Digital Identity with LEIs

LEI Digital Strategy – Digital Certificates and Introducing the verifiable LEI (vLEI)

Accredited Standards Committee (ASC) X9 Webinar
February 9, 2021
GLEIF
1. Introduction: GLEIF digital strategy for the LEI
2. Safeguard trust in tomorrow’s digital economy using the LEI
3. Delivering the vLEI with an interoperable and technically agnostic solution
- The LEI is a life-long code owned by the respective legal entity.
- It points to the associated reference data.
Introduction: GLEIF digital strategy for the LEI
LEI Digital Strategy
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.

- LEI delivers value to both the more mature product - Digital Certificates - and the more recent innovation of Verifiable Credentials.
LEI in digital certificates
Digital signatures offer the following main advantages:

- **Authentication**: legally enforceable proof of who actually signed the document

- **Non-repudiation**: assurance that a signer can’t falsely deny having signed

- **Integrity**: proof that a document has not been changed since signing

In addition:

- Embedding **LEI codes** into digital certificates brings true digital and updated identity of legal entities
Example 1: GLEIF Annual Reports

Digital Certificates & LEI

- Combine the strengths of the LEI and digital certificates
- In GLEIF 2018 Annual Report, eIDAS compliant certificates, for the first time, connect the role of the signatory to an organization through the LEI
- Watch how it works: https://youtu.be/w4muYdNlQ-Q
Chinese demonstration of embedded LEIs in certificates
With courtesy of CFCA (China Financial Certification Authority)
Safeguard trust in tomorrow’s digital economy using the LEI
LEIs in a digital world
Making LEIs verifiable

- When presenting an LEI, it is not clear if
  - The LEI is valid
  - the presenter is the LEI owner or an affiliate
  - the presenter has the right to use it

- As a result
  - the recipient of the LEI must still check and verify,
  - background checks are often done manually at a high cost

Verification examples

- The police verifies the driving license by comparing the photo on the ID with the presenter (biometrics are used widely)

- An employer calls the university to see if the job applicant’s diploma is real

- Despite the presented LEI, a bank asks for business register evidence during onboarding of a legal entity customer

Common problem is the lack of trust – and the costs involved for creating trust
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 certified by GLEIF.

GLEIF issues vLEIs to vLEI Issuers as attestation of trust.

GLEIF is the Root of Trust.

The LEI as a Verifiable Credential – the vLEI Trust Chain

GLEIF

vLEI Issuer

Legal Entity

Person

LEI Data User

Verifies

Issues vLEI Issuer vLEI

Issues Legal Entity vLEI

Issues Role VC with Legal Entity’s vLEI
Application of the vLEI Role Credential

- **Organization/Legal Entity**
- **Person**
- **Role**

- **vLEI Organization Wallet**

- **vLEIs**
  - Legal Entity Identifier (LEI Standard)
  - Person’s Name (String)
  - Role
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

**GLEIF vLEI credential schemas:**
- GLEIF credential
- vLEI Issuer credential
- Legal Entity credential
- Official person role credential
- Engagement context person role credential
Delivering the vLEI with an interoperable and technically agnostic solution
The vLEI ecosystem is in full accordance with ToIP standards

- Launched May 2020
- Grew from 27 to 125 member companies in less than six months
- Founding Members include Mastercard, IBM, Accenture, Government of British Columbia, LG, GS1, Mitre, SICPA, R3, Kiva, and 4 universities
- GLEIF joined ToIP as Contributor Member
- Hosted by the non-profit Linux Foundation
  - Home to over 250 of the world’s leading open source/open standard projects including Cloud Native Computing, Hyperledger, Automotive Grade Linux, Hyperledger, and the Decentralized Identity Foundation
vLEI Governance Frameworks

- vLEIs will be issued by vLEI issuers of two types:
  - Existing LEI issuers who elect to issue vLEIs
  - New issuers who will issue vLEIs by calling APIs provided by GLEIF & current LEI issuers

- All vLEI issuers will be qualified under the GLEIF vLEI Ecosystem Governance Framework
  - A ToIP-compliant Layer 4 governance framework

- The vLEI family of verifiable credentials will be defined by the GLEIF vLEI Credential Governance Framework
  - A ToIP-compliant Layer 3 governance framework

- Both frameworks are scheduled to be ready for initial review by Q2 2021
Network-of-networks
True universality and portability

vLEIs are hostable on both ledgers and cloud infrastructure

1. The decentralization of ledgers plus the control and performance of cloud
2. Portability enables GLEIF’s ecosystem to unify all ledger-based ecosystems that support the vLEI
GLEIF’s vLEI approach

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 (Key Event Receipt Infrastructure) 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.

https://keri.one
Limitations

- This presentation contains confidential and proprietary information and/or trade secrets of the Global Legal Entity Identifier Foundation (GLEIF) and/or its affiliates, and is not to be published, reproduced, copied, or disclosed without the express written consent of Global Legal Entity Identifier Foundation.

- Global Legal Entity Identifier Foundation, the Global Legal Entity Identifier Foundation logo are service marks of Global Legal Entity Identifier Foundation.