verifiable LEI (vLEI) Ecosystem Governance Framework: Legal Entity vLEI Credential Governance Framework

verifiable LEI (vLEI) Ecosystem Governance Framework

Legal Entity vLEI Credential Governance Framework

2021-12-15, v1.0 draft
Trust over IP Review

Document Name:	Legal Entity vLEI Credential Governance Framework
Document DID:	
Version Number:	V1.0 draft for Trust over IP Review
Version Date:	
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	
Copyright:	

1 Introduction

This is a Controlled Document of the GLEIF verifiable LEI (vLEI) Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). It is the authoritative Governance Framework for the Legal Entity vLEI Credential. It specifies the purpose, principles, policies, and specifications that apply to the use of this Credential in the vLEI Ecosystem. For more information about the vLEI GF, please see the vLEI GF section on the GLEIF website at [INSERT URL HERE].

2 Terminology

All terms in First Letter Capitals are defined in the vLEI Glossary.

3 Purpose

The purpose of the Legal Entity vLEI Credential is to enable the simple, safe, secure identification of a Legal Entity vLEI Credential Holder to any Verifier that accepts a Legal Entity vLEI Credential.

4 Scope

The scope of this Credential Governance Framework is limited to Issuers, Holders, and Verifiers of the vLEI Legal Entity Credential.

5 Principles

The following principles guide the development of policies in this Credential Governance Framework. Note that they apply **in addition to** the Core Policies defined in the vLEI Ecosystem Governance Framework.

5.1 Binding to Holder

The Legal Entity vLEI Credential shall be designed to provide a strong enough binding to the Legal Entity vLEI Credential Holder that a Proof Request for the Legal Entity vLEI Credential can be satisfied only by the Legal Entity vLEI Credential Holder.

5.2 Context Independence

The Legal Entity vLEI Credential shall be designed to fulfill a Proof Request for the legal identity of the Legal Entity vLEI Credential Holder regardless of context, including in-person, online, or over the phone.

6 Issuer Policies

6.1 Qualifications

The Issuer MUST:

1. be a Qualified vLEI Issuer (QVI) in the vLEI Ecosystem with qualification up to date.
2. follow all of the requirements specified in the vLEI Issuer Qualification Agreement.
3. use the GLEIF-supplied vLEI software for hosting Witnesses, Watchers, Discovery, and Oracles, and for Key Management.

6.2 Credential

The Issuer MUST:

1. use the Legal Entity vLEI Credential schema defined in section 8.1.
2. include the Claims marked as Required in section 8.1.

6.3 Legal Entity Identity Verification

1. Identity Assurance
    a. A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.
    b. A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity is Issued and Active in the Global LEI System.
    c. A QAR MUST perform identity assurance of a person serving in the role of an Authorized vLEI Representative (AVR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html)
2. Identity Authentication
    a. The Legal Entity MUST designate a set of one or more Authorized vLEI Representatives (AVRs) to act on its behalf.
    b. A credential wallet MUST be set up for the Legal Entity and for each AVR.
        i. The Legal Entity SHOULD designate at least three AVRs in order to use the greater security of KERI multi-sig protocols.

c. A QAR and the AVRs MUST establish a real-time OOBI session in which the QAR and all AVRs are present. An example is a continuous webmeeting attended by all parties on both audio and video.

d. The following steps MUST be performed in this completed during this OOBI session.

i. The QAR MUST perform manual verification of each AVR's legal identity for which the QAR has already performed identity Assurance. An example is each AVR visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the AVR Person.

ii. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with the AVRs.

iii. An AVR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the QAR.

iv. The QAR MUST send a Challenge Message to the Legal Entity AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the Legal Entity AID.

v. Each AVR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the AVR must acknowledge that this action has been completed.

vi. The QAR MUST verify in real time that a response to the Challenge Message was received from each AVR.

vii. When all responses to the Challenge Messages sufficient to satisfy the multi-sig threshold have been received, the QAR must verify the complete set of signatures.

6.4 Issuance

1. The Legal Entity vLEI Credential MAY be issued either via Unsolicited Issuance or Solicited Issuance.

   a. The Legal Entity Identity Verification process outlined in section 6.3 MUST be completed before Legal Entity vLEI Credential issuance can begin.

   b. In the case of Solicited Issuance, the Legal Entity vLEI Credential SHOULD be issued upon receipt by the QAR of a Fully Signed issuance request from the AVR(s) of the Legal Entity.

   c. In the case of Unsolicited Issuance, the QAR SHOULD send notice to the AVR(s) of the Legal Entity that a Legal Entity vLEI Credential has been solicited on the Legal Entity's behalf. The AVR(s) then send the Fully Signed issuance request to the by the AVR(s) to the QAR.

2. GLEIF MUST implement the vLEI Reporting API to enable QVIs to report each issuance event of Legal Entity vLEI Credentials. (out-of-band to KERI vLEI software)

3. A QAR MUST call the vLEI Reporting API with each issuance event of Legal Entity vLEI Credentials. (out-of-band to KERI vLEI software)

6.5 Revocation

1. Voluntary revocation
    a. A QAR MUST revoke a Legal Entity vLEI Credential upon receipt of a Fully Signed revocation request by the AVR(s) of the Legal Entity, e.g., if the Legal Entity chooses to no longer be the Holder of this Credential using the GLEIF-supplied vLEI software.
    b. A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).
2. Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).
3. A QAR MUST call the vLEI Reporting API with each revocation event of Legal Entity vLEI Credentials. (out-of-band of KERI vLEI software)
4. GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect vLEI credential revocations that have been reported by QVIs.
5. The QAR SHOULD remove the LEI of the Legal Entity from the process to monitor the status of LEIs used within vLEIs.

6.6 Level of Assurance

The Legal Entity vLEI Credential SHOULD be issued with only a single Level of Assurance. Future versions of this credential governance framework MAY define multiple Levels of Assurance.

7 Holder Policies

There are no restrictions on the Holders of vLEI Credentials specified in the vLEI Ecosystem. Restrictions may be introduced in other Ecosystems that use the vLEI Ecosystem.

8 Verifier Policies

There are no restrictions on the Verifiers of vLEI Credentials specified in the vLEI Ecosystem. Restrictions may be introduced in other Ecosystems that use the vLEI Ecosystem.

9 Credential Definition

9.1 Schema

The Legal Entity vLEI Credential MUST contain the LEI of Legal Entity Holder.

The credential elements, schema and the vLEI Credential examples can be found in:

https://github.com/WebOfTrust/keripy/blob/master/docs/Peer2PeerCredentials.md

This document covers both issuance and presentation exchange protocols.

The following text MUST appear in the Rules section of the Automatic Chained Data Container (ACDC) vLEI Credentials.

Usage of a valid vLEI Credential does not assert that the Legal Entity is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws.

Issuance of a valid vLEI Credential only establishes that the information in the requirements in the Identity Assurance and Identity Verification section 6.3 of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.

[Add URL of the vLEI EGF when assigned]