ALLIANCE FOR ETRADE DEVELOPMENT

ENABLING MSMES' CROSS-BORDER ECOMMERCE THROUGH A SCALABLE CORPORATE DIGITAL IDENTITY

30 September 2021

This document is made possible by the generous support of the American People through the United States Agency for International Development (USAID). The contents are the responsibility of Palladium and do not necessarily reflect the views of USAID or the United States Government.

ALLIANCE FOR ETRADE DEVELOPMENT

ENABLING MSMES' CROSS-BORDER ECOMMERCE THROUGH A SCALABLE CORPORATE DIGITAL IDENTITY

Agreement No:

7200AA19CA00021

Submitted to:

USAID Center for Economics and Market Development

Prepared by:

Kati Suominen, Founder and CEO, Nextrade Group and Technical Director Alliance for eTrade Development

DISCLAIMER:

The authors' views expressed in this document do not necessarily reflect the views of the United States Agency for International Development or the United States Government or of any members of the Alliance for eTrade Development.

TABLE OF CONTENTS

I. INTRODUCTION....4
II. PAIN POINTS FOR MSMES TO ACCESS SERVICES FOR CROSS-BORDER ECOMMERCE....6
III. USE CASES FOR CORPORATE DIGITAL IDS....14
IV. WHY THE EXISTING ID ARCHITECTURE DOES NOT SUPPORT MSMES IN ECOMMERCE 19
V. CORPORATE DIGITAL ID ARCHITECTURE TO PROMOTE DEVELOPING COUNTRY MSMES' CROSS-BORDER ECOMMERCE....26
VI. CONCLUSION....32

ACKNOWLEDGEMENTS

This report was produced for the Alliance for eTrade Development, a Global Development Alliance supported by the U.S. Agency for International Development. The author would like to thank Erica Vambell for excellent research assistance and Neha Gandhi, Alexander Huetink. Kok Kee Lim, Tony Murphy, and Kenneth Tay for most valuable comments and thought leadership.

I. INTRODUCTION

In 1996, Francis Fukuyama's book *Trust: The Social Virtues and the Creation of Prosperity* broke new ground in explaining why some societies prosper while others languish. Trust among individuals, Fukuyama wrote, is social capital or "unspoken, unwritten bond between fellow citizens" that "facilitates transactions, empowers individual creativity, and justifies collective action."[1]

Trust has for centuries been critical also for international trade. Lack of trust between buyers and sellers located far apart has curtailed trade and kept vast majorities of businesses from ever exporting. Buyers and sellers that did find each other would build trust over years, for example by paying each other many visits and over and again transacting in a mutually satisfactory manner—such as with the seller promptly shipping the ordered products and buyer paying in full and on time.

Over the past two decades, ecommerce has accelerated trust-building by enabling buyers to quickly find sellers, access sellers' customer reviews, use secure payments, and resort to online dispute resolution mechanisms, among other benefits. Yet one vexing problem remains in online transactions: how does the buyer at the other end of a transaction know that the seller is who they say they are, and vice versa?

This question is timely and policy-relevant, given the growing challenges posed by cybersecurity threats and identity theft to firms around the world, and the rapidly expanding opportunities for micro, small, and midsize enterprises (MSMEs) to use ecommerce to recover from the COVID-19 crisis. It is perhaps a particularly pertinent in B2B transactions that involve large volumes and greater risks than small B2C transactions—and an especially important question for MSMEs that often have less brand recognition than multinational sellers.

The challenges with trust online transcend the relationship between the seller and buyer—they shape MSMEs' access to the many services they need for doing cross-border ecommerce. Because B2B online marketplaces have no one way to validate that the seller they are onboarding is a legitimate business, they and aspiring sellers need to spend significant resources and time in paper-based processes to authenticate and verify sellers. Because banks cannot rely on the company's word that it is duly registered with the appropriate authority, owned by who it says it is owned by, and is engaged in a legal activity, they have to handle countless of documents and spend countless hours performing know your customer (KYC) diligence. Because large firms performing their know your supplier (KYS) processes cannot easily access the financial, reputational, environmental, and regulatory risks that suppliers may pose, they will stick to tested and tried suppliers. And because online buyers cannot easily verify that the seller behind an online storefront is real and can deliver, they have to make calls to the seller, get references, and perhaps visit the seller – or not bother at all.

For small businesses seeking to use online marketplaces to connect and transact with new customers and financial, logistics, and other trade services, these challenges cascade, resulting in paperwork, duplication of efforts, and transaction costs. The complexities involved with using B2B marketplaces and limited interoperability among marketplaces and other services also limits marketplaces' value to sellers and keeps most trade transactions offline.

A corporate digital identity that is unique to each seller and associated with the seller's enterprise and data would be a powerful solution to these challenges. It could dramatically accelerate marketplaces' customer authentication and verification (A&V) processes, banks' KYC processes, multinationals' supplier onboarding, and MSMEs' trust-building with prospective buyers. A digital ID could also promote interoperability across marketplaces and services: an MSME could use one "master key" with the same

credentials and data on their proof of existence, features, and transactions with each marketplace, bank, logistics provider and government agency. For example, a corporate digital ID could be used to enable MSMEs that sell on marketplaces to access a range of downstream financial, logistics, insurance, and payment services they need for fulfilling orders received on marketplaces – perhaps right through the marketplace's interface. A unique corporate digital ID could also enable different government agencies and different levels of government to quickly authenticate businesses and to better track, tax, and service MSMEs in their economies.

Instead of social capital discussed by Fukuyama, today's sellers need digital capital to build trust and transact with online buyers and service providers. A strong digital identity creates digital capital.

This concept is not new. A growing number of countries have adopted, or are adopting, individual digital IDs that enable citizens and residents to access public and private services efficiently; the United Nations has highlighted "legal identity for all" as a key 2030 Sustainable Development Goal. A set of countries such as Singapore, Estonia, Azerbaijan, and Netherlands have also already adopted a corporate digital IDs which firm representatives can use to access and use numerous government services, and, increasingly, private B2B services. The Legal Entity Identifier (LEI) launched by the G20 has sought to scale and internationalize the concept of a corporate digital ID and is now being used by some one million firms. In addition, both individuals and businesses are provided digital identities by a huge array of service providers and platforms—Facebook and Google logins are among the best-known services.

However, one critical piece is missing in this global constellation of ID systems: a globally scalable and secure digital identity for corporations, including MSMEs. Such an ID would be more trustworthy than a social media login and enable MSMEs to access the data they have provided to governments and service providers, and use it to build trust and authenticate themselves with prospective customers and service providers.

The purpose of this white paper is to help accelerate the adoption of this type of scalable and secure self-sovereign corporate digital IDs, with the goal of helping developing country MSMEs to engage in trade and ecommerce. Specifically, this paper:

- Reviews the pain points facing marketplaces, financial services, governments, and buyers and sellers in authenticating MSMEs online;

- Assesses the features, use cases, and value propositions of different types of corporate digital ID systems for MSMEs, service providers, and governments;

- Discusses the many challenges facing developing countries that might seek to build their own corporate digital ID systems from scratch, such as costs, legal responsibilities, and challenges of international interoperability; and

- Proposes a scalable self-sovereign ID system that draws on a wide range of public and private data sources and is globally interoperable.

The following section reviews pain points for MSMEs attempting to access services for cross-border ecommerce, and for service providers and government agencies to authenticate and authorize MSMEs to access their services. Section three reviews the use cases and value propositions of corporate digital ID systems for marketplaces, banks, and governments, and details ways in which the main existing corporate digital ID systems help solve these pain points. Section four discusses the optimal global corporate ID architecture, and section five concludes.

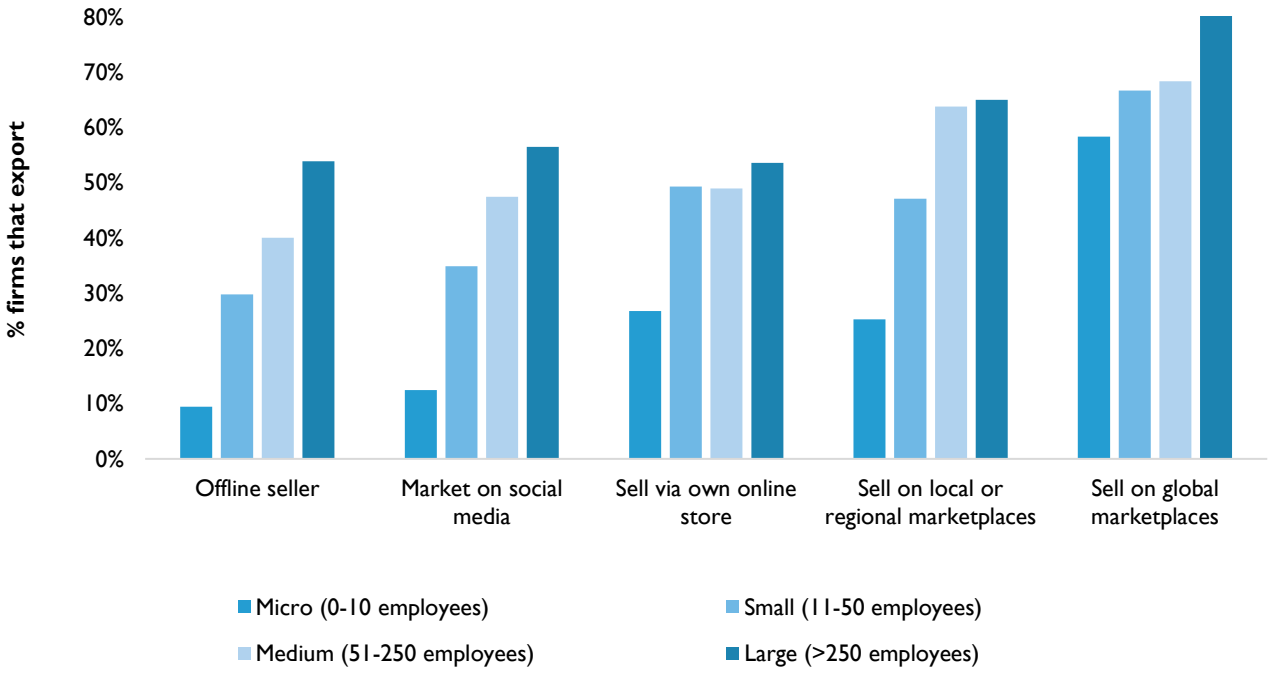
II. PAIN POINTS FOR MSMES TO ACCESS SERVICES FOR CROSS-BORDER ECOMMERCE

Ecommerce has revolutionized the opportunities for MSMEs to reach customers in new markets. By using ecommerce, especially global online marketplaces, businesses of all sizes become visible to prospective customers around the world. Survey data generated by Nextrade Group in over 50 countries consistently shows that online sellers are likelier to export, import, and grow faster than firms that do not use ecommerce (figure 1). Online sellers are also likelier than offline sellers or social sellers to be multimarket sellers (figure 2). Firms that procure goods and services online are also likelier to import than firms that do not buy online.

Of course, the use of marketplaces and ecommerce does not necessarily *cause* firms to trade – the correlation between exporting, importing, and ecommerce use may simply mean that existing exporters and importers have self-selected into ecommerce. However, surveys also consistently show that 25-50 percent of firms, depending on the country, started to export *after* starting to use ecommerce, and that majorities of existing exporters gained new international customers and grew exports to new international markets thanks to ecommerce.

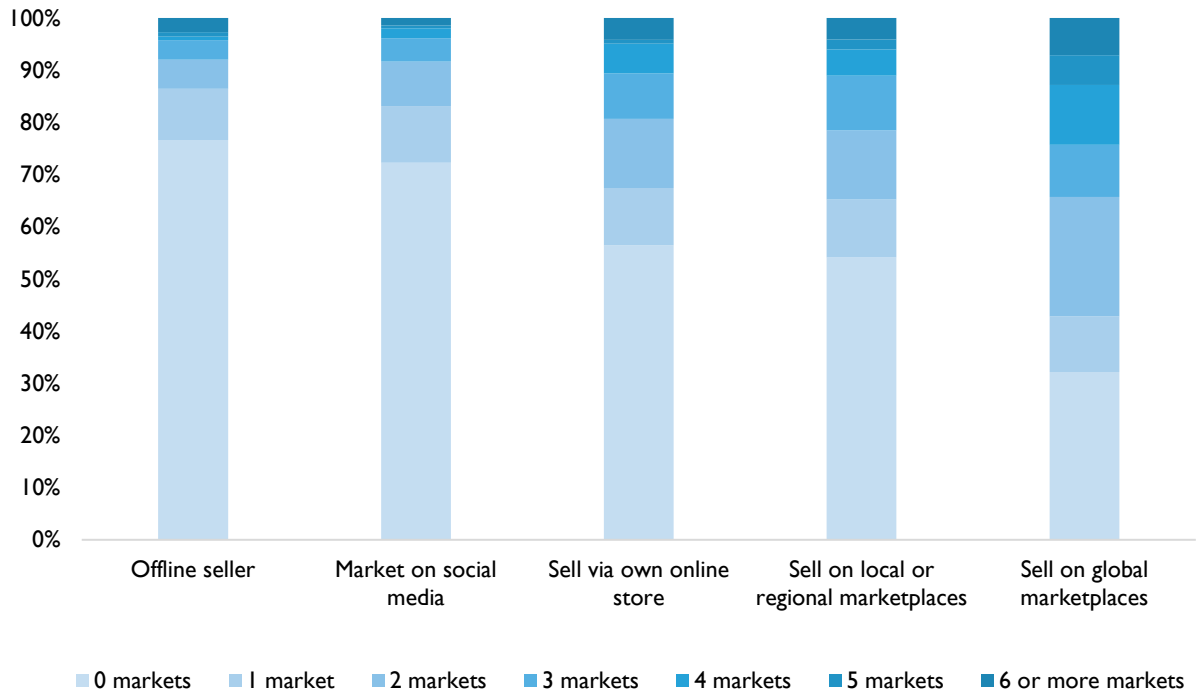
Ecommerce enables MSME to trade in part because it reduces the geographic distance that has for centuries limited visibility, trust, and trade between buyers and sellers located far from one another.[2] Such tools as online customer reviews, sophisticated and secure cross-border payments, and online dispute resolution mechanisms provide buyers a sense of trust, the lubricant for trade that used to build up over the course of repeated transactions between buyer and seller.

Figure 1: Share of Firms that Export, by Online Activity and Size



Source: Nextrade Group survey for the Alliance for eTrade Development with 2,034 Mexican MSMEs on 2-9 September 2020.

Figure 2: Share of Firms by Number of Export Markets and Products and Sales Channels



Source: Nextrade Group survey for the Alliance for eTrade Development with 2,034 Mexican MSMEs on 2-9 September 2020.

Ecommerce use has been found to have broader positive impacts on developing country firms, trade, and economies. For example, ecommerce can help reduce in-country disparities in enterprise formation and growth, level the playing field between men- and women-led firms in access to markets and services, and advance regional economic integration among developing nations.[3]

However, MSMEs looking to sell online, use ecommerce marketplaces, and access financial and logistics services face several challenges, including in authenticating themselves with the providers that enable them to engage in cross-border ecommerce. Firms face three distinct problems:

- **Paper-based processes to build trust:** Authenticating themselves with a new provider or a customer is often an expensive, time-consuming, paper-based process.
- **Duplication across providers:** once an MSME has been authenticated with one provider such as a bank or a marketplace, it cannot use the same credentials again with another marketplace but instead needs to repeat the onboarding process with each new provider.
- **Walled gardens:** Once authenticated and verified, the firm is stuck in the service provider's "walled garden," rather than being able to use two or more services easily.

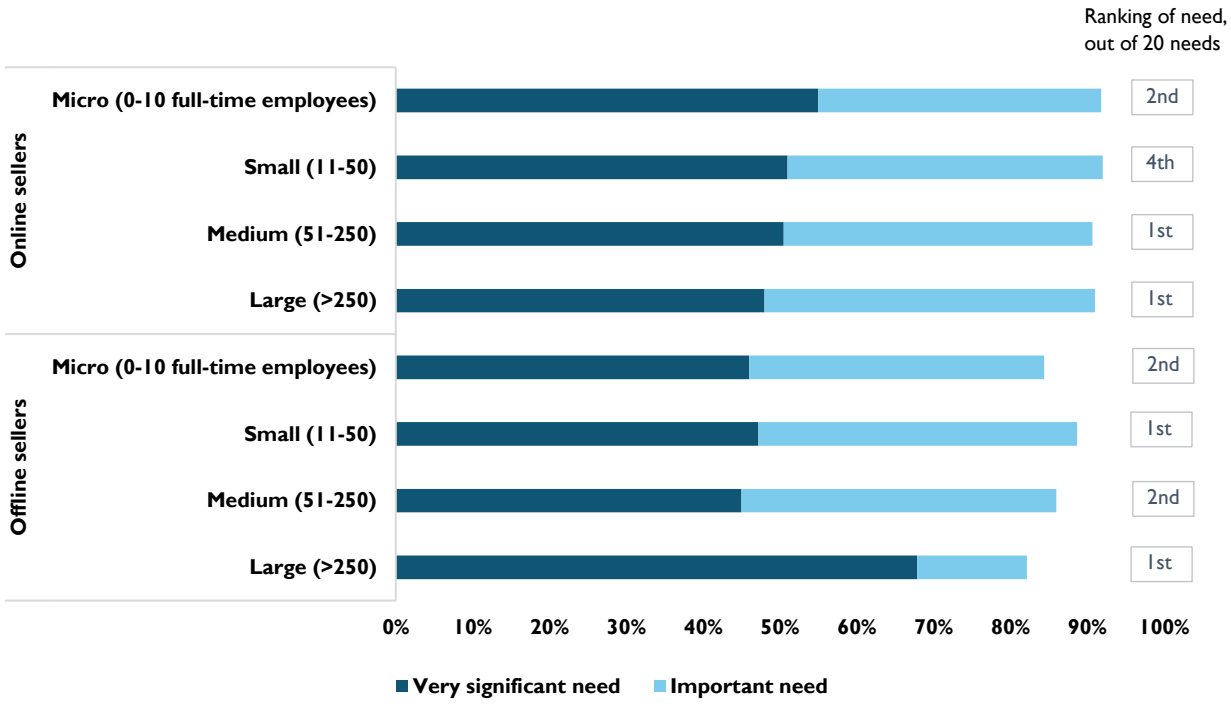
The following subsections look at these pain points in detail.

A. MSMES FACE A HIGH AUTHENTICATION AND DUE DILIGENCE COSTS

Buyers and sellers that meet online for the first time still need to build trust with each other. In a recent survey carried out by Nextrade Group for the eTrade Alliance, over 50 percent of Mexican micro and small firms that have yet to start selling online and over 40 percent of existing online sellers expressed a "great need" for tools like a digital identity or trustmark to authenticate themselves with their prospective customers (figure 3). Easier means to authenticate themselves was a top-2 need for the surveyed firms to engage in ecommerce, out of a list of 20 potential needs.

This challenge repeats across markets: the millions of MSMEs that are starting to sell online today have few ways to demonstrate they are trustworthy. This is perhaps especially true with small firms in emerging markets and developing economies, due to firms' limited track records, scant brand recognition, and buyers' concerns about online fraud.

Figure 3: Percentage of MSMEs that indicate digital identity or another similar tool to build online trust with customers and vendors is a "very significant need" or an "important need" for them to be able to engage in ecommerce and grow their online sales



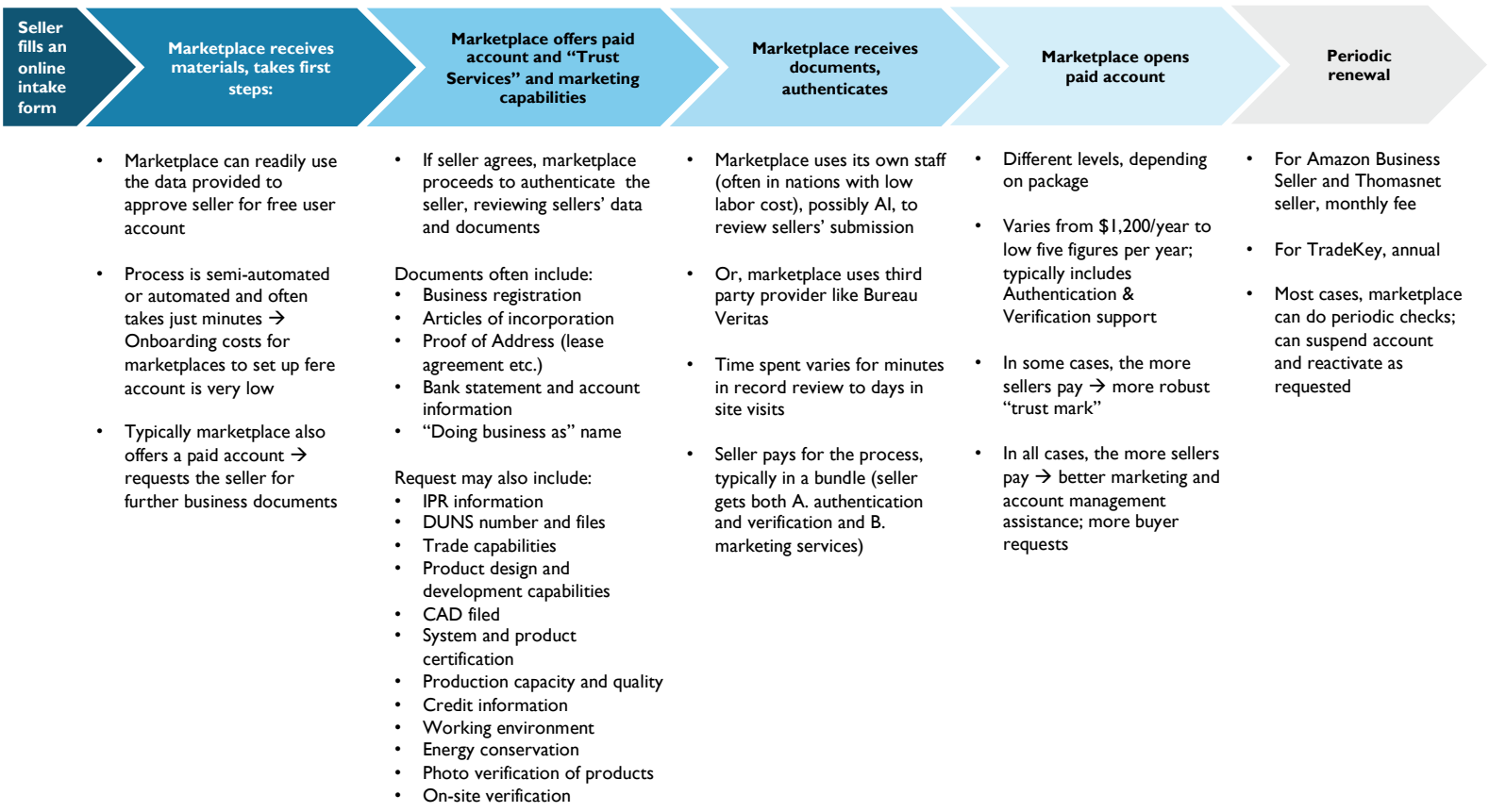
Source: Nextrade Group survey for the Alliance for eTrade Development with 2,034 Mexican MSMEs on 2-9 September 2020.

Players in the ecommerce ecosystem have sought to address these challenges to onboarding MSME customers and users more efficiently. B2B marketplaces have particularly sought to build buyers' trust by providing aspiring marketplace sellers fee-based A&V and marketing services.[4] During the A&V process, sellers essentially outsource trust-building to the marketplace they onboard. They provide the

marketplace with various business documents, such as articles of incorporation, business registration records, bank statements, utility bills, lease agreements, and so on (the standard marketplace onboarding process is described in figure 4; for further details on these processes in major B2B marketplaces, see appendix I). Some marketplaces outsource the A&V work to a third party—for example, Madeinchina.com uses Bureau Veritas and SGS to authenticate sellers; some marketplaces go even deeper, offering site visits as part of their A&V program.[5]

The process of authenticating themselves with B2B marketplaces implies real costs for MSMEs, typically ranging from $2,000 to $12,000, depending on the marketplace. This fee is payable by the firms that seek to onboard the marketplaces and include marketing services for firms once the A&V process has been completed. Verifying MSMEs is of course a sound business practice for the marketplace: it needs to vet sellers before championing sellers to buyers.

Figure 4: Selected B2B Marketplaces' Onboarding Requirements for MSMEs



Note: the analysis included Amazon Business Seller B2B, Tradekey, Thomasnet, MadeinChina.com, Alibaba, ConnectAmericas.

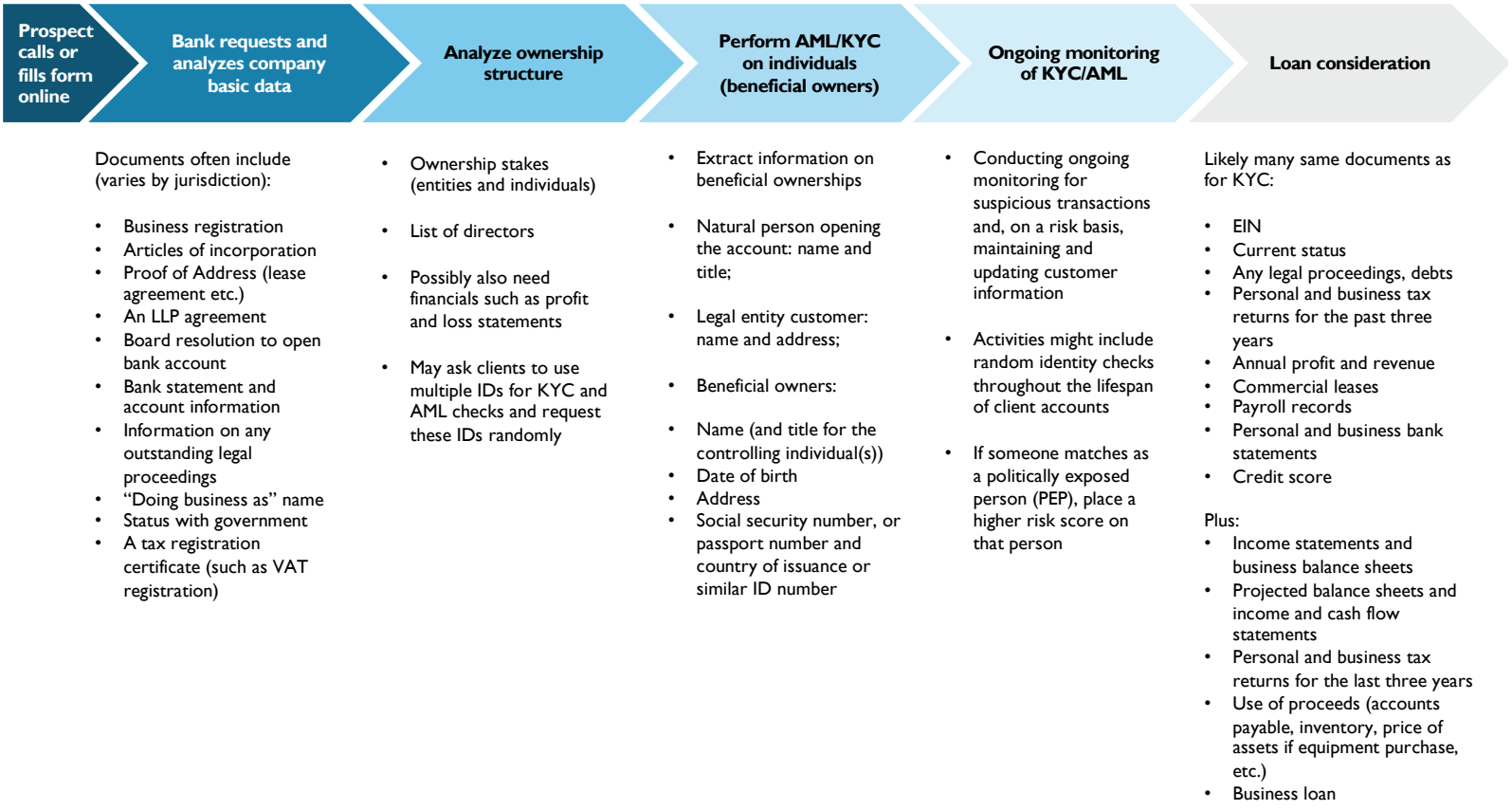
MSMEs' onboarding process with financial service providers is similar, albeit often longer and more taxing (figure 5). Banks have in recent years come under significant regulatory pressures to carry out thorough KYC processes and anti-money laundering (AML) checks with each new customer, and are often particularly hard-pressed to authenticate "thin-file" MSMEs that have opaque financials and limited track records. In some surveys, onboarding a single business costs a bank some $6,000, mostly due to labor in document checking.[6] Surveys also suggest that six in ten senior bank salespeople spend more

than 1.5 days of their week onboarding new customers, and more than five in ten agree that quality of data or lack of data on customers are major challenges.[7] These numbers have remained similar over time, even if digitization has simplified banks' access to data and facilitated their processes.
These costs continue through the life of the relationship. For example, a bank considering granting a loan to an MSME needs the latest business documents rather than those with which the account was originally opened. As the fixed cost of due diligence have risen in recent years relative to proceeds the MSME generates, financial services providers have fewer incentivizes to deal with small firms or extend loans to them.

For their part, MSMEs are unhappy with banks: even in the UK, a global leader in developing financial solutions for MSMEs, a group of MSMEs surveyed in 2019 singled out verification as one of the biggest pain points in dealing with banks, with 84 percent reporting a bad KYC experience.[8] More than half of MSMEs apply to one single loan provider because of the time and hassle associated with the application journey.[9] Some processes are simply unnecessary: 89 percent of UK companies reported they have to enter the same information multiple times in any one loan application. Globalizing companies duplicate processes even with their own bank: opening a bank account even with the same bank in a different country is another cost and process, as regulatory requirements vary across jurisdictions. [10]

COVID-19 has propelled the digitization of banking, but 68 percent of UK MSMEs surveyed in 2020 still said that the digital features of their business bank accounts are not as advanced as those of consumer bank accounts.[11] MSMEs are however readier to share data: 76 percent are willing to connect other business systems and share more data with their bank, if it means getting quicker loan approvals.[12]

Figure 5: Typical Bank Onboarding Process for MSMEs



B. MSME CARRY OUT DUPLICATE EFFORTS AND PAPER-BASED, MANUAL PROCESSES WITH EACH SERVICE PROVIDER

Buyers, marketplaces, and other service providers such as logistics and financial services companies typically have their own unique onboarding requirements, so that an MSME needs to repeat the onboarding process with each provider using the providers' respective forms and data fields—although the information MSMEs fill in is often the same they have just provided to another provider. Some of this data is still submitted in the form of paper-based business documents. This setting is akin to America's pre-electronic records healthcare system, where patients manually entered the same information on themselves on each distinct provider's forms.

Similarly, MSMEs often have to provide the same information to many distinct government agencies, such as tax authorities, employment agencies, small business agencies, and customs agencies. For example, a small business agency considering a loan guarantee to an MSME may not readily have access to data on the MSME's business licenses, employee headcounts, or annual revenues, and has to request those from the company. The company, in turn, has to gather the data and documents from its files and disparate filings with various government agencies, and likely re-enter various data manually. In a recent survey, small Canadian companies were found to spend C$6,744 per worker annually in dealing with regulations, most of it on this type of duplication of efforts.[13]

C. MSMES' SERVICE PROVIDERS' "WALLED GARDENS" AND LACK OF DATA PORTABILITY IMPEDE INTEROPERABILITY

Once onboarded onto a marketplace or another two-sided platform, an MSME is locked into dealing with buyers and users on that platform. The platform is in essence a "walled garden." MSMEs that wish to reach buyers or users on other marketplaces and platforms have to carry out new A&V processes on these platforms and pay the associated costs. This is much like an MSME seeking to get its products on various supermarkets' shelves—it has to deal with each supermarket's respective purchasing manager and supplier relationship management system, one-by-one. Numerous services used by MSMEs to engage in ecommerce and trade, such as financial, insurance, logistics, and customs services, are similarly siloed and do not interoperate.

In the consumer space, Facebook or Google have addressed digital platforms' lack of interoperability by opening their walled gardens and enabling consumers to log onto other online services with their Facebook or Google accounts. For example, a person interested in booking a stay on Airbnb can be authenticated with his or her Facebook account, without having to re-enter his or her credentials on Airbnb. These authentications of course do not offer much trust, as anyone can establish a Facebook account with any name and images. But they do provide the user a master key to use various digital services. They also enable some data-sharing; for example, a Gmail user can easily download her email contacts and export them to another email system.

Such interoperability is rarer in B2B markets. Instead, to access various services, MSMEs essentially need to carry a big bundle of different keys. In addition, MSMEs often have limited or no visibility or access to the data they have submitted to government agencies and various service providers, except in the records they themselves keep.

Data portability would be transformative for MSMEs. For example, if an MSME could provide a bank access to the MSME's business vitals from government business registries, transactional data from online marketplaces, credit data from other lenders, and data on the MSME's trade transactions and trade compliance from trade single windows, the bank could accelerate and streamline KYC and underwriting

processes. Similarly, B2B marketplaces could with these data accelerate and lower the cost of their seller A&V processes.

The processes of authenticating and verifying MSMEs imply significant transactions costs to service providers, government agencies, and MSMEs themselves (table 1). Could a corporate digital ID help reduce these costs? I turn to this question next, reviewing the landscape and properties of the world's major corporate ID systems.

Table 1: Pain Points for Marketplaces, Banks, Governments and MSMEs in Processes for Authenticating and Verifying MSMEs

	Pain points onboarding MSMEs	Pain points managing MSMEs' accounts
Marketplaces	• Need to extract from prospective customer extensive documentation for A&V • A&V is time-consuming and costly, which erodes user experience and interest • Rely on third-party providers to verify MSMEs	• Performing accurate, efficient and customer-friendly verifications • Meeting regulatory requirements for identity verification • Renewing A&V checks periodically, which may lead to abandonment
Banks	• Growing KYC and AML requirements that undermine customer acquisition and cause prospects to abandon process • Questionable MSME financial statements, lack of reliable data about trade history and invoice performance • Paper-based, manual processes, need for in-person meetings • Regulatory regimes vary by country, requiring a global bank to complete the same KYC process with the same customer in each jurisdiction	• Performing accurate and customer-friendly verifications • Meeting identity verification requirements, preventing fraud • Time and cost to manage loan and trade finance applications and discrepancies • High false positives in AML process, implying high costs of removal • Repeat KYC process when customer requests a loan • Files constantly out of date, leading to discrepancies
Government agencies	• Paper-based, manual processes • MSMEs need to log in with different credentials and IDs depending on agency and level of government, resulting in poor user experience	• Duplicative, time-consuming paper-based processes and costly workflows • Data silos instead of a 360-degree whole-of-government visibility into MSME data • Duplication discourages MSMEs from bidding for government contracts
MSMEs	• Extensive paper-based documentation with each respective provider, implying significant upfront labor costs • Limited visibility into and control over how company documents and data are used and secured • Duplicate same process when onboarding another marketplace, bank or service provider	• Management of multiple "keys" to use different services • Limited interoperability and ability to share data • Low portability of data to access new trade or financial services • Prospective customers want information even with A&V and KYC processes completed • With banks, duplicate process again and again with each new loan application

III. USE CASES FOR CORPORATE DIGITAL IDS

A digital identity is a unique representation of a person or a legal entity that verifies the person or entity is who they claim to be during an online interaction or transaction. Most countries have some type of physical government-issued ID system in place for citizens to vote and access public services. However, these can be susceptible to fraud and are complicated to use online. According to one estimate, 3.4 billion people cannot effectively use their official IDs to access the proliferating e-government services.[14]

In response, a growing number of governments are offering their citizens digital IDs for accessing online services, especially public services. The most famous digital ID system is India's Aadhar, which is a 12-digit unique identity number that can be obtained voluntarily by Indian residents or passport holders and is based on their biometric and demographic data. Estonia, United Kingdom, Australia, Belgium, the Nordic countries, and the United Arab Emirates are among the other countries with a digital ID provided either by the government or via a public-private partnership.[15]

Governments are just one of the instances that provide digital IDs: many entities such as social media platforms, email services, streaming services, marketplaces, and banks also provide users with IDs for logging into their services. These differ according to the strength of the identity proofing they entail: "self-asserted" identity (such as a social media login) is weak as it is relatively easy to create a social media account using any name and profile information, while an ID provided by a government or bank can be much stronger (table 2). IDs also differ in terms of their purpose: many are geared toward enabling transactions, such as among governments and citizens or banks and firms; however, there are also functional or industry-specific IDs that enable users to verify healthcare providers or travel agents as accredited providers, for example.

Table 2: Identity proofing types

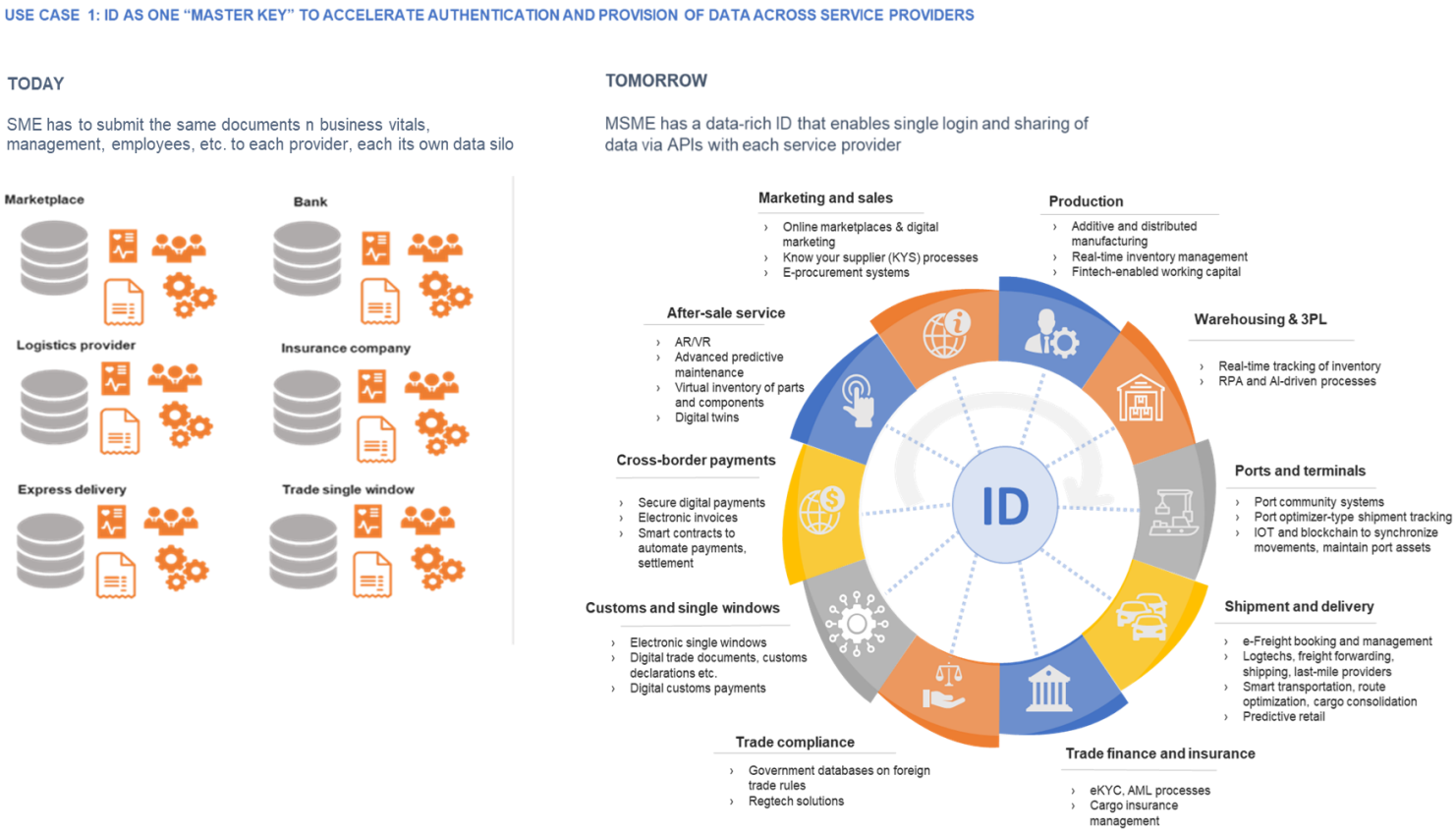
	Type 1: Transactional	Type 2: Transactional	Type 3: Functional
Value propositions for services providers	Service providers leverage "self-asserted" ID (e.g., social media login ID)	Service providers leverage highly trusted ID (e.g., ID provided by the government or a bank)	Services providers and customers verify industry expertise (e.g., healthcare provider)
Reliability	Low	High	Medium-high
Authentication	Weak	Strong	Medium-strong
Services and apps enabled	• Social media • Messaging apps • Media and entertainment • Online content • C2C platforms • Micro payments	• Banking and insurance • Telecommunications • B2B ecommerce • Transportation and logistics • Public services • Trade compliance	• Healthcare • Financial services and wealth management • Gambling • Travel agencies
Use cases	• Social media login • Streaming services • Online shopping	• Marketplace A&V • Banks' KYC/AML processes • Corporate procurement	• Verify healthcare provider is licensed • Verify broker is licensed

Source: Author based partly on ITU, Digital Identity Road Map Guide.

A corporate digital ID as referred to in this paper is type 2. There are at least four use cases for this type of robust corporate digital ID to enable MSME ecommerce.

Use case 1: Digital ID as a master key for MSMEs to access services for ecommerce and trade

A corporate digital ID and the data associated with it could serve as a master key that enables public and private service providers to authenticate and verify MSMEs easily during a sales cycle (use case 1).[16]



Use case 2: Digital ID as an enabler of interoperability among marketplaces

A corporate digital ID could also be used to enable MSMEs to access multiple B2B marketplaces and thereby access customers and transact on several marketplaces with a single login (use case 2).

USE CASE 2: ID AS AN ENABLER OF MARKETPLACE INTEROPERABILITY

TODAY:

SME has to onboard onto individual marketplaces, with limited access and limited resources to join others

TOMORROW:

SME onboards onto a single marketplace, but also unlocks access to demand supply from others

Use case 3: Digital ID for MSMEs to access working capital and trade finance

A corporate digital ID could also be used to enable MSMEs that sell on marketplaces to access a range of downstream financial, logistics, insurance, and payment services they need for fulfilling orders received on marketplaces—perhaps right as "embedded" service on the marketplace (use case 3).

USE CASE 3: DATA-RICH ID AS AN ENABLER OF MSME FINANCE

TODAY: TRADITIONAL B2B LENDING

SME presents & gets invoice accepted → SME takes invoice to potential lenders to get financing

TOMORROW: DATA-RICH ID-ENABLED LENDING LEVERAGING APIs

Marketplace presents & gets invoice accepted → Marketplace offers pre-approved financing in-app

Invoice Finance Offers:

	Bank	Details	Rating
select	**Abc bank**	80% invoice financing @ 7.75%	4/5
select	**Xyz bank**	90% Invoice financing @ 8%	4/5
select	**123 bank**	70% invoice financing @ 6.75%	3/5

- In addition to financial services, the marketplace could furnish cargo insurance services, logistics booking, trade compliance services, etc.

Use case 4: Trade facilitation and finance via traceability in trade transactions

A corporate digital ID would decrease transactions costs and automate "handshakes" in B2B interactions and transactions, including in supply chains and international trade transactions. When combined with data on a shipment, an ID would also enable shippers to trace their products in trade transactions—which in turn would unlock new opportunities for accelerating customs procedures and trade compliance and expanding shippers' access to cargo insurance and importers' access to trade finance.

Such traceability would also enable payments automation among logistics providers and from buyers to sellers as goods move from origin to destination. This in turn could help solve the chronic cash flow problems faced by buyers, sellers, and logistics providers in international trade transactions.

Figure 6 summarizes the value propositions for a corporate digital ID for MSMEs in cross-border ecommerce.

Figure 6: Value Propositions of a Corporate Digital ID in B2B Ecommerce Processes

	MSME buyer onboards B2B marketplace	Searches for sellers on marketplace	Negotiation and document exchange	Deal executed & Payment terms agreed	Buyer approaches lenders for financing	Supplier books logistics & insurance
BEFORE	• Tedious form-filling • Google/FB login	• Uncertain counterparty credentials	• Long & costly KYC and document exchange process • Often offline	• Mostly offline and paper-based • High risk of fraud / disputes	• High cost to serve • Hard to validate authenticity • Mostly offline	• High cost to serve • Often offline
AFTER	• Simplified onboarding requirements • Secure login	• Digital ID-verified credentials	• Digital ID-Authenticated digital data / documents from trusted sources	• Secure digital transaction sign-offs between parties	• Digitally onboard, risk-assess and offer finance • Digitally validated info reduces cost to serve for lenders	• Other trade service providers will benefit in similar ways to financiers

Granted, the trust engendered by a data-rich corporate digital ID will have benefits beyond lowering transaction costs for MSMEs in dealing with their customers, vendors, and governments. For example, studies that quantify trust in business relationships have found that high-trust relationships in such contexts as sales between auto manufacturers and their suppliers can halve face-to-face interactions to issue contracts and haggling after contracts have been signed. Trust also promotes information-sharing and technical assistance among parties.[17]

In addition, when a digital ID becomes widely accepted by service providers and helps MSMEs gain trust with suppliers and customers, it can generate various second- and third-order benefits such as improved

morale among service provider and MSME staff, greater transparency and accuracy in business processes, and opportunities for expanded MSME trade, growth, and job creation (table 3). When enabling the end-to-end digitization of transactions and interoperability, digital IDs could also increase the viability of smaller, more specialized platforms and marketplaces with smaller sets of users. These gains are difficult to quantify as they vary widely by an ID systems' user base and data. Perhaps the most comprehensive effort to date to quantify the value of a digital ID is McKinsey's analysis of 100 use cases for individual digital ID systems, which concludes that robust versions of digital IDs could increase GDP growth by 3-13 percent in developing countries, mostly by enabling more transactions and increasing efficiencies.[18]

Table 3: First-, second- and third-order benefits of corporate digital IDs for MSMEs, governments, and service providers

	First-order gains	Second-order gains	Third-order gains
MSMEs	• Single master key to log into all ecommerce-related services • Access own data • Apportion data across providers	• Reduce manual processes, paper, onboarding times and costs • Access finance and trade services • Keep records automatically up to date across providers	• Time-saving and reduced risk due to enhanced trust with customers and suppliers • More transactions and exports
Marketplaces	• Automate seller A&V process • Lower A&V costs	• End reliance on third-party verification agencies • Focus on customer service, digital marketing, matchmaking • Identify high-quality prospects faster • Lower buyer due diligence costs, improved buyer satisfaction	• More customers, more transactions, scale economies
Banks	• Accelerate KYC processes • Reduce KYC/AML costs • Keep business records up to date	• Reduce staff costs on compliance, increase and improve customer service • Improve staff morale and customer service • Lower MSME abandonment of onboarding process • Identify and focus on high-quality, low-risk customers	• More MSME customers • Larger loan books • Improved risk management and compliance • Financial inclusion for MSMEs
Government agencies	• More efficient and automated services to MSMEs • Improve MSME user experience • Enable whole-of-government data share	• Accelerated workflows and cost savings • 360-degree view of businesses	• MSME revenue growth, job creation • Financial inclusion for MSMEs • MSME participation in procurement processes • Increased government revenue • May enable central bank digital currencies

IV. WHY THE EXISTING ID ARCHITECTURE DOES NOT SUPPORT MSMES IN ECOMMERCE

The concept of a corporate digital ID is not new. There are numerous private sector-led MSME ID systems and international efforts, and some government-backed corporate ID systems.

A. INTERNATIONAL CORPORATE ID SYSTEMS

There have been various international attempts over the past two decades to build an identity system that would enable firms to authenticate themselves easily especially with banks. The most prominent system is the Legal Entity Identifier (LEI), an open-source global identifier of legal entities launched by the G20 in 2011 in response to the 2008-09 financial crisis.[19] A 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO), LEI identifies legal entities on a global database with 14 data fields (table 4).[20]

Table 4: LEI data fields

(Primary) Legal Name	Parent entities
Registered At [commercial register name]	Child entities
Registered As [number]	Registration date
Jurisdiction of formation	Last update
Entity legal form	Next renewal date
Entity status [active, inactive]	LEI issuer entity
Legal address	
Headquarters address	

The main challenge LEI has faced has been limited uptake. According to a May 2019 Financial Stability Board review, LEI has not reached a tipping point for mass adoption.[21] While in theory MSMEs could use LEI to build trust with their customers, vendors, and trading partners, they and their trading partners likely do not know what LEI is, how to use it to signal trustworthiness, or how LEI's $100 initial fee and $80 annual renewal fee will translate into new business opportunities. National regulators have reportedly been reluctant to impose LEI or other registration requirements on legal entities they regulate.[22]

The World Customs Organization's Trade Identification Number (TIN) is another international ID system for firms. It is used especially by customs to identify participants in Authorized Economic Operator (AEO) programs.[23] Unlike LEI, TIN is not open-source and is only used by customs authorities.[24]

In addition, some governments have recently pledged to collaborate on digital IDs. Perhaps especially notably, the Digital Economy Partnership Agreement signed on June 12, 2020, between Singapore, Chile, and New Zealand—the three partners that pioneered the Trans-Pacific Partnership years ago—aims to promote interoperability between different digital services and commits the parties to facilitating end-to-end digital trade by way of mutually recognized, secure digital identities.[25]

B. NATIONAL, GOVERNMENT-LED OR PUBLIC-PRIVATE CORPORATE ID SYSTEMS

Several developed country governments have built national corporate digital ID systems. The purposes, scope, and architectures of these systems vary widely, but fundamentally they are designed to enable firms to access multiple government services with a single login and authentication process. These IDs are typically a code or a combination of a passcode and a number associated with a company and connected to the personal digital ID of a company representative, which they use to identify themselves as the authorized legal representative.

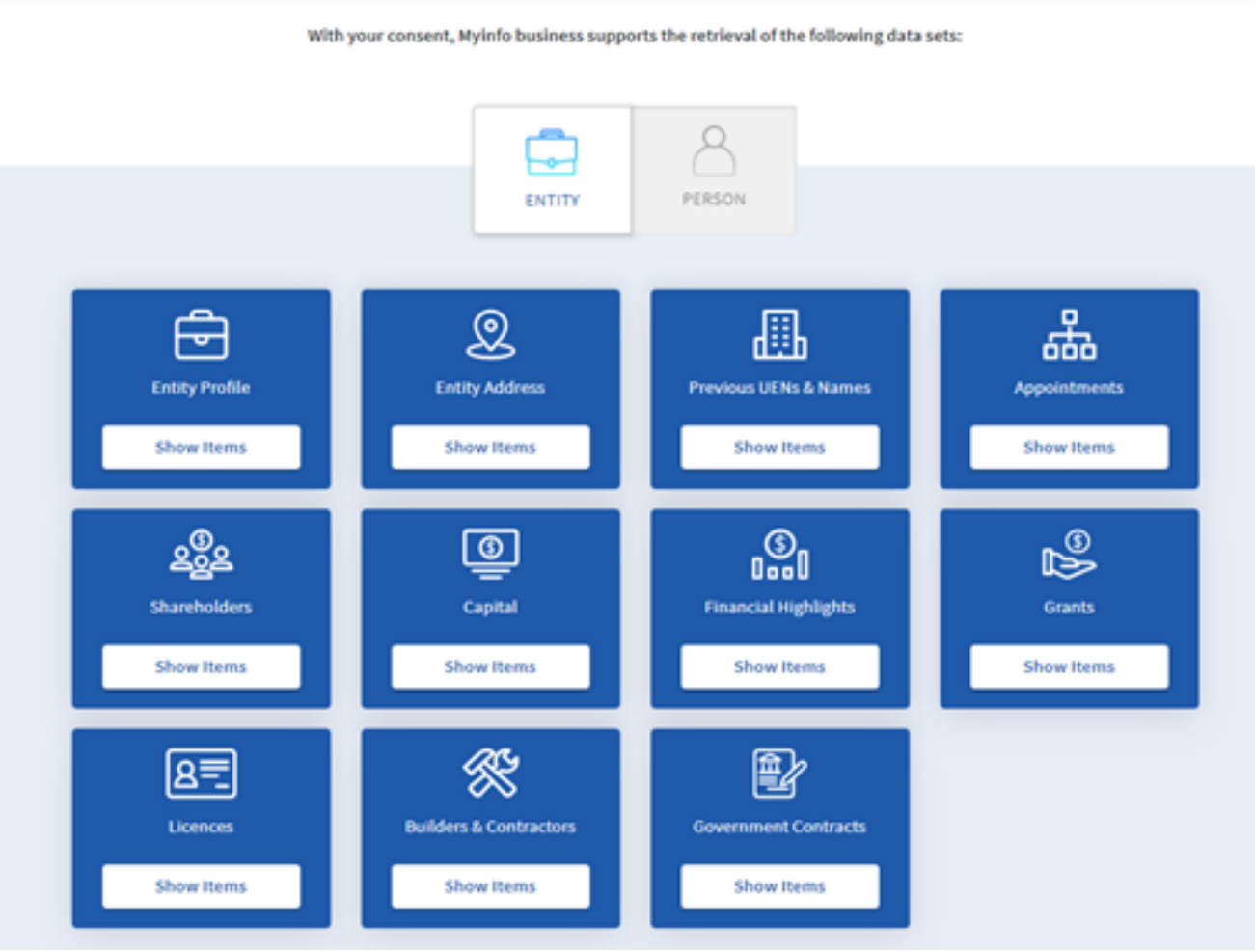
The leading example of a national corporate digital ID is Singapore's Corporate Access (CorpPass), which was launched in 2016. Developed by the Singapore Government Technology Agency (GovTech), CorpPass enables businesses and nonprofit organizations to access 140 government services within dozens of government agencies—including customs, the land authority, and health ministry—via a single login method. On September 1, 2018, CorpPass became the only method for businesses to log in to transact with government agencies, and more than 90 percent of Singaporean businesses are now using it to do so.[26]

CorpPass's main value proposition is that it enables a firm to access and use the data it has submitted to the government with private service providers. This data includes the company address and information on its employees, shareholders, capital base, accounting, tax records, and grants, all of which is stored in the MyInfo portal (figure 7). Data is shared with third parties via APIs, which essentially enables the ID holder to carry their data from government agencies to, say, a bank when seeking a loan. The ID holder is in control of what data is being shared with whom.

GovTech and the Monetary Authority of Singapore are currently working with the financial services industry to facilitate the use of CorpPass in MSME identity and credit assessments. Once a company has consented, the pilot enables three banks to draw on data associated with the company's CorpPass ID to enable it to open a bank account and quickly apply for loans.

Figure 7: Screenshot of MyInfo Data Sharing Portal Associated with Singapore's CorpPass

Source: https://www.singpass.gov.sg/myinfobusiness



Source: https://www.singpass.gov.sg/myinfobusiness

Table 4 describes selected other leading national corporate digital ID systems. These have primarily been designed to enable MSMEs to navigate and access e-government services. Of course, corporate digital IDs also have important immediate value propositions for governments, including facilitating the A&V process for MSMEs seeking government services, improved user experience for MSMEs using government services, and more efficient government processes and workflows.

Table 4: Features and Use Cases of Leading Corporate Digital ID Systems

ID system	Description	Functionalities for MSMEs	Data associated with ID	Third-party access to data
Singapore CorpPass	Enables businesses to access 140 government services using a single login that is tied to the company's Unique Entity Number (UEN), as well as to share data with private service providers.	Companies can carry their data from government to access private services- such as loans from banks- via APIs.	Entity basic profile Entity address Previous UENs & Names Shareholders Capital structure Financial highlights Grants	There are APIs available to share a firm's data with third parties.
Estonia E-Residency	Government-issued digital identity card to non-Estonians to form an Estonian firm and access EU markets. It is location-independent and allows for all business operations to be managed online using the digital identity.	e-Residents can establish a trusted EU company online in one day, manage the resulting company fully online, conduct secure e-banking, access international payment service providers, digitally sign and transmit documents, and file Estonian taxes online.	Basic personal details Contact information Identification details CV/Social media links Affiliated business details	No known access for third parties.
Azerbaijan E-/M-Residency	Enables businesses from anywhere in the world to set up a business based in Azerbaijan. E-Residency relies on a chip-enabled ID card for authentication, while M-Residency provides a special SIM card.	Access business banking and online payment service providers, declare taxes, file customs declarations for example to deal with the EU market, register new employees, sign documents electronically.	Personal details Contact information Identification details	No known access for third parties.
Netherlands eHerkenning	Standardized login system for Dutch firms to securely log in to more than 400 government organizations with a single login, using an eHerkenning token received from a government authorized supplier.	Companies can log in to more than 400 different organizations, such as UWV (Employee Insurance Agency), Chamber of Commerce and the Tax Authorities, as well as at municipalities, provinces and water boards and a number of private organizations.	The security level of the token Personal details Proof of identity Chamber of commerce number for company	Data is provided to the service provider whose web service has been logged into, with the explicit consent of the user.
Denmark NemID	Common secure login that consists of a user ID, a password, and a code card containing codes (one-time passwords). It is for use with government services, banks, and other private companies.	Users can access both public and private sectors, such as online banking, government websites, or engaging with one of the many businesses that use NemID.	Civil registration number Personal identification number (PID) Full address Email and mobile phone number optional	No known access for third parties.
Estonia eID/Smart-ID/Mobile-ID	Digital identification for individuals and firms they represent to log into multiple government and private systems. There are 3 forms: an eID card, a SIM based Mobile-ID, and a non-SIM mobile ID called Smart-ID.	Digital ID holders may access the 99% of public services that are available to citizens as e-services in Estonia.	Identification details	No known access for third parties.
European Union eIDAS	eIDAS enables EU businesses to use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries.	Ensures that electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication will work across EU borders and have the same legal status as paper-based equivalents.	The data already contained in one's own country eID	Due to EU open banking regulations, authorized third party providers with an eIDAS certificate may gain access to user data.
British Columbia OrgBook BC	OrgBook BC is a blockchain-based searchable public directory of open verifiable data about organizations legally registered in British Columbia.	The online directory makes finding authentic and authoritative data about BC companies fast and easy.	Registration Type Registration ID Registration Date Registration Status Affiliated companies	Anyone can access the data on OrgBook's database, as it is publicly available.

C. THE MISSING PIECE IN THE GLOBAL CORPORATE DIGITAL ID ARCHITECTURE: GLOBALLY SCALABLE AND INTEROPERABLE ID FOR MSMES

These many efforts notwithstanding, a critical component is still missing from MSME ecommerce: an interoperable, globally scalable ID. Indeed, the extent to which a corporate digital ID system promotes MSME ecommerce and internationalization depends on two main factors: (1) whether the system enables MSMEs to easily authenticate themselves with buyers and various B2B services, such as marketplaces, financial services, and logistics services; and (2) to what extent the ID is scalable and globally interoperable, so that it can be used by MSMEs and service providers around the world.

To date, no one ID system enables MSMEs' cross-border ecommerce and access to private downstream B2B services.

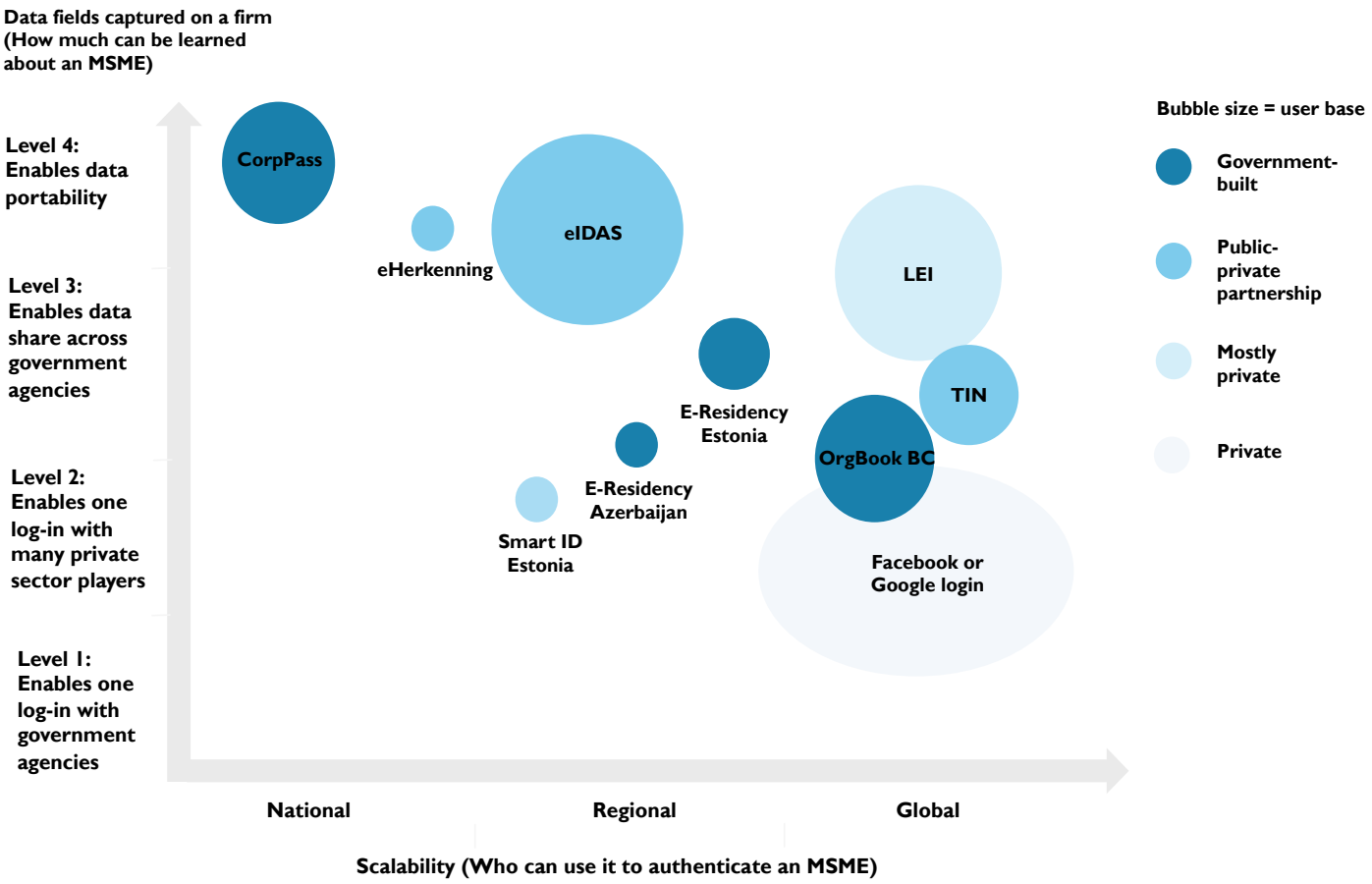
For example, while CorpPass enables seamless access to public services and "gold-standard" data on MSMEs, it has limited reach internationally—Singaporean firms are unable to use it to access trade-related services or build trust with trading partners outside Singapore. For its part, LEI is open-source and global but is has fewer data fields on a given company than CorpPass does and cannot be used by firms to log in to services. Private systems like B2B marketplace identities enable firms to access the marketplace's walled garden but not beyond, while Google and Facebook logins enable access across many digital services but provide only limited identity proofing and access to B2B services (table 5 and figure 8).

What kind of solution could then to pave the way for a scalable global corporate ID that enables MSMEs to better engage in ecommerce? The next section will discuss this question.

Table 5: Stylized Mapping of Leading Corporate Digital ID Systems, by Value Propositions

Capabilities	CorpPass - Singapore	eHerkenning - Netherlands	E-Residency - Estonia	Smart ID - Estonia	OrgBook - British Columbia	Legal Entity Identifier (LEI)	Trader Identification Number (TIN) for AEOs	IATA Identifier for travel services	Facebook and Google logins
Open source data to verify a firm exists									
Login to private B2C and C2C services									
Login to egovernment services									
Login to private B2B services									
Government agency can verify a domestic firm									
Government agency can verify a foreign firm									
Data share data across government agencies									
Customers or service providers can login and verify a firm									
Data portable: MSME can apportion its data to third parties such as banks via APIs									
Contains data fields needed to onboard B2B marketplaces									
Contains data fields needed to open bank accounts									

Figure 8: Stylized Mapping of Leading Corporate Digital Identity Systems, by Use Cases and Scalability



Source: Author.

V. CORPORATE DIGITAL ID ARCHITECTURE TO PROMOTE DEVELOPING COUNTRY MSMES' CROSS-BORDER ECOMMERCE

The optimal regime for all countries to enable MSME ecommerce is a globally interoperable digital ID that enables domestic and international buyers and sellers and service providers to easily authenticate and access data on an MSME. This system does not yet exist.

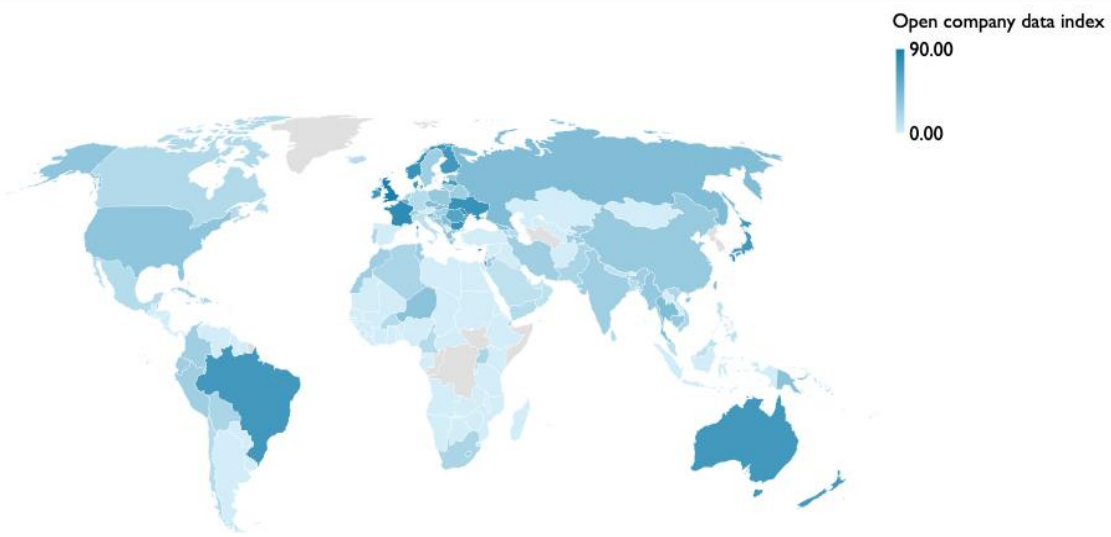
There have been recent useful proposals for ID systems to enable businesses' online transactions and trade. These have focused especially on the opportunities that blockchain provides for parties to self-manage decentralized identities. One thoughtful proposal is for a Global Trade Identity (GTID), a single ID that would enable its holders to engage in digital interactions with other actors in global trade.[27]

What options are practical, including for developing countries that want to enable their countries' MSMEs in cross-border ecommerce? And what should the architecture for a global corporate digital ID look like to optimally enable MSME ecommerce?

A decade ago, these questions would have perhaps been hard to answer. Today, however, many systems that could underpin corporate digital IDs are already in place in both the private and public sectors:

- Open banking and open finance practices and policies have socialized service providers into sharing data with each other.
- Increasingly sophisticated biometric ID systems have created opportunities for further data security in ID management.
- Individual digital ID systems are spreading, providing a basis for a natural person with his or her ID to be assigned to manage a corporation's affairs with a corporate digital ID.
- Official company registry data is increasingly readily available in machine-readable electronic format via APIs around the world (figure 9; appendix II, tables 2 and 3).

Figure 9: Openness of Government Company Registries (max. 100)



Source: Open Company Data Index, World Bank Institute.

However, there are also challenges to adopting corporate digital IDs, including:

- **Undigitized and incomplete corporate registries.** In most developing countries, corporate registries are still analogue and are also incomplete, given how vast the informal sector tends to be.

- **Setting up and managing ID systems create new costs and responsibilities.** The buildout of a corporate digital ID implies significant new costs—some of the systems currently in place have cost between tens and hundreds of millions of dollars. Managing a corporate digital ID creates new challenges and responsibilities for the identity providers like governments: as an identity provider, the government would need to take direct responsibility for identity governance and the full identity lifecycle, such as identity proofing, credential management, cybersecurity, the authentication (and, where needed, revocation) of identities, and integration with service providers.[28] The government would act as the regulator of the national corporate ID regime and be responsible for laws, regulations, procedures, and controls for the management of digital identities.

- **Challenges around international scalability remain.** National corporate digital ID systems developed by individual countries have not scaled and are unlikely to do so. After all, merging and harmonizing disparate national ID systems to make them interoperable enough to enable cross-border transactions would probably be extremely complex and time-consuming. In addition, when the goal of a corporate digital ID is to enable cross-border trade and MSMEs' access to global trade-related services, it is not in any country or service provider's interest to end up with a global architecture of 190 disparate national corporate ID systems, each with its own API to connect to service providers.

There are, however, potential pathways toward a global corporate ID architecture that leverage the advances in the digitization of corporate data without requiring each government to set up its own corporate digital ID system. Conceivable alternatives might include the following:

- **Scaling LEI**. LEI has already been set up and tested. However, for LEI to become a global de facto corporate digital ID, challenges such as upfront costs to MSMEs will need to be alleviated, and, to create awareness and promote adoption, national regulators would likely have to demand that firms use LEI. The underlying data would also unlikely substitute for B2B marketplace A&V process, as the data and documents LEI brings together are only a handful of those required of sellers by online marketplaces. Furthermore, LEI does not offer the login and authentication capabilities that solutions like CorpPass or Google or Facebook login provide—this capability would need to be built.

- **Scaling Smart-ID.** Possibly the most scalable option is Estonia's Smart-ID. It has strong identity proofing and login capabilities across services that wish to use it. However, Smart-ID does not bring together as much data on firms that use it as CorpPass does.

- **Docking onto an existing gold-standard national corporate digital ID.** Developing countries could possibly accelerate the adoption of a corporate ID by white-labeling an established corporate digital ID system such as CorpPass. If the data associated with the ID is as robust as that associated with CorpPass, it could also become a partial or even full substitute for the A&V data requested by marketplaces and other service providers. This would accelerate MSMEs' use of marketplaces and access to financial services. Pushing countries to dock onto an existing ID system is challenging, however, as governments would typically prefer their own ID systems and models.

- **Creating a private-sector-led, self-sovereign, scalable corporate ID.** Yet another option is to pursue a private-sector-led solution for self-managed identities that would enable MSMEs' customers, B2B marketplaces, and financial, logistics, insurance, and other service providers to authenticate MSMEs quickly and extract their key corporate vitals, based on government data, publicly available data, and privately apportioned data. As an added benefit, this architecture would enable service providers to use a single API rather than multiple national ones. This self-sovereign ID system would be far more scalable and cost-effective than countries building their own gold-standard IDs and then seeking to harmonize and merge them, a process that would take numerous years (figure 8). While it might sacrifice some of the standardization and rigor of a national ID system like CorpPass, it would be more scalable, easier, cheaper, and more flexible to use than national ID systems or LEI. Specifically, this system would:

    - **Be more flexible and democratic:** the system envisioned here is based on self-sovereign decentralized identity (DID). Drawing on data from multiple sources, it is more flexible than current aggregated models and could enable even informal companies to establish an identity.

    - **Be secured for verified company representatives to access**: just like CorpPass, the ID system grants rights and representations to verified company stakeholders and enables only these verified company stakeholders to manage their own DIDs and cryptographic keys for A&V.

    - **Have one master key that unlocks many services**: digital ID is a single key for firms to authenticate themselves across multiple digital services, such as marketplaces, services, websites, devices, and more.

- **Empower users through data:** users apportion their data to different parties depending on these parties' needs and thus have full visibility into how their data is being used.

- **Be extendable and adaptable**: the system is structured around a core that can be deployed in whole or partially, according to local country standards and regulations.

- **Offer real-time visibility across multiple data points and dimensions of interest:** the system would enable access to corporate vitals and financial risk, reputational risk, environmental, social, and governance (ESG) indicators, adverse media and headline risk, business and financial news, regulatory risk (such as drawn from sanctions watchlists), and operational risk in supply chains.

- **Enable real-time risk-weighting and compliance:** as this data is extracted in real-time, it enables parties in transactions to weight the risks posed by potential and current customers, suppliers, and service providers, and focus resources on high-risk parties and transactions. Real-time risk assessments enable real-time compliance.

- **Promote automation across supply chain:** the corporate ID system can also streamline supply chains and supply-chain financing. When IDs are combined with data on a given shipment, they will catalyze opportunities to automate the payment of goods as goods move through the logistics supply chain from seller to buyer. This would solve chronic financing needs and cash flow challenges among buyers, sellers, and logistics providers in international trade transactions.

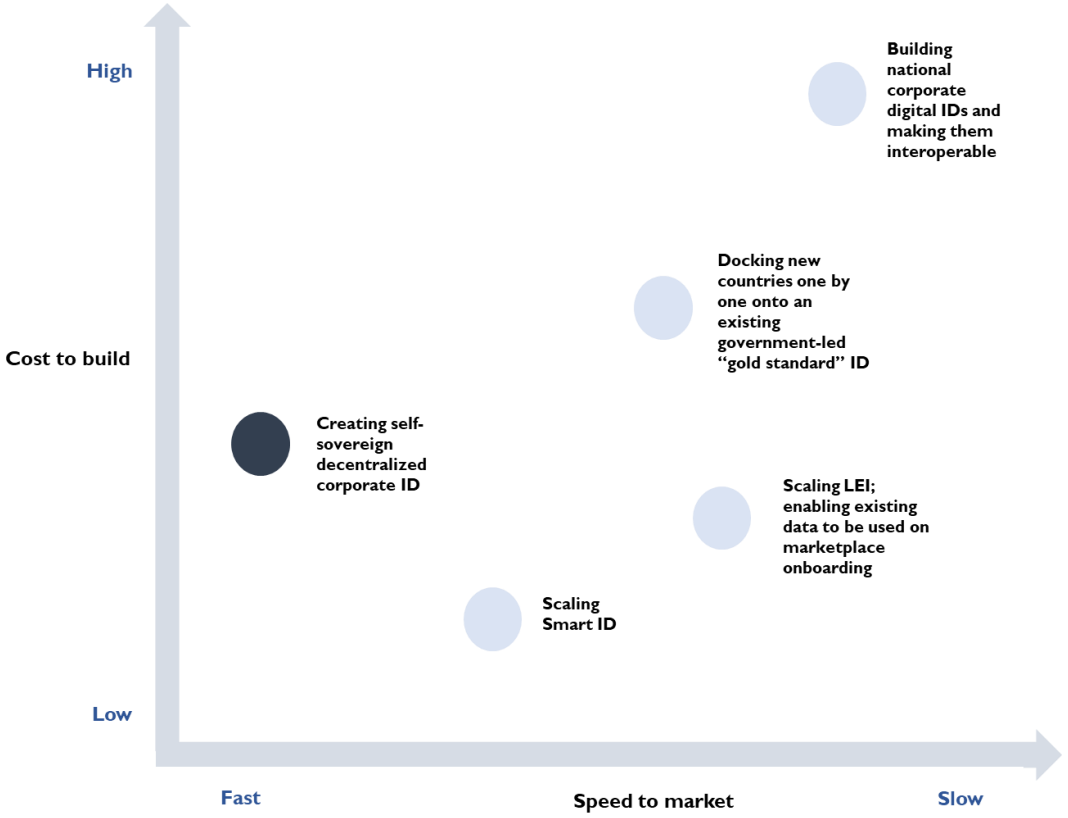
With these properties, a self-sovereign corporate digital ID would be a global digital public good that would balance the objectives of scalability, interoperability, credibility, and user privacy and control. Table 7 summarizes the value propositions of the different models.

The self-sovereign, private sector-led solution does not obviate national ID systems but instead draws and builds on them. But unlike national systems, it also enables cross-border scalability and can fast-track MSMEs in developing countries without ID regimes to engage in cross-border ecommerce.

Granted, certain conditions will need to be met for this system to work well, such as internet connectivity, cybersecurity, and data privacy and transfer regimes that are conducive to the transfer of data across borders.

The eTrade Alliance is working on a proof of concept for a digital ID system (see appendix III) and will report on the results, lessons learned, and further conditions for the deployment of this system in 2022.

Figure 10: Potential Different Global Corporate Digital ID Architectures, by Cost of Buildout and Time to Market



Source: Author.

Table 7: Features of different types of corporate digital ID systems and architectures

Level	Examples	Uses	Data fields	Level of trust	Time to market	Scalability	Value propositions
Private-sector IDs	• Social media login • Marketplace login	• Commonly used today • Log in to selected private services	Few	Weak	Short	High	• Easy to onboard • Interoperability of B2C online services
National IDs	• CorpPass (Singapore) • E-Estonia • E-Herkenning (Netherlands)	• Log in across all government agencies • Basis for tax filing, permits, etc. • Log in to selected private services	Several concerning company vitals and data submitted to government	Secure, "highly classified"	Long	Low	• Accelerate SMEs' access to and use of government and private services • Users are verified and authenticated • Data portability: User can carry data associated with ID e.g., to open bank account
Globally scalable ID	• Does not exist yet • Decentralized identity identifiers • Brings together rich set of company data across databases	• Authenticate MSME by B2B services (e.g., marketplaces, banks, financial and logistics services)—KYC tool • Assess vendors and customers in real-time	Real-time data from multiple public and private sources, including areas of growing interest (ESG, adverse media risk, etc.)	Strong, "classified"	Medium	High	• Multiple data sources for wide range of fields for compliance • Real-time risk monitoring and regulatory compliance • Users are verified and authenticated • Enables MSMEs to use marketplaces and B2B services • Cross-border interoperability • Potentially enables informal firms to gain an identity

VI. CONCLUSION

A growing number of MSMEs have set out to use ecommerce to reach buyers around the world, and COVID-19 has pushed even the most reluctant digitizers online. An MSME's success in cross-border ecommerce is only partly determined by the ingenuity of its team—to a large extent it depends on the company's ability to set up online stores and accept payments from foreign buyers, onboard global online marketplaces, build trust with buyers and sellers, and access a range of digital services that are key to managing any one ecommerce sales cycle, such as logistics, financial, insurance, and payments services.

Today, MSMEs that engage in B2B ecommerce struggle with each of these areas: they need to onboard marketplaces one-by-one and in the cases of many B2B marketplaces, pay significant fees to be authenticated and verified; they spend time on travel and trust-building with buyers that want to learn about their ability to deliver on their promises; and they engage in multiple time-consuming, paper-based processes to secure services from banks, insurers, logistics providers, government agencies, and others, often duplicating processes and data entries. Due diligence processes have become increasingly rigorous due to vendors and buyers' growing concerns about online fraud and regulatory pressures to authenticate and verify customers and suppliers. But for MSMEs, the time and transactions costs associated with these basic functions undermine their sales, growth, exports, and scalability, all areas that governments around the world are seeking to promote in response to COVID-19.

This paper has called for an overarching solution to these challenges—a corporate digital ID system and architecture that:

- Is globally scalable and interoperable across countries so that MSMEs can leverage it in international trade and ecommerce;

- Brings together a rich set of real-time data and enables users to manage access with counterparties and service providers;

- Enables marketplaces, banks, and other service providers to easily authenticate and verify MSMEs; and

- Builds on existing data-rich ID systems and open corporate registries but can also be used by firms in countries that do not have such corporate ID systems or that are informal.

Developing countries do not need to build national corporate ID regimes from scratch. This paper has put forth a concept for a self-sovereign corporate ID as a global digital public good that would balance the objectives of scalability, interoperability, credibility, and user privacy and control.

In the ecommerce era, where marketing, sales, financing, insurance, freight forwarding, and government services are accessible online, a corporate digital ID is the last piece needed for MSMEs to vet buyers and sellers and secure critical services in order to transact and scale their sales. A corporate digital ID is a crucial element in the journey to a world where even the smallest MSME, regardless of its location and resources, can become a thriving multinational business.

Appendix I: Table I-1 – Onboarding and authentication and verification processes of major B2B Marketplaces

	Seller fills an online intake form	Marketplace receives, takes step 1	Marketplace offers paid account and "Trust Services" and marketing capabilities	Marketplace receives documents, authenticates	Marketplace opens paid account	Periodic renewal
ThomasNet Thomasnet.com	• Respond to online query • Can open free account	To authenticate, need: • Business registration • Certificates (ISO etc.) • Capabilities statement • Product specs • Quality certifications • Diversity status • Product images • CAD models • White paper To list, need: • Name • Phone No • Employees • Sales	• Thomas.Net Supplier Analyst team • Mostly self-service by company; only some documents that have "legal" information like business registration	• Thomas Registered badge: $100/mo. Authenticates and receives priority positioning in the Thomasnet.com supplier search results • Thomas Verified Supplier badge: $200-$1,000/mo. Lets buyers know the product, services, and company information have been validated by the Thomas Supplier Analyst Team	• Not mentioned. Account payment is monthly.
Amazon Business Seller B2B program sell.amazon.com/programs/amazon-business.html	• Semi-automated for free account • Verifies and confirms address automatically as seller fills out intake form • Does as next step request EIN (tax number)	Documents heavily up to the seller and can include: • DUNS number • Logo • Address • Social media • Any certifications (ISO etc.) • Minority/diversity status	• Does not "certify" ("Sellers are expected to determine their own eligibility for a credential and how to best obtain the appropriate supporting documentation, depending on the credential."	• Monthly membership. If already sell on Amazon's B2C portal, no fee. • Membership enables access to RFQs, data and dashboards, discounts etc. • Offers also financial services, lines of credit etc.; and fulfillment	• Not mentioned. Monthly membership
TradeKey Tradekey.com	• Set up free account	**To authenticate, need:** • Business registration **To list, need:** • Name • Mobile no • Phone • Email • Messengers id (MSN, Skype, QQ etc) • Fax For exporting or importing pharmaceuticals, need: • Letter of Authority or License from the competent authority	• To be verified where completed and by whom	• Sellers get "Trust Points" that increase with level of fee and feedback from buyers: SilverKey (220 Trust Points); GoldKey (3000) Trust Points; Goldkey Plus (5000 Trust points); VIP (8888 Trust Points) • These services also entail many marketing and account management benefits	• Annual renewal; company has to sign a new contract but not resubmit documents.
Made-In-China made-in-china.com	• Respond with query for business documents • Can also establish a free account without licenses • Al suppliers are Chinese	**"Audited Supplier" process requires** • Basic information • Trade capabilities • Product design and development capabilities • System and product certification • Production capacity and quality • Credit • Working environment • Energy conservation • Photo verification • On-site verification	• SGS and Bureau Veritas, world's leading inspection companies, to A&V all premium suppliers on the platform and produce "an objective and comprehensive audit report for each supplier". Sample: https://www.made-in-china.com/attachment_file/audit_report_sample.pdf. • Buyers access reports for free	• "Audited Supplier" logo for trustworthy suppliers	• Not mentioned. Account can be closed for periodic data validity review – user should send valid business license by email to reactivate

Table I-1 (Cont.) – Onboarding and authentication and verification processes of major B2B Marketplaces

	Seller fills an online intake form	Marketplace receives, takes step 1	Marketplace offers paid account and "Trust Services" and marketing capabilities	Marketplace receives documents, authenticates	Marketplace opens paid account	Periodic renewal
Alibaba **Alibaba.com**	• Responds with query for business documents • Automated	**Proof of Registration:** • Valid business registration document • Articles of incorporation • DBA registration • Charter documentation **Proof of Address:** • Proof of registration/tax authority • Utility bill • Recent phone bill • Bank statement • Lease agreement • IPR information required to be submitted with identity information • Supplier verification performed by third party service provider	• Seller verification performed by third party service provider	• Offer Business Identity service that displays A&V status, helps build trust with buyers. Free of charge Marketing services: • Gold supplier that can interact with buyers online • Basic $2,399/yr; included Authentication & verification support • Premium $4,199/yr; included A&V and dedicated account manager	• Not mentioned. If account cancelled for some reason, seller can appeal for account reactivation online and submit required documents; response in 3-5 days
Ebay **Ebay.com** **(B2C)**	• Reroutes to PayPal to verify PayPal account • First-time use on PayPal: account verified by adding and confirming a bank account, or applying for and being approved for a PayPal Credit product		• Once sellers has some transactions (in hundreds of dollars), PayPal verifies seller data from a utility bill or equivalent • Once Verified, seller has confirmed its identity and can withdraw more money from sales • Total time is minimal, within minutes • Total cost is likely <$10, team is in India		

Appendix II – Selected leading national corporate ID systems

- **E-Residency of Estonia** launched by Estonia in 2014 enables non-Estonians to access Estonian services such as company formation, banking, payment processing, and taxation. E-Resident applicants need to be interviewed at Estonian consulates. Once authenticated, they are issued a digital ID card with two PIN numbers for secure digital authentication and digital signatures. e-Residents can, for example, establish and manage a location-independent company online from anywhere in the world, establish a trusted EU company online in one day, manage the resulting company fully online, apply for a business bank account and conduct secure e-banking, access international payment service providers (PayPal, Braintree, etc.), digitally sign and transmit documents, and file Estonian taxes online. Some 62,000 people have applied for e-Residency. E-Residency data are consumable in countries such as Finland, Iceland and Japan via an open source data exchange platform.

- **Smart ID of Estonia.** Estonia enables digital identity and establishment of legal entities through a mobile-based ID through use of a special SIM card (Mobile-ID), or a mobile-based ID that does not require a SIM card (Smart-ID). While e-Residency requires a personal visit to an Estonian consulate and a digital ID card, mobile-ID and smart-ID can be activated online with an ID card reader.[29] The ID enables access to public and selected private services and appears to be highly scalable: 18 months after the Smart ID was launched in the Baltics in 2017, a million Smart-ID user accounts had been registered; three years later, the system encompassed over 2.6 million users doing over 50 million transactions every month in more than 200 e-services.

- **E-Residency and M-Residency of Azerbaijan** is similar to E-Residency Estonia, enabling a user from anywhere in the world, without ever entering Azerbaijan, to open and run a business based in Azerbaijan and access financial, payment, and e-government services to declare their taxes, file customs declarations for example to deal with the EU market, register new employees, and so on.[30] E-residents receive a chip-enabled ID card for authentication and electronic signatures, while m-residents are issued with a special Asan İmza (Mobile ID) SIM card to perform the same function. The e-/m-Residency costs US$50; a company set up costs US$100, and a virtual office costs US$117 a year. Since the beginning of 2019, Azerbaijan has been offering a number of incentives for MSME owners, such as a three-year tax exemption. As of November 2019, more than a hundred people have applied for an e-/m-Residency.

- **Dutch eHerkenning** is a standardized login system for Dutch firms to securely log in to more than 400 government organizations with a single login.[31] It is a public-private partnership between the government and the Dutch business community. Logging in to a web service using their eHerkenning token, users can manage their companies' affairs online. However, also private service providers can log on to verify the identities of their suppliers. The system was launched in response to the proliferation of digital keys that curtailed the scalability of e-government and e-business solutions. The system has 466 affiliated organizations and 1,436 services, and over 13 million annual logins.[32]

- **Danish NemID** is a commonly used single login in Denmark for online banking, retrieving information about public services, or engaging with one of the many businesses that use NemID. NemID consists of a user ID, a password and a code card containing codes (one-time passwords). NemID Employee Signature enables a representative of a company to identify him/herself on behalf of his/her company; and NemID business banking solution for online corporate banking. There is also a new code app which enables the user to use NemID from a smartphone or tablet without needing the physical code card.

- **European eIDAS.** The European Union is seeking to further the interoperability of the various individual and corporate digital ID systems of the EU Member States through eIDAS, an EU-wide digital identity. eIDAS is envisioned to enable Europeans in any one member state to submit tax declarations, enroll in a university, open a bank account, set up a business, authenticate internet payments, bid for tenders and so on in other member states. The system is already in place and operational with some two dozen ID systems that are qualified to form part of it and cover a certain share of individuals and/or legal entities in a country.[33] The interoperability of national ID systems is however still limited given different national regulations and customer due diligence requirements, for example.[34]

- **British Columbia's OrgBook BC** is a blockchain-based online directory of companies in British Columbia.[35] Unlike the federated systems like CorpPass that imply one registration with a "trust anchor", OrgBook is a centralized identity that is created once and trusted universally: companies manage their own digital identities, and multiple entities contribute to any one company's credentials. OrgBook helps reduce the time to do due diligence on a new supplier or client from hours down to a few seconds. A business with government-issued digital credentials could save hours filling in government forms and agencies can shorten or eliminate forms, improve the accuracy of its data, and streamline its processes. Also the Province of Ontario has an OrgBook.

Appendix II - Table 1: Data on Top-20 Most Open Corporate Registries (max. 100)

	Freely Searchable	Licensing	Data Freely Available	Directors	Accounts	Share-holders	Total
Moldova	20	30	20	10	0	10	90
UK	20	30	20	10	10	0	90
Cyprus	20	30	20	10	0	0	80
France	20	30	20	0	10	0	80
French Guiana	20	30	20	0	10	0	80
Guadeloupe	20	30	20	0	10	0	80
Martinique	20	30	20	0	10	0	80
Mayotte	20	30	20	0	10	0	80
Réunion	20	30	20	0	10	0	80
Saint Barthélemy	20	30	20	0	10	0	80
Saint Martin (French Part)	20	30	20	0	10	0	80
Saint Pierre and Miquelon	20	30	20	0	10	0	80
Bulgaria	20	30	10	10	5	0	75
Denmark	20	5	20	10	10	10	75
Norway	20	30	20	5	0	0	75
Ukraine	20	30	20	0	0	5	75
Australia	20	30	20	0	0	0	70
Brazil	10	30	20	10	0	0	70
Finland	20	30	20	0	0	0	70
Ireland	20	30	20	0	0	0	70
Israel	20	30	20	0	0	0	70
Japan	20	30	20	0	0	0	70
Latvia	20	30	20	0	0	0	70
New Zealand	20	5	20	10	5	10	70
Romania	20	30	10	0	0	0	60
Belgium	20	30	0	5	0	0	55

Source: Open Company Data Index, World Bank Institute.

A number of countries have by now at least some type of individual digital ID systems and company registration data needed for a government-backed corporate digital ID (table I-3). Countries that are closer to the upper right-hand corner are best-paced to build a corporate digital ID; countries in bottom left-hand corner need to digitize both corporate registries and individual IDs.

Appendix II Table 2: Corporate Digital ID Readiness: Openness of Company Registry and Existence of Individual Digital ID

Best setting for a corporate Digital ID (if not yet in place)

	No Individual digital ID or no data			Digital identity in development or piloted		Individual digital ID available	
Open company data (>50% in place)	Bulgaria Cyprus French Guyana Guadeloupe Israel Martinique Mayotte Réunion	Romania Saint Barthélemy Saint Martin (French Part) Saint Pierre and Miquelon Ukraine		Brazil France New Zealand Slovenia		Australia Belgium Denmark Finland Ireland Japan Latvia Moldova Norway	United Kingdom
Partly open company registry (<50% data in place)	Algeria Armenia Aruba Bahamas Belize Bolivia Bosnia and Herzegovina Burkina Faso Cambodia Cameroon Cuba Curaçao Djibouti Dominica Dominican Republic Georgia Greece Greenland Haiti Iran Isle of Man	Jamaica Lebanon Lesotho Marshall Islands Mauritius Montenegro Niger Puerto Rico Rwanda San Marino Seychelles Solomon Islands St. Lucia Tajikistan Trinidad and Tobago United States West Bank and Gaza Yemen		Bangladesh Barbados Belarus Bermuda Canada Colombia Kyrgyz Republic Myanmar Nepal Papua New Guinea Philippines Russia Samoa Serbia South Korea Sri Lanka Taiwan Tonga Tunisia Uganda Vietnam		Albania Azerbaijan Bahrain Brunei Darussalam Chile China Croatia Czech Republic Ecuador Estonia Germany Guernsey Hong Kong Hungary Iceland India Italy Jersey Jordan Kosovo Kuwait	Liechtenstein Lithuania Luxembourg Malaysia Malta Mexico Morocco Netherlands Oman Pakistan Peru Poland Portugal Qatar Saudi Arabia Slovak Republic South Africa Sweden Switzerland Thailand UAE
No open company registry	Angola Antigua and Barbuda Benin Botswana Burundi Cabo Verde Central African Republic Chad Comoros Congo, Dem. Rep. Congo, Rep. Côte D'ivoire Equatorial Guinea Eritrea Fiji Gabon	Gambia Gibraltar Grenada Guinea Guinea-Bissau Guyana Honduras Iraq Kazakhstan Kiribati Liberia Libya Malawi Mali Mauritania Micronesia Mozambique Namibia Nicaragua Palau	Paraguay Senegal South Sudan St. Kitts and Nevis St. Vincent and the Grenadines Sudan Swaziland Syria São Tomé and Príncipe Timor-leste Turkey Vanuatu Zimbabwe	Bhutan Costa Rica Egypt El Salvador Ethiopia Kenya Lao Pdr Macedonia Madagascar Mongolia Panama Sierra Leone Suriname Tanzania Togo Uzbekistan Zambia		Afghanistan Argentina Austria Ghana Guatemala Indonesia Maldives Nigeria Singapore Spain Uruguay Venezuela	

Source: Open Company Data Index, World Bank Institute

Appendix III: Digital ID interoperability proof of concept to accelerate developing country MSMEs' access to online marketplaces and services

Both Estonia and Singapore are digital nations and aspire to connect national digital identities to 3rd party services that drive utilization and scale. These national digital IDs are also not interconnected today, nor being used by B2B marketplaces (only government services). A proof of concept considered by the eTrade Alliance seeks to change this.

The envisioned use case is as follows:

- Trader A located in Estonia forms a business relationship with Trader B in Singapore .
- Both Traders have been issued with an NDI in their respective sovereign jurisdictions.
- Trader B maintains a data repository on the Singapore Networked Trade Platform (NTP), via CorpPass.
- In the contract between A and B, Trader A is required to register on NTP and exchange data with Trader B.
- Trader A will use an identity token trusted by the relying party (Singapore GOVTECH) to grant access to NTP.
- Trader A's access rights will be limited to their security level.

This model is potentially highly scalable, enabling a global ecosystem of credential issuers, owners, and verifiers, all exchanging interoperable verifiable claims. This in turn would:

- Offer marketplaces a single ID solution to authenticate and authorize buyers and suppliers;
- Unlock especially MSMEs' access to downstream B2B logistics, financial, and other trade-related services; and
- Open new opportunities to streamline and automate handshakes and payments in global supply chains and trade logistics.

The proof of concept will test these value propositions, by connecting two data-rich "gold standard" ID systems. It will also consider (1) the costs associated for parties to verify claims; (2) the benefits for micro and informal firms in developing country contexts, and for firms with limited data; and (3) the extent to which the data associated with the solution is adequate for enabling firms access to downstream services.

The Alliance is currently working on a technology pilot to operationalize this ID – we will report back in 2022 on results and lessons-learned for scaling the system in developing countries.

Agreement Officer's Representative:
Devi Ramkissoon, USAID
USAID, Center for Economics & Market Development
dramkissoon@usaid.gov
+1 (347) 866–6298

Project Director:
Brett Johnson, Palladium
Brett.Johnson@thePalladiumgroup.com
+1 (202) 777–0960

Technical Director:
Kati Suominen, Nextrade Group
Kati@nextradegroupllc.com
+1 (202) 294–8871

www.allianceforetradedevelopment.org

References

[1] Fukuyama, Francis. 1996. *Trust: The Social Virtues and The Creation of Prosperity*. New York: Free Press.

[2] Andreas Lendle, Marcelo Olarreaga, Simon Schropp, and Pierre-Louis Vezina, "There Goes Gravity: How eBay Reduces Trade Costs," World Bank Policy Research Working Paper 6253, 2012.

[3] Economic Innovation Group, "The New Map of Economic Growth and Recovery," May 2016, https://eig.org/wp-content/uploads/2016/05/recoverygrowthreport.pdf.

[4] Onboarding B2B and B2C online marketplaces tends to take firms only a few minutes. For example, to register as a seller on eBay, an MSME or individual typically only needs to submit basic data such as their name, email address, and phone number. Onboarding a B2B platform such as Thomasnet for a free account tends to require only an individual's name, their business name, address, website, and business email. However, more data is required when the seller wants to transact with buyers. In the case of a B2C platform, this typically means the seller submitting its bank account or PayPal account, which needs to be connected to a bank account for the seller to get paid.

[5] The ConnectAmericas B2B marketplace, which is supported by the Inter-American Development Bank, is an exception and does not charge users—it uses data from export promotion agencies.

[6] GLEIF Infographic: LEIs Transforming Banks' Client Lifecycle Management, Global LEI Foundation, accessed May 2021, https://www.gleif.org/en/lei-solutions/mckinsey-company-and-gleif-leis-and-client-lifecycle-management-in-banking-a-u-s-4-billion-beginning/gleif-infographic-leis-transforming-banks-client-lifecycle-management#.

[7] GLEIF Infographic: LEIs Transforming Banks' Client Lifecycle Management, Global LEI Foundation, accessed May 2021, https://www.gleif.org/en/lei-solutions/mckinsey-company-and-gleif-leis-and-client-lifecycle-management-in-banking-a-u-s-4-billion-beginning/gleif-infographic-leis-transforming-banks-client-lifecycle-management#.

[8] David Pope, "Business Banking Cannot Be Disrupted Without Digital IN Onboarding," International Banker, June 18, 2019, https://internationalbanker.com/technology/business-banking-cannot-be-disrupted-without-digital-in-onboarding/.

[9] David Pope, "Business Banking Cannot Be Disrupted Without Digital IN Onboarding," International Banker, June 18, 2019, https://internationalbanker.com/technology/business-banking-cannot-be-disrupted-without-digital-in-onboarding/.

[10] Many efforts have been made to accelerate banks' KYC processes, such as eKYC and KYC Utilities, where banks can access some common pool of data on firms. These make perfect sense as KYC data needs are similar across banks—according to some estimates, 80 percent of the data fields to be filled are the same. For example, leading UK banks ask MSME customers seeking to set up a bank account 32 questions, 19 of which are the same across banks, while 13 are also asked by the businesses' electricity and telecom providers. However, this data is often shared poorly across providers, and each bank still tends to want to go through its own unique KYC process to establish an audit trail for bank regulators.

[11] Marqueta, "SME Banking: Business Banking Done Differently," white paper, 2020, https://resources.marqeta.com/businessbanking?submissionGuid=27648860-d9b0–4402-bc43-b287a44f4fb1.

[12] Marqueta, "SME Banking: Business Banking Done Differently," white paper, 2020, https://resources.marqeta.com/businessbanking?submissionGuid=27648860-d9b0–4402-bc43-b287a44f4fb1.

[13] "Nearly One Third of the $36 Billion Cost of Regulation in Canada is Unnecessary Red Tape," Newswire Cision Canada, January 22, 2018, https://www.newswire.ca/news-releases/nearly-one-third-of-the-36-billion-cost-of-regulation-in-canada-is-unnecessary-red-tape-670479063.html.

[14] Olivia White, et al., "Digital Identification: A Key to Inclusive Growth," McKinsey Global Institute Report, April 17, 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

[15] See, for example, "Malaysia Plans to Implement National Digital Id for Internet Users," Malaysian Wireless, August 29, 2019, https://www.malaysianwireless.com/2019/08/malaysia-national-digital-id/.

[16] World Economic Forum, "Inclusive Deployment of Blockchain for Supply Chains, Part 2: Trustworthy Verification of Digital Identities," white paper, 2019, https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-2-trustworthy-verification-of-digital-identities.

[17] Transaction costs were as much as five times higher for the least trusted automaker than the most trusted one. Jeffrey H. Dyer and Wujin Chu, "The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea," *Organization Science* 14(1), 2003: 57–68, https://doi.org/10.1287/orsc.14.1.57.12806

[18] We found that in 2030, digital ID will have the potential to create economic value equivalent to 6 percent of GDP in emerging economies on a per-country basis and 3 percent in mature economies, assuming high levels of adoption (exhibit 3). In emerging economies, much of the value could be captured through even basic digital ID with essential functionalities. For mature economies, many processes are already digital and the potential for improvement is more limited, necessitating advanced digital ID programs with data-sharing features. Of the potential value, we estimate that in emerging economies, some 65 percent could accrue to individuals, while in mature economies, about 40 percent could flow to individuals.

[19] Legal Entity Identifier, Wikipedia, Accessed May 2021, https://en.wikipedia.org/wiki/Legal_Entity_Identifier

[20] The ISO 17442 standard specifies the minimum reference data, which must be supplied for each LEI:
The official name of the legal entity as recorded in the official registers; registered address of that legal entity. country of formation; codes for the representation of names of countries and their subdivisions; date of the first LEI assignment; the date of last update of the LEI information; and the date of expiry, if applicable.

[21] "*Who is Who and What is What?*: The Need for Universal Entity Identification in the United States," Data Foundation, September 2017, https://www.datafoundation.org/lei-report-2017.

[22] Competition among local operating units (LOUs) that issue LEIs are expected to help drive the price down, but awareness and adoption among small firms in developing countries will still likely be challenging. In contrast, for large companies, the cost of a LEI is immaterial and the benefits are greater and more immediate as they can use LEI to deal with large financial services entities that know LEI well.

[23] World Customs Organization, "WCO Guidelines on Trader Identification Number," June 2018, http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/trader-identification-number/guidelines-on-trader-identification-number.pdf.

[24] Hannah C. Norberg, Emmanuelle Ganne, and Nadia Hewett, "Super Charging Trade With a Trusted Global Digital Identity System," policy brief, accessed May 2021, https://www.unescap.org/sites/default/files/86%20Final-Team%20Hanna%20Norberg-Sweden.pdf.

[25] Digital Economy Partnership Agreement, Ministry of Trade and Industry Singapore, accessed May 2021, https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

[26] Ann Williams, "Businesses Must Switch to CorpPass for Online Government Transactions from Sept 1," The Straits Times, August 23, 2018, https://www.straitstimes.com/business/economy/businesses-must-switch-to-corppass-for-online-government-transactions-from-sept-1

[27] Henrik Hvid Jensen, "Global Trade Identity Can Be the Cornerstone of Paperless Trade," World Economic Forum, May 13, 2019, https://www.weforum.org/agenda/2019/05/global-trade-identity-can-be-the-cornerstone-of-paperless-trade/.

[28] Digital Identity Road Map Guide, ITU, 2018, https://www.itu.int/pub/D-STR-DIGITAL.01-2018.

[29] The user also nees valid certificates, the latest version of the ID software, an operating system that supports the ID software, an ID card, mobile-ID or online banking passwords, ID card or mobile-ID PIN codes. See "Estonian companies can now be established just using Smart-ID," *The Baltic Times*, March 12, 2020, https://www.baltictimes.com/estonian_companies_can_now_be_established_just_using_smart-id/

[30] "Azerbaijan's Efforts to Attract Global Entrepreneurs: E and M-Residency," Fintech Switzerland, December 3, 2019, https://fintechnews.ch/govtech/azerbaijans-e-and-m-residency/31969/ and https://dth.azexport.az/become-resident.html and a digital ID - https://asanimza.az/en/.

[31] "eHerkenning: authentication and authorization," eHerkenning, Accessed May 2021, https://www.eherkenning.nl/english

[32] "eRecognition for organizations," eHerkenning, Accessed May 2021, https://www.eherkenning.nl/aansluiten-op-eherkenning

[33] The various trust services offered by eIDAS include electronic signature, electronic sea, electronic timestamp, electronic registered delivery service, and Website Authentication Certificates.

[34] "The Rise of Digital Identities," SIGNICAT, Accessed May 2021, https://cdn2.hubspot.net/hubfs/5310879/Downloads/signicat-AML-white-paper.pdf

[35] The Verifiable Organizations Network (VON) would assemble a software stack, open-source it, and encourage everyone to use it until the network effect took over, like it did with the telephone or AirBnB.