models must balance participant autonomy and collective governance to ensure equitable decision-making across diverse legal and regulatory landscapes. Moreover, effective governance must foster consistent compliance and impartial conflict resolution across different jurisdictions.

80 EU Blockchain Observatory and Forum. (2023, November 29). 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 FSDC. (2024, March). Realising the Potential of Blockchain in Advancing Hong kong's Financial Services Industry. https://www.fsdc.org.hk/media/t3tojry2/blockchain-report_en_final.pdf

82 Dock. (2024, January 11). Decentralised ID: The Ultimate Guide 2024. https://www.dock.io/post/decentralised-ID

83 Smith, S. M. (n.d.). Key Management for Self-Sovereign Identity. https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/10-ssi-key-management.pdf

84 Smith, S. M. (n.d.). Key Management for Self-Sovereign Identity. https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/10-ssi-key-management.pdf

85 Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. Information Polity, 24(4), 397-417.

Developing governance frameworks that respect cultural, legal, and ethical differences is crucial for achieving widespread acceptance. These frameworks must clarify stakeholder rights and responsibilities, nurturing trust and collaboration essential for the success of decentralised ID systems. While some countries have made progress in establishing such frameworks, a globally comprehensive legal and governance approach tailored specifically for decentralised IDs is still in its nascent stages. The launch of Mainland China's RealDID initiative represents a step in this direction, with its broader implications to be discussed in the later section of the paper.

Policy recommendations

Policy recommendations

Digital ID has emerged as a foundational element in the realm of digital transformation, particularly within the financial services industry. It plays a crucial role in keeping pace with rapid digitisation and escalating customer expectations.

In Hong Kong, significant efforts have been made to enhance digital ID and data-sharing capabilities, supported by both the public and private sectors. The iAM Smart platform stands as a notable example, streamlining identity verification processes and enhancing the client onboarding experience since its launch in 2020. It provides a consolidated digital services hub that integrates functionalities such as authentication, form filling, personalised notifications, and digital signing, thus facilitating digital interactions among citizens, public services, and private enterprises.

On the corporate front, the introduction of the Commercial Data Interchange (CDI) in 2022 represents a major step forward in secure and streamlined data exchange. Acting as a conduit between data providers and financial institutions, the CDI enhances credit evaluation processes and fosters financial inclusion for SMEs. Additionally, the 2024-25 Budget announced the development of a platform for digital identity of enterprises, i.e a business version of iAM Smart,[86] which aims to launch in 2026 to incorporate 1.8 million local businesses into this enterprise platform.

Moreover, integrating the Legal Entity Identifier (LEI) within the financial ecosystem bolsters transparency and trust, particularly in cross-border transactions. The initiatives collectively are transforming Hong Kong's financial services landscape, promoting efficiency and innovation across banking, securities, insurance, and other sectors. Detaileds on these initiatives are listed in Annex 3.

Building upon these advancements, the Hong Kong SAR Government has further demonstrated its ongoing commitment through the efforts of the DEDC. Recent proposals from the committee aim to enhance the city's digital policy framework and infrastructure. These proposals include refining governance structures to improve policy formulation and implementation, establishing a unified corporate digital ID, and expanding the coverage of the CDI and the Consented Data Exchange Gateway to additional sectors.[87,88]

This solid foundation paves the way for developing an advanced digital ID ecosystem, crucial for supporting the rapid growth of digital ID solutions while addressing security, privacy, and regulatory compliance to maintain user trust.

The policy recommendations outlined in this section articulate a strategic approach to developing a robust digital ID ecosystem by leveraging Hong Kong's existing infrastructure while addressing existing gaps. The goal is to create a resilient and user-centric digital ID solution capable of integrating with global frameworks, thereby fostering economic growth, innovation, and public trust.

These recommendations aim to chart a course for a future where digital ID enables, rather than inhibits, growth and dynamism, especially for the financial services industry, in a digital world.

Recommendation 1: Public-private synergy – exploring full-fledged implementation of iAM Smart and enabling the development of private digital ID wallets

The quest for control over personal information has become a cornerstone of the modern digital economy. In a world where data breaches are commonplace, individuals are progressively seeking autonomy over their data to safeguard its security and privacy. A digital ID wallet emerges as a transformative solution, ushering in a new paradigm for the storage, management, and sharing of personal data. This user-centric approach prioritises consent in data exchange, a concept that has recently gained significant traction worldwide.

86 HKSAR Budget 2024. https://www.budget.gov.hk/2024/eng/pdf/e_budget_speech_2024-25.pdf

87 A "Consented Data Exchange Gateway" ("CDEG") is being developed to allow members of the public to choose to authorize relevant government departments to exchange their personal data through the system and data sharing, together with the use of a single digital identity for authentication in government and commercial online transactions. LegCo. (13 May 2024). Panel on Information Technology and Broadcasting – Background brief on Digital Corporate Identity platform. https://www.legco.gov.hk/yr2024/english/panels/itb/papers/itb20240513cb1-552-3-e.pdf

88 HKSAR Government Digital Economy Development Committee. (2024, February). Core recommendations of the Digital Economy Development Committee. Hong Kong SAR Government. https://www.itib.gov.hk/assets/files/DEDC_Core_Recommendations_Eng_issued.pdf

Full-fledged implementation of iAM Smart

In Hong Kong, the iAM Smart platform has been pivotal in advancing the city's digital ID landscape. Serving as a centralised platform, iAM Smart performs multiple roles akin to a digital ID wallet — issuing credentials, providing digital ID services, and acting as a trusted entity for verification and attribute provision. Its central role in identity verification, leveraging its access to the Government's data to serve as a trusted "golden source", has streamlined citizens' access to various public and private services, as outlined in the previous section.

However, to harness its full potential, iAM Smart must evolve alongside the evolving needs of users and service providers, striving for deeper integration with a broader ecosystem, especially within the financial services industry which demands enhanced interoperability. While the current iAM Smart system has already synchronised data across multiple government departments, broader synchronisation and integration with public service are crucial to its widespread adoption and utility. In line with this, the development of the Consented Data Exchange Gateway (CDEG) by the Office of the Government Chief Information Officer (OGCIO), scheduled for launch by the end of 2024, is timely. The CDEG aims to facilitate data sharing from government departments to financial institutions with client authorisation, bridging the gap between government-held data and financial entities and promoting a more integrated digital ecosystem.[89]

To optimise these capabilities, increased collaboration among government entities is necessary, especially as legal constraints currently limit the platform's capacity to incorporate certain types of data. For instance, tax information governed by the Inland Revenue Ordinance (IRO) cannot be shared. High-level governmental discussions and strategic direction could explore modifications to such regulations to enable a more comprehensive digital profile, fostering adoption by individuals and businesses alike.

The role of private digital ID wallets and their coexistence with the iAM Smart

Moreover, cultivating a robust digital ID ecosystem extends beyond government collaboration. It necessitates a synergistic partnership between public authorities and the private sector. The interconnected infrastructure of iAM Smart exemplifies the notion of a digital wallet for an individual's ID, providing a digital ID authentication function for online services of government, public and private organisations. However, the burgeoning digital economy demands counterparts in the private sector.

The private sector generates numerous digital IDs daily, warranting separate, specialised private digital ID wallet(s).[90] These wallets would benefit from the support of a network of certified legal service providers operating under a trust framework. This approach promotes user choice and nurtures the growth of private digital ID wallets within the ecosystem.

In this context, iAM Smart also serves as the "golden source" for ID verification among private digital ID solutions. With user consent, data owners can potentially act on prompt actions through iAM Smart, confirming necessary information and/ or status without disclosing any additional personal data. This arrangement would encourage a swift, market-driven response and innovation, enabling private digital ID wallets to operate beyond government boundaries. Consequently, this fosters economic expansion and potentially extends services to international users.

The coexistence of government and private digital ID wallets has the potential to cultivate a symbiotic ecosystem, driving progressive development and innovation. iAM Smart's existing sandbox programme invites the private sector to develop services compatible with the platform, utilising its data and ID credentials for various functions such as ID verification and remote account opening. While the foundational concept is in place, a more detailed roadmap or explanatory framework is necessary to stimulate dynamic evolution in this sector.

In conclusion, the future of digital ID in Hong Kong hinges on a delicate balance between ensuring user autonomy and catalysing technological innovation. As iAM Smart continues to adapt, its integration with both the government and private digital wallets could herald a new era of secure, efficient, and user-centric identity management, positioning Hong Kong at the forefront of the global digital economy.

89 HKSAR Legislative Council. (2024, January 5). Policy Statement on Facilitating Data Flow and Safeguarding Data Security in Hong Kong. LC Paper No. CB(1)1198/2023(01). https://www.legco.gov.hk/yr2023/english/panels/itb/papers/itb20231212cb1-1198-1-e.pdf

90 Open Identity Exchange. (2023, October). Governments and Digital Wallet. https://openidentityexchange.org/user_assets/706.pdf

Recommendation 2: Establishing a trust framework for the digital ID ecosystem

As the digital landscape expands, the need for robust identity verification and secure online interactions becomes increasingly pronounced. In this context, a trust framework is essential to ensure the digital economy's integrity, promising a more cohesive digital environment where users can transact with confidence and organisations can innovate without compromising security and privacy. Hong Kong could draw valuable insights from similar structures proposed by countries like Australia, Canada, Sweden and the UK. [91,92,93,94]

Challenges arise when organisations operate in silos, lacking common ground in the creation and management of digital IDs. This fragmentation makes building trust difficult. In response, aligning with the digital ID trust framework represents an organisation's commitment to upholding stringent data protection and privacy standards. By providing a common direction and shared understanding, which includes legislation, standards, and good practice guides, the framework establishes a uniform approach to inclusivity, privacy, data protection, fraud management, and security. This uniformity facilitates a consistent description of digital IDs and attributes, fostering a network where information sharing is both simplified and secure.

To enhance accessibility and understanding, the framework should include detailed use cases that illustrate its practical applications across various sectors, demonstrating how it bolsters security, privacy, and user experience. This framework can build upon existing security procedures required for online service providers who adopt iAM Smart, further enhancing these standards. [95]

All related documents could be consolidated and presented on a repository site, including the Government's vision, roadmap, and related initiatives. This offers a transparent view of the strategic direction and ongoing efforts in the digital ID space. Regular industry consultations are recommended to develop a comprehensive digitalisation strategy and roadmap, as highlighted in a report published in March 2024 by the FSDC on the potential of blockchain technology in advancing Hong Kong's financial services industry.[96] Moreover, a dedicated task force could be established within this framework to monitor the evolution of global cryptographic standards, ensuring Hong Kong remains resilient against emerging threats, including those posed by quantum computing.

As the ecosystem continues to evolve, a certification scheme for digital ID solution providers can be introduced to further enhance the framework's robustness. This certification ensures the accuracy and reliability of shared information, with certified organisations being displayed on the framework site for reference. Compliance with these outcome-based rules guarantees the attainment of specific goals without mandating the use of particular technologies or processes. This approach champions innovation, granting service providers the flexibility to develop and customise their products to best serve their users while maintaining interoperability and adhering to open technical standards.

91 Australian Government's Digital ID system. (n.d.). Trusted Digital Identity Framework. https://www.digitalidentity.gov.au/tdif
92 Digital ID & Authentication Council of Canada. (n.d.). Trust Framework. https://diacc.ca/trust-framework/
93 Sweden Connect. (2022, October 5.). Swedish eID Framework - Introduction. https://docs.swedenconnect.se/technical-framework/latest/00_-_Swedish_eID_Framework_-_Introduction.html
94 UK Government. (2023, July 20). Policy paper - UK digital identity and attributes trust framework beta version (0.3). https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#what-the-uk-digital-identity-and-attributes-trust-framework-does
95 OGCIO. (2019, May 10). Hong Kong Legislative Council Panel on Information Technology and Broadcasting - Electronic Identity. https://www.ogcio.gov.hk/en/news/legco_papers/2019/05/doc/lb_20190510.pdf
96 FSDC. (2024, March). Realising the Potential of Blockchain in Advancing Hong kong's Financial Services Industry. https://www.fsdc.org.hk/media/t3tojry2/blockchain-report_en_final.pdf

Recommendation 3: Facilitating interoperability through a dual approach: infrastructure and legal frameworks

The seamless utilisation of digital IDs and the exchange of associated information across companies, sectors, and industries - including interactions between government and private sector digital ID wallets - are critically important. Ultimately, the vision extends beyond national borders, aiming for digital ID solutions that effortlessly traverse international lines.

A robust and universally recognised digital ID hinges on the dual pillars of interoperable infrastructure and a robust legal framework. Simultaneously addressing both is crucial for the solution's success. Interoperability must be built into the architecture of digital ID systems, enabling seamless connections and communications across diverse platforms and networks. This common ground in technical specifications is the key to reducing friction for both users and service providers. Among many approaches, integrating iAM Smart with CDEG and CDI could advance the creation of an interoperable digital ID ecosystem that facilitates data exchange and operational efficiency. Furthermore, being a government-led/ participated infrastructure, it is expected to enhance industry adoption of digital ID solutions due to its reliability and ease of access. This approach is in line with insights from the FSDC's blockchain report as well,[97] which advocates for a government-participated blockchain as a utility service in Hong Kong to promote the widespread adoption of blockchain technology across the financial services industry.

Apart from infrastructure, organisations and industries must rally around common standards and protocols. To effectively deploy digital ID in financial services, enhancing interoperability standards is imperative. A collaborative approach involving key regulatory bodies and engaging the private sector is critical. This strategy facilitates smoother integration and broader adoption, particularly across international boundaries, and also aligns with both regulatory requirements and practical industry needs. Such alignment is fundamental to supporting global financial operations and driving improved outcomes.

The guidance note on Digital Identity issued in April 2021 highlights the importance of managing digital IDs with care.[98] To complement this, balanced and trusted legal guidelines or frameworks are essential. Incorporating specific standards or an accreditation scheme into existing frameworks, such as the Personal Data (Privacy) Ordinance, would provide the necessary governance to ensure that digital IDs are managed securely, privately, and in compliance with legal requirements. This integration may facilitate the development of other digital ID service providers. The legal framework serves as the assurance that users and businesses need when their digital identities traverse the complex web of the digital realm. It acts as the backbone of trust that supports the technical infrastructure, ensuring a cohesive and secure digital identity ecosystem.

Integrating digital ID solutions within the financial services industry must prioritise interoperability while safeguarding sensitive data and adhering to strict verification and regulatory requirements. The sector's inherent complexities, marked by fraud risks and bound by rigorous AML and KYC regulations, warrant the development of a specialised standards framework. This framework would provide precise guidance to financial institutions, facilitating compliance and risk mitigation.

The regulatory sandbox, launched by Cyberport and the OGCIO on the iAM Smart platform, is crucial in bridging regulatory compliance and innovation. This platform enables the testing of fintech solutions, including digital ID-related fintech solutions, in a controlled environment, fostering innovation. To fully realise its potential, an increase in investment and an expansion in the capabilities of the sandbox are imperative. Additionally, to enhance the programme's effectiveness, it is crucial to ensure that the dedicated team under OGCIO will have adequate resources by drawing expertise from relevant departments. The team plays a pivotal role in managing the sandbox's operations and facilitating coordinated efforts with various regulatory bodies. This specialised team would provide the necessary coordination and support, allowing innovators to fully leverage the iAM Smart infrastructure to develop solutions that meet the unique demands of the financial sector. Such precise and strategic support is crucial for the sector to flourish in the digital era.

97 FSDC. (2024, March). Realising the Potential of Blockchain in Advancing Hong kong's Financial Services Industry. https://www.fsdc.org.hk/media/t3tojry2/blockchain-report_en_final.pdf

98 Hong Kong Computer Emergency Response Team Coordination Centre. (2021, April). Protect your digital identity. https://www.cybersecurity.hk/images/resources/digitalidentity_en.pdf

Recommendation 4: Harmonising digital ID standards for seamless cross-boundary/border interactions

Hong Kong is advancing its global economic presence by creating a digital ID infrastructure aimed at facilitating local transactions and potentially enabling seamless interactions across the Greater Bay Area (GBA). Central to this initiative is incorporating the "Standard Contract for GBA Data Transfers", a robust framework ensuring the standardised and secure transfer of personal data across borders. This framework is pivotal not only for reinforcing the functionality of digital IDs but also for instilling trust in international transactions and data exchanges.[99]

Additionally, iAM Smart has been recognised as a trusted source of identity by the Unified Identity Authentication Platform of Guangdong Province, which enables Hong Kong citizens to log in directly to the Guangdong Provincial Administrative Service website and the "Yue Sheng Shi" mobile app through iAM Smart to access a wide range of Guangdong's public services in a more efficient manner.[100]

The principle of compatibility, or interoperability, ensures that digital IDs issued in Hong Kong gain widespread recognition and acceptance across various services, industries and locations. It also opens the door for these digital IDs to be recognised within the GBA, fostering secure, efficient transactions and data exchanges. The potential extension of this interoperability sets the stage for Hong Kong digital IDs to gain global recognition, paving the way for international commerce and establishing a benchmark for global digital ID protocols.

The ripple effects of interoperability and standard data contracts are profound. They streamline international transactions, reinforcing trade and industry, and have the potential to establish a new benchmark for global digital ID protocols. Achieving this vision requires harmonising digital ID standards and data transfer agreements with global best practices, in collaboration with overseers from GBA and international regulatory entities, such as the Digital Bay Area initiative, as highlighted by the Hong Kong SAR Government.[101]

Hong Kong should enhance its legal frameworks to bolster support for digital IDs, ensuring privacy and secure data exchanges through public consultations and the establishment of clear, comprehensive guidelines. This involves implementing advanced tech infrastructure fortified with solid security measures to combat cyber threats, especially those involving cross-border activities. Forming strategic partnerships with tech leaders and international bodies will expand the reach and credibility of the digital ID initiative. Engaging public and private sector stakeholders is crucial for the practical application and widespread adoption of digital IDs.

Hong Kong's pursuit of a globally recognised digital identity system underscores its dedication to innovation and international cooperation. By fostering mutual recognition of digital identities, Hong Kong citizens could use their digital IDs worldwide, while businesses could accept digital IDs from other jurisdictions, thereby reinforcing the city's pivotal role in the digital economy.

99 Office of the Government Chief Information Officer. (2023). Facilitating cross-boundary data flow within the Greater Bay Area. Government of the Hong Kong Special Administrative Region. https://www.ogcio.gov.hk/en/our_work/business/cross-boundary_data_flow/

100 iAM Smart. (n.d.). Cross-boundary public services. https://www.iamsmart.gov.hk/cbps/en/

101 HKSAR. (2023, October 25). The Chief Executive's 2023 Policy Address. https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

Recommendation 5: Capacity building: fostering societal empowerment through trusted digital ID adoption and educational engagement

Providing incentives and implementing a phased strategy for rollout

The successful deployment of digital ID platforms like iAM Smart relies on public trust and understanding. Education and trust-building initiatives are of paramount importance, especially in privacy-sensitive sectors such as financial services. Clearly communicating the benefits and safeguards of digital IDs can foster a conducive environment for their widespread acceptance.

A thoughtfully designed policy framework is essential for encouraging the uptake of digital ID solutions. Furthermore, providing financial and technical incentives can alleviate the costs for businesses to integrate digital IDs. Additionally, to visualise the widespread access to the centralised system for digital ID by institutions, we should reference the successful implementation of the Faster Payment System across banks, payments, and wallet operators in Hong Kong. Cultivating a supportive environment for startups can also lead to a surge in innovative approaches to digital ID. Public-private partnerships are instrumental in this regard, creating digital ID solutions that are both user-friendly and economically viable, bridging the gap between public needs and market opportunities.

The key to individual adoption lies in making the digital ID process straightforward, inclusive, and secure. Robust protection of personal data and transparency in data management builds trust. Simplifying the acquisition and use of digital IDs encourages widespread use across various demographics. Introducing an opt-in/opt-out mechanism can empower residents to choose whether to use iAM Smart as their digital ID based on their needs and comfort levels.

A phased implementation approach can ensure a smooth transition. Starting with non-critical government services allows individuals to gradually acclimate to the digital ID ecosystem. The scope could extend to more essential services as the community becomes more comfortable with the technology. It is crucial to ensure that alternative access to services remains available, safeguarding against digital exclusion during this transition.

The establishment of iAM Smart exemplifies a phased and strategic approach to deploying digital ID solutions. As of May 2024, over 2.7 million registrants and more than 370 online services from government, public, and private organisations are already available on iAM Smart.[102] This phased rollout has ensured the introduction of more essential services in a manageable manner, with the ultimate aim of providing a one-stop personalised digital services platform. By fully adopting iAM Smart, Hong Kong aspires to realise the vision of a "single portal for online government services" by 2025.[103]

As government services increasingly integrate iAM Smart and citizens become more proficient in its use, the private sector is likely to recognise its advantages. This recognition can inspire businesses to develop compatible platforms, creating a synergistic ecosystem where Government initiatives and private sector innovation mutually reinforce adoption. The result is a cohesive, ever-expanding network of digital ID usage, setting the stage for continued growth and innovation.

Launching public awareness campaigns and education initiatives

The successful implementation and widespread adoption of digital ID systems, such as iAM Smart, hinge significantly on public trust and awareness. Recognising this, there is a pressing need for robust public awareness campaigns and educational initiatives aimed at clarifying the advantages and mechanics of digital IDs, addressing misconceptions, and showcasing their real-world utility, especially within the financial services industry.

102 Office of the Government Chief Information Officer. (n.d.). iAM Smart - Home. https://www.iamsmart.gov.hk/en/
103 HKSAR. (2023, October 25). The Chief Executive's 2023 Policy Address. https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

The OGCIO has been proactive in organising engagement sessions across various industries. It is vital that this momentum continues, particularly within the financial sphere. Targeted educational campaigns are imperative in building confidence and driving the adoption of iAM Smart. The transition to digital ID promises to transform the landscape of financial services, offering unprecedented levels of efficiency, security, and user convenience. Yet, harvesting these benefits is incumbent upon the industry's comprehensive understanding and adept application of these technologies.

To achieve this objective, the proposed strategy advocates for multifaceted educational campaigns tailored to meet the distinct requirements and apprehensions of the business and financial communities. These campaigns should concentrate on unravelling the operational benefits and the competitive edge offered by iAM Smart and the potential private digital ID wallet. Interactive learning modules, such as workshops and seminars, are envisioned to impart a profound comprehension of how digital ID can be integrated seamlessly into their existing infrastructure. This includes improving customer service, reducing fraud, and smoothing out regulatory compliance.

These initiatives must be inclusive, targeting all levels of financial operations to cultivate a culture of digital literacy. Tailored training modules will equip staff to assist clients in adopting iAM Smart, elevating the customer experience and reinforcing trust in digital ID systems.

Additionally, the scope of these educational campaigns could extend beyond financial institutions to engage the broader business ecosystem. By demonstrating the versatile applications of iAM Smart and potential private digital ID wallet across various financial transactions, from loan facilitation to asset management, these campaigns will illuminate the tangible value and strategic advantage inherent in digital ID adoption. It is essential to articulate how digital ID can catalyse innovative business paradigms and new revenue channels, nurturing a culture of progress and ingenuity within financial services.

Navigating through collaboration: engaging industry perspectives for unified progress

A concerted multilateral approach is crucial to effectively coordinate the efforts of all stakeholders. As outlined in the 2023 Policy Address, the Government has planned to establish a Digital Policy Office tasked with supervising digital government strategies, data governance, and information technology.[104]

Given the critical importance of digital ID for both businesses and individuals, proposing the establishment of a specific Digital ID Task Force, or a steering group, with a focus on the financial sector within this new office is a strategic move. Comprising representatives from financial institutions and fintech companies, this task force would serve as a bridge between diverse sectors. Its primary objective would be to craft a detailed strategy delineating the roles and responsibilities of each entity within the financial services industry. In addition, it would guide the industry's development, ensuring that initiatives align with broader strategic objectives.

The task force's mandate includes establishing a platform for continuous dialogue, idea exchange, and feedback to ensure that the digital ID infrastructure meets the unique requirements of the financial sector.

To facilitate open communication and the sharing of best practices and sector-specific insights, it is imperative to convene regular stakeholder meetings and workshops is imperative. These interactions serve as opportunities for stakeholders to forge partnerships, synchronise efforts, and align activities with the overarching goals of the digital ID initiative. Such collaborative endeavours are essential as they ensure that progress towards a digital future is driven by collective effort and a shared vision.

104 HKSAR. (2023, October 25). The Chief Executive's 2023 Policy Address. https://www.policyaddress.gov.hk/2023/public/pdf/policy/policy-full_en.pdf

Conclusion

The evolution of digital ID is integral to the ongoing digital transformation within financial services and the broader economy. These systems redefine accessibility, security, and efficiency through the utilisation of advanced technologies such as biometrics and cryptography. As a result, digital ID has become indispensable for daily operations, safeguarding against cyber threats while facilitating swift, seamless transactions. Its crucial role in maintaining consumer trust and securing a competitive edge in the global market cannot be overstated.

Hong Kong has laid a strong foundation for a vibrant digital ID ecosystem through the strategic implementation of initiatives like iAM Smart and related measures. By further integrating diverse private ID solutions within a mutually agreed-upon trust framework, Hong Kong can accelerate the development and adoption of digital IDs, positioning itself as a frontrunner in digital innovation and financial governance on a global scale. This inclusive framework empowers stakeholders to enhance operational capabilities, align technological solutions with strategic goals, and foster cross-sector collaboration. Moreover, it provides access to essential resources and aids in navigating regulatory complexities, ultimately driving significant outcomes in digital transformation.

To fully leverage this potential, Hong Kong should continue refining and expanding its digital ID infrastructure. Prioritising interoperability, infrastructure enhancement, and standard harmonisation will strengthen the digital ecosystem, ensuring it remains responsive to the evolving needs of the financial sector and catalysing broader economic benefits, including the emergence of innovative business models and the acceleration of digital transformation across industries.

By establishing a well-developed and effectively deployed digital ID ecosystem, Hong Kong not only solidifies its position as a leader in digital innovation but also boosts its capacity for international collaboration and connectivity. By exemplifying effective international cooperation in financial governance, Hong Kong cements its status as a global financial hub and sustains its competitive advantage in the international market. Embracing the transformative potential of digital ID systems is, therefore, crucial to the city's continued success as an international financial centre and technological innovation hub in the rapidly evolving digital era.

Annex

Annex 1: Stakeholders' role in each digital ID model

Centralised model: In a government-centric centralised system, the government is the primary stakeholder, acting as the custodian of the "golden source" repository. It holds the responsibility for creating, updating, and maintaining this authoritative database in compliance with national regulations and standards such as AML and KYC. The government's pivotal role lies in establishing a trusted and reliable golden source that financial institutions and other stakeholders rely upon for accurate verification and ID management.

Semi-centralised model:[105] The federated or semi-centralised model introduces a more diverse stakeholder ecosystem. While a central authority or consortium might maintain the overarching standards and protocols for the golden source, various accredited institutions—such as banks, credit agencies, and service providers—also function as custodians, issuing and managing digital identities within their domains. These stakeholders collaborate to ensure the golden source remains up-to-date and reliable, balancing distributed control with the need for standardisation and interoperability.[106]

Decentralised model: In the decentralised model, often supported by DLT, the responsibility for maintaining the golden source is distributed across a network of stakeholders. Instead of a single entity, multiple participants—including users, financial service providers, and technology experts—collectively validate and verify ID data, contributing to a decentralised ledger that serves as the golden source. This shared responsibility ensures the accuracy, security, and privacy of ID data, with each stakeholder having a vested interest in the integrity of the system.

Self-sovereign ID model: In the self-sovereign model, the individual user takes centre stage as the key stakeholder and the curator of their ID data, challenging the traditional concept of a centralised golden source. Users assert ownership and control over their personal information, with the option to selectively share portions of this data with trusted entities who may, in turn, contribute to a decentralised golden source. This model requires collaboration between users and service providers to strike a balance of ease of use with the security and verifiability of ID data.

In each model, the golden source stands as a critical asset requiring careful management and protection. The stakeholders involved—from governments to individuals—must navigate the complex interplay between security, privacy, compliance, and user convenience to ensure that the golden source serves its intended purpose as a bedrock for trustworthy digital ID verifications.

105 Centre for European Policy Studies. (2020). Europe's Digital ID Opportunity. https://theblockchaintest.com/uploads/resources/CEPS%20-%20Europes%20Digital%20ID%20Opportunity%20-%202020.pdf

106 Landau, S., Le Van Gong, H., & Wilton, R. (2009). 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.

Annex 2: Global case studies on the adoption and implementation of digital ID

1. Driving forces of global digital ID evolution

The adoption of digital ID technologies within the financial services industry has experienced rapid acceleration, driven by the critical demand for robust ID verification systems. Market analysis highlighted this trend, with forecasts predicting the global digital ID solutions market will expand from US$34.5 billion in 2023 to US$83.2 billion by 2028, marking a compound annual growth rate (CAGR) of 19.3%.[107] This growth is partly due to the collaborative efforts between governments and the private sector, underscoring the transformative impact of digital IDs on security, operational efficiency, and financial inclusion. Additionally, evolving international standards have played a key role in propelling this momentum, ensuring that digital ID solutions meet global interoperability requirements.

Key drivers in this arena include government-led national ID programmes worldwide, aimed at enhancing service delivery and security, alongside private sector initiatives prioritising customer experience and compliance with stringent regulations. These strategic endeavours encompass a spectrum of activities, from funding innovative tech startups to forging partnerships with established industry players. Such initiatives are further bolstered by governmental support and international aid for infrastructure development.

The momentum toward creating interoperable and universally accessible digital ID ecosystems is intensifying, propelled by rapid technological advancements and shifts in the financial services landscape. The emergence of online and virtual banks has generated a growing need for digital ID solutions capable of seamless operation across diverse platforms and legal frameworks. Simultaneously, the advent of Web3 and virtual assets has heightened the demand for robust digital ID frameworks. As the economy delves further into decentralisation and DLT, secure and verifiable digital IDs become integral for fostering trust and ensuring regulatory compliance within these evolving domains.

In response to these multifaceted challenges, the financial sector is taking the lead in advocating for the standardisation of digital ID structures. This endeavour aims to streamline the user experience by reducing redundant ID verifications and facilitating regulatory compliance. However, the impetus for this transformation extends beyond traditional banking, with telecommunications and fintech entities playing a crucial role. Leveraging their expertise in managing extensive digital ID records and consumer data, these entities contribute significantly to enhancing the digital ID framework.

Moreover, international cooperation contributes to this dynamic landscape as nations collaborate to synchronise their digital ID strategies, facilitating cross-border transactions and personal mobility. At the same time, advanced economies are refining their intricate systems with sophisticated technologies like biometrics and blockchain, while emerging nations leverage digital IDs to overcome traditional infrastructural limitations, thereby integrating millions of individuals into the formal financial services sector.

The widespread adoption of mobile technology is revolutionising the implementation of digital IDs, transcending geographical barriers and unlocking unparalleled access to financial services. However, while the proliferation of digital ID systems represents significant progress in financial inclusivity and security, it also raises concerns regarding privacy, data protection, and the risk of societal exclusion. To navigate these challenges, sustained international cooperation and investment are imperative to ensure that principles of fair access and ethical standards underpin the evolution of digital ID.

107 MarketsandMarkets. (2023). 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

2. Case studies in digital ID development and adoption

Mainland China

During China's National People's Congress in March 2022, Chinese Premier Li Keqiang revealed plans for the nationwide rollout of a digital national identification card. This initiative aims to simplify access to inter-provincial services for China's increasingly mobile population by enabling individuals to store personal identification information on their mobile devices. Users can access services by scanning a code on their phone with the Ministry of Public Security spearheading this digital transformation effort.

Cyber Trusted ID Platform (CTID)

At the World Internet Conference (WIC) 2020, the First Research Institute (FRI) introduced an authoritative network ID certificate through the National Internet + Trusted ID Authentication Platform.[108] This initiative aims to mitigate the risk of personal information leakage during traditional ID verification processes, where physical ID cards are required for presentation and photocopying.[109] The 'cardless' electronic ID verification system operates through a commercial mobile application, generating an encrypted certification upon the verification of the user's ID by the police in the backend, alongside a dynamic QR code on the user's mobile phone.[110] The CTID has undergone piloted testing in Guangdong, Fujian and other cities, with ongoing interlinkages with other entities, such as an interoperability arrangement with China Telecom in May 2022. At present, the CTID platform is recognised as a trusted ID authentication infrastructure for many regions and industries. Its concurrency capability reaches 20,000 transactions per second, with an average response time of 0.5 seconds, and it processes an impressive amount of data, reaching 5 billion units.[111]

Citizen Online ID Identification System (eID)

In 2015, the Citizen Online ID Identification System developed by the Third Research Institute (TRI) of the Ministry of Public Security (MPS) successfully passed the security review conducted by the State Cryptography Administration (SCA) and began issuing eID to citizens. The system boasts three key features: (i)) Mobile compatibility (restricted to designated types); (ii)) SIMeID sticker; and (iii) NFC-IC Card communication. eID supports online ID authentication, signature verification, and offline ID authentication. These functionalities enable precise identification of a natural person's ID while safeguarding citizens' personal information, particularly during bank account openings and other daily payment transactions, such as airline travel services and hotel accommodations.

Real-Name Decentralised ID (RealDID)

In December 2023, China unveiled its ambitious "Real-Name Decentralised ID (RealDID)" initiative, targeting its vast populace of 1.4 billion. This pioneering project represents a collaboration between the Ministry of Public Security and China's Blockchain-based Service Network (BSN), with additional support from tech giants such as China Mobile and China UnionPay.[112] RealDID aims to provide a comprehensive suite of services, including personal real-name verification, data encryption, secure login procedures, and business ID authentication. A notable feature of RealDID is its ability to allow citizens to register and interact with online platforms while preserving their privacy.

The RealDID system was built upon the CTID digital ID chain, establishing a distributed ledger for digital identities with verifiable, real-name credentials. This groundbreaking national-level system marks a significant milestone in the field and is expected to have diverse applications, ranging from social media verification to secure data transfers and personal ID certifications.[113] The introduction of this identification framework aligns with the swift advancement of DLT within China's digital landscape. BSN's initiative is part of a broader global trend aimed at empowering individuals with greater control over their personal information, granting them the autonomy to determine what data to share and with whom.[114]

108 Chen, J. A. (2020, November 25). The new mainland "Network Certificate" exposed: Officially replaces identity information authentication to protect privacy. HK01.
109 Liu, A. (2018, November 18). 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.
110 Liu, A. (2018, November 18). 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.
111 Xing, K. Y. (2022, March 15). Digital ID Cards Industry Special Topic: Digital ID Cards Lead a New Era of the Digital Economy. https://stock.finance.sina.com.cn/stock/go.php/vReport_Show/kind/search/rptid/700688401898/index.phtml
112 Blockchain Service Network. (2023). BSN real-name DID service launch will be held in Beijing.
113 CoinDesk. (2023, December 12). 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/
114 tech News Hong Kong. (2023, December 13). China to introduce blockchain-based identity verification. https://fintechnews.hk/24517/fintechchina/china-to-introduce-blockchain-based-ID-verification/

Singapore

National Digital ID (NDI), MyInfo Profile, SingPass & CorpPass

Singapore has launched the National Digital ID (NDI), enabling residents and businesses to engage in digital transactions across both public and private sectors conveniently and securely. The NDI constitutes a centralised digital ID system built on public key infrastructure (PKI) cryptographic security techniques. It was initially introduced in 2017 and has since undergone continuous enhancements. The NDI framework is built upon the authentication system "SingPass", which was launched in 2003 and is used by Singapore residents to access government e-services. Additionally, all "SingPass" users are automatically granted access to their own MyInfo Profile. This profile contains over 100 personal data items retrieved from various government agencies and is government-verified. On the other hand, "CorpPass" is given to corporations to facilitate their access to more than 130 government services and to manage authorisations for staff.

In 2019, Singapore started a pilot programme for MyInfo Business, which operates through "CorpPass". This initiative allows businesses to share their government-verified data, such as corporate profiles, financial performance, and ownership information, via the platform. The service is also undergoing trials with some local banks to facilitate processes such as opening corporate utility accounts and applying for SME loans.

Under the NDI framework, trusted ID layers are established using officially verified data provided by the government, fostering an open and federated ecosystem of authentication and digital signing services. One of the authentication service providers (ASPs) is operated by the Singaporean government, with MyInfo profiles serving as the trusted ID database of the NDI. Within this framework, users are only required to provide personal data to the government once, eliminating the need to provide data for every online transaction. Financial institutions can optimise customer onboarding processes and enhance operational efficiency by leveraging the MyInfo database, especially for bank account opening procedures. As of 2020, over 60 financial institutions utilise MyInfo to deliver 220 digital services, streamlining onboarding and CDD procedures.

Singapore actively pursues partnerships with other jurisdictions to optimise the interoperability of the digital ID. In 2020, an MOU was signed with Australia to explore mutual recognition of digital ID for cross-border applications, including expediting the bank account opening process and visa application. The collaboration is expected to enhance trade between the two countries. Subsequently, partnerships with similar objectives were established, such as the Digital Economy Partnership Agreement with Chile and New Zealand, and another MOU signed with the United Kingdom in 2021.

India

Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI)

Established in 2015, the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) operates as a company licensed under the Companies Act 2013. While the Government of India has a shareholding of 51%, the remaining portion is owned by several public sector banks and the National Housing Bank. The primary objective of the company is to administer a Registration System, serving as a registry for security interests in India. It facilitates the registration of transactions related to securitisation, asset reconstruction and security interest, as envisaged under the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (SARFAESI Act).

India Stack & Aadhaar programme

In 2010, The Unique Identification Authority of India, set up by the Indian central government, started issuing unique ID (UID or Aadhaar Number) to Indian citizens through the Aadhaar programme. Underlying the UID are minimal personal information and biometric readings (fingerprints and iris scans) that can be used for authentication. Aadhaar-based e-KYC allows users to provide personal data to financial institutions electronically, while service providers can conduct verification and authenticate it in real time via the platform, reducing both the paperwork required and the time spent.

To further strengthen the privacy and security of Aadhaar number holders, UIDAI introduced the implementation of Virtual ID, UID Token and Limited KYC and laid down the following process in 2018.

i. The introduction of Virtual ID, in which users can generate unlimited IDs independently. It provides an option to not share the user's Aadhaar Number at the time of authentication for potential security concerns, as the Aadhaar Number is linked to the entire demographic details of the user.

ii. Introduce limited KYC service to limit access to Aadhaar numbers. By categorising Authentication User Agencies (AUAs) into global and local AUAs, global AUAs, such as banks and tax authorities, have no restrictions on access to user's information. In contrast, local AUAs have limited rights and are given an "agency-specific" tokenised number (UID token) to match and verify ID. Thus, the unique Aadhaar Number does not need to be stored to conduct KYC for local AUAs.

India published the first draft of a Non-Personal Data (NPD) Governance Framework for the country for public consultation on 13 July 2020, which aims to create a data-sharing framework such that community data is available for social/ public/ economic value creation. However:

i. The majority of micro, small and medium enterprises (MSMEs) and startups have opposed the government's non-personal data policy framework in its current form, as allowing large businesses to sell their aggregate data for a price will not help most of the small businesses;

ii. Amazon, Facebook, and Google have also opposed the mandate, saying this undermines investments made by companies to process and collect such information.

Australia

The Digital Transformation Agency (DTA) has been developing a national digital ID framework known as the Trusted Digital ID Framework (TDIF). This framework establishes the rules and standards for a federated model of ID, where multiple accredited ID service providers offer digital ID services that can be used to access services across the government and the private sector.

myGovID

myGovID is a key component of Australia's digital ID system. It is an app designed to offer a secure method of online identity verification. Unlike traditional forms of ID, myGovID is accessible via smartphones, providing a convenient means of accessing government services digitally. This initiative is integral to the broader Digital ID programme, which seeks to create a more seamless and secure approach for Australians to access government services online, emphasising principles of privacy, security, and choice.

Furthermore, Australia has actively engaged in international discussions concerning digital ID recognition, exemplified by the 2020 MOU with Singapore. The initiative aims to create a connection that acknowledges each other's digital ID systems, thereby simplifying international transactions and travel between the two countries.

New South Wales – ServiceNSW

Looking at the state level, New South Wales (NSW) stands out for its successful adoption of digital ID initiatives. The Service NSW app, operated by the state government, serves as a prime example of this success, boasting near-total penetration among the state's population. This high adoption rate has been significantly driven by the app's integration of COVID-safe check-in functionality and the availability of Digital Driver Licenses, which have become virtually indispensable for many residents.

Expanding on this foundation, users have the option to create a digital ID within their MyServiceNSW Account, capable of verification at various levels of assurance, utilising existing government-issued physical documents. Users can upload digital versions of these documents to their account, alongside other verified personal details like mobile number, date of birth, and email address. These initial steps pave the way for the inclusion of more advanced verifiable credentials, such as those issued by the NSW Registry of Births, Deaths & Marriages. Credentials can be presented through either the ServiceNSW app or a dedicated app provided by the Registry.

Similarly, Hong Kong's "LeaveHomeSafe" mobile app played a pivotal role during the pandemic. However, unlike in NSW, where digital IDs have been expanded to include a wide range of functionalities and credentials, the post-pandemic landscape in Hong Kong did not see the full potential of digital IDs realized for broader and more frequent adoption in daily life.

The European Union (EU)

European Digital ID (e-ID)[115]

Previously, electronic IDs issued separately by different EU countries lacked the interoperability necessary to synchronise with other jurisdictions or sectors. This limitation hindered users' access to cross-boundary public and commercial services. To overcome this challenge, the EU proposed a new e-ID framework in June 2021. This framework aims to address the limitations and insufficiencies of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

The revised e-ID framework is set to ensure seamless verification of ID for all EU citizens and residents holding a national ID card. This enhancement enables them to access public and commercial services online and offline across the entire Union territory. This advancement is encapsulated in a personal digital wallet—an application designed to work across various electronic devices.

Universally accessible, the digital wallet is open to any EU citizen, resident, or business that opts in. Serving as a mobile digital repository for ID verification, it empowers users to manage their data confidently and transparently, regardless of their location within the EU. This innovative technology directly addresses concerns regarding the uncertain fate of personal information once shared online.

The EU Commission's commitment to a secure European e-ID directly responds to these concerns. It envisions a trusted and adaptable solution accessible to all citizens for an array of activities, from administrative tasks to everyday conveniences.

The eIDAS Regulation[116]

Enacted in 2014 and effective from July 2016, the eIDAS Regulation has been instrumental in shaping the digital horizon of the EU. It established a unified framework for electronic interactions within the region's public and private sectors, enabling seamless use of national electronic IDs to access cross-border public services. Additionally, the regulation standardised Trust Services, including e-signatures, e-seals, and time-stamping, thereby providing these digital measures with the same legal status as their physical counterparts and fostering a more efficient market.

Expanding upon the infrastructural improvements facilitated by the eIDAS Regulation, the introduction of the EU Digital ID aims to further bridge gaps in digital services accessibility. This initiative responds to the previously limited cross-border authentication capabilities, as evidenced by the low percentage of public service providers equipped to handle such interactions.

In the realm of banking and finance within the EU, the eIDAS framework is significantly enhancing customer engagement. It streamlines processes such as ID verification, compliance, contract execution, and secure agreement finalisation. Financial institutions that adopt the eIDAS provisions not only experience a reduction in administrative overhead but also provide improved customer experiences. The framework plays a crucial role in enabling these entities to extend their services more efficiently across the EU, supported by a reliable and secure identification foundation.

The Data Governance Act

In 2020, the European Commission proposed a "Regulation on European data governance (Data Governance Act)", a set of governance measures aimed at enhancing data exchange and supporting European data spaces. The instrument focuses on facilitating data exchange by addressing various scenarios, including:

(i) Promoting the reuse of public sector data.

(ii) Facilitating data sharing among businesses

(iii) Introducing an additional layer of intermediary to safeguard individual interests under the General Data Protection Regulation (GDPR).

115 European Commission. (n.d.). A Europe fit for the digital age. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
116 European Commission. (n.d.). Discover eIDAS | Shaping Europe's digital future. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/discover-eidas

(iv) Allowing data use on altruistic grounds.

Within this framework, a voluntary mechanism is proposed to allow organisations engaging in data altruism to register as a "Data Altruism Organisation recognised in the EU".[117] This mechanism aims to facilitate the establishment of cross-boundary data repositories. Recognised Data Altruism Organisations would be permitted to collect data from individuals or process data for the benefit of society. Additionally, the proposal includes the introduction of a new layer of data intermediaries. These independent data-sharing entities would safeguard the public interest and uphold data privacy by facilitating responsible data aggregation and exchange.[118]

117 Data altruism is about individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used in the public interest. (Quote from European Commission's Data Governance Act Explained, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#:~:text=Data%20altruism%20is%20about%20individuals,used%20in%20the%20public%20interest.)

118 European Commission. (n.d.). Data Governance Act explained. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#ecl-inpage-l4ihlqt9

Annex 3: Assessing Hong Kong's ecosystem and its readiness for related applications of digital ID

Hong Kong is shaping its digital ID framework to cater to the needs of an increasingly interconnected society. At the core of this transformation lies the government's iAM Smart initiative, facilitating seamless digital interactions among citizens, public services, and private enterprises. This initiative opens avenues for growth, particularly for private digital ID solution providers, who can capitalise on opportunities to enhance user experiences. The framework in Hong Kong is a result of collaborative efforts among regulators, financial institutions, and technology innovators, all striving to create a more cohesive and efficient digital infrastructure. However, while these ongoing developments underscore Hong Kong's commitment to progress, further action is necessary to propel the ecosystem toward full maturity. Critical next steps include refining policies, improving security measures, and maintaining an environment conducive to innovation while safeguarding privacy. A systematic approach to addressing these areas is critical for the advancement of the digital ID landscape in Hong Kong, with the ultimate goal of achieving a robust and user-centric digital society.

1. Hong Kong's Landscape

- **Government-led initiative – iAM Smart**

iAM Smart, previously known as eID, is a comprehensive digital services platform launched in 2020. It equips Hong Kong residents with a digital electronic ID, facilitating access to a broad spectrum of public services and streamlining online business transactions. Serving as the authoritative source (or the golden source) of personal ID, iAM Smart has extended to the private sector, encompassing industries such as banking, insurance, and utilities, including electricity and gas companies. The platform's foundation is built on four core functions:[119,120]

- Authentication: After verifying the HKID card during the registration process, users can log in to various online services using biometrics or a set of security keys for authentication, reducing the procedures and time needed to access different services.
- Form filling: The platform stores authenticated personalised data, enabling auto-filling forms upon receipt of consent from users.
- Personalised notification: : iAM Smart sends reminders to keep users updated with the latest information on government services and personal tasks.
- Digital signing: It enables legally binding eSignature backed by the Electronic Transactions Ordinance for statutory documents and procedures.

The essence of the programme lies in its comprehensive digital services hub, the iAM Smart mobile app, which delivers a personalised user experience. The platform's commitment to security is evident in its foundational design. Adherence to strict government IT security policies and guidelines, coupled with compliance with ISO 27001 and ISO 27701 standards, ensures the integrity and confidentiality of user data. Proactive completion of a thorough Privacy Impact Assessment, in compliance with the Personal Data (Privacy) Ordinance (PDPO) before the platform's launch, reinforces the commitment to user trust and privacy.[121]

As of the end of 2020, the Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), Insurance Authority (IA), and the Mandatory Provident Fund Schemes Authority (MPFA) have each issued circulars to their regulated entities endorsing iAM Smart as a pivotal platform for fostering growth in Hong Kong's fintech ecosystem. They advocate for integrating iAM Smart into online services offered by financial institutions, such as remote onboarding, account login authentication, and digital document signing, with the aim of providing customers with a streamlined and efficient experience while ensuring compliance with statutory and supervisory mandates. Regulators have recognised iAM Smart's capacity for reliable client ID verification and its utility for digital signing during the onboarding process, given its robust and independent verification of Hong Kong residents' identities. Institutions planning to implement iAM Smart for production use are encouraged to engage with the Sandbox Programme. Importantly, the adoption of iAM Smart is voluntary.

119 Office of the Government Chief Information Officer. (n.d.). iAM Smart. https://www.ogcio.gov.hk/en/our_work/community/iam_smart/
120 iAM Smart. https://www.iamsmart.gov.hk/en/ /
121 iAM Smart. (n.d.). Introduction on "iAM Smart" & Sandbox Programme. https://www.hklawsoc.org.hk/-/media/HKLS/Home/Support-Member/Professional-Support/AML/AML-Template/iAM-Smart-Information-Pack.pdf

Since the launch of iAM Smart in 2020, iAM Smart has garnered approximately 2.5 million registrants.[122] The focus has extended to beyond merely increasing the number of registrants to boosting the platform's annual usage. Specifically, the target is to escalate the total number of annual transactions from five million in 2021 to 17.5 million by 2025.[123] A primary factor driving the platform's adoption in financial services is the user experience it offers. Users are inclined to choose iAM Smart when it provides a more seamless and user-friendly interface than the current alternative.

- **Financial infrastructure supporting SMEs**

As outlined in the 2024 Budget, the Hong Kong government has envisioned the development of a digital identity framework tailored for enterprises.[124] This strategic initiative involves the integration of 1.8 million local enterprises into the enterprise version of the iAM Smart platform, which is set to launch in 2026.[125] This platform is engineered to streamline business operations by facilitating digital document signing and enabling electronic payments for government services. It will furnish robust digital identity verification for businesses, thereby enhancing operational efficiency through features such as auto-populated forms and secure storage for electronic credentials.

Commercial Data Interchange[126]

The Commercial Data Interchange (CDI) represents a significant advancement in corporate banking, establishing a robust platform for the secure and streamlined exchange of financial and commercial data. It acts as a conduit between data providers and financial institutions, fostering a more efficient and transparent financial ecosystem.

In 2020, the HKMA successfully conducted a Proof-of-Concept (PoC) in partnership with various banking partners to refine credit evaluation processes for SME financing. This initiative demonstrated the CDI's potential to revolutionise the trade finance application procedure by utilising a wealth of trade-related data. Building on this success, the next phase of the CDI's evolution will integrate diverse commercial data sources to strengthen banks' alternative credit scoring capabilities. Furthermore, the inclusion of the Companies Registry as a data provider promises innovative KYC applications driven by the rich data reservoir of the CDI.

The year 2022 marked another significant milestone with the HKMA's official launch of the CDI, positioning it as a cornerstone of its "Fintech 2025" strategy. The CDI initiative's efficacy was established during its pilot phase, which saw over HK$1.6 billion in SME loan approvals, with extensive participation from banks and data providers. In light of this success, ensuring the secure exchange of data is imperative. SMEs stand to benefit substantially from the CDI, and all stakeholders are encouraged to explore the opportunities it presents. By engaging with participating banks and exploring the CDI's online portal, businesses can access a comprehensive suite of services to enhance their financial inclusion and growth.

As the financial industry continues to evolve, the significance of the CDI becomes apparent, highlighting the advantages of streamlined data exchange. However, the comprehensive adoption and refinement of digital ID frameworks will truly catalyse the growth of the fintech sector. While the CDI and digital ID systems operate independently, they are complementary, forming a robust infrastructure of trust and innovation. This synergistic relationship is poised to propel the financial services industry to new heights, fostering an ecosystem that not only upholds the existing range of banking services but also stimulates the creation of novel, consumer-centric financial products. Such concerted efforts to develop and standardise digital ID protocols are essential for establishing a secure and reliable environment conducive to fintech expansion. Such an environment promises to usher in a new age of financial services characterised by greater accessibility, customisation, and alignment with the expectations of a digitally astute clientele.

122 iAM Smart. https://www.iamsmart.gov.hk/en/
123 Hong Kong SAR Government. (2023, February 22). LCQ2: Promoting development of personal digital identity. https://www.info.gov.hk/gia/general/202302/22/P2023022200263.htm
124 HKSAR Budget 2024. https://www.budget.gov.hk/2024/eng/pdf/e_budget_speech_2024-25.pdf
125 SCMP. (April 2024). Hong Kong finance chief Paul Chan vows to help 1.8 million firms make payments, use services on enterprise version of iAM Smart. South China Morning Post. 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
126 Hong Kong Monetary Authority. (2022, October 24). HKMA announces the official launch of Commercial Data Interchange. https://www.hkma.gov.hk/eng/news-and-media/press-releases/2022/10/20221024-3/

Interbank Account Data Sharing[127]

Meanwhile, HKMA is set to initiate the pilot programme for the Interbank Account Data Sharing (IADS) initiative on January 1, 2024. This ground-breaking project allows customers to securely share their banking data with other banks, given their consent.

Developed in collaboration with the Hong Kong Association of Banks and other industry players, the IADS stems from comprehensive studies conducted by HKMA's Fintech Facilitation Office. These studies indicate that sharing customer bank account data could significantly enhance banking operations, bolster risk management, and improve overall customer experience. Spanning across retail, corporate, and SME segments, the IADS pilot will incorporate deposit account information, including availability, status, balance, and transaction history.

With the involvement of 28 banks, the IADS pilot is poised to usher in innovative banking services, facilitating streamlined loan processes and personalised, data-driven solutions. The HKMA will closely monitor the pilot's progress, evaluating market responses to inform potential full-scale implementation strategies. In an era characterised by rapid digital transformation—further accelerated by the pandemic—Hong Kong has demonstrated agility in adaptation. There has been a marked surge in customer expectations for digital engagement, accompanied by increased demand for expedited access to a diverse array of public and commercial services, particularly those enabled by online ID verification. Moreover, the financial services industry now acknowledges the importance of remote customer onboarding.

Regulators have responded to this digital shift by issuing circulars and advocating best practices to navigate this evolving landscape. Simultaneously, industry associations have actively implemented supportive measures to drive these advancements. These concerted efforts signify a commitment to keeping pace with and shaping the future of digital finance, ensuring that innovations like the IADS seamlessly integrate into an ecosystem where security, efficiency, and customer satisfaction are paramount.

Development in the private sector

In the context of an expanding digital economy, where online transactions have become commonplace, the private sector is emerging as a catalyst in reshaping ID verification. A key development in this domain is the exploration by HSBC Lab of a decentralised ID solution at the retail level.

Decentralised ID technology represents a departure from traditional ID verification towards a system prioritising security and user control. HSBC Lab's experiments leverage public and private digital ledger protocols (also known as blockchain) to develop a prototype that streamlines the internal account opening process while maintaining strong data privacy and KYC controls. This system allows customers to directly use HSBC's verified digital credentials across various banking operations and products, thereby enhancing convenience and efficiency. HSBC Lab's decentralised ID platform aims to manage banking credentials and is engineered to authenticate and safeguard data from an array of issuers, such as government agencies and credit bureaus. Such interoperability is crucial for facilitating trust and simplifying the verification process for different transactions and account setups.

The HSBC initiative seeks to enhance the overall customer experience by eliminating the repetitive nature of traditional ID verification. The introduction of password-less authentication and the ability to build upon one's ID profile over time is anticipated to contribute to a more seamless user experience. HSBC's exploration of DID technology reflects a broader trend in the financial services industry toward systems that are simultaneously more secure, efficient, and customer-centric. The efficacy of the DID system in managing KYC and other ID-related procedures suggests its potential to refine operational processes and reinforce digital trust. The advancement of digital ID by private sector entities marks a significant progression towards a streamlined digital economy. Financial services are headed towards an era where personal credentials are securely managed and shared on demand, enhancing user experiences and interconnectivity.

Other developments in the banking industry

As the banking sector embraces technological advancements, service delivery has transcended traditional methods. Since the issuance of HKMA's first virtual banking license in 2018, Hong Kong has witnessed the emergence of eight virtual banks. Central to Hong Kong's virtual banking landscape is the e-KYC framework, leveraging "ID authentication &matching.". This system relies on the digital submission of ID documents,

127 Hong Kong Monetary Authority. (2023, December 21). Interbank Account Data Sharing pilot programme.https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/12/20231221-3/

coupled with liveness detection and facial matching technology, and is crucial for the onboarding process of new customers.

In their pursuit of enhancing operational efficiency and customer satisfaction, traditional banks are reimagining their approaches. Since 2019, many of these institutions have embraced mobile services for account openings, with some extending these services internationally to facilitate account openings for Hong Kong residents living abroad. Nonetheless, the absence of a unified e-KYC platform has resulted in a mosaic of practices across the industry, prompting financial entities to craft their tailored e-KYC solutions.

As retail banking increasingly integrates technology into its KYC processes, certain institutions are expanding their online services to include business and corporate clients, particularly SMEs. The documentation required is customised to suit the specific industry and nature of the business, which may encompass items such as buyer invoices, tenancy agreements, or business plans.

The accelerated shift towards remote client onboarding within Hong Kong banks—propelled in part by the COVID-19 pandemic—has prompted the HKMA to issue a series of circulars. These documents provide clear guidance on implementing Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) control measures.

- In February 2019, a document outlined the HKMA's regulatory expectations for remote onboarding of individual customers.[128] According to the document, authorised institutions (AIs) should employ technology solutions "*at least as robust as those performed when the customer is in front of the staff*" to mitigate the risks when identifying and verifying the ID of an individual customer.[129]
- The circular "F*eedback from recent thematic reviews of Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) control measures for remote customer onboarding initiatives*", published in June 2020, shares HKMA's key observations and good practices in AML/CFT control measures. [130]
- Subsequently, in September 2020, HKMA published a guidance in relation to "remote on-boarding of corporate customers".[131] While reiterating that a risk-based approach needs to be adopted in the CDD process and regulatory standards remain the same regardless of whether a traditional approach or technology is used, the circular confirmed that the CDD steps could (i) be carried out via teleconference or video conference or independent and appropriate intermediaries provided use of such methods was commensurate with the assessed ML/TF risks, for customer interaction and (ii) use reliable technology solutions to verify identities of representatives and owners.[132]

In May 2021, HKMA encouraged the adoption of iAM Smart for remote onboarding, aligning with FATF standards and its March 2020 digital ID guidance.[133] It clarified iAM Smart's use in meeting AML/CFT requirements, such as record-keeping through API data without needing additional documents, and the HKMA remained supportive of technology used to enhance CDD efficiency and customer experience.

Other developments in the securities industry

According to the Retail Investor Study 2023 conducted by the Investor and Financial Education Council, 80% of stock investors primarily conduct trading through online channels, with mobile applications being the most favoured mode.[134] This trend has catalysed the emergence of online brokers, which have significantly disrupted traditional securities firms by aligning with investors' dynamic preferences and behaviours. These digital brokers offer greater efficiency and cost-effectiveness compared to their brick-and-mortar counterparts, thus capturing a substantial share of the retail market. Many of these brokers have already made a mark in

128 Hong Kong Monetary Authority. (2019, February 1). Remote on-boarding of individual customers. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf
129 Hong Kong Monetary Authority. (2019, February 1). Remote on-boarding of individual customers. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf
130 Hong Kong Monetary Authority. (2020, June 3). Feedback from recent thematic reviews of Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) control measures for remote customer onboarding initiatives. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200603e1.pdf
131 Hong Kong Monetary Authority. (2020, September 24). Remote on-boarding of corporate customers. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200924e1.pdf
132 Deacons. (2020, November 26). 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
133 Hong Kong Monetary Authority. (2021, May 24). Remote on-boarding and iAM Smart. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210524e1.pdf
134 Investor and Financial Education Council. (2023). Retail investor study 2023.. https://www.ifec.org.hk/web/common/pdf/about-ifec/retail-investor-study-2023.pdf

the competitive financial sphere. While their underlying technologies may vary, a commonality among them is the adoption of a standard online account opening procedure, typically taking one to two weeks to complete.

In response to the digital shift, even traditional banks and securities firms are enhancing their online services. In today's digital era, a robust digital ID infrastructure is pivotal—it streamlines the onboarding process by enabling fast, secure verification of client identities, which is integral to enhancing customer experience and safeguarding the integrity of the financial system..

In accordance with the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct),[135] when a non-face-to-face approach is employed in the account opening process, the licensed or registered entity is responsible for taking all reasonable steps to verify a client's ID. The Securities and Futures Commission (SFC) has outlined five acceptable approaches to account opening, with online client onboarding becoming feasible if certain procedural steps are followed, including (i) obtaining electronic signature on client agreement with a copy of the ID document; (ii) transferring an initial deposit of HK$10,000 or more from the designated bank account to the intermediary's bank account; (iii) using the designated bank account as the sole trading account for future transactions; and (iv) maintaining proper record records of the account opening process. The update in 2019 expanded the acceptable approaches to include remote procedural steps, including but not limited to ID verification, ID document authentication and electronic agreement signing. This circular provides clarity on online account opening and facilitates development in this area.

Other developments in the insurance industry

Hong Kong's Insurance Authority (IA) has been at the forefront of embracing FinTech innovation, launching the Fast Track scheme in 2017 to expedite the development of exclusively digital distribution channels and catalyse the growth of Insurtech. Following the authorisation of the first virtual insurer in 2019, the landscape has rapidly evolved, with five digital insurers authorised by 2021.

The industry, in collaboration with associations like the Hong Kong Federation of Insurers, has responded quickly to the challenges posed by the pandemic. Collaborating with the IA, they introduced Hong Kong's inaugural Virtual Onboarding platform. This initiative facilitates the remote distribution of long-term insurance products, offering video conferencing advice and bridging the gap between insurers and consumers during these unprecedented times.[136] In the same year, the Insurtech Sandbox was established, providing a controlled environment for industry players to refine innovative applications while ensuring compliance with supervisory standards and addressing potential risks and cybersecurity concerns. This has empowered even traditional insurers to adopt new, non-face-to-face selling processes that align with the IA's regulations.[137]

IIn 2020, the IA published the Key Observations of Insurers' AML/CFT Control on Virtual Customer Onboarding,[138] to enhance the industry's comprehension of certain requirements outlined in the AMLO and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3"). To promote financial inclusiveness and maintain a level playing field, the IA indicated their long-term objective of establishing a shared-use virtual onboarding platform for different insurers, particularly smaller or mid-sized players who may lack the resources required to develop their proprietary platforms.[139]

Digital ID has emerged as a fundamental component in the evolution of the insurance industry, proving vital for insurers and policyholders. A robust digital ID infrastructure is set to revolutionise the insurance process, spanning from the initial policy purchase to claims management and settlement. Such a system suggests a more streamlined verification of medical records, smoother claims processing, and strengthened security for personal data.

When effectively implemented, a comprehensive digital ID framework could ensure that policy transactions and payouts are executed with exceptional efficiency and security. This advancement is expected to significantly reduce fraud and administrative overhead, fostering a more unified and secure environment for everyone involved. As the industry progresses, the critical role of digital ID solutions becomes increasingly apparent.

135Securities and Futures Commission. (2024). Code of conduct for persons licensed by or registered with the Securities and Futures Commission: January 2024 English final with bookmark. 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
136 Insurance Authority. (n.d.). Digital onboarding. https://www.ia.org.hk/en/digital_onboarding/index.html
137 DBS. (2021, June 21). DBS Hong Kong launches virtual insurance onboarding service. https://www.dbs.com/NewsPrinter.page?newsId=kq2bdwid&locale=en
138 Insurance Authority (2020, December 4). Key Observations of Insurers' AML/CFT Control on Virtual Customer Onboarding. https://www.ia.org.hk/en/supervision/antimoney_laundering/files/AML_Online_Sharing_Session_20201204_Presentation.pdf
139 Insurance Authority. (n.d.). Insurance Digital Onboarding. https://www.ia.org.hk/en/digital_onboarding/promotion_of_insurtech_development.html

They are not merely an additional feature but a fundamental leap toward a more accessible and secure insurance sector in Hong Kong.

2. Collaborative initiatives: establishing the iAMSmart sandbox programme with public sector partnership

The iAM Smart Pilot Sandbox Programme was launched in 2020 through a collaborative effort between Cyberport and the OGCIO. This partnership exemplifies a commitment to cultivating a digitally inclusive society by bringing together diverse public organisations to advance Hong Kong's digital empowerment. The programme underscores the importance of collaborative efforts in enhancing Hong Kong's digital ecosystem, aiming to facilitate the widespread adoption and innovative use of the iAM Smart platform.[140]

Designed as a testing ground for digital innovation, the Sandbox Programme offers businesses a secure environment to test API functionalities and conduct Proof-of-Concept trials with the iAM Smart infrastructure. Since its inception, the programme has made significant strides, with over 330 organisations participating to test and develop their applications using iAM Smart. In addition, more than ten public and private entities have successfully integrated iAM Smart into their service offerings, further illustrating the programme's growing impact on the digital landscape.[141]

The programme serves as a bridge for entities transitioning towards a government-endorsed digital ID framework. By offering a range of support services—including a dedicated helpdesk, specialised training workshops, and testing assistance—the initiative ensures that organisations can smoothly transition from concept to application, effectively incorporating iAM Smart features into their services.[142]

Participants embark on a structured two-phased developmental journey within the programme. The first phase focuses on initial testing and service refinement, while the second phase leverages an Integration Testing Environment that simulates the production setting.[143] This environment is pivotal for the meticulous fine-tuning of services before their public release. Successful completion of both phases provides participants with the necessary tools and confidence to integrate iAM Smart functionality into their online services and launch them to their user base.

With an inclusive approach, the programme caters to entities from the financial services sector—such as banking, insurance, and investment – as well as supporting organisations from a broad spectrum of industries, including ICT, telecommunications, healthcare, education, transport, logistics, and more.[144] This approach underscores the programme's commitment to developing a flexible and comprehensive digital ID ecosystem capable of adapting to diverse industry needs.

As the programme looks to the future, it aims to broaden participation further, welcoming additional sectors to leverage the iAM Smart platform. In doing so, the programme seeks to harness the full transformative power of digital ID. The continual evolution of the programme is marked by a sustained focus on nurturing a digital ecosystem that is not only technically proficient but also aligned with regulatory standards, optimised for user engagement, and conducive to cross-industry collaboration. These collective efforts are shaping a resilient and user-friendly digital ID framework, responsive to the dynamic needs of Hong Kong's diverse economic sectors.

3. Hong Kong's role in advancing global digital ID standards for business

Corporate digital IDs are as vital as individual ones, grounding trust in the digital economy and enabling transactions, regulatory adherence, and credibility. A corporate digital ID captures a company's legal standing, regulatory compliance, and financial behaviour, all critical for ensuring transparency and accessibility in the business landscape.[145]

140 Office of the Government Chief Information Officer. (n.d.). iAM Smart Adoption by Public and Private Organisations. https://www.ogcio.gov.hk/en/our_work/business/i_am_smart_adoption/

141 HKSAR Legislative Council. (2022, October 10). Panel on Information Technology and Broadcasting. (2022, October 10). Progress on the implementation of the "iAM Smart" platform and e-Government services (LC Paper No. CB(1)654/2022(02)). https://www.legco.gov.hk/yr2022/english/panels/itb/papers/itb20221010cb1-654-2-e.pdf

142 iAM Smart. (n.d.). Introduction on "iAM Smart" & Sandbox Programme. https://www.hklawsoc.org.hk/-/media/HKLS/Home/Support-Member/Professional-Support/AML/AML-Template/iAM-Smart-Information-Pack.pdf

143 Insurance Authority. (2020, September 30). iAM Smart Pilot Sandbox Programme - Phase 2 [Circular letter]. https://www.ia.org.hk/en/legislative_framework/circulars/reg_matters/files/Circulars_iAM_Smart_Pilot_Sandbox_Programme__Phase_2.pdf

144 Office of the Government Chief Information Officer. (n.d.). iAM Smart Adoption by Public and Private Organisations. https://www.ogcio.gov.hk/en/our_work/business/i_am_smart_adoption/

145 BIS. (June 2022). Corporate digital identity: No silver bullet, but a silver lining. https://www.bis.org/publ/bppdf/bispap126.pdf

Hong Kong is at the vanguard of incorporating corporate digital identities into its economic infrastructure, supported by its robust financial sector and commitment to technological innovation. This strategic move is not only aimed at optimising local operations but also at influencing the establishment of international digital ID standards.

Adopting corporate digital IDs in Hong Kong is expected to streamline administrative processes, enhance due diligence, and elevate transparency in business dealings, hence supporting regulatory efforts to combat financial malfeasance and uphold market integrity. Initiatives such as the HKMA's Open Application Programme Interface (API) framework[146], are pivotal in modernising Hong Kong's financial services. Equally important is the adoption of Legal Entity Identifiers (LEIs), recommended as the top priority by the Hong Kong Trade Repository (HKTR) for identifying the parties involved in a transaction.[147] The city's dedication to this cause is further highlighted by the People's Bank of China's strategic roadmap for LEI adoption,[148] along with UnionPay's incorporation of the system.[149]

Established market mechanisms and a vibrant tech scene are crucial for navigating the complexities of digital ID integration. Hong Kong's investment in professional development across cybersecurity, data analytics, and fintech reflects its commitment to this transition. Nevertheless, the journey ahead is replete with challenges. Ensuring privacy, securing data, and achieving system interoperability are paramount issues that require a concerted, collaborative effort from government agencies, financial institutions, technology firms, and civil society. As Hong Kong explores digital ID solutions, it stands at a crossroads. The city's engagement with LEIs hints at the potential to reshape its business and financial landscape, striving for a more robust and inclusive future. Support from organisations like the Global LEI Foundation and local initiatives such as the HK PKI Forum is pivotal for this advancement. Hong Kong's digital ID strategy is expected to refine corporate operations, bolster global trade, and improve financial service accessibility, thus stimulating economic growth. Against this backdrop, corporate digital ID signifies efficiency and serves as vital infrastructure for global economic connectivity.

146 Hong Kong Monetary Authority. (n.d.). Open Application Programming Interface (API) for the Banking Sector. https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/

147 Yeung, I. (2018, June 29). Hong Kong mandates use of legal entity identifiers for OTC derivatives. https://www.centralbanking.com/regulation/3596946/hong-kong-mandates-use-of-legal-entity-identifiers-for-otc-derivatives

148 People's Bank of China. (2020, December 11). Release of the Implementation Roadmap for the Application of Global Corporate Identity Codes (2020-2022). https://www.gov.cn/xinwen/2020-12/11/content_5568976.htm

149 UnionPay International. (2022, June 3). UnionPay's LEI safeguards cross-border payments, boosting innovation in digital payment. https://www.unionpayintl.com/en/mediaCenter/newsCenter/marketUpdate/3015078.shtml

Acknowledgements

The FSDC would like to thank the following working group members for their valuable input:

Dr Adrian Cheng
Prof. Douglas Arner
Mr Kelvin Au
Mr Leiming Chen
Mr Philip Chiu
Mr Victor Ho
Ms Helen Hui
Mr Vincent Lau
Mr Robert Lui
Mr Wiley Pun
Mr Benjamin Quinlan
Mr Wingo Wong

The FSDC would like to express appreciation to
the China Academy of Information and Communications Technology for providing valuable input for research.

The operation of the FSDC is led by:

Dr King Au
Executive Director

This report is prepared by the FSDC Policy Research Team:

Dr Rocky Tung
Director, Head of Policy Research

Ms Wivinia Luk
Senior Manager, Policy Research

Ms Joyce Lee
Senior Manager, Policy Research

Mr Kendrew Leung
Manager, Policy Research

Ms Jessie Chen
Manager, Policy Research

Ms Erica Chung
Manager, Policy Research

Ms Mickey Sze
Analyst, Policy Research

About the FSDC

The FSDC was established in 2013 by the Hong Kong Special Administrative Region Government as a high-level, cross-sectoral advisory body to engage the industry in formulating proposals to promote the further development of the financial services industry of Hong Kong and to map out the strategic direction for the development.

Contact us

Email: enquiry@fsdc.org.hk
Tel: (852) 2493 1313
Website: www.fsdc.org.hk

FSDC Weblink

Financial Services Development Council