

The digital identity of legal entities: Current status and the way forward

Gerard Hartsink

Received (in revised form): 16th January, 2018

Global Legal Entity Identifier Foundation (GLEIF), St. Alban-Vorstadt 5, 4052 Basel, Switzerland
E-mail: gerard.hartsink@gleif.org

Gerard Hartsink is Chairman of the Global Legal Entity Identifier Foundation. He is also a member of the World Trade Board, the International Chamber of Commerce Digital Economy Commission and the Dutch government's Forum Standaardisatie. His previous roles include Senior Executive Vice President of ABN AMRO Bank, Chairman of CLS Bank International and the European Payments Council and Board Member of SWIFT, LCH.Clearnet Group, Euroclear Netherlands and the Euro Banking Association.

ABSTRACT

Electronic communication continues to grow in importance as a tool to support trade in goods and services, in particular between buyers and sellers based in different countries. Banks, for example, have notably extensive experience in this area, while public administrations are increasingly developing e-government services for their domestic needs. As the supply chain has become international, the need has arisen for global standards to define the identities of trading partners for the purposes of invoicing, customs declarations and payments. Businesses, consumers and government agencies are all faced with the challenge to understand 'who is who' in the digital and global supply chain. This requires a global approach to identity management. This paper discusses the fundamental issues regarding identities in business applications and payment systems.

Keywords: digital identity of natural persons, digital identity of legal entities, payment systems, know your customer, know your supplier

INTRODUCTION

Consumers and businesses are increasingly buying goods and services online as well as communicating online with government agencies. This requires a trusted environment for counterparties to communicate with each other and for payments linked to those transactions.

Banks, together with card schemes, have developed card services to meet the needs of many businesses for both offline and online transactions. Around the world, consumers are buying increasing volumes of goods and services online and want assurance that web merchants can be relied upon to deliver the goods or services as asked for. However, 'know your supplier' (KYS) data on businesses can be complicated or costly for consumers to obtain. This makes it difficult for consumers to check the legal status of their potential suppliers. To further complicate matters, some payments must be made to a business other than the actual supplier of the goods or services. In short, it is increasingly complex for consumers to obtain KYS information in the global digital economy.

Generally speaking, businesses have more experience with the management of customer and supplier data. They understand their growing responsibilities for the customer and supplier data they hold in terms of data protection for consumers as well as the fiscal and legal requirements such as 'know your customer' (KYC) obligations to manage the risks of money laundering



Gerard Hartsink

or terrorist financing. They also know that managing such data is important for operational risk management and that it requires substantial operational costs.

Financial firms are required by law to take care of their customers' data. In June 2017, the Basel Committee on Banking Supervision published an updated general guide for the opening of accounts in line with a sound risk management profile for anti-money-laundering and terrorist finance risks.¹ The supervisors of those licensed firms are expected to review the implementation of these policies and legal obligations.

DIGITAL ENTITIES

In the digital world, the question of 'who is who' is important for business transactions and communication with government agencies. Legal systems make a distinction between natural persons and legal entities. The specifics of that distinction are embedded in national legislations. Not all natural persons have the same rights and duties in all jurisdictions and a limited number of attributes of natural persons may change over time. Legal entities are dynamic and may change over time as a consequence of corporate actions. Such facts represent important data to manage in files on customers and government registers of natural persons and businesses. Meeting KYC and KYS principles requires a regular and costly review of the data.

In the digital economy, identifiers are assigned not only to natural persons and legal entities, but also 'things'. Examples of recognised global 'things' include credit cards (ISO 7812), barcodes (GS1), containers (ISO 6364) and the registration of ships and aeroplanes. All these things (assets) are uniquely identified in the digital economy. Their respective registers clarify 'who owns what', which can only be a legal entity or a natural person.

NATURAL PERSONS

For private and public purposes, there are many numbering systems to identify citizens or consumers. The governments of about 200 jurisdictions issue via their government agencies ID numbers, tax numbers, social security numbers, driving licence numbers and passport numbers to identify their citizens for the current world population of 7.5 billion natural persons. Such identification systems are based on national standards (numbering systems) and are created by specific government agencies at the national level for public sector rather than commercial purposes.

To meet the public sector needs for the identification of travellers, the International Civil Aviation Organization developed a system that captures the data of travellers based on issued travel documents, such as a passport, which can be used for border control and custom purposes.²

There is no cross-jurisdiction interoperability of data with respect to the registers of natural persons. In 2014, the European Union approved the eIDAS Regulation 2014/910, making it possible for a citizen of an EU member state to identify him/herself with the authentication tools of the notified national electronic identification schemes to get access to the government agencies of the other EU member states.³ This does not create any interoperability between the registers of the EU member states, but rather facilitates European residents' access to the government agencies of all other EU member states.

Commercial organisations have their own registration systems for their consumers. Customer data often come from multiple sources. A consumer may have many customer numbers and multiple identities from various social media profiles, in addition to the identification numbers issued by his/her government.

Organisations must comply with the data protection rules of their jurisdiction. Under

the General Data Protection Regulation 2016/679,⁴ the EU has created stringent new rules for organisations to manage the personal data of EU residents from 25th May, 2018 onwards.

The reality is that there is no globally accepted unique identifier standard for natural persons. Consumers can buy goods and services online from any web merchant around the world and may have contacts with the government agencies of multiple jurisdictions. Government agencies and commercial organisations, meanwhile, must store and process the data of natural persons from many jurisdictions.

Natural persons also include the directors of boards, executives or proxy holders of legal entities of the same or of other jurisdictions.

In the absence of a global standard for natural persons, the ISO TC 68 Financial Services technical committee is investigating whether a global standard for natural persons should be developed to support the public and private sector to conduct business processes in the digital world.

LEGAL ENTITIES

In any jurisdiction, the legislator will have created multiple legal forms for the public sector and the private sector (commercial and non-commercial), each with specific rights and duties (such as tax).

At the request of the public sector, ISO TC 68 Financial Services developed the ISO 20275 Entity Legal Form standard to specify the elements of an unambiguous scheme to identify the distinct entity legal forms in any jurisdiction in order to facilitate a better classification of legal entities. The overview, containing over 1,800 entity legal forms from 50 jurisdictions, is available free of charge⁵ and scheduled to be completed in 2018 for all jurisdictions.

The public sector of each jurisdiction created one or more business registers to

register the legal entities of their jurisdiction. The overview of business registers is also available online.⁶ Something that business registers have in common is that they have their own business models, local legal and technical standards and that they were not created for the challenges of the global supply chain and digital economy.

The recording of the data in business registration is based on self-registration. Legal entities are ‘living organisations’ that change over time as a consequence of corporate actions, such a name change, mergers, unbundling, change of legal form or change of activities. These facts have a substantial impact on the quality of the data in business registers.

In its Cannes Summit in 2011, the G20 concluded that the Financial Stability Board (FSB) should take the lead for an appropriate framework, representing the public interest for a global legal entity identifier (LEI) in the form of a reference code to uniquely identify legally distinct entities that engage in financial transactions.⁷ The FSB established the LEI Regulatory Oversight Committee (ROC) in 2012 (<https://www.leiroc.org/>) and the Global Legal Entity Identifier Foundation (GLEIF), a Swiss foundation, in June 2014 (<https://www.gleif.org/>). The mission of GLEIF is to support, on a not-for-profit basis, the implementation of a global LEI system to make high-quality LEI data available free of charge to users in both the public and private sector. GLEIF is subject to the oversight of the LEI ROC.

By January 2018, over 1 million legal entities had registered with a GLEIF accredited LEI issuer for an LEI.⁸ The LEI ROC estimates that, over time, between 200–400 million legal entities could be eligible for an LEI.⁹ A large number of listed companies that operate in multiple jurisdictions already have an LEI.

The LEI is based on the ISO 17442 standard designed by ISO TC 68 Financial Services. It is a unique legal identifier, and a

legal entity can have only one. Legal entities obtain an LEI by means of self-registration with their chosen LEI issuer, much as they would with a business register. A rigorous quality programme is applied to ensure the LEI data record is of the highest possible quality. This process includes the annual validation of all data elements in every LEI record, an option for users to dispute data elements, and a free quality report on all LEI issuers which is published every month.¹⁰ This quality programme is not part of the business registration processes.

With respect to financial transactions, the quality of the data on legal entities is important for cash management at corporates, small and medium-sized enterprises and treasuries in the public sector. In addition, financial institutions have a huge interest in data quality in order to meet the legal requirements for customer data and for managing their credit and liquidity management risks. Open source LEI data provided free for any user to download will over time lead to fewer risks and lower operational costs.

Among commercial organisations (eg data vendors, financial institutions, FinTechs, certification solution vendors), there is a growing interest in the inclusion of LEIs in customer and supplier files due to the high quality of this standardised digital legal entity identifier and the fact that the data are free of charge.

Together with its partners, GLEIF is exploring the inclusion of LEIs in business processes for the global supply chain (together with GS1¹¹) and for the market participants of the capital and money markets. The planned free-of-charge LEI mapping services with the ISO BIC 3166 standard (together with SWIFT¹²) and ISO 6166 ISIN standard (together with ANNA¹³) will facilitate the digital linking of the unique LEI with these identifiers. Legal entities may have multiple Business Identifier Code (BIC) or International Securities Identification Number (ISIN) identifiers.

IDENTITY MANAGEMENT FOR PAYMENT SYSTEMS

Identity management has always been an important building block for electronic payments systems in order to manage the operational risks of the scheme and for the scheme participants. The Financial Action Task Force (FATF) recommendations on combating money laundering and the financing of terrorism¹⁴ on the legislation in any jurisdiction have increased the need for an end-to-end approach on identity management for payments. Scheme participants must, among other things, be responsible for high-quality data on their customers for the purposes of customer due diligence, record keeping and wire transfer processes.

For retail payment systems, the trend is towards the further unbundling of the payment process as a consequence of legislation (such as the Second Payment Services Directive, with the creation of licensed payment initiation service providers) and market developments like overlay service providers. All direct and indirect participants of retail payment schemes and systems need to ensure that correct customer data are used for the transfer of funds (domestically or cross-border). The quality of the data from participants of national or international payments schemes too often fails to meet the high-quality standard that supervisors require for their licensed financial institutions.

Principle 22 of the PFMI states that ‘an FMI should use, or at minimum accommodate, relevant internationally accepted communication procedures and standards to facilitate efficient payment, clearing, settlement and recording’.¹⁵ The principle does not, however, clarify what the international standard should be for legal entities and for natural persons and what the data quality level should be for scheme participants in order to meet the requirement of the overseers. The ISO 17442 LEI standard is an international standard for legal entities,

but for natural persons there is not yet a standard available. Because most payment scheme participants have an LEI already, the addition of the high-quality LEI to the file of the scheme participant could improve risk management for the scheme owner (scheme manager) without additional cost.

Cards are important identification and payment instruments for consumers to buy goods and services from online merchants. For card issuers, an LEI mapping service with the ISO 7812 identification standard for issued cards could improve data quality. Among too many compliance officers of card acquirers, card processors and card schemes, there are strong signals that the quality of merchant data fails to comply with the Payment Card Industry Security Standard (PCI).¹⁶ Access to high-quality merchant data is in the interest of consumers in terms of the KYS principle and of card scheme participants to aid the management of their operational risks. Adding the LEI to the PCI requirements could reduce the operational costs and risks associated with card schemes for their acquirers and processors.

IDENTIFICATION AND AUTHENTICATION

As part of their customer due diligence processes, banks (and other licensed firms) rely on formal documentation from the government agencies of the jurisdiction involved. Maintaining data on legal entities requires more time compared with maintaining data on natural persons.

In the digital economy, authentication is the process of confirming that the claimed identity is true.

The following business models can be observed in the authentication of natural persons for business processes in a given jurisdiction:

- *issuers of the authentication tools*: government agencies, banks, telecom providers;

- *acceptors of authentication tools*: government agencies, banks, merchants.

In some jurisdictions, government tools for the authentication of citizens may be used only by government agencies and not by commercial organisations (eg DIGID in The Netherlands — <https://www.digid.nl/en/>). Meanwhile, in some jurisdictions, one bank's authentication tools may also be available for other banks, web merchants and government agencies to use (eg BankID in Sweden — <https://www.bankid.com/en/>).

The cross-border authentication of consumers, businesses and government agencies is more complex. Those certification authorities that use the X.509 protocol for digital certificates (<https://cabforum.org/>) know well that the weak part of their end-to-end communication services is the (legal) identity of the sender and of the receiver.¹⁷

COSTS AND RISKS OF IDENTITY MANAGEMENT

Businesses, in particular their data managers, compliance officers and procurement officers, have become aware of the substantial costs and potential risks involved in managing the data of customers and suppliers.

Many banks have multiple IDs for the same business partner, such as a national government-issued business registration number, VAT number (in the EU), Employer Identification Number (in the USA) or industry-issued number such as the ISO BIC, DUN,¹⁸ PERM ID¹⁹ etc. The attributes of those registration numbers may not be exactly the same. In addition it is not clear how a legal entity fits into its group structure.

To overcome the data-quality challenges in the supply chain, the LEI could add value for all parties engaged in commercial transactions. There is no other global, open legal entity identification system with such a strict regime of regular data verification to ensure

the high quality of its data. The LEI data record also gives insight on the national business registration number in addition to the direct and/or ultimate parents — if available — of that legal entity.

It is estimated that banks active in trade financing could save US\$500m per annum by using the LEI in trade finance and the issuance of letters of credits alone, with other potential benefits also possible.²⁰

SELF-SOVEREIGN IDENTITIES FOR THE PAYMENT INDUSTRY

A self-sovereign identity model has many attractive elements for consumers that buy goods and services from web merchants. It allows consumers to make explicit choices regarding which data to disclose to web merchants, similar to the way that consumers use a non-digital proof of identity such as a passport. However, self-sovereign identity models do have limitations with respect to legal requirements in the payment industry because banks must hold records of official data issued by government agencies (such as nationality, citizen number, name, address etc), while the recommendations of the Basel Committee on Banking Supervision and of the FATF require certain KYC data for account opening and for cross-border payments. Consumers have no choice regarding the data they must share with their bank.

THE WAY FORWARD

The supply chain is becoming increasingly global and digital. This requires a stronger system for the identification of trading partners for public purposes and private purposes. The LEI is a promising candidate because it is a high-quality identifier of legal entities that is provided free of charge to any user.

Where web merchants add their LEI to their website (preferably on the payment page), this would benefit consumers as it would meet the KYC requirements of consumer organisations.

Business, meanwhile, would benefit if their counterparties in the supply chain have an LEI because this would reduce the onboarding and maintenance costs of their customers and suppliers and reduce their operational risks.

Banks (and other financial firms) would benefit if their business customers had an LEI because this would facilitate the onboarding of those customers and the maintenance of customer data. Banks would benefit even more if correspondent banks, the financial market infrastructures and real-time gross settlement systems to which they are connected included the LEI in their messages because this would make their risk management and liquidity management less costly due to lower operational risks.

Payment schemes and automatic clearing houses (clearing and settlement mechanisms) would benefit from the addition of LEIs to the files of their participants and customers as this would reduce operational risks. In addition, the inclusion of the LEI of businesses in the scheme-rules of the rulebook and in the clearing messaging service would create additional added value for banks that are keen to deliver better payment reporting services to their business customers. The inclusion of the LEI of the business customer in a credit transfer will make the reconciliation of such payments easier during the incoming cash-management process of those businesses and government treasuries that receive the payment message.

Card schemes, card acquirers and card processors would benefit were the LEI included in the PCI requirements as this would reduce their operational risks.

All participants in the supply chain and the public sector would benefit from a global ISO standard for natural persons. The ISO TC 68 Financial Services needs to be encouraged, as was done for the LEI standard, to develop such a standard to facilitate the processing and storage of data on natural persons (from different jurisdictions) for public and private purposes. However,

the creation of a global register for natural persons is not recommended because of data-protection challenges.

As rule-maker of the PFMI Principles, the Committee on Payments and Market Infrastructures is encouraged to specify in more detail the ‘internationally accepted standards’ for legal entities and natural persons for the efficient payment, clearing, settlement and recording of the payments and card payment business to ensure efficient, safe and innovative payment systems for society.

REFERENCES

- (1) Bank of International Settlements (2017) ‘Guidelines sound management of risks related to money laundering and financing of terrorism, Annex 4 General guide to account opening’, available at: <https://www.bis.org/bcb/publ/d405.pdf> (accessed 9th January, 2018).
- (2) International Civil Aviation Organisation (n.d.) ‘Passenger data exchange: the basics’, available at: [https://www.icao.int/MID/Documents/2013/FAL%20Seminar/Passenger%20Data%20Exchange_The%20Basics.pdf#search=passenger%](https://www.icao.int/MID/Documents/2013/FAL%20Seminar/Passenger%20Data%20Exchange_The%20Basics.pdf#search=passenger%20) (accessed 9th January, 2018).
- (3) European Commission (2014) ‘Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC’, available at: https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf (accessed 9th January, 2018).
- (4) European Commission (2016) ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’, available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 9th January, 2018).
- (5) Global Legal Entity Identifier Foundation (n.d.) ‘About LEI: ISO 20275: Entity Legal Forms Code List’, available at: <https://www.gleif.org/en/about-lei/iso-20275-entity-legal-forms-code-list#> (accessed 9th January, 2018).
- (6) Global Legal Entity Identifier Foundation (n.d.) ‘About LEI: GLEIF Registration Authorities List’, available at: <https://www.gleif.org/en/about-lei/gleif-registration-authorities-list#> (accessed 9th January, 2018).
- (7) Global Legal Entity Identifier Foundation (n.d.) ‘About LEI: GLEIF Statutes’, available at: <https://www.gleif.org/en/about/governance/statutes#> (accessed 9th January, 2018).
- (8) Global Legal Entity Identifier Foundation (n.d.) ‘Overview of LEI issuers’, available at: <https://www.gleif.org/en/about-lei/how-to-get-an-lei-find-lei-issuing-organisations> (accessed 9th January, 2018).
- (9) Legal Entity Identifier Regulatory Oversight Committee (2015) ‘Progress Report by the Legal Entity Identifier Regulatory Oversight Committee: The Global LEI System and regulatory uses of the LEI’, 5th November, p. 22, available at: https://www.lei.org/publications/gls/lou_20151105-1.pdf (accessed 9th January, 2018).
- (10) Global Legal Entity Identifier Foundation (n.d.) ‘LEI Data: GLEIF Data Quality Management’, available at: <https://www.gleif.org/en/lei-data/gleif-data-quality-management#> (accessed 9th January, 2018).
- (11) GS1 (n.d.) ‘About GS1’, available at: <https://www.gs1.org/about> (accessed 9th January, 2018).
- (12) SWIFT (2017) ‘BIC Policy’, available at: https://www2.swift.com/uhbonline/books/public/en_uk/bic_policy/bic_policy.pdf (accessed 9th January, 2018).
- (13) Association of National Numbering Agencies (n.d.) ‘About ANNA’, available at: <http://www.anna-web.org/> (accessed 9th January, 2018).
- (14) Financial Action Task Force (2017) ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation’, available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (accessed 9th January, 2018).
- (15) Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions (2012) ‘Principles for Financial Market Infrastructures’, PFMI Principle 22, available at: <https://www.bis.org/cpmi/publ/d101a.pdf> (accessed 9th January, 2018).
- (16) Payment Card Industry Security Standard (n.d.) ‘About us’, available at: https://www.pcisecuritystandards.org/about_us/ (accessed 9th January, 2018).
- (17) International Telecommunications Union (2017) ‘X.509: Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks’, available at: <https://www.itu.int/rec/T-REC-X.509> (accessed 9th January, 2018).
- (18) Dun & Bradstreet (n.d.) ‘D-U-N-S® Number’, available at: <http://www.dnb.com/duns-number.html> (accessed 9th January, 2018).
- (19) Thomson Reuters (n.d.) ‘PermID: Connecting Data to the World’, available at: <https://permid.org/> (accessed 9th January, 2018).
- (20) McKinsey and GLEIF (2017) ‘The Legal Entity Identifier: The Value of the Unique Counterparty ID’, available at: <https://www.mckinsey.com/industries/financial-services/our-insights/the-legal-entity-identifier-the-value-of-the-unique-counterparty-id> (accessed 9th January, 2018).