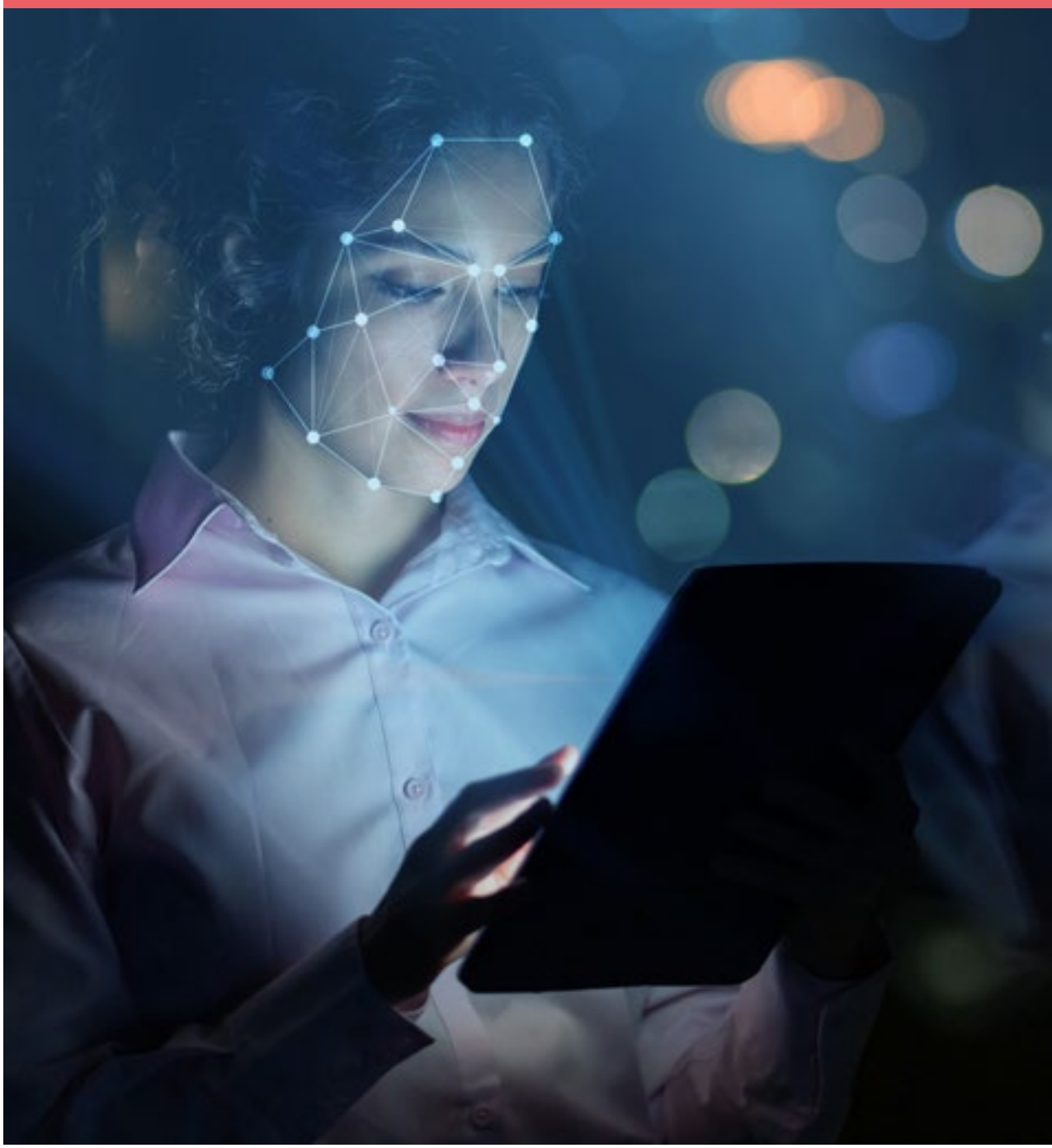
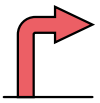
3
GLOBAL DIGITAL IDENTITY



Identity and trust lie at the core of each trade interaction. As global value chains become increasingly digital, organizations need to ensure that they can trust the digital identity of legal and physical persons[1] or products they deal with, and can efficiently link that digital identity with a real organization, specific product or device (see Box 17).

This process of dynamically verifying counterparts is a critical step in onboarding suppliers and establishing trust in trade (World Economic Forum, 2019). The global nature of value chains requires a global approach to digital identities to avoid creating digital identity silos.

A | DIGITAL IDENTITY OF NATURAL AND LEGAL PERSONS



Accessing reliable information in order to verify a party's identity is a critical step for a wide range of international trade transactions and processes, including, *inter alia*: contract formation; exchange of data and e-documents; onboarding of new suppliers and partners; social and environmental compliance; know-your-customer processes; anti-money-laundering processes; counter-terrorist financing; ultimate-beneficial-owner processes; and customs clearance.

Both public and industry actors have developed digital identity systems for entities to help to identify the supply chain actors involved and gain insights into from whom the data message has originated. However, these systems are often sector-specific (e.g. customs, financial companies, business registration).

Hence, an entity's digital identity is traditionally held in different registries and is generally not recognized outside its system and across borders. For instance:

- The World Customs Organization (WCO), in collaboration with customs authorities and industry stakeholders, developed technical standards and guidance for establishing the trade identification number, which is commonly used by customs authorities to identify authorized economic operators (AEO). AEO programmes are trusted traders' schemes which aim at securing global supply chains and facilitating customs processes for companies deemed trustworthy.
- The Global Legal Entity Identifier was established in 2011 by the G20 in the wake of the financial crisis, with oversight provided by the Financial Stability Board. Now administered by the Global Legal Entity Identifier Foundation, the legal entity identifier (LEI) is a 20-digit code based on ISO 17442:2020[2] standards, which provides a unique identification to participating parties (see Box 18).
- Business at OECD and the B20 Saudi Arabia Secretariat submitted a joint proposal to the G20 on a global value chain passport.[3] The passport aims at proving that an entity complies with relevant financial regulations and requirements, thereby avoiding the burden of having to prove identity multiple times across borders.
- Industry stakeholders have also developed their own initiatives. The Data Universal Numbering System (DUNS) is a proprietary system developed and managed by Dun & Bradstreet, which assigns a unique numeric identifier (a DUNS number) to a single business entity. Global Location Number (GLN) is managed by GS1 and enables organizations (i.e. business entities) and their subgroups (i.e. departments, divisions) to be able to identify themselves anywhere in the world by using an unambiguous, globally unique identifier that can be safely used by any other organization in the world. GLNs are currently used by millions of organizations in various sectors.

> **"Blockchain and DLT bring a new dimension to digital identities, allowing physical and legal persons to manage their own identity."**

BOX 17

DIGITAL IDENTITY

A digital identity comprises attributes and identifiers, just as in the physical world. It is a digital representation of the information known about a specific individual, group, organization or product.

A digital identity ensures that you know with whom you are interacting and thereby fosters trust throughout supply chains. It involves authentication ("Who are you?") and authorization ("What are you allowed to do?") processes. The concept of digital identity can apply to natural and legal persons, as well as physical and digital objects.

BOX 18

LEGAL ENTITY IDENTIFIER

Each LEI contains information about the company – "who is who", "who owns whom" and soon "who owns what". A uniform global LEI system will make it easier to identify legal entities and to verify their status. Global adoption of LEIs would help banks:

- to conduct know-your-customer due diligence;
- to mitigate the risk of correspondent bank relationships being cut (i.e. de-risking – an action observed by banks in many regions today);
- to increase access to finance for small business in emerging markets by easing the flow of reliable information about small companies;
- to promote the development of emergent technologies such as blockchain, thereby reducing costs.

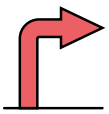
Without a unique and globally harmonized identifier, finding information about a small business in a sea of metadata is difficult, if not impossible (Patel and Ganne, 2021). LEIs make this process workable and help to realize the potential of financial technology to make finance more accessible. LEIs can drive more transparency and underpin the promise of financial technology to deliver greater inclusion of small businesses in the global economy. However, adoption of LEIs remains limited. By the end of 2020, only 1.8 million companies in over 250 jurisdictions had acquired an LEI. In order to encourage adoption, the ICC has recently established a working group on mass LEI adoption.

Blockchain and DLT bring a new dimension to digital identities, i.e. decentralized identity systems (see Box 19 for a description of the various types of digital identity systems). Systems based on blockchain allow physical and legal persons to manage their own identity (i.e. self-sovereign identity). These decentralized systems enable companies to limit the sharing of identity data to what is strictly necessary for the provision of a service or for the access to goods and online public and private services.

Various decentralized identity systems are already in production, although they currently have limited commercial use. The Sovrin Network, for example, is a public-permissioned blockchain designed to support self-sovereign identity and verifiable claims, and is used by the British Colombia and Ontario's Verifiable Organizations Network.

Despite their usefulness in fostering transparency and trust throughout supply chains, the number of identities and the commercial costs to manage them increase as companies reach foreign markets. Existing identity silos make supply chains less efficient and agile and may be challenging for small business to handle, as they do not have the resources to deal with multiple systems. Global alignment on what attributes matter and constitute an identity is needed to promote mutual recognition and to break existing silos.

B | DIGITAL IDENTITY OF PHYSICAL AND DIGITAL OBJECTS



Traceability is the ability to identify and trace the history, distribution, location and use of containers, consignments, shipments and products from end to end. It enhances planning and risk management, and the greater transparency that this brings to supply chains' operations can play a key role in mitigating the impact of supply chain disruptions, such as those experienced during the COVID-19 pandemic.

Traceability of sustainability credentials can also provide greater insight into the environmental footprint and social impacts of final and intermediate goods in global value chains. Increasingly, governments require companies to ensure that their products be produced according to minimum standards (e.g. legally logged timber, legal employment). Governments may deny the entry of goods which fail to meet requirements.

Traceability and transparency can make it easier and cheaper to show both regulatory conformance and that production standards meet the expectations of customers (e.g. organic methods, environmentally friendly goods, fair wages). This requirement is increasingly reflected in intergovernmental initiatives, such as the United Nations Economic Commission for Europe (UNECE) and the United Nations Centre for Trade Facilitation and Electronic Business

BOX 19

DIGITAL IDENTITY SYSTEMS

Digital identity systems typically fall into three types:

- centralized: one entity manages identities centrally;
- federated: users can use the same verification method for access to various applications;
- decentralized: users manage their own identity (i.e. self-sovereign identity).

The difference between the types is who controls the identity — an intermediary or the physical or legal person itself. Each type has a fundamental structure that sets them apart, with implications for adoption and trust levels, and advantages and challenges for users.

(UN/CEFACT) initiative Enhancing Traceability and Transparency for Sustainable Value Chains in the Garment and Footwear Sector (see Box 20). With the rapid growth of online trading, correctly identifying products and accurately providing all the relevant information online are vital for consumer confidence and brand reputation. Traceability can also help to monitor the lifecycle of a product with a view to reducing fraud and theft or to assessing its contribution to a global circular economy.

TradeTech opens new opportunities to identify and track physical and digital objects. For instance, IoT devices can collect and monitor information in real-time. According to experts, around 20 per cent of cargo now has a device attached for tracking international shipping, collecting diverse information (e.g. location, temperature, speed, humidity) and even estimated time of arrival.

The use of blockchain and DLT to store IoT data guarantees the quasi-immutability of the data, thereby fostering trust in supply chains. Used on its own, blockchain makes it possible to track transactions recorded on the ledger in a highly secure environment. AI can be used to optimize inventory management systems by estimating orders, thereby avoiding inventory over or under-stocking as well as missed responses to trends.

Various object identification systems exist,[4] and stakeholders have developed proprietary databases,

> **"Integrating multiple identities and attributes from different sources about a given product can improve traceability."**

with both public and private records, that contain a product history in digital form. However, existing systems and proprietary ledgers are not always compatible. Objects traced can thus have multiple identities stored in different places, creating redundancy and high frictional costs for reconciliation and verification of disparate identities. Because product classification is a manual process even among very large global companies, it is a constant source of risk and complexity for trade teams, and dealing with multiple countries intensifies the complexities and manual burden.

The lack of consistent identification and traceability of objects significantly limits the potential of traceability and automatic tracking from one end of the supply chain to the other. Integrating multiple identities and attributes from different sources about a given product can improve traceability.

In addition to enhanced transparency of sustainable practices of stakeholders involved in international trade the "use of industry standards leads to better supply chain outcomes for all stakeholders such as improved product traceability and visibility across international borders; seamless sharing of regulatory documents

BOX 20

TRADETECH APPLICATIONS PROVIDING OBJECTS WITH A DIGITAL IDENTITY

UNECE Blockchain Pilot for Traceability and Due Diligence in Cotton Value Chains*

Traceability and transparency in the garment and footwear sector have become a priority for consumers, governments and the industry due to the environmental footprint and social impacts resulting from decades of unsustainable consumption and production practices. In 2020, UNECE launched a pilot project to develop a blockchain system for traceability and due diligence in the cotton value chain, from field to shelf. The pilot aims to provide governments and companies with a set of tools to advance traceability, transparency and sustainability in this industry and to support the identification and coding of the key data to assess the sustainability performance of products, processes and facilities.

The pilot tests a selected set of sustainability claims, identified jointly with partners, which concern origin, content (organic and recycled), use of chemicals, and compliance with due diligence requirements. Partners have also been asked:

- To identify those products and materials (traceable assets) to which one or more of the selected sustainability claims should be applied;
- To collect and exchange relevant information and documents with business partners (e.g. shipping documents, delivery notes, invoices) and sustainability certificates and inspection reports that are collected at relevant nodes of the value chain.

Traceability is ensured by the application of DNA markers. A public, permissionless, Ethereum blockchain, which allows for the running of smart contracts, is used to increase the trustworthiness of the data as well as the connectivity, cost-efficiency, scalability and transferability of the solution. Later, the transfer of data from existing systems will be allowed through an application programming interface (API). The following considerations and recommendations are emerging from the ongoing implementation of the pilot:

- Need for an enabling environment for engagement and collaboration of all upstream and downstream value chain actors;
- Tailored policy and regulations which reference standards for data interoperability and take into account other evolving technologies (i.e. AI, IoT, big data and cloud computing);
- Open source, inclusive solutions and capacity-building for scaling up, particularly with small business;
- Support of frameworks for data security, privacy and governance as preconditions for accelerating adoption;
- Data models for inspection reports, certificates and credentials based on international standards for information exchange (e.g. UN/CEFACT e-business standards).

Naveo – Navigation and Geocoding Technologies Ltd**

Naveo's platform, used by around 300 corporate clients in Africa and the Indian Ocean region, tracks fleets by capturing GPS locations, fuel tank levels, speed and engine status, among other sensitive vehicle-related information. Thermal sensors installed on vehicles monitor refrigerators transporting foodstuffs and medicines to alert any sudden rise in temperature. The data captured through IoT devices are sent in real-time to cloud databases. The model mines data along food supply chains, from farms and distributors to markets, such as the condition of vehicles, fuel consumption, the behaviour of drivers as well as recommendations for optimizing road routes. These analytics help businesses to be more productive and save money through the efficient use of transportation resources.

Other traceability initiatives

There are many initiatives to track the provenance of products, assert ethical, social or environmental claims, track counterfeit products or reduce supply-chain inefficiencies. Some companies active in this field include:

- Provenance, which has carried out several projects in the food and drinks and beauty and fashion sectors to assert the sustainable provenance of goods;
- Everledger, which tracks the movement of diamonds from mines to shores;
- Agridigital and Agriledger, which help agricultural businesses to solve supply chain inefficiencies and to track the origin of their products;
- Cardano, which works with a small Georgian winemaker (Baia's Wine) to enable end-to-end supply chain traceability for their organic wines;
- Minehub and Minespider, which use blockchain for traceability and responsible mining and mineral supply chains;
- Blockverify and Blockpharma, which help to fight counterfeit in pharmaceuticals and other sectors.

* See https://unece.org/trade/traceability-sustainable-garment-and-footwear.

** See https://www.naveo.mu/en/home.

and data accurately determining jurisdiction and risk profile for each product; and enhanced consumer safety related to unsafe, recalled or counterfeit products."[5]

Moreover, these product identification systems could be linked to product classification systems, such as Harmonized System (HS) codes, to enhance transparency of supply chains and help to increase border efficiency (see Box 21). However, digital identity of objects is not sufficient to support end-to-end traceability. Another issue mentioned by experts is the uneven customs treatment of IoT devices (see Box 22).

There is an urgent need for international alignment to break existing digital identity siloes. Some international initiatives are emerging to try and address this issue. The draft UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services accommodates different levels of reliability.

"There is an urgent need for international alignment to break existing digital identity siloes."

The governments of some EU member States (Finland, Germany, Spain), Canada (British Columbia, Ontario) and Latin America have also announced a digital identity wallet to link national digital identities with proof of other personal attributes (e.g. driving licences, diplomas, bank accounts) so that individuals and companies can prove their identity by using one single platform.[6]

Industry is also working towards interoperable digital identity systems. The World Wide Web Consortium (W3C) has developed the Verifiable Credentials (VC) Data Mode and Decentralized Identifiers (DIDs) protocol to provide a standard way to express

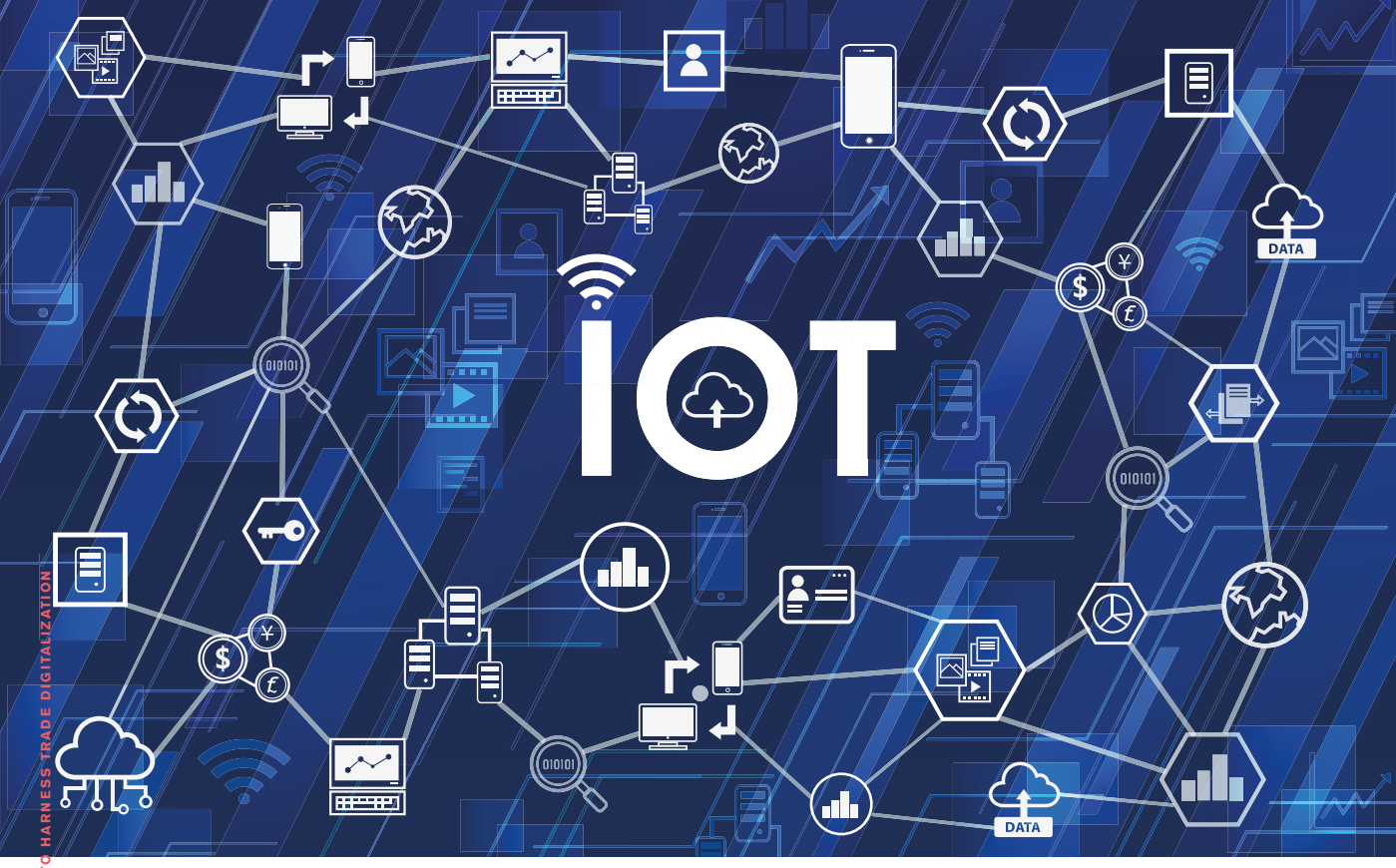
BOX 21

PRODUCT IDENTIFICATION AND CLASSIFICATION

The GS1 Global Product Classification (GPC) coding system and the Global Trade Item Number (GTIN, also known as UPC, EAN, SKU number, barcode number) are widely used in business to business exchanges to verify product data, including country of origin, product type and content, among other things. The GTIN uniquely identifies products both online and in-store, and border agencies are increasingly requiring traders to provide GTINs in addition to HS codes.

Linking global product identification systems, such as GPC and GTIN, and HS codes could prove very powerful and provide the global trading system with more information about products moving across borders and with new functionalities. It could simplify processes for economic operators, since the data from their systems would be recorded only once and eliminate (or significantly reduce) the need for a one-off manual data input.

Source: See https://www.unescap.org/sites/default/files/113%20Final-Team%20Patrik%20Jonasson-GS1.pdf.



BOX 22

UNEVEN CUSTOMS TREATMENT OF IOT DEVICES

In many countries, customs authorities treat the IoT device used in a container as a definite import (instead of temporary or in transit), and thereby impose duties or delay the release of the IoT device, even though the device is to be used in subsequent shipments and will eventually leave the country. Custom duties applied could be substantial considering the value of the devices themselves.

In many cases, these additional costs force companies to either store a large number of IoT devices to mitigate customs delays or risk not attaching IoT devices to cargo, ultimately harming companies' abilities to market IoT devices and to deploy transparency and security solutions for international trade. The use of a common temporary import regime, or transit regime, could encourage the re-usability of IoT devices, which are often discarded after one use in the destination market.

Diverging customs treatment of IoT devices undermines traceability, efficiency, safety and security of supply chains.

identity credentials online for any subject (i.e. person, company, physical or digital good or document). W3C provides standardized components constituting a verifiable credential (i.e. identity of an issuer) and a verifiable presentation (i.e. data shared with a verifier). These W3C credentials are used by both public and private stakeholders. For instance, the United States Department of Homeland Security is funding the development of DID-based verifiable credentials as a standard the United States Customs and Border Protection service can use for supply chain verification in response to the COVID-19 crisis. DID-based decentralized digital credentials are also being used by the IATA in relation to COVID-19 digital health passes. An important and business-friendly feature of the DID/VC technology stack is "selective disclosure", which is that a holder of a credential can choose to only disclose selected data to a recipient and select different data from the same credential to disclose to a different recipient.

Trade agreements have thus far focused on the identification of a person in the context of e-signatures and have largely disregarded the broader issue of digital identity of persons. With respect to identity of objects, trade agreements have focused on interoperability of product classification systems (e.g. HS codes) but disregarded interoperability of product identification systems

and linkages between product classification and identification systems.

As of 15 October 2021, none of the 350 RTAs currently in force and notified to the WTO addresses the issue of identity. They exclusively focus on e-authentication and e-signatures and do not cover issues relating to the management of identifiers and attributes, despite the increasing number of digital identity systems. Nor is digital identity discussed in the context of the WTO Joint Initiative on E-commerce.

DEPA and SADEA are two notable exceptions. These recent agreements include provisions on digital identities that call for interoperability and mutual recognition of digital identity systems and the exchange of best practices.

Where do we stand and what can be done from a trade policy perspective to address digital identity silos?

Governments could use trade agreements to avoid divergence of digital identity systems relating to legal and natural persons by:

- Supporting and leveraging international initiatives aimed at fostering mutual recognition of identifiers and attributes, such as the UNCITRAL Working Group IV (Electronic Commerce) on digital identity and trust services[7] and the W3C Verifiable Credentials Data Model.
- Leading by example through the setting up of a minimum level and type of business data (or attributes). Governments would ensure that updates to the legal status of an entity are continually maintained and immediately communicated. As soon as a legal entity changes status, the change would be made accessible to all parties involved in real-time and on-demand (see Annex for detailed suggestions).
- Encouraging the development of a global certification framework whereby accredited digital identity operators would issue globally recognized digital identities.

With respect to identities of physical and digital objects, governments could leverage trade agreements by:

- Promoting the use of open, global standards for product identification and data sharing across global value chains.
- Creating a linkage between product identification and classification systems, such as HS codes, UN/CEFACT data models, the W3C verifiable credential standard and product identification systems (e.g. GPC and GTIN). The GS1 Digital Link standard offers a method for achieving this linkage based on existing product, organization and object identifiers.[8]
- Encouraging customs authorities to agree on a standardized treatment of IoT devices to promote their use and contribute to better traceability of objects throughout supply chains.

ENDNOTES

1. The digital identity of individuals involves issues such as human rights or privacy concerns that do not apply to digital identity of companies. These issues are not discussed in this publication although they remain important for any digital identity project involving individuals.
2. Financial Services: Legal Entity Identifier (LEI), ISO 17442:2020.
3. See https://www.tradefinanceglobal.com/posts/global-executive-forum-b20-business-at-oecd-exclusive-gvc-passport and Business at OECD and B20 Saudi Arabia Secretariat (2020).
4. See https://www.ccpit.org/image/1331845279825047554/906569dc45284dfeb39dcbcce1d550e4.pdf.
5. See https://www.unescap.org/sites/default/files/113%20Final-Team%20Patrik%20Jonasson-GS1.pdf.
6. See https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663.
7. The Working Group is discussing legal issues relating to identity management and trust services with a view to introducing different levels of reliability of methods, processes and technologies used in the identification and authentication processes, as well as to specify the legal consequences attached to each reliability level.
8. See https://www.gs1.org/standards/gs1-digital-link.