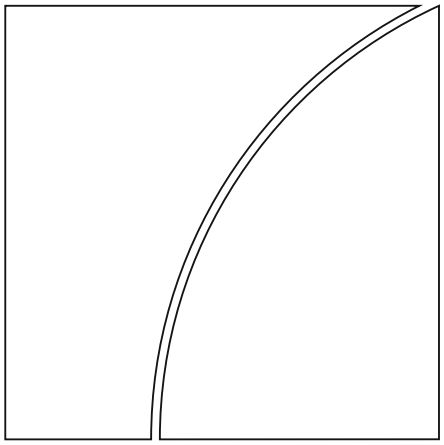
BANK FOR INTERNATIONAL SETTLEMENTS



BIS Papers

No 126

Corporate digital identity: no silver bullet, but a silver lining

by David Leung, Bénédicte Nolens, Douglas Arner and Jon Frost

Monetary and Economic Department

June 2022

JEL classification: D22, F23, G28, G38, L22.

Keywords: identification, identity verification, corporate structure, beneficial ownership, taxes, legal entity identifier, anti-money laundering / combating the financing of terrorism, prudential regulation, small and medium-sized enterprises, financial inclusion.

The views expressed are those of the authors and not necessarily the views of the BIS.

This publication is available on the BIS website (www.bis.org).

ISSN 1682-7651 (online)
ISBN 978-92-9259-577-7 (online)

Corporate digital identity: no silver bullet, but a silver lining

David Leung (Bank for International Settlements (BIS) Innovation Hub), Bénédicte Nolens (BIS Innovation Hub), Douglas Arner (University of Hong Kong) and Jon Frost (BIS and Cambridge Centre for Alternative Finance (CCAF))[1]

Abstract

Corporate digital identity (ID) has the potential to dramatically simplify the identification and verification of companies and to reduce the risks and costs of doing business. It forms a kind of admission ticket for a company to access financial and non-financial services while at the same time enhancing access to information about the company for counterparties, customers, regulators and financial services providers. Provided there is political will, technological innovation and policy can help in several areas to facilitate corporate digital ID and thus enhance overall efficiency, market integrity, financial stability and inclusion. Yet there is no silver bullet that can achieve all these benefits at once. Nor can any single stakeholder drive all the needed changes; corporate registries, banks and other financial institutions, established vendors, emerging regtech firms, and regulators and policymakers all have a role to play. The Legal Entity Identifier (LEI), decentralised identifiers (DIDs) and reforms built on public individual digital ID systems show particular promise, particularly for small and medium-sized enterprises, thereby supporting broader sustainable development, employment and innovation. In this paper, we examine these innovations in corporate digital ID and explore pathways for the future.

Keywords: identification, identity verification, corporate structure, beneficial ownership, taxes, legal entity identifier, prudential regulation, anti-money laundering / combating the financing of terrorism, small and medium-sized enterprises, financial inclusion.

JEL codes: D22, F23, G28, G38, L22.

[1] The views expressed here are those of the authors and not necessarily the Bank for International Settlements.

The paper includes references to a number of private companies and financial service providers involved in corporate digital identity solutions. These references should not be construed as an endorsement by the BIS, the BIS Innovation Hub or any of the authors, nor do they imply any conclusion about the status of any product or service described under applicable law. They are instead offered as illustrative of new business models and emerging technologies currently being contemplated, proposed or offered.

Acknowledgements

For input in interviews and/or helpful comments, the authors thank (in alphabetic order by name of company or organisation): Shi Piao and Ida Yuan (Ant Group), Ficoal Dong (AsiaVerify), Rod Boothby (formerly Banco Santander), Frederic Boissay, Leonardo Gambacorta, Ross Leckow, Asad Khan, Cristina Picillo and Christian Schmieder (BIS), Kanwaljit Singh (Bill and Melinda Gates Foundation), Bryan Zhang (Cambridge Centre for Alternative Finance), Pascal Nizri (Chekk), Dante Disparte (Circle), Kay Turner (FinCEN at the US Department of the Treasury), Stephan Wolf (Global Legal Entity Identifier Foundation), Ben El-Baz (HashKey), Yvonne Tsui and Lai-chun So (Hong Kong Monetary Authority), Gerard Hartsink (ICC DSI Industry Advisory Board), Malcolm Wright (InnoFi Advisory), Brad Carr (formerly at Institute of International Finance), Oswald Kuyler (ICC Digital Standards Adviser and MonetaGo), Julia Walker (International Regtech Association), Claus Christensen (Know Your Customer), Edmund Lowell (KYC Chain), Myles McLaren (Kyckr), Ankur Patel (Microsoft), Robin Lee (Napier), Lewis McLellan (OMFIF), Rana Datta (Protiviti), Rob Leslie (Sedicii), Michael Sugirin (Standard Chartered Bank), Barte Claeys (SWIFT), Sijuade Animashaun (University of Hong Kong), Dirk Andreas Zetzsche (Université du Luxembourg), Ross P. Buckley (UNSW Sydney), Tracy Paradise (The Wolfsberg Group and HSBC) and Harish Natarajan (World Bank).

We thank Gun Wu Kim and Brian Tang (LITE Lab, University of Hong Kong) for research assistance, and Oonagh van den Berg, Martina Wojtaszek and Garima Agarwal of the Virtual Risk Solutions for consultancy support. We thank Nicola Faessler for editorial support and Louise Egan for support on communications.

Acronyms

5AMLD	Fifth Anti-Money Laundering Directive
4AMLD	Fourth Anti-Money Laundering Directive
ADB	Asian Development Bank
AML	anti-money laundering
API	application programming interface
BIS	Bank for International Settlements
BISIH	BIS Innovation Hub
CDD	customer due diligence
CFT	combating the financing of terrorism
CPMI	Committee on Payments and Market Infrastructures
DIACC	Digital Identity and Authentication Council of Canada
DID	Decentralised Identifier of the W3C
DLT	distributed ledger technology
eIDAS	electronic identification, authentication and trust services
EMDE	emerging market and developing economy
ESAP	EU Single Access Point
ESG	environmental, social and governance
FATF	Financial Action Task Force
FIU	financial intelligence unit
FSB	Financial Stability Board
GLEIF	Global Legal Entity Identifier Foundation
HKMA	Hong Kong Monetary Authority
IBAN	international bank account number
ICC	International Chamber of Commerce
ICCR	International Committee on Credit Reporting
ID&V	Identification and verification
IdM	identity management
IIF	Institute of International Finance
ISSB	International Sustainability Standards Board
KYB	know your business
KYC	know your customer
LEI	Legal Entity Identifier
LOU	local operating unit
NLP	natural language processing
OCR	optical character recognition
OGCIO	Office of Government Chief Information Officer
PCTF	Pan-Canadian Trust Framework
RBI	Reserve Bank of India
SME	small and medium-sized enterprise
SWIFT	The Society for Worldwide Interbank Financial Telecommunications
UBO	ultimate beneficial owner
UNCITRAL	United Nations Commission on International Trade Law
vLEI	verifiable LEI
VOC	verified organisation component
W3C	World Wide Web Consortium
WEF	World Economic Forum

Executive summary

Corporate digital identity (ID) provides electronic verification of the identity of a legal entity. In other words, in order to be "digital", the attributes associated with a corporate digital ID should be electronically captured, stored and made available to potential data users.

In many aspects of business and finance, customer identification and verification (ID&V) is a necessary first step. In financial services, it is not only driven by regulatory requirements, particularly around market integrity (such as anti-money laundering rules) and prudential objectives, but also by sound business and risk management practices, ie to avoid losses and fraud and to better understand customers and counterparties. Corporate digital ID has the potential to dramatically simplify the ID&V of legal entities and, thereby, to reduce the risks and costs of customer acquisition, counterparty analysis and doing business. It forms a kind of fast-track admission ticket for a legal entity to access financial and non-financial services. Beyond its core function in providing certainty of identity, corporate digital ID is able to offer further benefits by digitally linking to other information and attributes about that legal entity. This helps to facilitate know-your-customer (KYC) and other mandatory due diligence procedures, in addition to providing information about counterparties and customers central to the risks and opportunities being evaluated, whether business, finance or related to broader sustainable development objectives.

Corporate digital ID, as such, is foundational for operational efficiency, market integrity, financial stability and inclusion. By allowing private actors to demonstrate who they are, to know definitively who they are transacting with, and to integrate data from different sources, corporate digital ID overcomes information asymmetries, allowing better evaluation by investors, creditors, counterparties and others, and it supports trust. It also supports the work of public authorities – eg central banks, financial regulators and tax authorities – who need to know the full ownership and control structures of corporates.

There are a number of parallels with digital ID for individuals, yet corporate digital ID is not a mere extension of individual digital ID. Indeed, a legal entity may be part of a complicated corporate structure whose attributes (such as directors) may change frequently. Data privacy has very different implications for "legal persons" than for natural persons, in particular since most data protection regimes differentiate explicitly between personal and non-personal (eg company) data. That said, individual digital ID is a very significant complement to corporate digital ID, due to the need of external users to identify and authenticate individuals that claim to represent a company (eg directors authorising a transaction) and to enable interlinking of data and identities between companies, their representatives, owners and controllers.

A *unique* legal entity identifier is essential for any corporate digital ID solution since it is often confusing to identify a company just by its name, especially as a name can appear in different versions and different languages. Corporations are often identified by their business registration or company registry number. However, these systems are not standardised, generally not interoperable and often not digitised. Information is frequently unverified and not updated. The Legal Entity Identifier (LEI), developed in the aftermath of the 2008 financial crisis to simplify counterparty identification in financial markets, is a sounder starting point for corporate ID as it is global, unique and widely recognised. Yet enhancements are needed to increase its adoption rate in order to create network effects, notably outside the financial industry

and in emerging markets and developing economies (EMDEs) and small and medium enterprises (SMEs).

Related to these are efforts to develop decentralised identifiers (DIDs), led by the World Wide Web Consortium (W3C) DID Working Group. This initiative seeks to develop a set of standards to interlink different sources of data, under the control of the individual or entity. This is a "self-sovereign" framework to allow control and use of disparate data. Yet fundamentally, both corporate and individual systems require a base form of identification. This is increasingly seen to be best served as a public good infrastructure, provided by public authorities (as in India's Aadhaar or Singapore's MyInfo) or by the private sector with public standards and regulation. So far, corporate systems are developing more slowly, with the likelihood that a hybrid system involving both a base ID and linkages to other data offers the greatest potential.

Technological innovation can help in several areas to give shape to corporate digital ID and to enhance overall efficiency, market integrity, financial stability and inclusion. However, based on what we know today and can reasonably foresee in the near future, there is *no silver bullet* that can achieve all these benefits at once, nor can any single stakeholder drive all the needed changes. The *silver lining* is that, working together, these stakeholders can address the main pain points of corporate ID&V:

- *Corporate registries*: registries are indispensable in any corporate digital ID solution since they provide "golden source" data about companies. To enhance their role, they need to strive for better data openness, data availability (notably beneficial ownership data), data quality, digitalisation and data connectivity. Data should be verified for accuracy, regularly updated and made easier to access.
- *Banks and other financial institutions*: they collect and verify huge amounts of corporate data for their own operations and to meet regulatory requirements, and can use these data for corporate ID services. But sharing of such data, eg in the context of KYC utilities, is challenging. In many cases this requires legislative or regulatory action, as has been the case in credit information sharing systems and capital markets disclosure systems around the world.
- *Established vendors / service providers and emerging regtech firms*: large companies currently underpin most banks' and corporates' KYC and onboarding processes, and are now building new and innovative capabilities. Meanwhile, newer regtech firms use innovative technology to solve pain points in corporate ID&V. For example, they provide automated connectivity among multiple data sources and tools to extract information from corporate documents or unstructured data.
- *Regulators and policymakers*: in recent years a growing number of jurisdictions are building public individual digital ID systems, as highlighted by the World Bank's Identification for Development (ID4D) initiative and reflected in the UN Sustainable Development Goals (SDGs). While these systems interrelate with corporate systems, they are invariably separate, with both opportunities and challenges in building linkages. Regulators and policymakers have a key role in coordination, also across borders. This is seen particularly in the context of existing processes relating to tax information sharing and beneficial ownership disclosure (coordinated by the OECD), anti-money laundering / combating the financing of terrorism (AML/CFT) (coordinated by the FATF), OTC derivatives and financial infrastructure (coordinated by the FSB, CPMI and IOSCO), and others

such as capital markets data (coordinated by IOSCO and the ISSB), credit reporting (ICCR) and sustainability (ISSB).

This paper discusses innovative corporate digital ID solutions and the policy enablers that may be needed to support their adoption. It documents both the promise and risks of various solutions. In this way, it seeks to support policy efforts aimed at efficiency, market integrity, financial stability and financial inclusion, and thus broader sustainable development goals.

1. Introduction

The term "corporate identity" often conjures up an image of company trademarks, logos and branding. In order to project a consistent appearance to customers, vendors or investors, companies often use such symbols to demonstrate that disparate communications (letters, websites, advertising), persons (management, staff) and physical locations (offices, stores, warehouses) all belong to the same entity – the firm – and that this firm can be viewed as being the same entity across places and over time.[2]

Indeed, many firms take the form of a "legal entity", such as a company. A legal entity is a creature of individual legal jurisdictions. The company, trust and association laws and other legal frameworks enable the creation of legal entities and establish the necessary requirements. Each "legal person" created by national laws and (in the case of international organisations) international conventions has a unique, formal identity. Yet unlike natural persons (individuals), they do not have an objective identity or a physical body subject to physical or biometric identification. In order to denote a specific business, actors in both the public and private sector use a range of specific identifiers for a company. Common examples of identifiers are the company name, a registration number assigned by a corporate registry, a tax identification number issued by a tax authority, business licenses issued by specific governmental departments or exchange registrations for listed companies. The company name may not be a reliable identifier, as it can appear in different versions (eg full vs abbreviated, acronyms) and in different languages, and it may not be unique.[3] The corporate registration number is somewhat equivalent to a passport number or a driving licence number for an individual. However, complexity arises because corporations can contain many entities from many different jurisdictions in a given group under a single name, with each entity having its own company registration. These can then be combined with registrations and licences across a range of different jurisdictions.

Corporate identity (ID) is far more than an identifier. It is above all a tool for the identification and verification (ID&V) of a company and of its relationships with other companies within the same ownership structure. Functionally speaking, corporate ID is analogous to an admission ticket. With this ticket, a company is able to enter a

[2] Such symbols have been used as long as firms have been in existence. For instance, the Dutch East India Company, commonly understood as the first joint-stock corporation, used a stylised version of its Dutch acronym "VOC" as a logo on official documents, goods, ships and even on fortresses in locations around the world.

[3] In one recent example, the US Securities and Exchange Commission (SEC) halted trading of Zoom Technologies, a small Chinese technology company, that investors were confusing with the company Zoom. See Murphy (2020).

marketplace that provides a wide array of financial services (eg lending, insurance) and other services (eg customs and border clearing for import/export). Corporate identity is able to serve this function because it is linked to corporate information (known as attributes) associated with that company. Such attributes enable external parties to uniquely identify and verify the exact identity of the company and link that identity to other attributes essential for "know your customer" (KYC), due diligence and counterparty evaluation and risk management. The corporate ID in turn relates also to individual identification and signatures, whether physical ("wet"), digitised or digital, which are necessary for authorisation of individual transactions with, and actions, by the company.[4]

Such unique identification of companies is important for a range of reasons. Fundamentally, by helping actors to know which entity they are doing business with, corporate identity helps to reduce information asymmetries and to enable trust in economic exchange. Indeed, in pre-industrial societies, reputation and trust were often built among ethnically homogenous groups who could identify one another through shared cultural and kinship ties, thus allowing trade to flourish over long distances.[5] Technological innovations and legal institutions have helped to improve ID&V of companies, both within jurisdictions and across borders. This makes international trade and complex financial transactions possible between companies that we know in the modern global economy – thanks to the certainty that ID&V provides. Corporate ID plays an important role in counterparty identification for financial regulatory purposes, particularly in the context of over-the-counter (OTC) derivatives and credit, but also in an increasing range of other areas of financial regulation including capital markets disclosures and environmental, social and governance (ESG) reporting and monitoring.

On top of these basic business and financial needs, public authorities need to identify and verify private companies for policy reasons. Moreover, regulators in many jurisdictions also require ID&V of a corporate customer as the starting point for processes to pre-empt money laundering, terrorist financing and other financial malfeasance. According to the Financial Action Task Force (FATF), financial institutions should be required to undertake customer due diligence (CDD) measures on many occasions, such as when establishing business relations. The CDD measures to be taken are as follows:[6]

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the ultimate beneficial owner (UBO), and taking reasonable measures to verify the UBO's identity. For legal persons and arrangements this should

[4] Digital signatures often make use of cryptography, in which the relevant signed information is scrambled into an unreadable format and subsequently decoded for the recipient of the relevant signed information. This is different from digitised signatures, in which a document is typically printed, signed, scanned and sent. For details, see National Centre for Asia Pacific Economic Cooperation Working Group on E-Signatures (2022).

[5] A well-known example is the Jewish Maghribi traders, whose networks of kinship and trust allowed trade to flourish across medieval North Africa. More recently, Hokkien-Chinese rubber traders played an important role in mid-20th century Malaysia and Singapore. See Greif (1993) and Landa (1994) – seminal works on the economics of identity.

[6] Virtual asset service providers (VASPs) might be required to observe these CDD rules by effective procedures to identify and verify, on a risk basis, the identity of a customer. For details, see FATF (2021c).

include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

KYC procedures are relevant not just to banks and other regulated financial institutions. Under the FATF recommendations, countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. Non-banks are also subject to such compliance duties, and they are required to report suspicious transactions to the FIUs of their jurisdictions.

Corporate ID&V and complying with relevant laws are highly resource-intensive. This is part because such activities are necessarily adversarial, and firms and authorities are constantly working to keep up with the evolving practices of illicit actors. High-profile scandals and disclosures have also led to greater demands to combat illicit activity.[7] The rising demand for compliance with anti-money laundering / combating the financing of terrorism (AML/CFT) rules leads to a significant workload for the firms concerned. In a survey of treasury and finance professionals by EuroFinance and SWIFT in August / September 2019, 93% of respondents said KYC requests were more challenging now than they were five years ago, and 59% said that KYC requests are "much more challenging". Overall, a corporate treasurer typically has to spend 10% of his or her time to meet KYC requirements.[8] This was of course prior to the massive expansion of digitisation globally driven by Covid-19.

In addition to KYC and AML/CFT, tax policy provides another reason to focus on corporate identity. In 2015, following a request of the G20, the OECD agreed on a common framework for automatic exchange of information on accounts of their respective citizens. The "Common Reporting Standard" (CRS) has been implemented by over 100 jurisdictions across the world as of October 2021. A similar initiative applying to transparency of beneficial ownership. In October 2021, 137 countries agreed on a global minimum corporate tax rate of 15% to prevent firms from shifting profits to low-tax jurisdictions. In order to enforce these rules, the tax authorities of many jurisdictions have a vital interest in understanding the complete ownership and corporate structure of tax-reporting companies. This is all the more important since, for tax purposes, subsidiaries of multinational companies are treated as independent entities that buy and sell goods and services from each other.[9] These issues have become very clear to financial institutions and others seeking to identify ownership

[7] The Panama Papers, Paradise Papers, FinCEN files, 1MDB scandal and opaque corporate structures used by sanctioned individuals to mask asset holdings are just a few illustrations of the challenges that corporate ID&V presents.

[8] For details, see SWIFT and EuroFinance (2019).

[9] For details, see GLEIF (2021).

and control of counterparties and customers seeking to comply with the myriad of sanctions on individuals and entities in the context of the Russia-Ukraine war.

Last but not least, corporate ID&V is relevant to legal entities in the public sector as many public sector agencies behave like corporates, and procurements account for a significant share of public expenses. Like private firms, these public sector agencies experience pain points in the process of corporate ID&V, though often to a lesser extent.

What is corporate digital identity?

Digital innovation can further facilitate ID&V of companies, through corporate digital identity (ID).

In order to be "digital", the attributes associated with a corporate digital ID should be electronically captured, stored and made available to potential data users. Unlike its paper-based equivalent, a digital system offers much greater functionality. In particular, linking to attributes is potentially automatic, thus facilitating remote retrieval and authentication of the corporate data by external users. Moreover, if attributes are well-structured and machine-readable then they can be easily collated and analysed by computer algorithms. In order to serve this purpose, these attributes must be verified, verifiable, secure and trusted by all of the parties involved, as well as ideally recognised for legal and regulatory purposes.

Apart from these core features, a relatively new but noteworthy concept is "self-sovereign" digital ID, which gives companies greater control over their identity. For example, they can give access rights to certain data (eg only selected aspects of verifiable credentials) to selected parties. The access right to these attributes may be managed in a decentralised manner so that the ID subjects do not depend on third-party providers to store and centrally manage their data. Through these solutions, which are sometimes based on distributed ledger technologies (DLT), owners are able to decide which parts of their verifiable credentials are to be shared with which parties. That is, all the data-sharing should be conducted on the basis of consent. In addition to private systems, similar systems have been developed to network sovereign individual identity information spread across a range of different – often "golden source" – databases, sometimes offered by private firms, in other cases on the basis of network public infrastructure such as India's Aadhaar, Singapore's MyInfo or Hong Kong's iAMSmart system.

Note that the above definition of corporate digital ID applies to different type of digital ID issuers. In other words, the issuer can be a national or local government, a consortium of private-sector firms or a non-profit organisation. The key is that the underlying data are supplied by a trustworthy provider (eg a government agency, international organisation or other trusted party) and linked to some form of trustworthy core digital identity so that users see a digital ID as reliable. In some cases, the identity can even be issued by the company itself, provided that the corporate identity is verifiable by trustworthy data, and technological solutions could ensure that the identity, once verified, cannot be further tampered with.

What else does corporate digital ID facilitate?

A well-run and widely trusted corporate digital ID system helps a company and its representatives to prove they are who and what they claim to be. Beyond this, a sound

corporate digital ID has benefits in four broad categories: (1) operational efficiency, (2) financial inclusion, (3) financial stability and (4) market integrity (Arner, Zetzsche, Buckley and Barberis, 2019).

Operational efficiency

Compared to traditional paper-based or face-to-face approaches of identifying and verifying a company, a reliable corporate digital ID system has the potential to boost operational efficiency and reduce manual workload substantially, reducing transactions costs. Such a cost reduction gives a company the capability to access more services and interact with other parties, without having to resort to human intervention or physical documentation. Anecdotal evidence suggests that it could shorten the time required for a financial institution to complete its KYC, CDD, AML/CFT and other due diligence procedures for onboarding a new corporate customer – from a typical period of five to six weeks currently to within a few days or even less for an SME. In the context of sovereign individual ID systems such as Aadhaar in India the reduction in time and costs of bank account opening have been dramatic, from weeks to minutes and from $15 to 7 cents per account (D'Silva et al, 2019). Furthermore, since the global outbreak of the Covid-19 pandemic in early 2020, remote customer onboarding and ongoing CDD have increasingly become necessities and not just nice-to-have features. This is because it has been very challenging to conduct business using the traditional face-to-face and paper-based approach when lockdown measures are imposed and cross-border business traveling is severely restricted. In this context, most significantly, the FATF recognised in 2020 that sovereign digital ID is at least as good as sovereign physical ID, thereby putting in place the foundation for regulatory recognition of such systems globally.

Efficiency gains resulting from corporate digital ID are not confined to the narrow sense of reducing the cost of compliance by banks and other regulated financial institutions. In addition to cost-cutting, errors due to manual processing of data and inconsistencies in human judgment can also be minimised. In fact, being able to better identify customers and counterparties has important benefits for market integrity and reduction of fraud and crime as well as enhancing the risk management of financial institutions. In a broader sense, it facilitates commerce by shortening the time for approval and reducing the requirements for credential documents during an application process – efforts that are sometimes unnecessarily duplicated when a company begins a relationship with another financial institution.

Financial inclusion

Financial inclusion is often considered in light of individuals, but it is also relevant with regard to small and medium-sized enterprises (SMEs). Access by SMEs to financial services can be enhanced by corporate digital ID since a reliable and well-run corporate digital ID system can address information asymmetries. Such asymmetries are often more severe for SMEs than for large corporates, as the former typically lack accounting records and a long operating history. As such, financial institutions tend to prioritise larger corporates, often at the expense of SMEs, even though the latter also contribute significantly to the global economy.[10] By reducing the cost of identifying and verifying a company, a digital ID system streamlines the

[10] For example, micro, small and medium-sized enterprises account for around 70% of employment globally, approximately a quarter of GDP in low-middle income countries, and over 50% of GDP in Organisation for Economic Co-operation and Development (OECD) countries (ILO, 2019).

costly KYC and AML/CFT processes, thus alleviating a significant disincentive to provide financial services to SMEs. The system can also integrate with other solutions (eg trade document digitisation, credit risk profiling by alternative data) that further lower the information barriers for SMEs and corporate borrowers in EMDEs to obtain external financing. From a system-wide perspective, the outcome can be a more efficient allocation of resources through the reduction of market frictions. As highlighted above, individual digital ID is now seen as a core tool for enhancing financial inclusion, with the lessons increasingly also being directed towards the challenges facing SMEs.

Easier ID&V of firms can also help to formalise activities that are currently informal, ie hidden from authorities for monetary, regulatory and institutional reasons. Particularly in emerging market and developing economies, firms in the informal economy are important producers of goods and services and an important source of income for many individuals, but often find navigating formal processes to open a business or file taxes to be unduly cumbersome. Corporate digital ID can lower these costs and provide concrete benefits to informal firms, thus opening the door to legal protections and benefits and formal financial services (eg entering the formal economy, credit history can be established, and by implication the greater ability to borrow to grow the business). In this way, such reforms can support wider economic growth, employment and legal protections, and help to bring currently unrecorded activities into national accounting.

Financial stability

A well-run corporate digital ID system is also conducive to financial stability, as it increases the transparency of financial markets. In particular, corporate digital ID makes it easier to identify the interconnections among counterparties and thereby locate potential risks of excessive concentration. Such transparency is an essential prerequisite for the implementation of the Basel core principles for effective banking supervision, notably Principle 19 that covers concentration risk and large exposure limits, and Principle 20 that covers transactions with related parties (BCBS, 2012). In the 2008 financial crisis, data gaps resulting from the opacity of asset-backed securities made it very challenging for policymakers to fathom the extent of contagion risks, with significant macroprudential implications. This was also a key element in weaknesses in the global market for OTC derivatives which emerged in the context of the failure of Lehman Brothers in 2008. The introduction of the Legal Entity Identifier (LEI) recommended by the Financial Stability Board (FSB) in 2012 is a system to remedy to this lack of asset and firm-level transparency. Digital IDs based on the LEI could be an important mechanism to broaden the use of corporate digital ID (ESRB, 2021).

Market integrity

A reliable corporate digital ID can foster financial market integrity since it improves the effectiveness of fraud detection, reduces the criminal and terrorist use of the financial system and helps authorities and companies to combat corruption and tax evasion. Such an improvement is not confined to the onboarding of a corporate customer (FATF, 2020). The ability of financial institutions to digitally capture changes in the structure of the legal entities (including change of the ultimate beneficial ownerships and directorships), plus solutions to enable transaction monitoring in real time and on an ongoing basis, can be a game changer in the AML/CFT space. This can reduce the leeway for criminals and terrorists to exploit information asymmetries

amongst banks located in different jurisdictions. Such systems are also central in the context of transparency for corruption and taxation purposes as well as very significant in the context fraud, market manipulation and financial crime.

How can corporate digital ID work?

Conceptually, there are two modes of operation for corporate digital ID solutions: (1) a centralised model and (2) a decentralised model. The former presupposes a central party such as a corporate registry in charge of collecting all relevant information about companies and coordinating the activities of other parties. The merit of this model is that it is generally consistent and efficient. In addition, interoperability might not be a big concern since similar formats and structure of data allow for the use of application programming interfaces (APIs). However, the requirement for the central party in terms of technical capacity is tremendous. It also runs the risk of a single point of failure or a single target for potential hackers' attacks, as has arisen eg in the case of Equifax, a major credit information provider.

Conversely, in a decentralised model, the identity data are provided by multiple parties, sometimes coordinated by the use of DLT such as blockchain. The merit of this model is more flexibility and lower risk otherwise increased by a single point of failure. Yet this requires a well-defined, widely-accepted and well-executed governance model so that all participants have sufficient trust in the decentralised model. And access to data is another issue – this approach does not allow for a holistic view to begin with, and it may require a lengthy process for all the pieces in the system to be aggregated.

A third option is a hybrid approach, where there may be a single source of corporate identity (such as a company registry), but the various attributes and data are then linked in a network structure, linking disparate sources of data to the central point. This model is becoming increasingly common in the context of individual ID, given the risk of concentration in the centralised model and the coordination challenges inherent in the decentralised model. MyInfo in Singapore and Aadhaar in India provide useful examples: a single sovereign individual identity links to a variety of golden source data in various sources; data are not aggregated in a single point but rather linked as needed for different purposes under the control of the individual. It is also emerging in the context of corporate digital ID.

Corporate digital ID vs individual digital ID

The development of jurisdictional corporate digital ID is far more challenging than jurisdictional individual digital ID. Individual digital ID solutions have already been well-established in a number of jurisdictions (eg public sector systems in Estonia, Hong Kong SAR India and Singapore, and public-private systems in Denmark and Sweden) are being developed. Yet it is not straightforward to extend and transfer their experiences to corporate digital ID.

Some challenges of corporate digital ID include:

1. The core attributes of a company (eg directors, major shareholders and ownership structure) are usually much more numerous and complicated than those of an individual (eg name, gender, country of birth, date of birth). What counts as essential attributes might also depend on the industry or sector in which a company operates. Furthermore, these attributes are usually subject to

more frequent changes, thus requiring a solution that accommodates updating data on an ongoing basis. All these could be complicated by the legislation of individual jurisdictions.[11]

2. A company may have complicated and nested ownership structures, with some of its affiliated companies located and/or incorporated across multiple jurisdictions, thus making it difficult to identify the ultimate beneficial owners. This is particularly true if some of the associated companies are incorporated in corporate registries that do not require the submission of UBO information or restrict public access to such information.

3. For business processes involving more than one jurisdiction (eg trade and foreign direct investment), a corporate digital ID solution may need cross-border harmonisation of data standards and mutual recognition, on top of the usual technical requirements. While individuals in cross-border activities also face such issues, corporate digital ID is particularly challenging due to the complexity of corporate attributes. For example, different jurisdictions have different forms of legal entities, which may make it more difficult to harmonise across borders.

4. There are very different demands on data privacy and confidentiality. While individuals keep their attributes (name, date of birth), address and transactions private for personal reasons, related to fundamental rights of data privacy firms do so for business reasons, eg to prevent competitors from gaining insights on future plans or intellectual property. Balancing these legitimate demands for confidentiality as well as data regulation requirements (such as localisation) with the prevention of fraud and abuse can be a key challenge.

Nonetheless, a well-established individual digital ID is very important support for corporate digital ID. Indeed, a company conducts its business through representatives such as staff, agents, directors and major shareholders. To accomplish end-to-end identification of a company, a corporate digital ID solution ideally should be seamlessly integrated with an effective individual digital ID solution so that the identification process does not fail when it comes to the final task of identifying the company's representatives, directors and owners (NCAPEC, 2022). This may happen if, for example, paper-based documents are needed to identify the individuals representing the company. This can be seen as particularly important in the context of SMEs, where there may be little differentiation between the financial and other history of the individual owner(s) and the business.

Many jurisdictions are focusing on corporate digital ID platforms after the development of an individual digital ID system. For example, in Hong Kong SAR, the Office of the Government Chief Information Officer (OGCIO) has been working with the Hong Kong Monetary Authority (HKMA) on a proof-of-concept (PoC) trials and research on the business version of the "iAM Smart", which is an individual digital ID platform.[12] The first phase of the PoC have been completed in the second quarter of 2021. Based on the PoC results, OGCIO is currently exploring the feasibility of devising a sustainable development proposal through a public-private partnership approach and will continue to deliberate with the HKMA and other stakeholders on rolling the

[11] Take for example the entity legal form code list – each legal form has a specific legislation in a specific jurisdiction and the developing organisational roles standard – each entity legal form in each jurisdiction will have specified roles recognised in local legislation.

[12] For details, see https://www.iamsmart.gov.hk/en/

next phase of digital authentication of business identities. Issues for deliberation include assessing the acceptability by industry of the proposed solution and exploring its application, the governance framework of the platform and the detailed implementation plan. Once a consensus among relevant stakeholders on the implementation plan is reached, a sandbox test will be conducted for assessing, among other things, system security, protection of users' privacy and compatibility with related platforms. with a view to working out the feasibility of the sustainable development of the platform, as well as to performing the corresponding legal and regulatory consultation.

In sum, corporate digital ID can support many economic and societal benefits, but it is highly challenging. Different stakeholders each hold a piece of the puzzle – ie just one part of the overall solution. This is quite different from individual sovereign digital ID systems, which will often require centralisation of control of the core elements with one player in an individual jurisdiction. Because corporate digital ID involves a wider range of participants across different jurisdictions, it is less subject to the potential centralisation through a single actor in a single jurisdiction. Cross-jurisdictional issues become even more challenging from the standpoint of coordination.

Private innovation is ongoing, contributing new potential tools and approaches. In addition to traditional vendors offering KYC services, some banks have recently established consortiums to provide corporate ID services, thus capitalising on the corporate ID data that they collect and verify to meet regulatory requirements. Big techs (eg major social media platforms and internet browsers) are also becoming *de facto* digital ID gatekeepers. Using the data generated from their e-commerce platforms, they offer ID solutions that allow their users (both individuals and firms) to authenticate on third-party websites and services with their user profiles. Successful fintech start-ups in the payment space are exploring efficiencies and economies of scale through better automated corporate ID&V. Regtech start-ups are also increasingly catering for corporate ID&V solutions.

Given the corporate digital ID solutions currently available, the most likely outcome in the foreseeable future is that different approaches are used in different areas and use cases. Corporate digital ID solutions suitable for large multinational corporates might not be applicable to SMEs. Although new technologies (eg blockchain and APIs) could tackle some bottlenecks, a corporate ID system still needs to overcome hurdles from other sources, such as legal and regulatory issues. This work is far from finished, but there is an increasing consensus around the value and importance of the public and private sector seeking common development approaches and solutions.

Research objectives

Against this background, this paper seeks to investigate the current landscape of corporate digital ID. Our research has a practical orientation so that stakeholders, including policymakers and industry practitioners, are better informed about possible opportunities, recent innovations and the way forward. Specifically, the objectives of the research are as follows:

- To understand how corporate digital ID solutions can alleviate the pain points of corporate ID&V, notably for SMEs that usually face a high hurdle in accessing banking and financial services.

- To compare current corporate digital ID solutions and forthcoming initiatives, examining their strengths, limitations and suitability for different types of use cases.
- To investigate why the adoption of corporate digital ID is relatively low in many countries, and explore possible remedies that would potentially overcome the hurdles to adoption.
- To highlight potential opportunities to build on existing international regulatory cooperation processes in order to support the wider objectives of efficiency, financial stability, market integrity, financial inclusion and sustainable development.

Research approach

In order to investigate the pain points of corporate digital ID from different perspectives and explore the potential solutions to these pain points, we conducted qualitative interviews with various stakeholders, such as banks, bank-related organisations, e-KYC and other fintech solution providers, policymakers, international organisations, academics and industry experts. Some of these interviews were arranged by the consultancy firm Virtual Risk Solutions. We also participated in ideation workshops organised by the ICC Advisory Group on Trade Finance (ATF) and the BIS Innovation Network Working Group of Open Finance. Moreover, the Institute of International Finance (IIF) set up two focus groups to discuss the core issues in corporate digital ID with major banks and financial institutions. Through these channels, we exchanged views with and obtained insights from industry practitioners and policymakers. During our research process, more than 70 meetings were conducted. The views obtained in these meetings are analysed and supplemented with information from other sources, such as a literature review and a written survey of the stakeholders.

2. Regulatory landscape and digital standards

As a starting point to identify and verify a business, corporate digital ID is an essential part of understanding a counterparty. In addition to its centrality from the standpoint of business processes and risk management, it is also an important element of regulation, particularly financial regulation, but also of data regulation and a range of other regulatory requirements.

From a regulatory standpoint, market integrity regulation addressing AML/CFT focuses on processes of initial and ongoing customer due diligence. AML requirements are a major focus of financial regulation and compliance globally and therefore a major focus of attention for businesses and regulators. AML/CFT requirements are a cost particularly in the context of customer acquisition. They also often form a barrier to financial inclusion, both for individuals and businesses, particularly SMEs. Therefore, it is important to understand the AML/CFT regulatory landscape and how corporate digital identity can play a role in it. Internationally, joint efforts in AML/CFT have a long history, dating back to 1989 when the Group of Seven nations launched the FATF. The FATF and its standards have brought significant

changes to the ways that banks and businesses around the world conduct their affairs through regulatory changes in laws and in governmental operations.

In addition to the direct role of the FATF, a range of other international financial regulatory standard-setters have also incorporated related standards, including the Basel Committee on Banking Supervision (BCBS) and International Organization of Securities Commission (IOSCO). As one landmark in the regulatory landscape, in 1997, the BCBS issued the first "Core Principles for Effective Banking Supervision".[13] It states that "*Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict 'know-your-customer' rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements*". It also urges nations to adopt the FATF's 40 Recommendations.

The 2008 financial crisis highlighted systemic risk within the global financial system, leading to a range of regulatory reforms and related market initiatives to protect the financial system. From the standpoint of corporate digital ID, a major initiative emerged to better identify legal entities involved in complex financial transactions such as OTC derivatives and asset backed securities, particularly those involved globally systemically significant financial institutions (G-SIFIs). As one aspect, the G20 mandated the FSB to establish a global system for legal entity identification in order to better understand interconnections between institutions, transactions and markets. The resulting identifier was embedded in new international standards from the FSB, BCBS and IOSCO and their implementation across G20 / FSB members. One aspect of this process involved the creation of new "Legal Entity Identifiers" (LEIs) and their use in a range of post crisis financial regulatory reforms.

In 2012, a revised set of measures and recommendations from the FATF came into force. These recommendations at a high level require all countries to have effective systems for preventing and addressing money laundering, terrorist financing and the financing of proliferation. They set out measures that countries should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and other businesses and professions; measures to ensure transparency on the ownership of legal persons and arrangements; the establishment of competent authorities with appropriate functions, and powers and mechanisms for cooperation; and arrangements to cooperate with other countries. As countries have diverse legal, administrative and operational frameworks and different financial systems, they cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances, with implementation in turn monitored by the FATF.

At the same time, from around 2016, also arose an increasing international recognition of potential conflicts between market integrity objectives in the context of AML and wider developmental and inclusion objectives in the context of financial inclusion, reflected in the idea of "de-risking" both from the standpoint of the emergence of significant barriers to individuals and SMEs in individual countries, particularly developing countries, and from the standpoint of exclusion of large segments in the context of reduction of correspondent banking relationships (see Rice et al, 2020).

[13] These principles have been integrated into the Basel core principles. For details, see BCBS (2012).

2.1 Legal Entity Identifier (LEI)

Corporate ID&V typically starts with a corporate identifier, which ideally is a unique mechanism to distinguish one company from another. Historically, corporate identification has mainly come from company registries in individual jurisdictions. A company is a legal entity, a creature created by law, in most cases under the standardised legal framework of a given jurisdiction's company law as implemented by the domestic company registry, but in some cases directly via legislation. Creation of a company thus involves the filing of certain required documents and information and the paying of necessary fees. In exchange, the company registry registers – creates – the legal entity: the company. Each company is then identified by a name and also typically by a company registration number. In addition to the company registry number for a given entity (and a group could include many entities across a range of jurisdictions), a company will also typically have a tax registration number in one or more jurisdictions and also possibly a range of licenses and license numbers, in addition to a registered address, contact information, directors etc. There may also be separate numbers for individual shares in one or more custodians as well as numbers for any listings on exchanges. While each of these numbers may be unique in a given jurisdiction, there is generally no standardisation across jurisdictions and no harmonised system of corporate identification.

With greater globalisation of business and finance, this has become an increasing source of inefficiency and risks from the standpoint of financial stability, market integrity and investor protection.

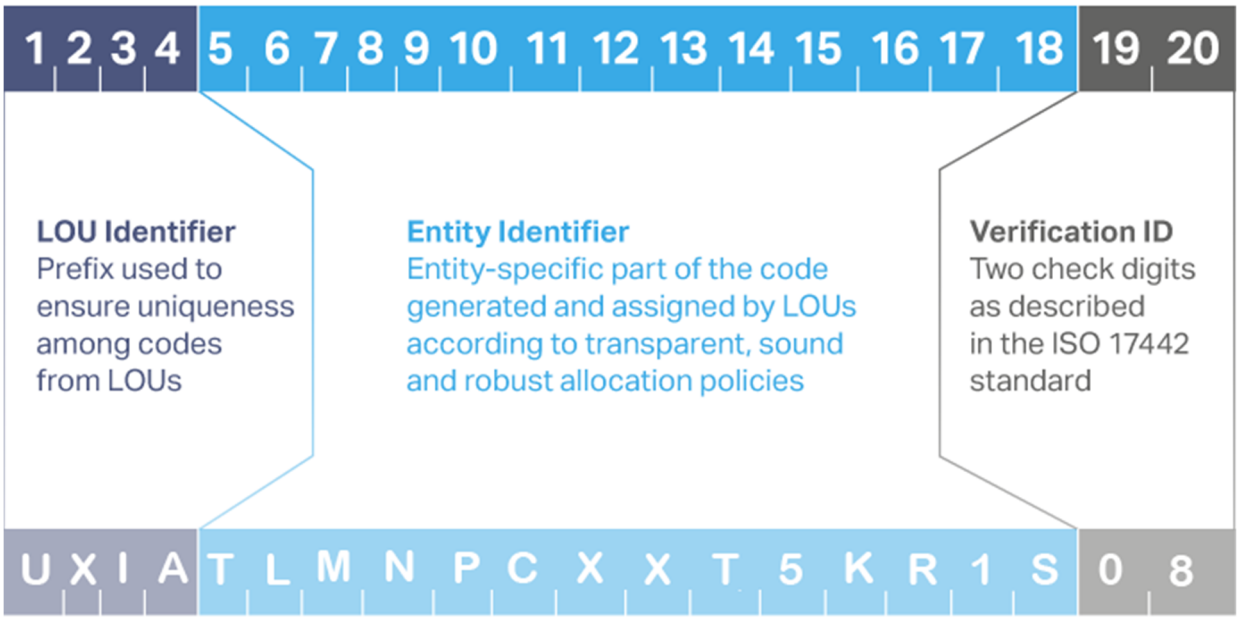
In response to the clear gaps in ID&V of legal entities in complex transactions before the 2008 financial crisis, the G20 mandated that the Global LEI was launched in 2012 as a global system of corporate identification. Each registered entity receives a unique LEI under a system administered by a not-for-profit organisation, the Global LEI Foundation (GLEIF), and designed in accordance with the ISO 17442 standard. The LEI is a 20-character alphanumeric code that uniquely identifies a legal entity. It is not necessarily the same as a company registration number – which is jurisdictional by nature - but does seek to provide a universal system of designation for individual entities to enable their identification and tracking across global markets.

Using the BIS as an example, the LEI is structured as follows (Graph 1):

- Characters 1-4: represent the LEI issuer known as Local Operating Unit (LOU)
- Characters 5-6: two reserved characters currently set to zero
- Characters 7-18: entity-specific part of the code generated and assigned by LOUs
- Characters 19-20: two check digits as described in the ISO 17442 standards

In this example, the BIS is not a traditional corporate entity. While it is in fact a company limited by shares (held by 63 central banks), it also has the characteristics of a public-sector international organisation. Still, the format used is the same as that of other public and private entities, and it can use this for ID&V purposes. Note that a LEI represents a single legal entity and that many business groups consisting of multiple subsidiaries have more than one entity.

The LEI of the BIS Graph 1



Example: Bank For International Settlements

Source: GLEIF.

The LEI complies with two fundamental principles:

1. **Uniqueness**: Once assigned to a unique entity, the code would not be assigned to another entity, even if the initial entity ceases to exist.
2. **Exclusivity**: A legal entity that has obtained an LEI cannot obtain another one. Entities may port the maintenance of their LEI from one operator to another, but the LEI remains unchanged in the process.

A key feature of LEI is that it is a *global* identifier for legal entities, meaning that uniqueness and exclusivity principles apply at global level and the LEI validity is not confined to a particular jurisdiction, sector or industry, and it is well recognised all over the world, with over 220 countries and jurisdictions having LEI service availability. This is different from local identifiers (eg registration number issued by a corporate registry) that are valid only within a particular jurisdiction and are not standardised and unique across jurisdictions and thus usually not recognised beyond the national borders. Obviously, for the purpose of transactions involving multiple parties across borders, such as trade finance and foreign investment, a global identifier is preferrable to a local one.

Additionally, the global identity links to the local business registration within the LEI reference data. The LEI and its referenced data are supported by a not-for-profit Swiss Foundation (GLEIF) overseen by a Regulatory Oversight Committee (ROC) composed of more than 65 financial markets regulators and other public authorities and 19 observers from more than 50 countries. The drivers of the LEI – the G20, FSB and many regulators around the world– have emphasised that the LEI is a broad public good. The LEI and its reference data are made available by GLEIF conveniently and free of charge.

Beyond their initial regulatory application in the context of identification of counterparties in complex transactions (such as the OTC derivative transactions) and institutions (particularly significant in insolvency), LEIs are also being used for a range of other purposes, including market integrity requirements (AML/CFT), investor protection requirements (listing identification, ongoing disclosure requirements and trade reporting) and taxation. A new G20 initiative focusing on transparency of beneficial ownership of entities is being operationalised internationally by the OECD and FATF and implemented on a jurisdictional basis, bringing together many of these pieces. They also offer opportunities in the context of new ESG reporting requirements, including in the context of the proposed EU Single Access Point (ESAP), intended to standardise and centralise reporting of all EU listed company reporting under both capital markets and ESG regulation.

According to a joint study by McKinsey and GLEIF,[14] the LEI can allow for savings of at least 10% of total operations costs for client onboarding and trading processing for banks that adopt it. For the broader investment banking industry alone, this would yield savings of over $150 million annually. Banks in trade financing could save an additional $500 million per annum overall by using the LEI in the issuance of letters of credit. Further savings are likely from the reduction of spending on seller identification for e-invoicing, and from a more automated process for commercial credit extension.

These savings not only enhance efficiency, financial stability and market integrity but also reduce the costs and risks of customer acquisition, and they can also enhance goals of financial inclusion and broader balanced sustainable development, with particular potential in the context of SMEs.

Reference data

Each LEI is linked to a set of reference data about the legal entity to be identified. Basically, reference data consist of: (1) business card information: answering the question "who is who" and (2) relationship information: answering the question "who owns whom". As such, anyone can go to the official website of the GLEIF, enter the LEI of a company into a box, and then retrieve the reference data about this company, without paying any charges. As the data are already verified by the LEI issuer, often using information from local registration authorities, users can trust the validity of the data and treat this as the starting point for further business processes such as KYC and AML/CFT checks.

How does LEI work?

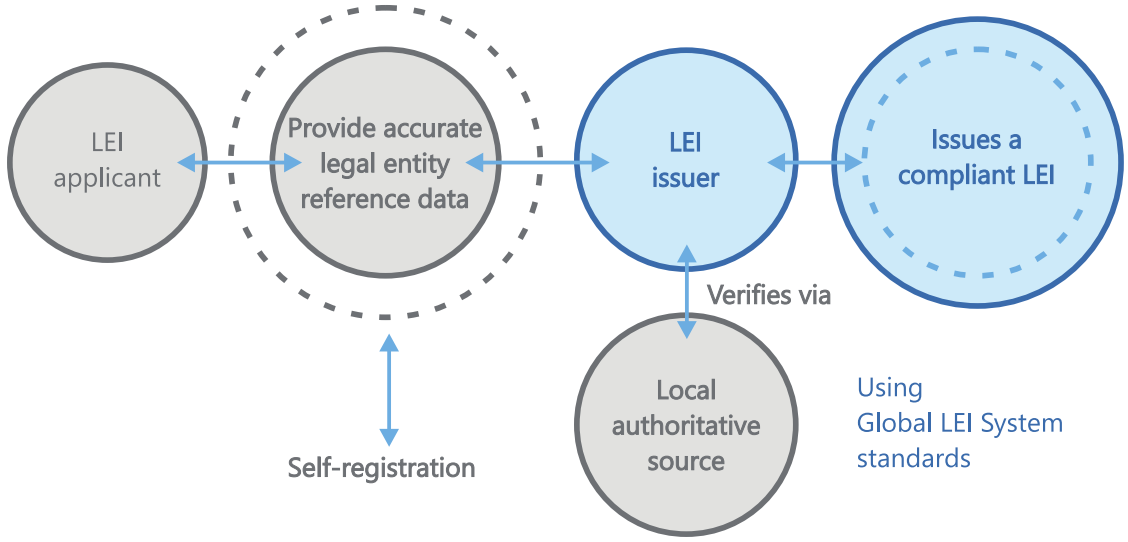
Companies file an application for a LEI by means of self-registration with their chosen LEI issuer (LOU), which is accredited by the GLEIF. The process is analogous to that by which they are incorporated and registered in a corporate registry (Graph 2): The LEI issuer has then a function of validating the self-reported information against a local authoritative source, such as company registries, and ensuring uniqueness and exclusivity of the LEI. As of January 2022 there are 3,841 LEI issuers serving 226 countries worldwide, and a company can choose any LEI issuer that is accredited for

[14] For details, see McKinsey & Company (2019) and the GLEIF (2017). *The Legal Entity Identifier: The Value of the Unique Counterparty ID*.

its jurisdiction to apply for a LEI. This design is to maintain competition among LEI issuers so that the application fee is subject to market discipline.

A quality control program is applied to ensure the validity of the LEI data record. The program includes: (1) annual validation of all data elements in every LEI record, (2) an option for external users to dispute the data elements, and (3) a GLEIF-managed quality program which scans the full repository daily and publishes the results monthly in free quality reports at the global and individual LEI issuers level. Note that company registries typically do not offer similar types of quality programs for the corporate data they provide. Rather, most company registry data is declarative – provided by the registrant – and independently checked. As a result, it often requires validation by counterparties and others for simple errors like misspelling of city names.

Issuance of an LEI — Graph 2



Source: GLEIF.

Origin and adoption of the LEI

The launch of the LEI can be traced back to the global financial crisis in 2008–9. During the crisis, one of the toughest issues was identifying the tens of thousands of entities having financial exposures to or being owned by a financial institution on the verge of collapse, with these entities located at multiple jurisdictions. In response to this challenge, the G20 chose a federated model composed by a central unit, the GLEIF,[15] and the LOUs, overseen by the ROC.[16] The mission of GLEIF is to support, on a not-for-profit basis, the implementation of a Global LEI System to make high-quality LEI data available free of charge to users in both the public and private sector.

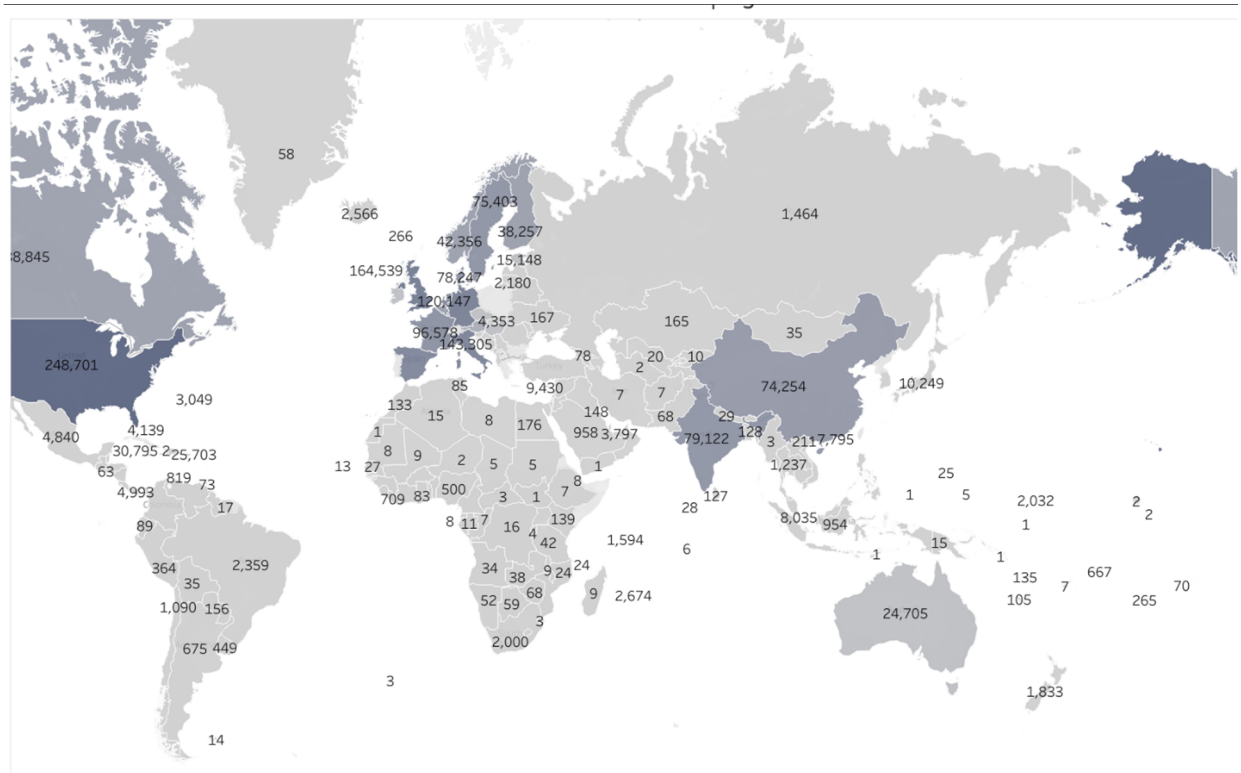
[15] For details, see https://www.gleif.org/en/

[16] For details, see https://www.leiroc.org/

Reflecting its history, use of LEI was initially confined to financial institutions, and financial instruments traded in OTC markets. As at 22 March 2022, 129 regulations and laws globally mandated LEI use largely in financial services reporting.[17] Yet the design of the LEI is agnostic to industry type. In recent years, LEI adoption has been extended to non-financial companies. Globally, there were 1.95 million active LEIs at the end Jan 2022, with the bulk of them located in advanced economies, eg in Europe (Graph 3). China and India are among the top jurisdictions by growth in recent quarters and both countries have initiatives under way that leverage the LEI. In November 2020, the People's Bank of China, China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission and State Administration of Foreign Exchange jointly released a roadmap, outlining key milestones of LEI adoption for 2020-2022. Besides, the Reserve Bank of India mandated that, effective from 1 April 2021, all entities conducting payment transactions of value INR50 million (~USD 650,000) and above for real-time gross settlement and National Electronic Funds Transfer should be identified with the LEI. On 21 April 2022, the RBI further announced that non-individual borrowers of INR50 million and above should be required to obtain LEI codes according to a 2023-2025 timeline, depending on the loan amount. In the longer term, the GLEIF estimates that, over time, between 200–400 million legal entities could be eligible for an LEI.

Global adoption of LEI

Graph 3



The graph shows the total number of active LEI by jurisdictions.

Source: GLEIF.

[17] For details about LEI regulatory requirements by country/region, see https://www.gleif.org/en/lei-solutions/regulatory-use-of-the-lei.

How can LEI be further enhanced?

As a tool to identify entities such as companies, the LEI is powerful since it is truly global in nature. In addition, as information associated with the LEI is validated, users have a higher level of assurance regarding its authenticity. However, LEIs alone can only resolve certain pain points in ID&V, thus calling for further enhancement.

The LEI has a crucial role in today's digital economy given its ability to provide companies with unique, permanent identification globally. This is especially important in the context of identifying legal entities involved in digital transactions. LEI delivers value to both the more mature product – digital certificates – and the more recent innovation of verifiable credentials. Compared to other corporate digital ID solutions, it is further along in the so-called "hype cycle" (Gartner, 2022), having demonstrated its effectiveness over time. Still, further efforts are needed to increase adoption. Key to this is likely to be a combination of:

– international guidance recommendations:
    - recommendations regarding sanctions, customer due diligence, and wire transfers could include the LEI as identifying information for sanctions lists or the primary means of identification for legal entity customers or beneficiaries (FATF recommendations 6, 10 and 16),
    - BCBS could update its current recommendation of the LEI as a complementary information to be part of the minimum requirements set out in the Guidelines for sound management of risks related to money laundering and financing of terrorism.
– regulatory requirements (especially banking, market integrity, capital markets, tax and ESG regulatory reporting), and
– market demand, as investors and counterparties find the efficiencies increasingly valuable.

Focusing on the market demand in the short to medium term, there are four critical steps that could potentially enhance LEI and boost its adoption rate:

(a) Verifiable LEI (vLEI)

- LEI *per se* is simply an identifier telling one legal entity from another. When a LEI is provided to external users such as banks and suppliers, they still need to undertake the verification and authentication process to ensure that the company and its representatives (eg officers, general staff, directors) are really what or who they claim they are. This process can be painstakingly slow and inefficient. This is possibly a major reason that discourages banks from onboarding SMEs, as banks generally perceive it unprofitable to undertake the verification process, even if a SME has already obtained an LEI.
- In order to improve the above-mentioned verification process and mindful of the increased needs to empower entities in the management of their identity in digital contexts, the GLEIF launched the verifiable LEI (vLEI) in early 2021, and the vLEI Ecosystem Governance Framework was released in February 2022. Its basic idea is to embed the LEI in a digital document of a company. The digital document format for the vLEI is based on the W3C Verifiable Credential and Decentralised Identifier standards. These standards provide interoperable mechanisms for verifying the authenticity of the vLEI. Section B provides more details about these standards.

- By increasing the expected benefits of a LEI, the vLEI initiative could potentially boost the LEI adoption rate, notably for SMEs. To many SMEs, the application fee of a LEI and the annual renewal fees, though not negligible, are not prohibitively high. One of the reasons why they have little interest is that they perceive few material benefits in obtaining their LEIs. There are also relatively few direct regulatory requirements for LEIs that extend to SMEs. This could be supported by outreach and digitisation initiatives with support from international and other organisations. If viewed as a public good, corporate registry systems could benefit from an initiative similar to ID4D.
- The vLEI initiative may benefit from further integration with local authorities, who should inform the GLEIF immediately (or almost immediately) about any changes in the structure of the legal entities. This could be done for instance through digitisation of processes of domestic company registries, including requirements for verification and ever-greening of data submitted. This would have tremendous value for the users of data of individual company registries. It would be empowered by international standardisation and harmonisation. It could also be encouraged through capital markets and other forms of regulatory requirement for LEIs and information access, such as in the context of digital regulatory reporting systems such as the U.S. SEC's EDGAR or the proposed EU ESAP.

(b) LEI in digital certificates

- Digital certificates are used in many ways, and the standards and technology platforms are mature and audited. Many jurisdictions have included digital certificates in their digital signature legislation as legally supported tools for authentication.[18] Products and services are widely available.
- GLEIF does not seek to become a Certificate Authority nor does GLEIF envision that existing LEI issuers will become issuers of digital certificates. In order to foster the use of LEIs in digital certificates, GLEIF works with Certificate Authorities and Trust Service Providers, downstream application providers, private companies and public authorities to encourage organisations to embed LEIs whenever legal representative certificates and electronic company seals are issued in a business context. This would apply to company seals as well as certificates for persons acting on behalf of a business.
- Embedding the LEI in digital certificates enables easier cross-border trade verification and enables holders of the electronic company seal or legal representative certificate to enhance security and credibility of their operations. Business Case examples include e-invoicing, e-trade and e-purchases.

(c) Bulk LEI issuance

- Another initiative that can potentially accelerate the adoption process of LEI is bulk issuance. The idea is that LEIs would be issued, in one take, to all the companies registered in a registration authority. Effectively, this means that any corporate registry can serve as an LEI Issuer and issue LEI to all its applicants,

[18] ` For the case of Asia-Pacific economies, see National Centre for Asia Pacific Economic Cooperation Working Group on E-Signatures (2022).

provided that a registry meets the GLEIF requirements regarding the verification of corporate reference data.[19]

- This could dramatically enhance efficiency and reliability of data collection since the corporate registry already should have information about the core attributes of any registered company. Furthermore, through economies of scale, a massive issuance could possibly reduce the cost per company in applying for an LEI. This would also reduce burden on the local registration authority as the company data would be publicly available via the Global LEI Index meaning the local registration authority could leverage this access point also for its customers.

(d) Validation agents

- In September 2020, the GLEIF introduced a new role in the global LEI system known as a validation agent. This move could potentially simplify and accelerate LEI issuance. A validation agent is usually a financial institution or any other organisation involved in identity verification and validation that liaises with the LEI Issuers on its clients' behalf to 'validate' that key data checks and processes have been undertaken. The idea is to capitalise on the information that the Validation Agent has already acquired for the purpose of meeting regulatory requirements (eg KYC, AML/CFT, taxation, data reporting) and customer due diligence processes not only for AML but also for credit evaluation and anti-fraud purposes.
- From the perspective of emerging markets, the GLEIF launched a pilot project in August 2021 that would enable African banks to issue LEIs to SMEs.[20]

In addition, in 2020, the FATF released new guidance on digital identification, highlighting its value, particularly in the context of individuals but also for legal entities. The guidance enabled recognition of digital ID for regulatory and CDD purposes. Similarly, in 2022, the FATF released new guidance on beneficial ownership transparency requirements, highlighting the necessity for jurisdictions to establish mechanisms to assure identification of beneficial owners of legal entities.

2.2 Decentralised identifiers (DIDs) standard

Some of the more recent proposed solutions to the challenges of corporate digital identity are based on the decentralised identifiers (DIDs) standard proposed by the World Wide Web consortium (W3C). Designed as a technical protocol, DIDs attempt to resolve challenges of digital identity solutions that often suffer from centralised bottlenecks, thus discouraging widespread adoption, especially in underdeveloped markets, across jurisdictional areas or within smaller market segments. The DIDs proposal emphasises the basic principles of interoperability, ownership and control and digital verification. Specifically, the W3C has formulated the requirements for this new type of identifiers:

- *Decentralised:* there should be no central issuing agency;

[19] The corporate registries of some European countries have already been serving as LOUs.

[20] For details, see https://www.businesswire.com/news/home/20210810005561/en/GLEIF-Launches-Global-Business-Identity-Initiative-to-Boost-Financial-Inclusion-for-African-SMEs

- *Persistent:* the identifiers should be inherently persistent, not requiring the continued operation of an underlying organisation;
- *Cryptographically verifiable:* it should be possible to prove control of the identifier cryptographically;
- *Resolvable:* it should be possible to discover metadata about the identifier.

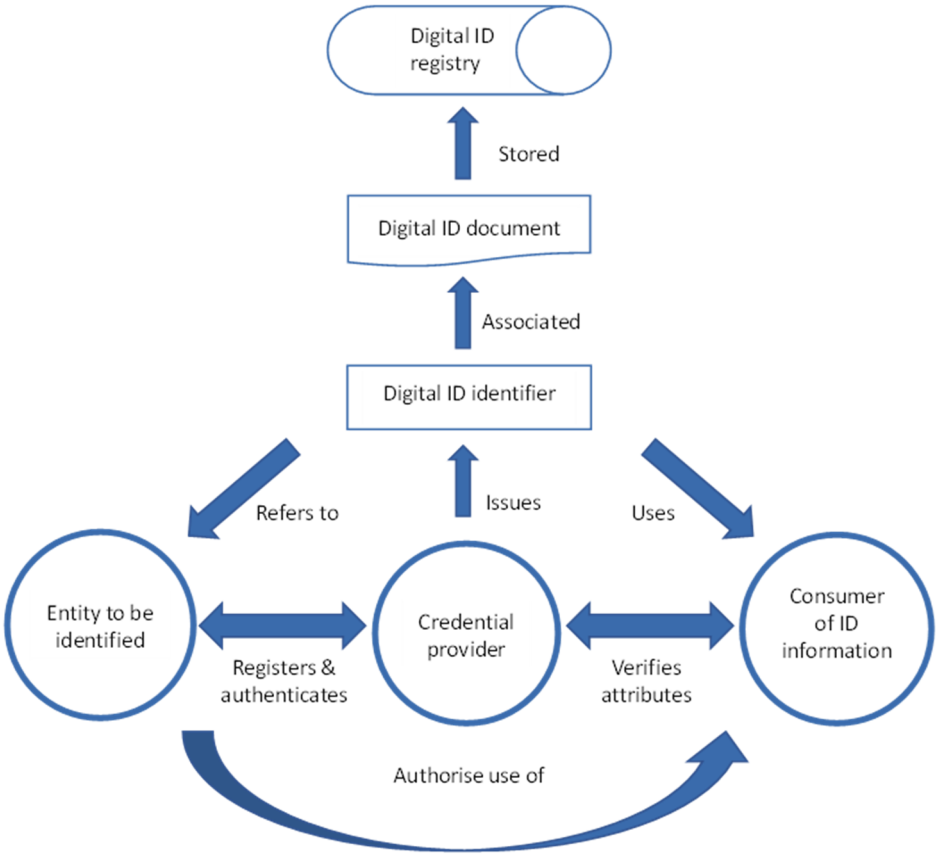
In order to resolve traditional identity bottlenecks, the standard defines a decentralised mechanism that unbundles the common components of a corporate digital identity system and proposes a new model for these components to work together. These components include: (1) the entities to be identified, (2) the credential providers that verify the identity of each entity, and (3) the consumers of the identity information. In simple terms, DIDs provide a protocol for connecting these actors in such a way that each party exhibits an appropriate amount of control over the portions of the identity solution that they are liable to.

One of the defining features of DIDs is user ownership and control, which is also a reason why the solution is coupled alongside "self-sovereign identity". Unlike traditional identifiers, DIDs are constructed in such a way that they could be decoupled from centralised registries, identity providers and certificate authorities. While these parties would be needed for the discovery of information about the entity behind a decentralised identifier, DIDs ensures that the owner of the identifier can prove control without requiring permission from any other party. DIDs are uniform resource identifiers (URIs) that associate a digital ID subject, the entity, with a DID document, a set or subset of metadata about the entity. This allows for trustable interactions associated with that subject. Note that the W3C defines a digital ID subject as "the entity identified by DIDS. Anything can be a digital ID subject: person, group, organisation, physical thing, digital thing, logical thing etc."

How does the DIDs model work?

The DIDs model is technology-agnostic, though it is often associated with the usage of distributed ledger networks such as blockchain. Succinctly, the standard works as follows (Graph 4).

How the digital ID standard helps enable the key identity concepts Graph 4



Source: authors' elaboration.

Suppose a corporation is an entity to be identified (lower left of Graph 4). After a registration and authentication process with the credential provider, a decentralised digital ID identifier is recorded on a registrar system. Within the registrar, the identifier corresponds to a decentralised digital ID document, which contains optional verification methods that are used to facilitate one or more identity related services.[21] A consumer of ID information (lower right of Graph 4), such as a bank that is going to onboard a corporate customer, would interact with the credential provider in order to verify the attributes of that corporation – on the condition that the corporation provides authorisation for the use of such attributes. In this way, the combination of the identifier, document, and verification methods allow for flexible workflows to be used around the creation, management and sharing of a digital identity.

Blockchain or not?

One of the key principles of DIDs is the use of a persistent, reliably available registrar source. The W3C standard itself is technology agnostic but given the availability and

[21] Identity related services include, for example: (1) authentication of the entity associated with the identifier, (2) validation of information associated with this identity, and (3) authorisation of services related to the usage of this identifier. The DIDS document can further contain service endpoints which are the technical access points that facilitate many of these functions.

immutability potential proposed by blockchain technology, blockchain-based networks are often a commonly used source for storing identifiers in DIDs implementations.

There may be economic and institutional considerations for whether a solution should use blockchain, permissioned distributed ledger technology or conventional data technologies. In situations with a weak rule of law or limited contract enforcement (for instance in fragile or developing states), blockchain or permissioned DLT could offer potential benefits, but it may need to contend with high rents to validators and limits to scale (Auer, Monnet and Shin, 2021). In other cases, security and scale considerations may favour a centralised ledger. This may be further supported by privacy and data confidentiality concerns, as a publicly viewable, immutable ledger can clash with considerations such as the right to be forgotten (Finck, 2018).

Benefits of DIDs

DIDs provides an opportunity to reduce costs and barriers to entry, serving as an interoperability protocol between existing identity networks and solutions and provides a scalable foundation for long-term projects. These benefits stem from the core of the standard that provides a single place in which identifiers can be registered and a method of communication established between the potentially infinite number of entities, credential providers and consumers. DIDs-based solutions seek to enhance the application of existing registrars and identity providers, while also enabling the creation of a new ecosystem of providers and participants.

Challenges with DIDs

The adoption and mainstream use of DIDs are not without challenges. For users, there may be up-front costs to establish new infrastructure in the form of identity wallets, digital ID services and registrars. This combines with the general challenge of encouraging adoption of a new standard. Because of the reliance on decentralised technologies and the absence of a central service provider, bespoke technical solutions will be required to perform several key steps in gaining and using a DID. Each of these solutions will need time to mature their usability, especially for user-facing components that require interaction with some of the more technically challenging areas – such as when cryptographic keys are used for digital signatures. Similar maturity issues can be seen in solutions that incorporate emerging technology components, such as blockchain networks.

3. Legal and regulatory aspects

A company is a legal construct, a "legal entity" or "legal person", created either under a standard form of statutory framework or via legislative promulgation. While companies and other forms of legal entity have a long history, arguably back to Roman law, Islamic law and Canon law, their modern form begins with companies established by sovereigns to provide trading and other state monopoly type services in early modern Europe. These early companies were generally created by royal or parliamentary charter, with examples including the Dutch and British East India Companies and the Bank of England. This period of history culminated in the Bubble of 1720. The reaction against companies as a result of the collapse slowed their

development for a century, but this changed during the course of the nineteenth century as a series of company and corporation laws were enacted in major jurisdictions to provide simple frameworks for company creation absent a specific royal or parliamentary charter. As a result, the company can be seen at the heart of the industrial revolution and of modern economic and financial globalisation.

Under these standardised legal frameworks, companies have legal personality, perpetual existence and their owners have limited liability, in exchange for certain requirements – both initial and ongoing. Corporate personality provides that a company is an artificially constructed legal person, treated just like a natural person and separate from its founders, directors and shareholders. As a company holds its own rights and liabilities, its income and assets are separated from its owners'. Note that a company does not conduct business on behalf of its founders, owners, directors or shareholders; it is a separate entity.

A company acquires its corporate personality only after it is duly incorporated and receives a certificate of incorporation issued by a company registry. Before this certificate is issued, a company does not, legally speaking, exist. As corporate personality exists only in incorporated companies – an SME organised as sole proprietorship, partnership or other unincorporated form does not carry a separate legal personality. From the legal point of view, its identity is not separable from those of its owner or owners.

3.1 Legal issues in corporate digital identity

The principle of technology neutrality can serve as a guiding principle for laws governing corporate digital ID. By this principle, the laws only consider the substance of a business process rather than the technological means adopted to undertake this process. In other words, it makes little difference whether the identification and verification of a company is conducted remotely through a digital solution, or by means of traditional paper-based documents in a physical meeting.

However, in the context of corporate digital ID, the principle of technology neutrality alone might not be sufficient because legislators still face a trade-off about how detailed and specific the laws should be. On the one hand, if the laws are very detailed and specific, they could reduce legal uncertainties but run the risk of being made obsolete by rapidly evolving technology. As legislative processes are usually lengthy, it is impractical to modify laws frequently in response to every new piece of technological innovation. On the other hand, if laws only consist of general principles or criteria, the risks of becoming obsolete could be reduced, but many legal uncertainties might arise for the industry practitioners as well as other stakeholders. This might in consequence cause confusion and discourage the adoption of new technology. Therefore, it is important to strike an appropriate balance between these two extremes.

There are other important issues to be resolved. First, as corporate digital ID solutions involve sensitive and possibly confidential information, it is crucial that the data are perceived to be authentic, verifiable and cybersecure. In order to build trust among all the participants, there is a need for a widely accepted governance framework that is based upon legislation. Second, a mechanism should also be established to delineate the potential liabilities of various parties, and well-defined procedures put in place to resolve disputes that could potentially arise. Finally, it is

very useful to consider integration between corporate digital ID and related aspects, including digital signatures and individual digital ID.

The following sections highlight some of the currently available corporate digital ID legal frameworks that could provide insights about how these issues could be addressed. These frameworks include: (1) the UNCITRAL Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services, (2) the European Digital Identity Framework (PCTF) and (3) the Pan-Canadian Trust Framework.

3.2 UNCITRAL draft provisions on the use and cross-border recognition of Identity management and trust services

Broadly speaking, identity management (IdM) services consist of managing identity proofing or electronic identification of legal entities. These services essentially seek to answer two basic questions: (1) "Who or what is seeking to prove identity?" and (2) "How reliably is identity proven?" They often then relate to a third aspect, which is interlinking proof of identity with a range of other attributes to provide details of the activities of the entity or individual in question.

With a view to promoting electronic IdM, the United Nations Commission on International Trade Law (UNCITRAL), which is the United Nations body focusing on private international trade law, has been receiving relevant submissions from member states and international organisations since 2016. Based on the inputs of these stakeholders, UNCITRAL published a Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services ("Draft Model Law"). The latest version was distributed on 21 February 2022.

The Draft Model Law does not aim to establish a comprehensive IdM regime, which should be the work conducted by individual jurisdictions that take into account their specific circumstances. Instead, it is "designed to regulate the provision of IdM to the extent necessary to give legal recognition and effect to those services." In other words, it has no legal standing nor signatories. Its objective is to provide a pattern for lawmakers in national governments to consider adopting as part of their domestic legislation for IdM services and clarify the major legal issues that might arise.

Amongst the legal issues of an IdM system, the most important concerns the obligations and liabilities of IdM service providers and the subscribers to their services. This is important because a lack of clarity on the liabilities of the parties involved often constitutes a major impediment to promoting trust in the use of IdM services. All the parties in the digital identity system need to be able to define access rights and obligations clearly and to allocate risks. Basically, the Draft Model Law postulate the general principle that IdM service providers shall be liable for damage caused to any person due to intentional or negligent failure to comply with its obligations. However, the IdM service provider shall not be liable to the subscriber for damage arising from the use of an IdM system to the extent that:

a. Use exceeds the limitations on the purpose or value of the transactions for which the IdM system may be used; and

b. The IdM service provider has notified the subscriber of those limitations in accordance with the law.

In addition, the Draft Model Law attempts to clarify some legal issues that often lead to uncertainties among stakeholders. For example, it has provisions that specify the legal status of electronic identification, the definition of users' consent and cross-border recognition of IdM services. Specifically:

- *Legal status of electronic identification*: The electronic identification of a person shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that the identity proofing and electronic identification are in electronic form (Article 5).
- *Users' consent*: While the use of IdM and/or trust services should not be imposed on a person who has not agreed to using these services, the Draft Model Law suggests that users' express consent is not necessary. The phrase 'consent may be inferred from the person's conduct' suggests that a consent is made when the users use and rely on the IdM (Article 3).
- *Cross-border recognition of IdM services*: An IdM system operated outside the enacting jurisdiction shall have the same legal effect in the enacting jurisdiction as an IdM system operated or a trust service provided in the enacting jurisdiction if it offers a substantially equivalent level of reliability (Article 25).

The IdM thus provides the potential basis of an agreed legal framework which could in fact operate jointly with the DIDs and LEIs to enable the basis of a hybrid system of base ID linked through technology and with an appropriate legal basis. The possibility particularly at the regional level is illustrated by the EU eIDAS and European Digital Identity framework. The challenge with model laws and treaties however is often the time involved. As a result, there may be scope as an option to embed rules into international guidance or into system rulebooks. The Pan-Canadian Trust Framework provides a useful example.

3.3 European digital identity

On 3 June 2021, the European Commission proposed a framework for a European Digital Identity which will be available to all European Union (EU) citizens, residents and businesses in the EU. Although this framework is expected to prioritise individual digital ID during its initial years, it is noteworthy that it also accommodates the establishment of corporate digital ID.

Under the European Digital Identity framework, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (eg driving licence, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognised by a Member State. Public services and certain private services will be obliged to recognise the European Digital Identity. As such, the new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they are expected to have full control of the data they share.

The European Digital Identity will be:

- *Available to anyone who wants to use it:* Any EU citizen, resident or business in the Union who would like to make use of the European Digital Identity will be able to do so.

- *Widely useable:* The European Digital Identity wallets will be useable widely as a way either to identify users or to prove certain personal attributes, for the purpose of access to public and private digital services across the Union.
- *Users in control of their data:* The European Digital Identity wallets will enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared will be shared.

The European Digital Identity framework is built on existing cross-border legal framework for trusted digital identities, namely, the European Electronic Identification, Authentication and Trust Services (eIDAS) initiative. Adopted in 2014, the eIDAS provides the basis for cross-border electronic identification, authentication and website certification within the EU.

Currently, approximately 60% of Europeans already benefit from the current system. However, there is no requirement for Member States to develop a national digital ID and to make it interoperable with the ones of other Member States. This leads to high discrepancies between countries. The current proposal will address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use.

3.4 Pan-Canadian Trust Framework

In September 2020, the Digital ID and Authentication Council of Canada (DIACC), a non-profit coalition of public and private sector organisations committed to develop Canadian digital ID solutions, launched the Pan-Canadian Trust Framework (PCTF) as "a set of rules and tools designed to help businesses and governments to develop tools and services that enable information to be verified regarding a specific transaction or particular set of transactions."

The PCTF is composed of seven components, with each component defining Trusted Processes and Conformance Criteria related to its specific area. The Verified Organisation Component ("VOC") is the most relevant to corporate digital ID. Overall, from an operational perspective, the PCTF is well structured and fairly comprehensive. But it requires further laws and regulations for actual implementation.

Verified Organisation Component ("VOC"): strengths and limitations

The VOC defines the processes and conformance criteria for: (1) establishing and verifying the organisation's identity and (2) creating an organisation's trusted digital representation (ie digital identity). Conformance criteria are "the requirements, specifications, recommendations and guidelines that comprise a standard to assess the trustworthiness of specific processes. Participants can use these criteria to inform the design and development of their products and services." An identification process that accords with the conformance criteria will become a trusted process which can be adopted as a reliable digital identity system.

There are two primary strengths of the VOC:

1. It is wide enough to apply to virtually every organisation, including – (i) unincorporated organisations; (ii) large organisations (eg multinational conglomerates); and (iii) small organisations found by a single person (eg sole proprietorships).

2. It is a multi-party system where organisations exchange trustworthy information about themselves with those of the external parties. And the PCTF explicitly recognises the use of information for KYC purposes.

However, the PCTF is only a very broad framework. The seven conformance profiles enlist over a hundred conformance criteria. This will call for heightened compliance. It being just a framework, participants voluntarily adopt the framework. There is no legal obligation for all industry experts (including the participants) to strictly observe the conformance criteria. Besides, the PCTF provides little guidance to reduce the legal uncertainty arising from digital corporate identity systems since the legal obligations and liabilities of the participants are not explicitly provided. Participants have to resort to existing laws.

4. Company registries

Company registries play a fundamental role in any corporate ID ecosystem, no matter how technologies evolve or whatever operational models are adopted. First, these public-sector agencies are the core provider of company identification, often issuing a unique identifier (eg registration number) for every company under their registration. They are also the most comprehensive provider of corporate credentials – regardless of company size and industry types. Second, only a corporate registry has the legal power to mandate companies to submit accurate data about themselves and update these data on a regular basis. No private-sector KYC firms or data vendors have such legal authority, nor do they have the incentive and research capabilities to administer such voluminous corporate data for the whole economy. Therefore, corporate registries are often regarded as the "golden source" of information; at the very least they are the "golden source" of the corporate ID and of its central attributes, in particular its directors and registered office. Admittedly, there are limitations to these data, notably the lack of data verification by most of these registries. However, users such as banks, data vendors and KYC firms realise that corporate registries often serve as the first step of their due diligence procedures, on top of which they can conduct further analyses and more in-depth investigation to verify the registry data.

In order for corporate registries to better perform their role in a corporate digital identity ecosystem, they need to address a number of basic issues:

- Do they collect all the necessary information about the companies, notably information about beneficial ownership that is required for KYC/AML in many jurisdictions?
- Do they undertake necessary quality control of their company data (eg verification of the data submitted by companies, requirement of more frequent updating of data)?
- Do they make the company information (including personal information about its directors and major shareholders) available to the public, up to the extent that data privacy laws permit?
- Do they take measures to facilitate the retrieval of corporate data by external users through the use of information technology (eg automated remote access to data through APIs, data stored in machine-readable formats)?

In this section, we first give an overview of company registries around the world, assessing the different aspects of their performance in providing company data. The subsequent section focuses on their provision of data about beneficial ownership, as the FATF recommendations specify that the identification and verification of a corporate's ultimate beneficial owners form an important part of customer due diligence procedure and also an increasing requirement of G20 / FSB members. Finally, we examine the limitations and challenges of registries in general, and then examine the major issues that need to be resolved.

4.1 Openness of company registries

In order to evaluate the performance of corporate registries, we make use of the Open Company Data Index (OCDI) compiled by the OpenCorporates with the support of the World Bank Institute since 2012. The OCDI currently covers 208 company registries all over the world. As the most updated scores of all the company registries are freely available in the OpenCorporates website (https://opencorporates.com), this report would not list out the scores of individual company registries. Instead, a statistical analysis of all the registries is provided.

The OCDI scores company registries on a scale of 0-100 using a consistent methodology described in its website. In summary, the total score is based on the following criteria, with their weighting in brackets:

1. *Freely searchable:* Online searchability with minimum hindrances in terms of costs or other barriers (20%)
2. *Licensing:* An explicit open government license that allows free use of the data obtained from the registry (30%)
3. *Data freely available:* The registry information is available as data, either as a free data dump or via a free API (20%)
4. *Data depth:* availability of data to the general public regarding the following areas:
    a. List of company directors (10%)
    b. List of significant shareholders (10%)
    c. Annual accounts of the company (10%)

Based upon the OCDI, the data openness of company registries all over the world is quite divergent. Globally, 27 registries (13% of total) are classified as "Open", with a total score of 46-100. Larger groups are classified either as closed (77 registries, 37% of total) or "Relatively Open" (104 registries, 50% of total) (Chart 5, left panel).

Chart 5 (right panel) shows the average of all the sub-scores of the OCDI. First, it is obvious that company registries perform relatively well in terms of Criterion #1 (Freely Searchable), with an average normalised score of 54.9%, significantly higher than the overall average score of 21.1%. In other words, most company registries are able to provide online searchability without prohibitive costs or other hindrances. Therefore, what makes an open company registry stand out from a closed one is their performance in the remaining criteria. Specifically, in order for company registries to provide better support to corporate digital identity systems, there is much room for them to make improvement regarding:

(a) issuance of an open government license that clearly defines the free use of the registry data;

(b) making their data machine-readable; and

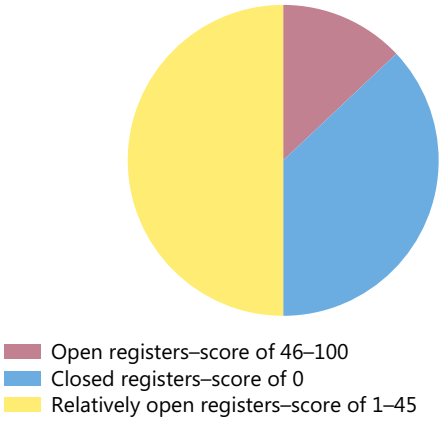
(c) improving data depth in terms of information about company directors, significant shareholders and annual company accounts.

Openness of company registries and their average sub-scores

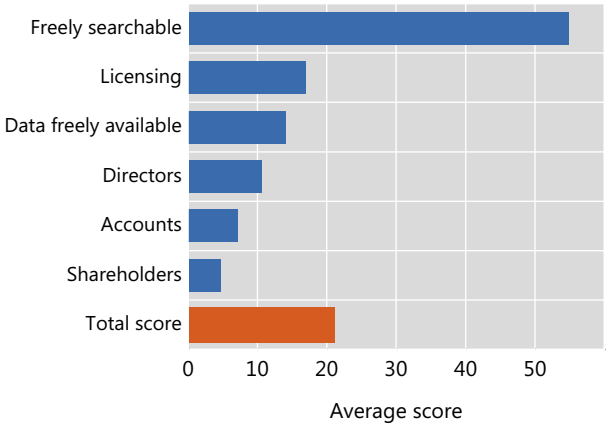
In per cent

Graph 5

Status of openness of corporate registries in 208 jurisdictions[1]



Open Company Data Index sub-scores



[1] Closed registries: jurisdictions where registries are closed for public access altogether and basic search on company and directors is not available. Relatively open registers: jurisdictions with registries open to the public for restrictive information about a company's basic incorporation details, and its directors with most of this information provided free of cost. Open registers: jurisdictions with registries open to the public for detailed information about directors, shareholders including beneficial ownership, licensing along with documents and some of them also offering API feature. All the sub-scores are normalised to the range 0%-100% for easy comparison.

Source: Open Company Data Index; authors' elaboration.

4.2 Beneficial ownership data in company registries

Broadly speaking, an ultimate beneficiary owner (UBO) is an individual that ultimately benefits from a transaction initiated by an organisation. The benefit can be obtained directly, or indirectly through many methods, such as a web of nested ownership of companies. While different jurisdictions have different definitions of a UBO, a UBO is generally defined as an individual who holds a minimum of capital or voting rights in the underlying entity. That minimum is mostly around 25% but it also depends on the rules of specific jurisdictions.

UBO identification is an important part in the identification and verification process of a company because this can pre-empt the misuse of a legal person for illegal activities such as money laundering and terrorist financing. This is notably applicable to banks and other financial institutions that are subject to regulatory requirements regarding KYC and AML/CFT.

As a result, in 2014 the G20 agreed a new set of policy approaches to beneficial ownership transparency, building on the existing FATF guidance: the High-Level

Principles on Beneficial Ownership Transparency. In 2022, the FATF released revised guidance requiring implementation of beneficial ownership transparency.[22]

In this section, we look at the major issues around UBO identification by making use of company registries in some jurisdictions.

(a) United States

In 2021, the US Congress enacted two acts related to corporate transparency. They are: (1) the Corporate Transparency Act ("CTA") and (2) the National Defense Authorization Act for Fiscal Year 2021 ("NDAA 2021") – which became Public Law on 1 January 2021. In short, these laws provide the legal basis for certain types of companies to disclose their beneficial ownership to the public.

CTA imposes an obligation on certain companies to submit a report on beneficial ownership to the Treasury Department's Financial Crimes Enforcement Network ("FinCEN"). Basically, beneficial ownership refers to any individual who (1) exercises substantial control over the entity or (2) holds at least 25% of the ownership interests of the entity. Note that the CTA does not define "substantial control" and does not describe how ownership interests are to be measured. The beneficial ownership information must include: (1) full legal name, (2) date of birth, (3) current residential or business address and (4) unique identifying number. [23] However, the beneficial ownership information submitted under the CTA is not publicly available. The FinCEN will only share the information with American and some global law enforcement agencies and financial institutions for due diligence purposes.

The NDAA 2021 provides for the launch of a public beneficial ownership registry, ie information related to UBO of certain companies would become publicly available. However, not all companies will be required to provide UBO information because the NDAA imposes the regulation only on companies receiving federal contracts over $500,000. In addition, not all kinds of beneficial owners will be publicly known because the NDAA's definition of beneficial ownership is not wide enough.

(b) European Union

The Fifth Anti-Money Laundering Directive (5AMLD) stipulates that all EU member states should establish public beneficial ownership registers ("registers") by 10 January 2020. Information in these registers should be accessible to the general public. The 5AMLD replaces the 4AMLD that did not require the information to be publicly accessible. For corporate and other legal entities, the following information about its beneficial owners is required: (1) name, (2) month and year of birth, (3) country of residence, (4) nationality, (5) nature and extent of beneficial interest held. It is notable for demanding trusts to disclose beneficial ownership information like companies do. In the longer term, the European Commission has a goal of interconnecting the registers of member states. The European Digital Identity framework announced in 2021 is expected to facilitate the identification and

[22] For details, see https://www.fatf-gafi.org/publications/fatfrecommendations/documents/r24-statement-march-2022.html

[23] For details about the CTA-related regulations proposed by FinCEN, see https://www.federalregister.gov/documents/2021/12/08/2021-26548/beneficial-ownership-information-reporting-requirements

verification of a company's beneficial owners once this framework is fully implemented. However, the exact mechanism and plan are yet to be announced.

In practice, however, it will take time before all the member states can establish a truly public register. According to the Global Witness, as late as March 2020, only 5 of 27 member states have implemented a public register which is free to access. Another 5 member states have a centralised register of the beneficial owners of companies that is available to the public, but with significant restrictions that hinder its usefulness in combatting money laundering. These restrictions include setting up a paywall or only being able to search using a company's tax identification number. Meanwhile, 17 of 27 member states do not yet have a centralised register of the beneficial owners of companies that is available to the public. This category includes some countries which do not yet have a register of beneficial owners that is accessible to members of the public with a legitimate interest, which was required to have been implemented by the 4th AML Directive by June 2017.[24]

(c) United Kingdom

The United Kingdom's register is called the People with Significant Control Register (PSCR). One notable feature is that the entire list of beneficial owners of all legal entities is downloadable as a .json file and this file is updated daily. This is tremendously helpful to the KYC solution providers, who can simply import the .json file data into their own database without further work.

(d) Hong Kong SAR

The Companies Registry of Hong Kong has already largely digitised its systems. The registry is open to enquiries, providing general corporate information, including company directors and charges created along with the documents. Given these features, the prerequisite for a corporate digital identity system is already in place. Currently, the Office of the Government Chief Information Officer (OGCIO) of Hong Kong is working with the Hong Kong Monetary Authority (HKMA) on Proof-of-Concept (PoC) trials and research on the business version of the "iAM Smart", which is an individual digital ID platform.

The equivalent of UBO in the laws of Hong Kong is known as "significant controllers". Effective from March 2018, Hong Kong's companies are required to maintain a significant controller register (SCR), in which required particulars (eg name, date of becoming a significant controller, nature of control over the company, correspondence address, identity card number or passport number) of every significant controller of the company would be recorded. While UBO information is available to the Companies Registry, access to the information is limited to law enforcement officers of different government departments or agencies. Banks and KYC service providers are unable to make use of the SCR directly, and they can only infer the UBOs of a company using other pieces of information.

(e) Singapore

Singapore's business registry, which is part of the Accounting and Corporate Regulatory Authority (ACRA), provides online search services for the business profile

[24] For details, see https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/5amld-patchy-progress

of companies under its registration. Since December 2018, API connection to corporate information has been available. The API service also updates share ownership information in the ARCA's registry directly from the source to improve timelines and data accuracy. Meanwhile, digital ID is provided to both individuals and corporates. The corporate digital ID, known as CorpPass, was launched in 2016 and it allows businesses and other entities (eg non-profit organisations) to transact with government agencies online. Note that CorpPass does not disclose data on UBO, even though the government is in the process of collecting information on UBOs as companies are required to submit data to government about shareholders that have ownership beyond 25%.

4.3 API Integration

Application programming interface (APIs) are a set of rules and specifications followed by software programmes to communicate with each other, and an interface between different software programmes that facilitates their interactions. By allowing a utility or user program to securely share data and request services, APIs allow the operating system to access different file systems and services. An example would include the Google Maps API. The API lets developers embed Google Maps on webpages using a JavaScript or Flash interface.

Company registries with API integration can allow for the sharing of a company's credentials including details about shareholders and directors. This can aid in automation and significantly reduce the time spent researching a corporate client's identity. For example, an API-integrated registry may allow director details to be embedded into a company's system. In this way, where once user clicks on the name, he/she can access additional details about him or her.

Company registries with API Integration include the following:

- *Singapore:* The SingPass API Portal enables developers to access SingPass API specifications and use the sandbox to experiment, build and test solutions quickly and securely.
- *UK:* The registry allows users to sign up to the Financial Services Register API Developer Portal. This service is currently free of charge and enables users to generate a unique key to access the Register APIs as well as providing self-help support materials.

4.4 Limitations and challenges facing registries

There are a number of limitations and challenges facing existing company registries:

1. *Lack of data verification:* Given resource constraints, it is usually not feasible for a company registry to audit and verify every piece of data submitted by companies. In addition, many registries lack legal power to remove inaccurate information from the register. As such, company registries often confine their role to taking information from companies and making it available to searchers. Nonetheless, there is room to improve data inaccuracy through automated checking for data inconsistencies. Besides, registries may provide better connectivity of their data with other sources (eg tax authorities) so that users are in a better position to verify the data.
2. *Lack of data openness:* Different jurisdictions have adopted different policies regarding the accessibility of company data to the public. For example, while the

registries of the European Union member states are required to be open under the 5th and 6th AMLD, many other registries are less open for various reasons, such as data privacy. As a result, access to sensitive information about a company's directors and shareholders is often confined to certain law enforcement officers.

3. *Lack of common data standards:* It is a lengthy process for various jurisdictions to define and agree upon one common baseline or basic threshold for all companies to be included into the registry. Rules and regulations are different for different jurisdictions, including thresholds for UBO share ownership, tax requirements, etc. This poses a challenge for the KYC and AML procedures of a company that has multiple subsidiaries incorporated in different jurisdictions. It also poses a challenge for corporate ID&V solutions.
4. *Cost and resources:* The scaling and onboarding of KYC data for registries along with tools to continually refresh the data with latest changes is a huge task. It will require substantial cost and resources such that the total cost incurred may be higher than the tangible result that is expected.
5. *Technology*: As discussed, API access can be highly beneficial. Short of this, regular web interface without an API can also bring benefits. Yet some corporate registries are not connected digitally at all such that user needs to walk to the physical office location to access data. It is crucial that the registries falling into this category, without any digitisation, work to invest in technologies – at the very least a web interface.
6. *Insufficient digitalisation*: Many company registrations have long histories and many have not fully digitized their data, records, systems and processes.

5. Bank-related initiatives

In a corporate digital ID ecosystem, banks and other financial institutions are often perceived as consumers of corporate ID information since they need such information for identifying and verifying corporate customers, as well as undertaking procedures to meet regulatory requirements.

Yet conceptually, banks are able to play a more pro-active role by serving as service providers of corporate digital ID, thus turning a cost centre into a profit centre. The Open Digital Trust Initiative is such initiative, jointly launched by the Institute of International Finance and the Open ID Foundation.[25] Justification for such an approach could be multi-fold:

- *Monetise KYC/AML investment:* In order to meet regulatory requirements and conduct internal risk management, banks have already invested heavily in KYC and AML/CFT processes. As a result, they have accumulated a significant amount of information about their corporate clients. As such information is already verified and updated on a regular basis for customer due diligence, it can be readily used to provide services to third parties.

[25] For details, see https://www.iif.com/Innovation/Open-Digital-Trust-Initiative

- *Overcome information asymmetry:* A bank might only hold only one jigsaw puzzle piece of data about a business entity, notably if the entity is a multi-national business group spanning across multiple jurisdictions. If banks can pool and share the data they hold, they can gain a more complete picture about the business entity and therefore reduce the room for malicious behaviour that is made possible by exploiting the information gaps among banks.
- *Customer service:* When a company seeks to onboard with another bank, rather than repeating the whole KYC process, the company could provide consent basis to obtain verified information from its existing bank. This type of portability would lead to improved customer experience.
- *Reduce duplicated processes:* Operational efficiency in the KYC process can be improved and cost can be reduced through reduction of duplicated processes.

Banks could also collaborate with each other by establishing a KYC utility to provide corporate digital ID solutions. The first generation of shared KYC utilities can be dated back to Clarient Entity Hub, which was formed in 2014 and went live in February 2015. Its objective was to serve as a single repository of commonly used KYC data of customers, which could be used by participating financial institutions. It was acquired by Thomas Reuters in 2017.[26] The SWIFT also has a KYC Registry that was founded in 2014.[27] Another example is that six major Scandinavian banks launched the Nordic KYC Utility in 2019, which was later renamed as Invidem.[28] Similar initiatives at PoC stage were undertaken in Singapore and Hong Kong respectively.

None of these KYC registry or utility efforts is comprehensive so far. Notwithstanding this, there is precedent for banks to share other types of data. For example, in the context of lending, banks (and increasingly other lenders as well) have been required to share credit information about borrowers – individual and corporate – to prevent fraud and also to address information asymmetries (see ICCR 2018). In the context of derivatives, data on OTC derivatives transactions must be submitted to G20 / FSB member trade repositories. Likewise, information on financial transactions involving company shares is a core focus of financial regulation, with the companies' registries and custodians established to maintain core information. Finally – because company directors, responsible officers and owners are individuals – systems interlink not only for market integrity but also for tax information sharing, particularly in the context of the G20 / OECD Common Reporting Standard (CRS).

Looking forward, more and more jurisdictions are considering how to maximise the value of aggregate data for competitiveness and development, in addition to core financial regulatory objectives of financial stability, market integrity, efficiency, financial inclusion and customer and investor protection.

[26] For details, see https://www.thomsonreuters.com/en/press-releases/2017/february/thomson-reuters-strengthens-kyc-managed-services-and-legal-entity-data-through-clarient-and-avox-acquisitions.html.

[27] For details, see https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/kyc-registry

[28] For details, see https://invidem.com/

5.1 Challenges of bank-related initiatives

While the idea of a KYC utility is promising in principle, its implementation needs to overcome numerous challenges, including the below.

(a) Cost

The cost of setting up a KYC utility is significant, including the overhead cost of constructing the computer hardware architecture and the governance model of the platform, and ongoing operating expenses. In order to operate successfully, the utility should achieve efficiency gains that are sufficient to justify these costs. A telling example is Singapore's KYC utility, which was proposed in 2017 but abandoned in 2018 as the expected savings were not enough to cover the costs.[29]

(b) Operational processes

Since banks have different practices and risk appetite regarding their KYC processes, it is important that they can arrive at a consensus about data standards and code of practices. This process of consensus-building and harmonisation of standards might take significant amount of time, notably if the banks are located in multiple jurisdictions and have to meet divergent requirements about their KYC processes due to different regulatory regimes.

(c) Cybersecurity

Cybersecurity is an issue to overcome as the KYC utility involves the storage and transmission of confidential corporate information. This issue is of particular concern especially if the utility is operating in a centralised mode such that it is easy to become a single honey pot to attract hackers' attacks. The risk of a single point of failure is another concern that needs to be addressed.

(d) Legal liabilities

The KYC utility needs to have a governance model that clearly specifies the liabilities of various parties. In particular, in the event of error, it is crucial to know beforehand whether it is the KYC utility or the bank that relies on this utility should be held liable. According to FATF Recommendation 17, countries may permit financial institutions to rely on third parties to perform some CDD measures if certain criteria are met, and the ultimate responsibility for CDD measures remains with the financial institutions that rely on the third parties. The inability to shift liability remains one of the key concerns as banks decide whether or not they would participate in a KYC utility. This, however, has not proven a major issue in the context of credit information registries, where data can be relied on for purposes of credit evaluation but any liability for any lending decision rests with the lender and borrower. A similar approach would appear sound in the context of potential corporate data registries: information must be shared but responsibility for the conclusions drawn remains with the institution concerned. This would also reflect the approach of capital markets data systems such as EDGAR and ESAP.

[29] For details, see https://abs.org.sg/docs/library/kyc-aar-faqs-for-abs-website.pdf

(e) Data privacy

The KYC utility needs to comply with regulations regarding data privacy. For example, there should be well-established procedures to ensure the transparency of data collection and processing. Furthermore, the transfer of data should be permission-based. This is an issue that is increasingly arising and which is being addressed in very different manners in major jurisdictions such as the EU, China, the US and India.

(f) Competitive dynamics

Banks are the custodians of their customers' information. This information is strategically and competitively valuable. In the absence of a regulatory requirement or clear savings for the bank (the "what's in it for me" dilemma), the incentives to share may be low. However, this may change as new competitors enter the market, offering new solutions and frictionless customer onboarding, in part due to high digitisation of such processes. This may move the goalpost for banks to offer a smoother customer onboarding experience. In credit and capital markets information – as well as ESG information in the EU – this is addressed via regulatory requirements as the most appropriate way to support data as a public good.

5.2 SWIFT's KYC registry

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) was founded in 1973 when 239 banks from 15 countries grouped together to solve a common problem on how to communicate information concerning cross border payments. These banks formed the cooperative utility known as SWIFT, headquartered in Belgium. Its messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. It also creates the standards so that SWIFT members can operate more effectively. According to SWIFT, there are currently more than 1.3 million bilateral correspondent relationships across the industry, presenting a sizable administrative burden for banks each time a new relationship is formed or information needs updating. A community approach is essential to accelerate compliance processes and create new collaborative ways of tackling financial crime.

Launched in 2014, SWIFT's KYC Registry has become the industry standard for correspondent banking due diligence, allowing more than 6,500 banks to streamline their KYC compliance processes. And, following a rollout to SWIFT-connected companies in December 2019, the registry helps simplify this process between banks and companies too.

KYC Registry is a global platform that enables its member institutions to securely exchange SWIFT-verified due diligence information with one another. It is built on a standardised set of information for KYC processes, agreed in collaboration with banks across the globe. For example, the predefined questionnaire features AML/CFT-related questions, including the latest Wolfsberg Group Correspondent Banking Due Diligence Questionnaire, and documentary evidence to validate the data users provide.

The registry baseline covers a significant portion of global KYC requirements, containing both private and publicly available KYC information. This standardisation can support the due diligence process and enables users to focus on more value-

added work, especially when dealing with multiple data requests. In order for the data provider to retain control of the data, access to the KYC profile by third parties is on a permission basis. Both the KYC data providers and users are on a voluntary basis. Neither of them pays for the data or receives rewards for providing the data. The registry also enables an API connection.

5.3 Open Digital Trust Initiative and related services

The Open Digital Trust Initiative (ODTI) is a joint initiative of the Institute of the International Finance (IIF) and the Open ID Foundation. The goal of the initiative is to create a multipurpose identity verification solution provided by banks under one common global open-source standard that can be used across the public and private sector. In September 2021, it announced a user-centric and high-trust identity paradigm known as the Global Assured Identity Network (GAIN), expected to be launched in 2022. The basic idea of the GAIN is to leverage existing bank investments in KYC and multifactor authentication, as well as banks' role as a trusted protector of customer data and privacy. Conceptually, this will help customers trust each other online without compromising privacy. Initially, the services cover eKYC and outsourced login solutions.

In the Nordics, BankID provides a similar type of service. The average person in the Nordics uses BankID 198 times a year. Identity verifications cost between €0.10 and €1.00 per successful API call. There are additional revenue opportunities for associated insurance products. The ODTI attempts to implement a similar concept in a broader region, with a view that it would eventually be practised globally. At the same time, it seeks to create a free open-source standard that could be used to create a genuinely competitive market for digital trust services. To drive the standard, the ODTI team partnered with the IIF to encourage other banks to consider providing similar services.

In the digital ID ecosystem of the ODTI, there are four major parties:

Banks: Own trust relationship with their clients

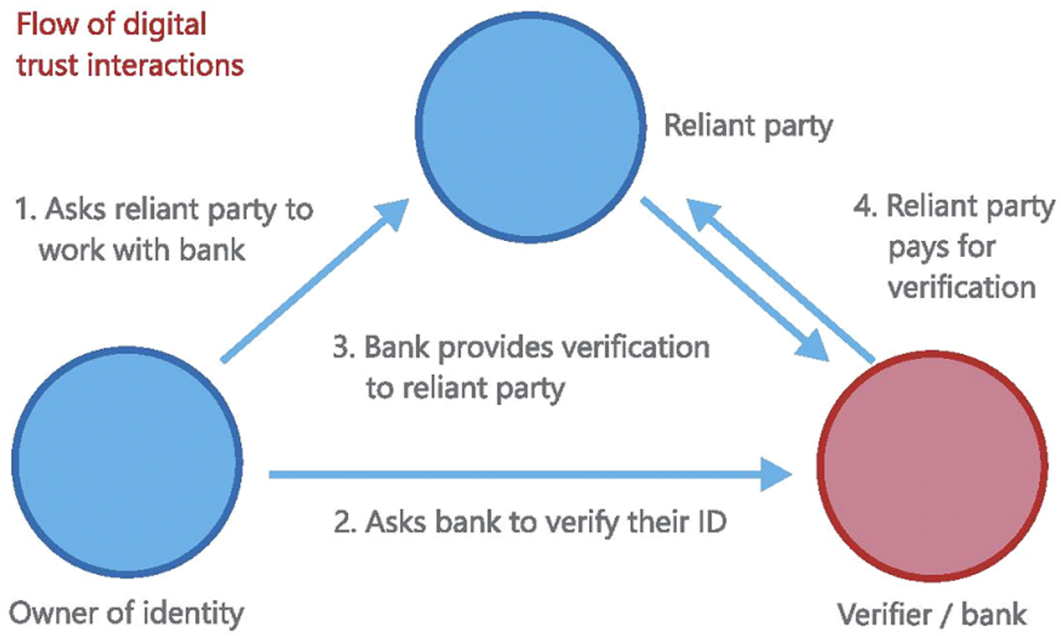
Relying parties: *Buy e-KYC and per-session authentication services*

Aggregators: *Intermediaries to connect thousands of relying parties to* hundreds of banks. The key to being a successful aggregator is making it very easy for developers to tap into your network.

Technology providers: *As this is an open-source standard, there are lots of options* for technology providers to participate.

The flows of interactions are shown schematically in Graph 6. First, the owner of identity (eg a company) asks the relying party (eg an insurance company) to work with the bank. Second, the owner of identity asks the bank to verify its identity. Third, the bank provides verification to the relying party. Finally, the relying party pays a service fee to the bank for verification.

Interactions of various parties in the digital ID system Graph 6



Source: Open Digital Trust Initiative

6. Established vendors and regtech solutions

Traditionally, a number of established vendors have played a role in corporate ID&V. Recently, a range of regtech firms have started to provide solutions for corporate digital identity. While the solutions provided by these stand-alone firms cannot substitute for a full-fledged ID system, they can make it easier to conduct some aspects of customer due diligence. The clients of these regtech firms are typically banks and other regulated financial institutions that are required to identify and verify their customers before onboarding, which is usually the first step to KYC, AML/CFT and other due diligence or risk control procedures. More recently, the clients of regtech firms are extended to the companies and individuals that are subjects to be identified, as technology (eg portable digital wallets, self-sovereign identity) is increasingly enabling these companies and individuals to share their verified identity data with third-party users in a trusted manner and on a consent basis.

There are strengths and weaknesses of emerging regtech firms in providing corporate digital ID solutions. First, these firms usually have a short history, with some of them being start-ups founded in the past five years. In terms of resources, they are far behind well-established data vendors and banks that have already invested significantly in acquiring and verifying corporate data. The strength of regtech firms mainly lies in innovative use of technology such as artificial intelligence (AI), machine learning, natural language processing (NPL), optical character recognition (OCR) and blockchain to solve pain points in the process of corporate identification and verification. As they are relatively new, they are not encumbered by legacy IT systems

that often hinder the adoption of new technologies. Their small size also means that they are more agile and flexible than well-established organisations to adapt to latest technological changes.

In order to understand the value propositions of the regtech firms, it is useful to understand the workflow of the KYC process so as to identify the pain points at each step and how technology solutions could add value. Based on interviews of these emerging regtech firms, their workflows can be broadly summarised into the following four steps:

1. *Retrieve company data*
   - Either via direct access to official registers and government clearing houses or via APIs to data aggregators and other intermediaries
   - Access should be in real-time, automatic and time-stamped
2. *Extract and clean relevant KYC data*
   - NLP and OCR technology are used to digest KYC documents and conduct data cleansing and enhancement
   - Key datapoints and persons of interest are highlighted
3. *Identify ultimate beneficial owners (UBO)*
   - UBOs are identified and connections to companies/shareholders are highlighted
   - Calculation of total ownership stake and management control of individuals
   - Graph visualisation and analytics
   - Access to shared UBO registers
4. *Perform AML/KYC checks on individuals*
   - Politically exposed persons (PEP), negative news and sanctions screening tools
   - Automated post-transaction and ongoing monitoring with red flag capabilities
   - Network analysis to identify related parties and UBOs.

6.1 How can regtech solutions help?

(a) Data connectivity

One of the pain points in identifying and verifying a company is that the required information is scattered in multiple sources, in some cases located in different jurisdictions. Even if an identity data user is able to access all these sources of information, it would take much work to collect and aggregate the required information.

In order to resolve the pain points of collecting information from multiple sources, some regtech firms offer solutions to enhance data connectivity. For example, Chekk, a Hong Kong-based regtech firm established in 2016, offers connectivity to business data sources that cover more than 350 million companies in 200 countries worldwide. These business data come from a variety of sources, such as corporate registries and third-party data vendors. Users of the Chekk platform are able to access these data through a variety of channels (eg desktop computers, tablets, mobile phone). Alongside data connectivity, it also makes use of various technologies (eg API connections, AI, NLP, OCR) for data access and analysis.

Another example is kompany, an Austrian-based regtech firm established in 2012 and acquired by Moody's in 2022. It offers its clients real-time API connections to

more than 200 business registries, financial authorities and tax offices around the world so that its clients can access original data and documents on more than 115 million companies. Meanwhile, value-added services including change monitoring and alerting (Perpetual KYB), tax ID and IBAN Verification, and document translation services are also provided.

In the capital markets and credit information context, the benefits of centralisation have resulted in the development of standardisation systems and processes. The EU ESAP provides an example how this could be extended to ESG data as well, which suffers from many of the same issues as KYC data.

(b) Digestion of company documents

With the adoption of digital technologies, company documents are increasingly available in electronic format. Unlike traditional paper-based documents, these electronic documents are much easier to store, retrieve and transfer. Nonetheless, it still requires a significant amount of manual work to read through these documents and extract relevant information, as the data contained in these electronic documents are not in a well-structured and consistent format, which means that they are not readily machine-readable. In this regard, regtech firms have offered innovative solutions to reduce the burden of reading these documents. For example, Belgium-headquartered firm Complidata provides technology tools such as OCR and NLP to digest company documents and extract useful information. It also offers solutions for negative news and sanctions checks on an automated basis. In other contexts, digital regulatory reporting requirements are developing rapidly, offering the potential for machine-readability.

(c) UBO discovery

The identification of beneficial ownership has increasingly become a mandatory regulatory requirement for financial institutions in many jurisdictions, but such information is often not directly available to the general public. Although a number of company registries have required companies under their registration to submit UBO information and provide updates to such information on a regular basis, such information is often accessible only to specified law enforcement officers.

In the absence of first-hand information provided by authoritative sources, many regtech firms offer solutions to identify the UBO of a company. For example, kompany makes use of primary source data from government registers and provides AI-enabled tools to uncover the cross-border ownership structures of legal entities from around the world so that the UBOs of a multinational business can be uncovered. The output of the analysis is user-friendly as it can be visually presented in ownership trees that are intuitive to understand and easily exportable.

(d) Data portability

From the viewpoint of the subjects to be identified and verified, the pain point is primarily to collate massive amounts of documents to prove their identity. Some of these documents may still be in paper form and a face-to-face meeting is required to verify their authenticity. This tedious process repeats itself every time a company begins a relationship with a new bank, supplier or other service provider, introducing substantial costs. Data portability of the ID owner provides an efficient solution to solve this pain point and potentially transition to a remote interaction for onboarding and monitoring. For example, Chekk provides data portability by a digital wallet that

is securely encrypted. A company and its representatives (eg CEO, directors, major shareholders) can store their identity data in this wallet. On a consent basis, the wallet owner can share any part of the data with a bank or other third-party users. The users can trust that these data are authentic because they are verified by a number of official data sources. Additionally, the use of technology also ensures that the data cannot be tampered with once they are verified. Note that the data encryption is end-to-end so that even Chekk cannot see the data of its customers.

6.2 The example of ZOLOZ

One particularly illustrative example is the ZOLOZ eKYB solution in Asia.[30] The solution includes three pillars: business verification (RealBID), individual verification (RealID) and risk prediction.

(a) Business verification

RealBID business verification starts from registration documents such as business registration certificates and corporate bank account statements. Images of these documents are submitted by clients in digital format and then run through OCR and anti-counterfeit algorithms to arrive at a confidence score of authenticity. If an SME is unable to provide all the registration documents, alternative data sources will be used. For example, businesses submit photographs and addresses of their operational venues and/or their website URLs. AI together with human supervision will then derive a confidence score.

(b) Individual identify verification

The objective of RealID is to verify the identity of individuals acting on behalf of a company, such as its directors, supervisors and senior management. Similar to other commercially available individual digital ID solutions, RealID requires each of these individuals to capture an ID document image and a selfie picture. A first-level quality check is then performed over these images.[31] After the individual passes this check, ZOLOZ verifies the ID authenticity based on AI algorithms. The next step is a liveness check to determine whether the individual presented is a live person. ZOLOZ's liveness technology is certified under the ISO30107-3 level 2 certification, meaning ZOLOZ' liveness solution is robust enough to identify face printing, video playback (including deepfake), as well as 3D face mask impersonation attacks. As the whole process is fully digitized, the turnaround time is seconds.

(c) Risk prediction

RealID performs cross-comparison on all document submissions to detect whether there are cases of face forgery (different faces appearing in the ID with the same particulars), ID particulars forgery (different particulars are appearing in the ID with

[30] Users include AlipayHK, Antbank HK and Macau, Touch 'n Go Digital in Malaysia, DANA in Indonesia, TrueMoney in Thailand, as well as GCash in the Philippines. So far ZOLOZ RealID solution has verified over 100 million users in Indonesia, Philippines, Malaysia, Korea Thailand, Vietnam, Bangladesh, Singapore, Macau, and Hong Kong.

[31] A user is asked for immediate retrial in real time if the images' quality is poor. If there are too many failed attempts from a certain device over a period of time, ZOLOZ RealID SDK blocks the submission as part of product velocity protection.

the same face) as well as multiple clients using the same ID. By mapping out the relation of companies and ingesting updates from data source providers, RealBID gives a risk rating at client onboarding, raising alerts when required. For example, when any directors, supervisors or senior management of a client are flagged, all the related entities and their respective second-degree related entities are also subject to risk flags.

By combining an individual identify and a business verification solution, ZOLOZ pursues digitised onboarding of SMEs, supporting SME financial inclusion.

7. Public sector digital ID initiatives

The public sector has an important role to play in supporting corporate digital ID, not least through its central role in the enabling of legal entity creation and – in many cases – the extension of individual digital ID. Moreover, many government initiatives explicitly support financial inclusion for SMEs. Indeed, the hurdles for SMEs to access finance are well documented. According to the Asia Development Bank (ADB), for example, SMEs account for only 23% of trade finance demand but 40% of trade finance rejections. Their difficulty in accessing trade financing is a key factor for the global trade finance gap that soared to an all-time high of $1.7 trillion (or 10% of global goods traded) in 2020, as the Covid-19 pandemic dealt a devastating blow to the global economy.[32]

One of the major hurdles for SMEs to accessing financial services is the prohibitively high cost incurred in the process of ID&V, which is mandatory for all AML-regulated companies such as financial institutions, businesses engaged in international commerce and most B2B companies. This process is in place to deter money laundering, fraud, terrorist financing and other criminal activities. KYC / KYB typically involves two key steps: first, verifying company registration certificate, business license and other relevant documents to ensure that the business is real; second, identifying the ultimate beneficial owner (UBO), where KYC is performed for these individuals. Based on these key steps, customer due diligence processes then undertake wider investigation of firms' and their owners' finances and history, for both business (credit evaluation, risk-management, fraud prevention) as well as regulatory requirements (in particular AML and also increasingly data protection).

In this final section, we discuss initiatives by which the government takes the lead to provide the foundational digital infrastructure and data-sharing framework as a public good for the identification of corporates and/or individuals, though the participation of private-sector service providers is not precluded. A noteworthy example is the Aadhaar digital identity system of India, together with its data governance framework known as account aggregators. We thus discuss this and other selected examples.

[32] For details, see Asian Development Bank (2021). "2021 Trade Finance Gaps, Growth, and Jobs Survey", *ADB Briefs* No. 192.

7.1 India's Aadhaar, account aggregators and corporate digital ID

The underlying principle of the data aggregation approach is that individuals and SMEs should reap the benefits of the data generated from their business activities. These data should not be cornered by the state or any private sector firm in "walled gardens" of data, with the original data owners being precluded from the benefits generated. Applying this principle to banking and financial services, this means that individuals and SMEs should be able to make use of their own data to gain better access to these services. For example, SMEs should be able to provide these data to banks so that their credit risk can be properly assessed. In order to operationalise this principle, India introduces data intermediaries known as account aggregators that facilitate data aggregation and sharing. Many jurisdictions require sharing of credit information, both to reduce fraud, credit risk and information asymmetries but also to enable more effective lending practices to support financial inclusion and broader developmental objectives.

The ecosystem of account aggregators is built on the foundation of Aadhaar, which is a 12-digit identification number issued by the Unique Identification Authority of India. Launched in 2009, Aadhaar has developed rapidly in a little more than a decade. By the end of October 2021, 1.26 billion Indians (92.6% of total population) already had an Aadhaar.[33] The rapid growth in its adoption rate reflects the merits of the system, such as minimal information requirement, low cost per identification and various features to protect data privacy. For example, an applicant for an Aadhaar number only needs to provide four pieces of information, namely, his or her name, date of birth, gender and residential address. Financial institutions are able to use an eKYC API to access the Aadhaar details for verification. Studies have found that the Aadhaar system led to a significant increase in bank accounts and a significant reduction in the exclusion of marginalised groups such as low-income people and those in rural areas.[34]

The account aggregator framework was announced by the Reserve Bank of India (RBI) in 2016 and came live in September 2021. Key participants of system consist of account aggregators, financial information providers (FIPs) and financial information users (FIUs) (Graph 7). Account aggregators are data intermediaries registered as non-bank financial companies with the RBI. Their role is to ensure that the aggregation and sharing of financial data proceeds in a secure, transparent and efficient manner. Specifically, they retrieve or collect data about the financial assets of a customer from the FIPs and then aggregate, consolidate and present it to the FIUs. Data transfer is conditional on an explicit consent of the FIPs. An important feature is that these data intermediaries are blind to these data. Once approved, data flows directly between the FIPs and FIUs on an encrypted basis, and the account aggregators are incapable of reading or storing the data for further use. In addition, the account aggregator accounts are portable so that individuals are able to freely change their account aggregators. They can also restrict consent in terms of time and data categories, and revoke it at any time. In the first 30 weeks since coming live, 230,000 consent requests from the FIUs were processed, or around 1000 per day. In

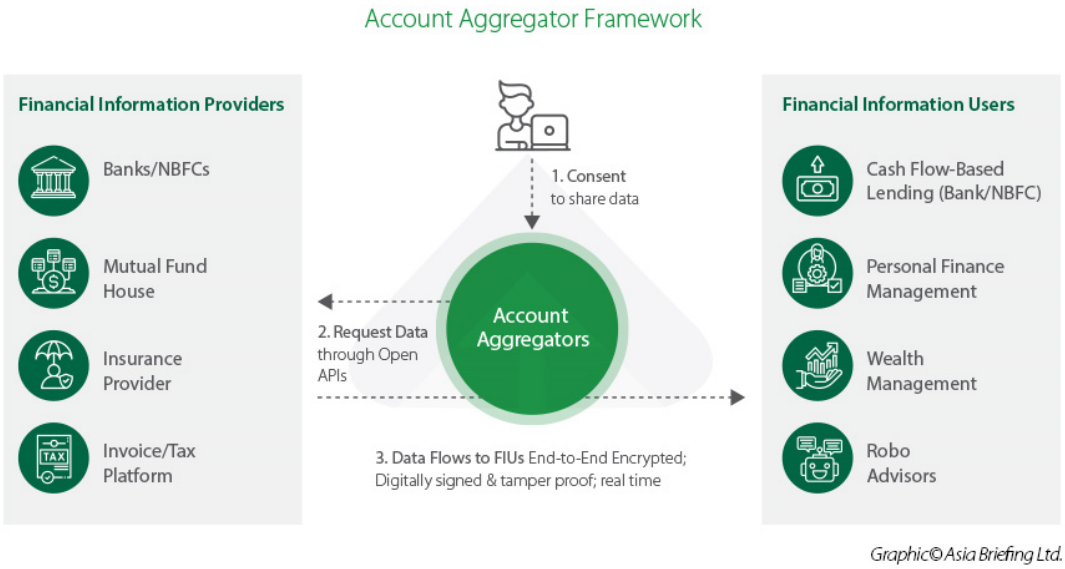
[33] For details, see https://uidai.gov.in/aadhaar_dashboard/.

[34] See D'Silva et al (2019).

90-95% of cases, the FIPs have successfully addressed consent requests with an average response time in seconds.[35]

Here is an example of how the account aggregator framework can promote financial inclusion. An SME seeking a loan finds that its financial data resides in multiple institutions, and it is hard for the SME to consolidate and share the data with the lender. Under this framework, the SME can demand that a list of information (eg tax returns, bank account data, mortgage loan payments) be shared with the lender (eg a bank) with the intermediation of an account aggregator. Compared to conventional methods of collecting information from multiple sources, many of which are still paper-based, this is much more efficient. This also allows the use of cash-flow based data to process the loan application, as opposed to the traditional asset-based lending secured by physical collateral such as property. To an asset-poor SME, it is often more feasible to prove its creditworthiness by cash-flow based evidence than by pledging collateral to secure a loan. Furthermore, such evidence is usually more up to date and dynamic and therefore more relevant to their financial health and a better input for the loan approval process.

India's account aggregator framework — Graph 7



Source: Asia Briefing

7.2 Other public sector initiatives

The public sector plays a role in several other important areas supporting corporate digital ID. For instance, regulators and policymakers have a key role in the coordination of existing processes relating to tax information sharing and beneficial ownership disclosure (coordinated by the OECD), AML/CFT (coordinated by the FATF), OTC derivatives and financial infrastructure (coordinated by the FSB, CPMI and IOSCO) and others such as capital markets and ESG data (coordinated by IOSCO and

[35] For details about the adoption, see Tiwari et al (2022).

the ISSB). In this last sub-section, we survey a few further relevant public sector initiatives.

Singapore's MyInfo

MyInfo provides a useful example of a hybrid system in the context of individual digital identity. It features a sovereign digital ID at the base, which is then linked to a range of other golden source data from government and other sources that can be shared via the system under the control of the individual. This, in turn, can support ID&V of firms. Through the MyInfo Business API, firms can easily query data and verify features of individual companies in Singapore.

Netherlands eHerkenning

In the Netherlands, in addition to the digital ID platform for individuals (DigiD), the government offers companies a standardised log-in system to access over 500 public and private sector service providers. The eHerkenning ("e-recognition") system offers four successive levels of assurance, depending on the needs of the use case in question. As of 2020, it counted over 600,000 companies and 17 million successful authentications. In early 2022, it added additional functions around chain authorisation.

UN Sustainability Development Goals (SDGs)

International policy efforts also recognise the link between individual and corporate ID. Globally, it is estimated that 1 billion people lack formal ID credentials. Reflecting the significance of identification for inclusion and development, legal identity for all has been included as one of the SDG targets. As shown in the country examples discussed above, this too can support corporate digital ID for SMEs in particular.

ID4D

In support of the SDGs, the World Bank launched its Identification for Development (ID4D) initiative in 2016. As part of this process, the initiative has developed Principles on Identification for Sustainable Development comprising 10 principles, addressing issues such as trust, security, interoperability, privacy, technology and governance. While the Principles are focused on individual ID, the broad principles are likewise the central concerns of corporate digital ID. In addition to principles, the initiative coordinates a range of organisations, provides assistance and has developed a series of case studies and technical standards based on country experiences around the world.

8. Conclusion

Corporate digital ID can significantly speed up identification and verification of a company, thus enabling its counterparties, such as banks and suppliers, to manage business risks and meet regulatory requirements more efficiently. As a result, a company can build business relationships with these counterparties much more swiftly with corporate digital ID. In addition, digital ID facilitates the establishment of trust since technology allows corporate data to be verified more easily and transmitted to users more securely. Looking beyond operational efficiency or user

experience, a well-established corporate digital ID is also a crucial enabler for promoting financial inclusion and safeguarding financial stability and market integrity.

In many ways, corporate digital ID parallels individual digital ID, but there are important differences. Unlike an individual, the attributes of a corporation (eg directors) may change much more frequently and therefore require timely updating. A corporation can be part of a complicated corporate structure, with parts of it located in multiple jurisdictions, thus making it a challenge to identify its beneficial ownership as required by some regulations. Therefore, corporate digital ID is not a mere extension of individual corporate ID. That said, individual digital ID is a very significant supplement to corporate digital ID, due to the need to identify and verify the identities of individuals that claim to represent the corporation.

With the innovative use of technology and appropriate policies, this study finds that important progress can be made in corporate digital ID by a variety of stakeholders, including corporate registries, banks and other financial institutions, established vendors and service providers, regtech firms and public authorities. Some initiatives are foundational, such as LEI, that serves as a global identifier to connect multiple networks, each of which can contribute important attributes to a corporate digital ID. The decentralised identifiers (DIDs) standard can help to aggregate information from different sources. Meanwhile, some solutions are more tailor-made to specific sectors. For example, digital ID solutions for SMEs make use of alternative data in lieu of more official documents that are not available to some SMEs. As a complementary approach, the public sector can aim to build further infrastructures, potentially building on publicly provided individual ID. Each of these stakeholders have their own strength in terms of resources, technology sophistication and trust by the public, but also their own challenges to overcome.

Based on what we know today and can reasonably foresee in the near future, there is no silver bullet that can achieve all the potential benefits at once, nor can any single stakeholder drive all the needed changes. Many stakeholders are involved. Nor is the solution purely technological in nature. Political will is necessary to drive change and achieve necessary network effects. Non-technological factors, such as common data standards, governance models and clarification of legal or regulatory uncertainties, are also important for realising the promises of corporate digital ID. The silver lining is that, working together, these stakeholders have the potential to address the main pain points of corporate ID&V.

References

Arner, D (2002), "Development of the American law of corporations to 1832", 55 *SMU Law Review*, no 23, pp 23–57.

Arner, D, G Castellano and E Selga (2022), "Financial data governance", European Banking Institute Working Paper no. 117, March.

Arner, D, D Zetzsche, R Buckley and J Barberis (2019), "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities", *European Business Organization Law Review*, 20, 55–80.

Asian Development Bank (ADB) (2021), "2021 trade finance gaps, growth and jobs survey", ADB Brief, no 192, October.

Auer, R, C Monnet and HS Shin (2021), "Distributed ledgers and the governance of money", BIS Working Papers, no 924.

Basel Committee on Banking Supervision (BCBS) (2012), *Basel Core Principles*.

D'Silva, D, Z Filková, F Packer and S Tiwari (2019), "The design of digital financial infrastructure: lessons from India", BIS Papers, no 106.

Financial Action Task Force (FATF) (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, Paris.

FATF (2020), "Guidance on Digital Identity", Paris.

FATF (2021a), *Opportunities and Challenges of New Technologies for AML/CFT*, Paris

FATF (2021b), *Revisions to Recommendation 24 and its Interpretative Note – Public Consultation*, Paris.

FATF (2021c), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers , Paris.

Finck, M (2018), *Blockchain Regulation and Governance in Europe*, Cambridge: Cambridge University Press.

Garber, E, M Haine, V Knobloch, G Liebbrandt, T Lodderstedt, D Lycklama and N Sakimura (2021), *GAIN DIGITAL TRUST: How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network*, European Identity and Cloud Conference, Munich, September.

Gartner (2022), "Gartner Hype Cycle", accessed 1 February.

Global Legal Entity Identifier Foundation (GLEIF) (2021a), "How can the LEI contribute to the technical implementation of the global minimum corporate tax rate and reallocation of taxable profits of large multinational corporations (MNCs)?", GLEIF Working Document.

GLEIF (2021b), "Introducing the Legal Entity Identifier (LEI)".

GLEIF (2021c), "Introducing the Verifiable LEI (vLEI)".

Greif, A (1993), "Contract enforceability and economic institutions in early trade: the Maghribi traders' coalition", *American Economic Review*, vol 83, no 3, pp 525–48.

Institute of International Finance (IIF) (2020), *Digital Identities in Financial Services - Part 3: The Business Opportunity for Digital Identity*.

International Committee on Credit Reporting (ICCR) (2018), *Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs operating in the Informal Economy, Guidance Note*.

International Labour Organization (ISO) (2019), *Small Matters: Global evidence on the contribution to employment by the self-employed, micro-enterprises and SMEs*.

Landa, J (1994), *Trust, ethnicity and identity: the new institutional economics of ethnic trading networks, contract law and gift-exchange*, Ann Arbor: University of Michigan Press.

Mickelthwait, J & Woodbridge, A (2003), *The Company: A Short History of Revolutionary Idea*, Random House.

McKinsey Global Institute (2019), *Digital identification: A key to inclusive growth*.

Monetary Authority of Singapore (2021), *Foundational Digital Infrastructures for Inclusive Digital Economies*.

Murphy, H (2020), "SEC steps in after investors buy up the wrong Zoom", *Financial Times*, March.

National Centre for Asia Pacific Economic Cooperation (NCAPEC) Working Group on E-Signatures (2022), *Advancing Digital Transactions in APEC: Enhancing e-signatures and digital signatures*.

Rice, T, G von Peter and C Boar (2020), "On the global retreat of correspondent banks", *BIS Quarterly Review*, March.

Tiwari, S; Sharma,S; Shetty,S and Packer,F (2022), "The design of a data governance system", BIS Papers, No 124, 05 May 2022.

Society for Worldwide Interbank Financial Telecommunication (SWIFT) and EuroFinance (2019), *Solving the KYC Conundrum*.

World Bank (2018), *Technological Landscape for Digital Identification*

World Economic Forum (WEF) (2018), *Identity in a Digital World - A new chapter in the social contract*, September.

WEF (2016), *A Blueprint for Digital Identity – The Role of Financial Institutions in Building Digital Identity*, August.

Annex: Survey questions

In order to supplement the contents obtained from the interviews, we conducted an open survey on fintech firms offering corporate digital ID solutions and other stakeholders from 24 August to 10 September 2021, seeking their views on corporate registries, LEI and existing technologies. The survey questions are as follows.

Existing corporate registries and related services and automation

1. In your view, for financial crime compliance purposes, which jurisdictions have the most accurate, accessible or useful corporate registries?
2. Which jurisdictions have automated corporate registries that are easily accessible and useable?
3. What are the key automated functions you have experienced when using these automated corporate registries?
    a. API (Application Programming Interface)
    b. Blockchain Technology
    c. LEI (Legal Entity Identifier)
    d. Vendor Tools
    e. Other
4. Which automation function do you find most useful and why?
5. Are there any registries that to your knowledge provide corporate identity verification services (to identify real persons behind the corporate) as compared to only enabling look-up of registration?
6. What are your current challenges in terms of online access to registries and availability of information?
    a. Lack of beneficial ownership details
    b. Details of directors and shareholders not accessible
    c. Data not refreshed
    d. Inaccurate data
    e. Other
7. What are your main challenges in using corporate registries?
8. Where, in your view, is innovation lacking in the current capabilities and functionality of corporate registries?
9. Any other observations or breakthrough thinking you would like to share about corporate registries?

Use, adoption and opportunities of Legal Entity Identifier (LEI)

10. Are you familiar with LEI?
    a. Yes
    b. No
11. What in your view are the most useful aspects of using an LEI?
12. How do you currently use LEI within your organisation, in particular in financial crime controls and as part of corporate identity verification and Know-Your-Customer (KYC) processes?
13. Do you use LEI in your Financial Crime compliance processes? If not, then please explain why?

14. Do you use LEI in any other area of your business and operations? If not, then please explain why?
15. Do you think that if corporate registries requested an LEI for every corporate registration, such may improve corporate onboarding speed with bank and non-bank financial institutions and therefore foster financial inclusion?
    a. Yes
    b. No
16. If your answer to the above question is Yes, then please answer why?
17. Any other observations or breakthrough thinking you would like to share about LEIs?

Existent technology that bridges the gap and can be used for corporate identity verification and KYC

18. What are the key challenges that your organisation has experienced in verifying corporate identity and identifying UBOs?
19. Do you use third party or API services to support your KYC processes, information gathering and automation?
    a. Third Party Support
    b. API Services support
    c. Other
20. If you utilise third party services (eg Bureau Van Dyke, Dun & Bradstreet, Trulioo, Chekk), please specify their name.
21. What are the steps taken by your organisation towards digitisation of the corporate identity verification and KYC processes?
22. Do you think any novel technologies like artificial intelligence and confidential computing will be exponentially helpful to corporate identity verification?
    a. Yes
    b. No
23. If your answer to the above question is yes, then please specify which ones, why and over which time frame?
24. What are the key factors that you consider in adopting new and innovative technologies in corporate identity verification and KYC and why, eg legal recognition and regulatory approval?

Any other observations, innovative or breakthrough thinking you would like to share about technologies for corporate identity verification and KYC processes?

Previous volumes in this series

No	Title	Issue date
BIS Papers No 125	Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies	May 2022
BIS Papers No 124	The design of a data governance system	May 2022
BIS Papers No 123	CBDCs in emerging market economies	April 2022
BIS Papers No 122	The monetary-fiscal policy nexus in the wake of the pandemic	March 2022
BIS Papers No 121	Covid-19 and the monetary-fiscal policy nexus in Africa	February 2022
BIS Papers No 120	Virtual banking and beyond	January 2022
BIS Papers No 119	Non-bank financial institutions and the functioning of government bond markets	November 2021
BIS Papers No 118	A taxonomy of sustainable finance taxonomies	October 2021
BIS Papers No 117	Fintech and the digital transformation of financial services: implications for market structure and public policy	July 2021
BIS Papers No 116	CBDCs beyond borders: results from a survey of central banks	June 2021
BIS Papers No 115	Multi-CBDC arrangements and the future of cross-border payments	March 2021
BIS Papers No 114	Ready, steady, go? – Results of the third BIS survey on central bank digital currency	January 2021
BIS Papers No 113	Financial market development, monetary policy and financial stability in emerging market economies	December 2020
BIS Papers No 112	The dawn of fintech in Latin America: landscape, prospects and challenges	November 2020
BIS Papers No 111	Inflation dynamics in Asia and the Pacific	March 2020
BIS Papers No 110	Measuring the effectiveness of macroprudential policies using supervisory bank-level data	February 2020
BIS Papers No 109	The digital economy and financial innovation	February 2020
BIS Papers No 108	Stress testing in Latin America: A comparison of approaches and methodologies	February 2020

All volumes are available on the BIS website (www.bis.org).