verifiable LEI (vLEI)
Ecosystem Governance Framework

Preparing for ToIP Public Review

ToIP All Member Meeting
December 8, 2021
GLEIF
1. Introduction to LEIs and vLEIs
2. Examples of opportunities for the vLEI
3. The vLEI Ecosystem Governance Framework
4. GLEIF’s role in the vLEI Ecosystem
5. vLEI workflows
6. vLEI infrastructure technology (KERI and ACDC)
7. vLEI sandbox demo
8. Next steps
Introduction to LEIs and vLEIs
Who is Global Legal Entity Identifier Foundation?

- GLEIF is a not-for-profit Swiss foundation, founded by the Financial Stability Board (FSB).

- GLEIF is overseen by 65 regulators and 19 observers in the Regulatory Oversight Committee (ROC) from more than 50 countries.

- GLEIF Board has 15 independent directors.

Partners for LEI issuing (LOUs)

Issued LEIs to date

39 and growing

> 1,983,000
Introducing the Global LEI System

In 2011, the G-20 leaders supported "the creation of a global legal entity identifier (LEI) which uniquely identifies parties to financial transactions."

**Regulatory Oversight Committee (ROC):**
Represents public financial market authorities from around the world

**Global Legal Entity Identifier Foundation (GLEIF):**
Ensures the operational integrity of the Global LEI system

**Local Operating Units (LOUs):**
Issue LEIs to legal entities
The LEI is a life-long code owned by the respective legal entity.

It points to the associated reference data.

The LEI is an ISO standard ISO 17442
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.
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

Use case for the vLEI:

- Decentralized identification and verification for organizations as well as the persons who represent their organizations either in official or functional roles

Solving the common problem of lack of trust and the costs involved for creating trust
Digital transformation, e.g., Platform Economy, Artificial Intelligence, Distributed and federated Networks etc., is changing the way we interact with each other.

Digital Identity and Strong Authentication become vital for distributed systems spanning many actors.

vLEIs are going to address many business needs in all industries.

Each vLEI requires an underlying LEI!

* Source: https://sdlt.asia/blockchain-platforms/
Embedding the LEI in digital tools
Representing Organizations, Persons and Roles

Organization/ Legal Entity

Person

Role

Legal Entity Identifier (LEI Standard)

Person’s Name (String)

Role

Real World

Digital Representation

Cryptographically bound to the owner of the keys
The LEI as a Verifiable Credential – the vLEI Trust Chain

- GLEIF is the Root of Trust
  - Root AID (Autonomic Identifier) to establish the Root of Trust
  - Delegated AIDs to issue Credentials

- GLEIF will establish a trusted network of Qualified vLEI Issuers (QVIs)

- QVIs are qualified to issue Entity and Role Credentials:
  - to Legal Entities
  - to Persons who represent Legal Entities either in official or functional roles

GLEIF

Qualified vLEI Issuers

Legal Entities

Persons Representing Legal Entities
The vLEI Ecosystem Chain of Trust and vLEI Credentials

- **Qualified vLEI Issuer**:
  - Elements: Qualified vLEI Issuer LEI

- **Legal Entity**:
  - Elements: Legal Entity LEI, Person’s name, Engagement Context Role
  - Issues Official Organizational Role vLEI

- **Entity Credentials**
  - Role Credentials

- **Legal Entity**
  - Issues Legal Entity vLEI

- **GLEIF**
  - Issues Qualified vLEI Issuer vLEI
  - Issues Legal Entity vLEI

- **Elements**:
  - Legal Entity LEI
  - Person’s name
  - Official Organizational Role

© 2021 GLEIF and/or its affiliates. All rights reserved. | Author: GLEIF | verifiable LEI (vLEI) Ecosystem Governance Framework ToIP | GLEIF Public
Broader application of the vLEI Role Credential

vLEI Role Credentials issued by Legal Entities to Persons whose Official Organizational Roles 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

ISO 5009 standard awaiting publication, GLEIF will be managing the code list.

vLEI Role Credential 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 – Employees in Functional Roles
  - Legal Entity – Authorized Suppliers
  - Financial Institutions - Clients
Examples of opportunities for the vLEI
Network-of-networks
True interoperability and portability

- Development of the capabilities needed for issuance, verification and revocation of vLEIs do not need to operate on blockchain or distributed ledger technology.
- This would allow GLEIF to connect to any blockchain or distributed ledger technology SSI network or cloud infrastructure without the need for custom implementation, cost and overhead of operation.
Expanding the use of LEIs using vLEIs

First core use cases for the vLEI

- **Finance**
  - Trade Finance
  - Transaction banking – Payments infrastructure

- **Supply Chain/Digital Trade**
  - Materials/Product tracking
    - Raw materials-manufacturing-distribution-finished goods traceability
    - Materials/manufacturing sustainability traceability
    - Pharmaceuticals e-Leaflet verification

- **Telecom**
  - ‘Approved’ SMS campaigns

- **Client on-boarding, monitoring, compliance**
  - KYC/AML/CFT by financial institutions

---

Realize the vision statement of GLEIF:
A Legal Entity should have one global identity and this should include a digital identity

Expand the use of the LEI to become the broad public good envisioned and endorsed by the G-20
Examples of opportunities

- **Aviation**
  - Pilot’s licenses
  - Customs/Aviation/Cargo
  - COVID testing and vaccine credentials for air travelers

- **Telecom**
  - Smishing (SMS phishing)
  - eBot calls

- **Pharmaceuticals**
  - Supply-chain
  - Clinical trials
  - eConsent clinical trial participants

- **Education credentials**
  - Transcripts, degree certificates

- **Healthcare exchanges**
  - Hospitals, doctors’ practices, insurance companies, patients

- **National initiatives**
  - Digital identities for companies (3 jurisdictions)

- **Regulation**
  - Technology software certification to regulators
The vLEI Ecosystem Governance Framework
GLEIF will provide the governance for the vLEI Ecosystem

- The GLEIF vLEI Ecosystem Governance Framework, under development for the past year, is one of the most comprehensive frameworks developed using the ToIP Governance Metamodel.

- The Framework is designed from the ground up to complement GLEIF’s existing LEI governance—one grows from the other.
### Primary Document

1. Introduction
2. Terminology
3. Localization
4. Governing Authority
5. Administering Authority
6. Purpose
7. Scope
8. Objectives
9. Principles
10. General Requirements
11. Revisions
12. Extensions
13. Schedule of Controlled Documents

### Controlled Documents

1. Glossary
2. Risk Assessment
3. Trust Assurance & Certification
4. Governance Requirements
5. Business Requirements
6. Technical Requirements
   - Part 1: KERI & Key Management
   - Part 2: Identifiers & Credentials
7. Information Trust Requirements
8. Inclusion, Equitability, and Accessibility Requirements
9. Legal Agreements
10. vLEI Identifier and Credential Frameworks
A closer look at documents for the vLEI Issuer Qualification Program and Identifier and Credential Frameworks

<table>
<thead>
<tr>
<th>vLEI Issuer Qualification Program</th>
<th>Identifier and Credential Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. vLEI Issuer Qualification Agreement</td>
<td>1. GLEIF Identifier Governance Framework</td>
</tr>
<tr>
<td>Appendices</td>
<td>vLEI Credential Governance Framework</td>
</tr>
<tr>
<td>1. Non-Disclosure Agreement</td>
<td>1. Qualified vLEI Issuer vLEI</td>
</tr>
<tr>
<td>2. Program Manual</td>
<td>2. Legal Entity vLEI</td>
</tr>
<tr>
<td>3. Program Checklist</td>
<td>3. Legal Entity Official Organization Role vLEI</td>
</tr>
<tr>
<td>4. Contact Details</td>
<td>4. Legal Entity Engagement Context vLEI</td>
</tr>
<tr>
<td>5. vLEI Services Catalog (Service Level Agreement to be added)</td>
<td></td>
</tr>
<tr>
<td>6. Terms of Use Qualified vLEI Issuer TrustMark</td>
<td></td>
</tr>
<tr>
<td>7. Qualified vLEI Issuer Legal Entity Required Contract Terms</td>
<td></td>
</tr>
</tbody>
</table>
The vLEI Ecosystem Governance Framework Highlights

- Covers all 4 layers of ToIP stack
- Establishes GLEIF as vLEI Root of Trust using KERI Autonomic Identifiers (AIDs)
- Includes Credential Governance Frameworks for 4 ACDC vLEI Credentials
- First EGF to include Technical Requirements for
  - Key management, including high security key pre-rotation
  - Integrated multi-sig digital signature protocols for all vLEI Credentials
  - Identity Verification of Legal Entities and Persons representing them includes
    - NIST 800-63A LOA2 Identity Assurance
    - Out-of-band Introduction (OONB) Identity Authentication
    - High security credential chaining using ToIP ACDC specifications
Risk Assessment and Trust Assurance Framework

- Comprehensive Risk Assessment by Ecosystem Roles and Layers
  - GLEIF as the Root of Trust
  - Qualified vLEI Issuers
  - Verifiers
  - Ecosystem Utilities
- Corresponding Trust Assurance Framework
GLEIF’s role in the vLEI Ecosystem
GLEIF also will provide vLEI services focused on a Qualification Program for a trusted network of partners - Qualified vLEI Issuers

- vLEI Issuer Qualification and Annual vLEI Issuer Qualification
  - vLEI Issuers must seek initial Qualification by GLEIF and maintain Qualified vLEI Issuer’s compliance with its expected requirements within its vLEI operations

- Termination of vLEI Issuer Qualification
  - if the Qualified vLEI Issuer does not meet ongoing requirements of Qualification, allows its LEI to lapse or wants to cease vLEI Issuer operations

- Provide Relationship Management for Qualified vLEI Issuers
  - Dedicated Relationship Managers as well as a portal for communications between GLEIF and Qualified vLEI Issuers
vLEI workflows
Business Logic Workflows vLEI Identifiers

- GLEIF Autonomic Identifier (AID) Genesis
  - Creation of GLEIF Root AID
  - Creation of the GLEIF Delegated AIDs
  - Rotation Event to delegate the GLEIF Delegated AIDs
  - Creation of QVI Delegated AIDs
  - Interaction Event to delegate QVI Delegated AIDs
  - Rotation Event to delegate QVI Delegated AIDs
- GLEIF Root AID Publication
- Abandonment
Business Logic Workflows vLEI Credentials and Key Rotation

- Issuance of a Qualified vLEI Issuer vLEI Credential by GLEIF
- Issuance of a Legal Entity vLEI Credential by a Qualified vLEI Issuer (QVI)
- Issuance of a Legal Entity Official Organizational Role (OOR) vLEI Credential by a QVI
- Issuance of a Legal Entity Engagement Context Role (ECR) vLEI Credential by a QVI
- Revocation of a QVI vLEI Credential by GLEIF (voluntary revocation)
- Revocation of a QVI vLEI Credential by GLEIF (involuntary revocation)
- Revocation of a Legal Entity vLEI Credential
- Revocation of the Legal Entity vLEI Credential (involuntary revocation)
- Revocation of a Legal Entity Official Organizational Role (OOR) vLEI Credential
- Revocation of a Legal Entity Official Organizational Role (ECR) vLEI Credential
- Automatic Key Rotation
- Triggered Manual Key Rotation
Creation of GLEIF Root AID in two parts
Creation of GLEIF Root AID Part 2
vLEI infrastructure technology (KERI and ACDC)
What makes KERI different the best choice for developing the vLEI infrastructure?

- Security first, always!
- Portability
- Result
  - Interoperable security and universal adoptability
The Internet Protocol (IP) is broken because it has no trust layer.

Instead ... We use bolt-on identity system security overlays (DNS-CA)
Security – End-to-End Verifiability

*End-to-End Verifiability*

If the edges are secure, then the security of the middle doesn’t matter.

*Ambient Verifiability*: any-data, any-where, any-time by any-body

*Zero-Trust Computing*
Security and Portability - Root-of-Trust

- **Administrative** Root-of-Trust:
  - Insecure, Not-Portable, Fully Centralized

- **Cooperative (shared algorithmic)** Root-of-Trust:
  - Secure, Not-Portable, Shared Governance

- **Cryptographic** Root-of-Trust:
  - Secure, Portable, Fully Decentralized
Cryptographic Root-of-Trust: Self-Certifying Identifier and Key Event Log

EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148
did:un:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=secure#really
• Secure attribution of any communication to its source
• Establish authorship of data, documents, credentials
• = authentic data provenance
• Secure attribution via *non-repudiable* digital signatures
• via (public, private) key pairs (PKI)
• Duplicity evident appraisal of key state
• Key state proofs are verifiable data structures
• Dumb crypto is adoptable crypto (minimally sufficient means)

Share duplicity evident verifiable public key state.
Protect private keys (secrets).
Self-Certifying Identifier (SCID): Issuance and Binding

Cryptographic root-of-trust
Establish authenticity of Internet Protocol packet’s message payload.

The overlay’s security is contingent on the mapping’s security.
Security – Key Rotation addressing flaw of PKI (DNS/CA)

- Use of private keys exposes them to side-channel attack.
  - Over-time, exposure makes private keys weak.
- Therefore, from time to time must revoke and replace the controlling private keys for a given identifier
  - Hence key rotation
  - Existing PKI must re-establish the root-of-trust with each rotation thereby making it vulnerable to attack
  - Re-establishment breaks the chain of trust of control over the identifier
Security - Solution: Key Pre-Rotation
Forward commitment to next one-time use rotation key(s)

<table>
<thead>
<tr>
<th>Inception</th>
<th>SN 0</th>
<th>initial $C^0$</th>
<th>next digest $C^1$</th>
<th>current $C^0$</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rotation</th>
<th>prior event digest 0</th>
<th>SN 1</th>
<th>current $C^1$</th>
<th>next digest $C^2$</th>
<th>current $C^1$</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rotation</th>
<th>prior event digest 1</th>
<th>SN 2</th>
<th>current $C^2$</th>
<th>next digest $C^3$</th>
<th>current $C^2$</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rotation</th>
<th>prior event digest 2</th>
<th>SN 3</th>
<th>current $C^3$</th>
<th>next digest $C^4$</th>
<th>current $C^3$</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Rotation</th>
<th>prior event digest 3</th>
<th>SN 4</th>
<th>current $C^4$</th>
<th>next digest $C^5$</th>
<th>current $C^4$</th>
</tr>
</thead>
</table>

Duplicity evident verifiable data structure

Digest of next key(s) makes pre-rotation post-quantum secure
Security - Multi-Signature

- Each identifier has multiple controllers each with its own private key.
- Convenient mechanisms for managing multiply signed events.
- Enterprise grade fractionally weighted signing thresholds.
Security - Identifier Delegation
Delegated Self-Addressing SCID

Random Seed → Stretch → Private Key
one-way function

Generation → Public Key
one-way function

Delegating Prefix → Delegating Configuration

Inception Configuration

Prefix
Derivation
Inception Digest

Key Event Logs

Inception Statement
Inception Data

Derivation Public Key Configuration
Signature

EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

did:keri:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=sec#yes
Security - Identifier Delegation

Allows scalability and nested protection

Delegator
A
Key Event Stream

A Inception
A Rotation

A Interaction
Δ ↦ X Inception

A Interaction
Δ ↦ Y Inception

A Interaction
Δ ↦ X Rotation

A Interaction
Δ ↦ Y Rotation

A Interaction
Δ ↦ Z Rotation

A Interaction
Δ ↦ X Rotation

A Interaction
Δ ↦ A Rotation

A Rotation

Delegate
X
Key Event Stream

X Δ ↦ A Inception
X Interaction
X Interaction

X Δ ↦ A Rotation
X Interaction
X Interaction

X Δ ↦ A Rotation
X Interaction
X Interaction

X Δ ↦ A Rotation
X Interaction

Delegate
Y
Key Event Stream

Y Δ ↦ A Inception
Y Interaction
Y Interaction

Y Δ ↦ A Inception
Y Interaction
Y Interaction

Y Δ ↦ A Rotation
Y Interaction
Y Interaction

Y Δ ↦ A Rotation
Y Interaction

Delegate
Z
Key Event Stream

Z Δ ↦ A Inception
Z Interaction
Z Interaction

Z Δ ↦ A Rotation
Z Interaction
Z Interaction

Z Δ ↦ A Rotation
Z Interaction
Z Interaction

Z Δ ↦ A Rotation
Z Interaction

Protected by Root Key(s)

Root ID

Protected by Delegate Key(s)

Delegate ID

Delegate Key(s)

Protected by Delegate Key(s)

Delegate ID

Delegate Key(s)

Δ ↦ X : Delegation to X
Δ ↦ A : Delegation from A
vLEI sandbox demo
Next steps
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.