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

Document Name:	Legal Entity Official Organizational Role 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 Official Organizational Role vLEI Credential (OOR 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) Ecosystem Governance Framework, please see the following 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 OOR vLEI Credential is to enable the simple, safe, secure identification of an OOR vLEI Credential Holder to any Verifier that accepts a OOR vLEI Credential.

4 Scope

The scope of this Credential Governance Framework is limited to Issuers, Holders, and Verifiers of OOR vLEI Credentials.

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 OOR vLEI Credential shall be designed to provide a strong binding to the OOR vLEI Credential Holder that a Proof Request for the OOR vLEI Credential can be satisfied by the Legal Entity, the OOR vLEI Credential Holder, and/or against one or more public sources.

5.2 Context Independence

The OOR vLEI Credential shall be designed to fulfill a Proof Request for the legal identity of the OOR 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) that has been contracted by a Legal Entity holding a valid Legal Entity vLEI Credential to issue OOR vLEI Credentials.

6.2 Credential

The Issuer MUST:

1. use the OOR vLEI Credential schema defined in section 8.1. Additional schema elements may be added depending on the requirement of a use case.
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. The QAR MUST confirm that the Legal Entity has obtained the consent of the Official Organizational Role Person (OOR Person) for the OOR Person's name and Official Organization Role to be published by GLEIF as part of the OOR vLEI Credential elements on the LEI page of the Legal Entity.
2. Identity Authentication
    a. Identity Authentication for the Legal Entity is not applicable for the issuance of an OOR vLEI Credential.

6.4 Authorized vLEI Requestor (AVR) Identity Verification

Identity Assurance and Identity Authentication for the AVR are specified in section 6.3 of the Legal Entity vLEI Credential Governance Framework.

6.5 OOR Person Identity Verification

1. Identity Assurance

a. A QAR MUST perform identity assurance of a person serving in an Official Organizational Role (OOR Person) 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. A credential wallet MUST be set up for the OOR Person.
   b. A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources.
   c. If the the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the request for the issuance of the OOR vLEI Credential MUST be made by a subset of (at least two) AVRs of the Legal Entity. An example is the case of an Interim CEO for which the entity registration records of the Legal Entity may not reflect the name of the person assigned to this role.
   d. A QAR and the OOR Person MUST establish a real-time OOBI session in which the QAR and the OOR Person are present. An example is a continuous webmeeting attended by all parties on both audio and video.
   e. The following steps MUST be performed in this order and completed during this OOBI session.
      i. The QAR MUST perform manual verification of the OOR Person's legal identity for which the QVI has already performed Identity Assurance. An example, the OOR Person visually presenting one or more legal identity credentials and the QAR compares the credentials verified during Identity Assurance to the OOR Person.
      ii. A 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. The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share the its AID with the QAR.
      iv. The QAR MUST send a Challenge Message to the OOR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the OOR Person's AID.
      v. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.
      vi. The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.
      vii. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.

3. A workflow MUST be implemented in the operations of the QVI which requires, prior to issuing an OOR vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR and then approved separately by another QAR.

6.6 Issuance

1. The Legal Entity and OOR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before OOR vLEI Credential issuance can begin.
2. The Legal Entity OOR vLEI Credential MAY be issued via Solicited Issuance upon receipt by the QVI of a fully signed issuance request by the AVR(s)of the Legal Entity.
3. GLEIF MUST implement the vLEI Reporting API to enable QVIs to report each issuance event of OOR vLEI Credentials (out-of-band to KERI vLEI software).

4. A QAR MUST call the vLEI Reporting API with each issuance event of OOR vLEI Credentials for which the Legal Entity has communicated that consent has been obtained by the OOR vLEI Credential Holder (out-of-band to KERI vLEI software).

6.7 Revocation

1. Voluntary revocation
    a. The Legal Entity MUST notify the QVI to revoke an OOR vLEI Credential upon receipt of a fully signed revocation request by the AVR(s) of the Legal Entity using the GLEIF-supplied KERI vLEI software.
    b. A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).
2. GLEIF MUST implement a vLEI Reporting API to enable QVIs to report each revocation event of OOR vLEI Credentials.
3. A QAR MUST call the vLEI Reporting API with each revocation event of OOR vLEI Credentials.
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.

6.8 Level of Assurance

The OOR 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.

6.9 Monitoring

GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance or revocation of OOR vLEI Credentials which were not reported using the vLEI Reporting API.

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 OOR vLEI Credential MUST contain the following elements at a minimum - the LEI of the Holder of the Legal Entity vLEI Credential, the Legal Name of the Person in the Official Role at the Legal Entity and the Official Organizational Role itself. The Legal Entity MAY include additional elements in this

credential, some of which may be private information pertinent to the Legal Entity and the Person in the Official Organizational Role.

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 Verification sections, 6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.

[Add URL of the vLEI EGF when assigned]