Response of the Global Legal Entity Identifier Foundation (GLEIF) to the Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies White Paper

June 2018

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to the Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies White Paper. GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI) in the consultation.

First some background on the LEI.

The development of a system to uniquely identify legal entities globally had its beginnings in the 2008 financial crisis. Regulators worldwide acknowledged their inability to identify parties to transactions across markets, products, and regions for regulatory reporting and supervision. This hindered the ability to evaluate systemic and emerging risk, to identify trends, and to take corrective steps. Recognizing this gap, authorities, working with the private sector, have developed the framework of a Global LEI System (GLEIS) that will, through the issuance of unique LEIs, unambiguously identify legal entities engaged in financial transactions. Although the initial introduction of the LEI was for financial regulatory purposes, the usefulness of the LEI can be leveraged for any purpose in identity management for legal entities both by the public and private sectors. This includes but is not limited to supply-chain, digital markets, trade finance, and many more.

The LEI initiative is driven by the Financial Stability Board (FSB) and the finance ministers and governors of central banks represented in the Group of Twenty (G20). In 2011, the G20 called on the FSB to take the lead in developing recommendations for a global LEI and a supporting governance structure. The related FSB recommendations endorsed by the G20 in 2012 led to the development of the Global LEI System that provides unique identification of legal entities participating in financial transactions across the globe and the subsequent establishment of the GLEIF by the FSB in 2014. The GLEIF is overseen by a committee of global regulators known as the LEI Regulatory Oversight Committee (LEI ROC), including the Reserve Bank of India represented by Nanda S. Dave, Executive Committee, Vice-Chair.

The LEI itself is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization. The developer of ISO 17442, ISO/TC 68, also maintains a liaison with ISO/TC 307.

The LEI connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Moreover, the LEI provides freely accessible look up (identification) of the parties to transactions. GLEIF has explored the impact of rising digital technologies on entity verification and the potential capabilities and benefits afforded by adopting a standardized method using the LEI.

The LEI offers businesses a one-stop approach to identifying legal entities, which has the potential to take the complexity out of business transactions. Via the Global LEI Index, GLEIF makes available the largest online source that provides open, standardized and high quality legal entity reference data. No other global and open entity identification system has committed to a comparable strict regime of regular data verification.

Integrating the LEI into other entity verification methods, including solutions based on digital certificates and blockchain technology, therefore will allow anyone to easily connect all records associated with an organization, and identify who owns whom. By becoming the common link, the LEI will provide certainty of identity in any online interaction, making it easier for everyone to participate in the global digital marketplace.

GLEIF believes that digital certificate technology based on strong cryptography is critical to the smooth operation of the evolving digital economy. The proliferation of digital certificates, whether issued by governments or the private sector, has allowed organizations and individuals do business digitally. However, the current manner in which digital certificates are issued is causing identity challenges in today's digital world. These challenges need to be resolved to ensure they can effectively support the smooth operation of the global digital economy.

The major challenge with digital certificates stems from the current practice of obtaining certificates from a host of different issuers and records are kept in multiple silos by a variety of organizations globally. Digital certificates come with a unique public-private key pair and a fingerprint. When they expire, a new certificate must be obtained with a completely different public/private key pair. Organizations usually hold multiple certificates from different certificate schemes, e.g. eIDAS and CAB/Forum, at the same time and for different use cases.

The reference data, e.g. the name, legal form and address, are embedded as strings. These strings are not harmonized across different certificate issuers. It is not possible to relate one certificate to another or determine the links between different parties without repeating the same manual matching exercise. Digital certificates today are strong in ad hoc authentication but lack the ability to view their owners in an unambiguous way.

Furthermore, certificates carry information that was available at the time of issue. During the period during which a certificate is valid, an owner could change its name, address or legal form, which cannot be reflected by changing the certificate content as this would break the cryptographic checks. As a result, the information held about organizations is not kept up to date in a systematic way, or at all, by the certificate issuers. With no connection between different digital certificates relating to one entity and no way to decide which is out of date and which is current, determining identity in the digital sphere only will become even more complex.

Organizations and individuals need a way to ensure the information they are obtaining through a certificate is correct and up to date. A solution is needed to build certainty and trust in the system and the information it provides.

GLEIF wishes to simplify identification for the digital age by combining the LEI with digital certificates which would result in an easy approach to relate all records associated with an entity, determine which are current and clear up any variances. It will also allow business users easily assess information on who owns whom.

This seemingly minimal addition will significantly reduce the complexity and cost – both people and technology-related – associated with due diligence and validation of customers, partners and suppliers. LEI codes would represent the reference data of a legal entity as well as the issuer entirely. Certificate handling would become faster (less payload) and most current information could be obtained on demand from the Global LEI System (GLEIS) via APIs. The LEI could become an essential building block for the usage of digital certificates in any kind of distributed supply-chain.

Digital certificates are already integral for organizations and individuals interacting and transacting digitally, and their usage is only set to increase with emerging technologies, such as IoT and blockchain. Today, different digital ID systems are based on varying standards, keys and encryption and the only common link between them is the entity name, which can vary widely and change over time. Without a consistent numerical link between IDs, automated methods will always result in errors and further challenges for organizations. The LEI could provide this consistent link and cement its position as a force for good digital identification.

In case any blockchain/DLT application is not going to use digital certificates for authentication of individuals acting on behalf of a business, the LEI should be embedded in the ledger directly, linked to the way any use is identified, e.g. biometrics. This applies also for self-sovereign ledger systems.