Response of the Global Legal Entity Identifier Foundation (GLEIF) to the ICANN North America Engagement Plan – Regional Engagement Plan for Fiscal Years 2021-2015 – Draft Plan for Public Comment

June 30, 2021

The Global Legal Entity Identifier Foundation (GLEIF) is pleased to provide comments to *the ICANN North America Engagement Plan – Regional Engagement Plan for Fiscal Years 2021-2015 – Draft Plan for Public Comment.* GLEIF will focus its comments on the use of the Legal Entity Identifier (LEI).

Potential Usage and Benefits of the LEI with Domain Names

GLEIF proposes that the LEI could be used to identify uniquely the legal entity organizations behind their domain names. Every domain owner could obtain an LEI. Leveraging the LEI and its reference data could make the registration process for domain names easier for ICANN to validate both entity level and relationship information about these entities. Domain look up capabilities also could be enriched by providing access to the reference data about entities through their LEIs as well as support the management of namespaces. These features would enhance security and transparency of the domain registry. Finally, the LEI could be leveraged in its digital form through use of the vLEI for decentralized identification and verification of organizations.

First, some background information on the LEI and GLEIF.

The Legal Entity Identifier (LEI) itself is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). The code connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions including their ownership structure. The LEI and its associated reference data are accessible to all as open, public data.

Established by the Financial Stability Board in June 2014 under the mission of improving financial stability and transparency due to the aftermath of the financial crisis, GLEIF is tasked to support the implementation and use of the LEI. Even though the primary and initial usage and adoption of the LEI was around financial markets and financial instruments, the LEI is use agnostic and therefore has been embraced by different industry sectors and regulators since its introduction by the Regulatory Oversight Committee and the Financial Stability Board in 2012. Further details on the use of the LEI in regulatory initiatives is provided here.

The LEI is the only global standard for legal entity identification. There are innumerable national or regional standards for entity identification across the world. Different identifiers might serve national needs, however, these differences create conflicts and inefficiencies when it comes to the reconciliation of data across borders. Therefore, the LEI responds to the critical need for a universal system of identifying entities across markets, products, and regions.

The Global LEI System is open and non-proprietary. The LEI data provides entity reference data in the local language of the entity and the transliterated version (as applicable). This enables data users to capture the data in the official language used to represent the entity and have a roman character

representation of the name. Use of the LEI ensures a holistic and accurate identification system consisting of data about the entity itself as well as knowing 'who is who' and 'who owns whom', which the LEI facilitates as a globally recognized identifier across 200+ jurisdictions. Also, the GLEIF API is a globally accepted protocol for accessing identity information for legal entities in a digital and machine-readable fashion.

**GLEIF's Digital Strategy for the LEI**

From banking to production to supply chain management, industries worldwide are adjusting to the digitization of processes and transactions.
Yet there is a fundamental principle that hinders this development: trust. How can an organization trust that a supplier located hundreds of kilometers away is who they say they are? How can persons verify that the organization receiving their personal data is indeed who they believe them to be? The process of confirming a stakeholder's legal identity digitally has become a foundational requirement; it enables the determination of 'who's who' within a digital community.

The Global LEI System (GLEIS) has a unique opportunity to solve the problem of trust for legal entities on a global scale. It can enable digital transformation in a way that is interoperable, independent and autonomous. As a regulatory endorsed system overseen by the Regulatory Oversight Committee (ROC), the GLEIS is the only system that establishes a recognized, monitored and standardized global identity for legal entities that, whenever possible, is linked to the national ID system in that jurisdiction. The system is underpinned by open data, meaning any person or company can access the LEI and its associated reference data. The GLEIS also bridges traditional and online processes by serving as a tool to identify the counterparty in any transaction and can aggregate data on legal entities held in repositories.

GLEIF's digital strategy for the LEI centers on two methods for cryptographically binding the LEI to its organization – digital certificates and Verifiable Credentials.
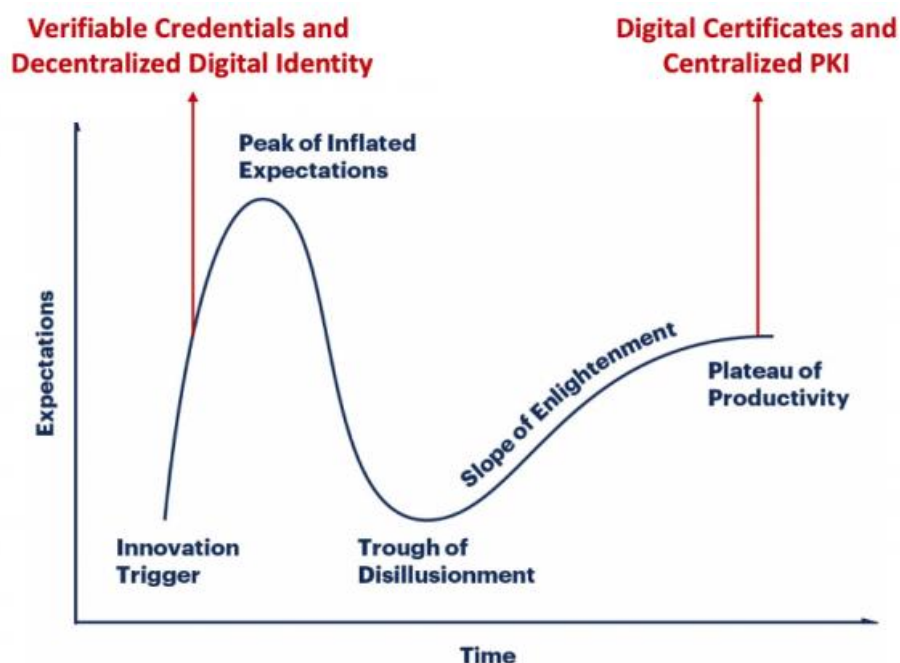
Digital Certificates as well as Self-Sovereign Identity Networks

The LEI has a critical role to play in today's digital world through its ability to provide organizations with unique, permanent identification globally. This especially is important in the context of identifying legal entities involved in digital transactions. The LEI delivers value to both the more mature product - Digital Certificates - and the more recent innovation of Verifiable Credentials.

Digital certificates, even though highly applicable, widely used and covered in many legislations, have not solved digital identity entirely. Certificates are not unique, the information contained within might be outdated, and revocation has always been an issue. Furthermore, there are so many schemes at the same time. A digital certificate issued in one country under a local scheme might not be usable by the owner in another country or context. Digital certificates do not provide the mission that has been envisioned by GLEIF: Each business worldwide should have only one global identity.

The industry has considered these issues and has devised with a new approach to digital identity management. Thanks to advances in distributed ledger/blockchain technology, digital identity management with the additional feature of decentralized identity verification now is possible. Based on a concept known as self-sovereign identity (SSI), this new approach to authentication and verification of digital identity began as a means by which a person, the identity holder, has control of his/her personal data over how, when, and to whom that data is revealed.

This approach is set to transform the nature of identity management and how person-to-entity, or entity-to-entity, interactions take place in the digital world. It can address the need for automation in verification while maintaining data privacy and confidentiality. The LEI will have a key role in this process. GLEIF therefore will focus its comments on the use of the LEI in the more recent innovation of Verifiable Credentials.

Verifiable Credentials (VCs) and the emerging role of the LEI

Verifiable Credentials are defined by the Verifiable Claims Working Group of the W3C standards organization as the format for interoperable, cryptographically-verifiable digital credentials. A second W3C Working Group is creating the Decentralized Identifier (DID) specification for cryptographically-verifiable identifiers that leverage distributed ledger technology. Together, these two W3C Working Groups have developed two important standards:

- https://www.w3.org/TR/vc-data-model/
- https://www.w3.org/TR/did-core/

Use of VCs began in the domain of self-sovereign identity through so-called 'individual wallets,' which contain digital versions of credentials issued to and carried by natural persons. Examples include driver's licenses, passports, store loyalty and membership cards. All of these exist as physical credentials today and will likely have both an analog and a digital version in the near future. Self-sovereign identity is based on the principle that natural persons should have control over the personal information contained in their credentials and can choose to prove their identity and certain facts about themselves in a controlled and safe manner.

GLEIF asserts that the LEI is the ideal foundation on which to establish a chain of trust for organizational identity.
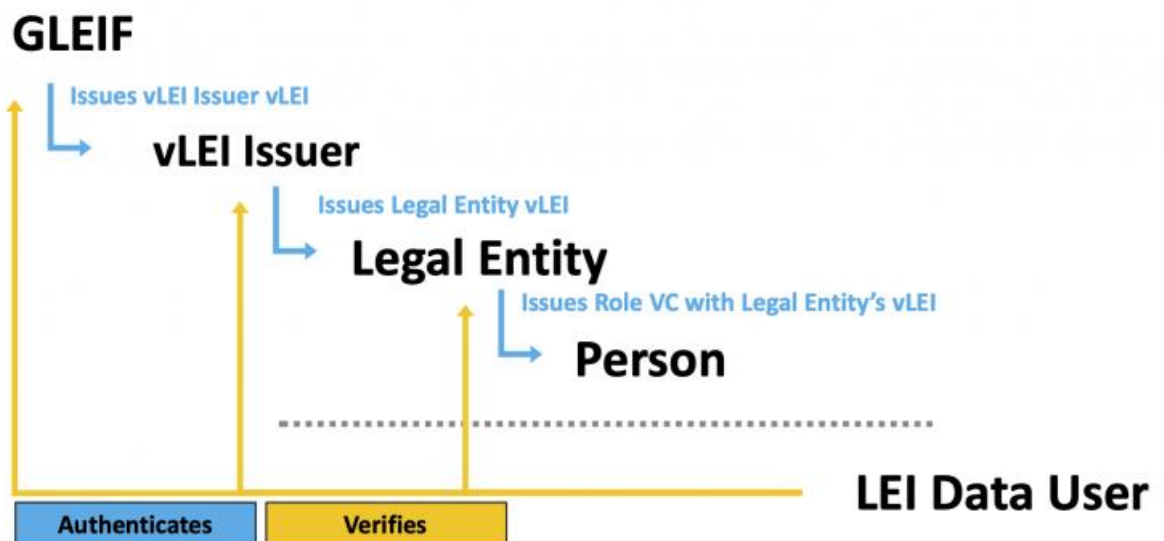
The LEI as a Verifiable Credential – the vLEI Trust Chain

- Every Verifiable Credential is created by an **issuer**
- The issuer **cryptographically** signs the credential with its private key
- An issuer is the organization or entity that asserts information about a **subject** to which a credential is issued
- In our example, the vLEI Issuer is an organization **qualified** by GLEIF
- GLEIF issues vLEIs to vLEI Issuers as attestation of trust
- GLEIF is the Root of Trust

By combining three concepts – the organization's identity, represented by the LEI, a person's identity represented by their legal name, and the role that the person plays for the legal entity, vLEI credentials can be issued and become part of organizational wallets.
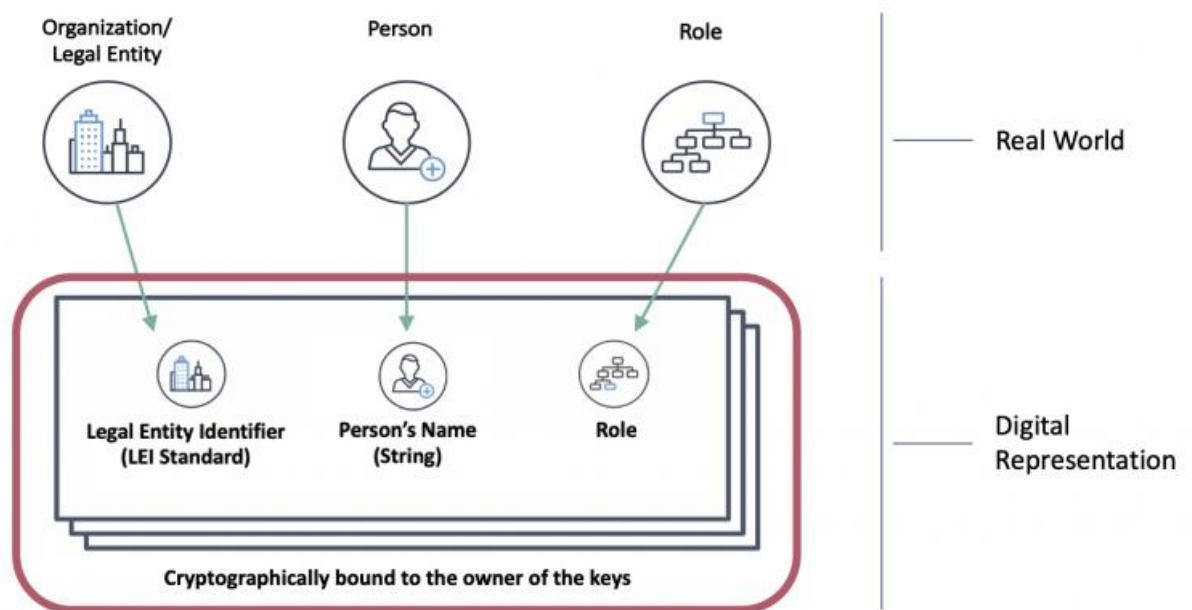
Broader application of the vLEI Role Credential

vLEI Role Credentials issued by Legal Entities to Persons whose Official Organizational Roles (ISO 5009 standard in development) that can be verified both by the Legal Entity as well as against one or more public sources.
Examples:
- Legal Entity – CEO
- Legal Entity – Board Chair

vLEI Role Credentials issued by Legal Entities to Persons in the context of the engagement of those Persons with the Legal Entities which can be verified by the Legal Entity.
Examples:
- Legal Entity – Other Employees
- Hospital/Physician's practice – Patients
- Community/Ecosystem/Exchange/Registered Member
- Trusted Supplier/Provider/Registered Member

In December 2020, GLEIF announced its plans to create a fully digitized LEI service capable of enabling instant and automated identity verification between counterparties operating across all industry sectors, globally.

GLEIF has invited stakeholders from across the digital economy to engage in a cross-industry development program to create an ecosystem and credential governance framework, together with a technical supporting infrastructure, for a verifiable LEI (vLEI), a digitally verifiable credential containing the LEI.

The vLEI will give government organizations, companies and other legal entities worldwide the capacity to use non-repudiable identification data pertaining to their legal status, ownership structure, authorized representatives and employees in a growing number of digital business activities. This includes approving business transactions and contracts, onboarding customers, transaction within import/export and supply chain business networks and submitting regulatory filings and reports. GLEIF already is engaged in research partnerships and technical trials with stakeholders across the pharmaceutical, healthcare, telecom, automotive and financial services sectors.

The vLEI infrastructure will be a network-of-networks of true universality and portability, developed using the KERI (Key Event Receipt Infrastructure) protocol. It will support the full range of blockchain, self-sovereign identity and other decentralized key management platforms. vLEIs will be hostable on both ledgers and cloud infrastructure supporting both the decentralization of ledgers plus the control and performance of cloud. Portability will enable GLEIF's vLEI ecosystem to unify all ledger-based ecosystems that support the vLEI.

Network-of-networks True universality and portability

Agnostic to any network
Development of the capabilities needed for GLEIF to issue and verify vLEIs for vLEI Issuers does not need to operate on blockchain or distributed ledger technology.

GLEIF can implement **KERI** to support fully decentralized portable secure key management operations on self-certifying identifiers.

GLEIF is undertaking development of the capabilities based on KERI during 1Q to 3Q of 2021 and aim for initial live beta implementation with an SSI Network starting in 4Q.

Interoperability
This would allow GLEIF to **connect to any blockchain or distributed ledger technology SSI network** without the need for custom implementation, cost and overhead of operation.

KERI is **Quantum Safe**. It is resistant to attacks by both classical and quantum computers.

GLEIF would be happy to discuss further the potential uses of the LEI and vLEI with ICANN.

Submitted by:

Stephan Wolf, CEO GLEIF

Stephan.Wolf@gleif.org