Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v1.0

Legal Entity Official Organizational Role
vLEI Credential Framework

Public
Document Version 1.0
2022-12-16

Version	1.0
Date of version	2022-12-16
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Legal Entity Official Organizational Role vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2022-12-16_Legal-Entity-Official-Organizational-Role-vLEI-Credential-Governance-Framework_v1.0_final.docx
Governing Authority	Global Legal Entity Identifier Foundation (GLEIF)
Copyright	The verifiable LEI (vLEI) Ecosystem Governance Framework is published on the GLEIF website. All documents published on the GLEIF website are published under the Creative Commons Attribution license.

1 Introduction

This is a Controlled Document of the 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.

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 fulfil 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 9.1.
2. include the Claims marked as Required in section 9.1.

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 has a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Pending Archival in the Global LEI System.

2. Identity Authentication
    a. Identity Authentication for the Legal Entity is not applicable for the issuance of an OOR vLEI Credential.

6.4 Legal Entity Authorized Representative (LAR) Identity Verification

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

6.5 OOR Person Identity Verification

1. Identity Assurance
2. Identity Assurance of a person serving in an Official Organizational Role (OOR Person) MAY be performed either by a QAR, directly or through the use of Third-Party Services, or by a LAR.
3. When the Identity Assurance is performed by a QAR, the Identity Assurance MUST be in the same Supervised Remote In-person session as the Identity Authentication by the QAR.
4. Identity Assurance of an OOR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required as specified 6.d below (essentially including the IAL3 requirement for a Supervised Remote In-person session).
5. If Identity Assurance and Identity Authentication to generate the AID of the OOR Person is performed by the LAR, then Identity Assurance and Identity Authentication can be performed by a separate Supervised Remote In-person session.
6. Identity Authentication by a QAR
    a. A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources.
    b. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person.

c. The QAR MUST call the GLEIF API to look up the OOR code for the OOR Person role provided by the Legal Entity to be used in the OOR vLEI Credential (when the lists of OOR codes and reference data are accessible using the API). In the interim, a text string will be used for the OOR in the OOR vLEI Credential.

d. In all cases, 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 web meeting 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 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. The Challenge Message MUST be unique to the OOBI session.

   ii. 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.

   iii. The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

   iv. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.

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 LAR(s) MUST issue a QVI AUTH OOR vLEI Credential to a QVI to request issuance of a OOR vLEI Credential.
3. A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing an OOR vLEI Credential. The first QAR will perform the required above-mentioned Identity Authentication and out-of-band validations and then signs the credential. Another QAR then approves the issuance and signs the OOR vLEI Credential.
4. A QAR MUST call the vLEI Reporting API for each issuance event of OOR vLEI Credentials.
5. GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect OOR vLEI credential issuances that have been reported by QVIs.

6.7 Revocation

1. To revoke an OOR vLEI Credential:
    a. The Legal Entity MUST notify the QVI to revoke an OOR vLEI Credential.
    b. To revoke a previously issued OOR vLEI Credential, the LAR(s) MUST revoke the QVI AUTH OOR vLEI Credential related to a specific issuance of an OOR vLEI Credential.
    c. The QAR then MUST revoke the OOR vLEI Credential.
    d. A QAR MUST perform the revocation within the timeframe specified in Appendix 5 Service Level Agreement (SLA).
2. A QAR MUST call the vLEI Reporting API for each revocation event of OOR vLEI Credentials.
3. If the QVI has been terminated:
    a. At the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, the QVI MUST revoke all of the OOR vLEI Credentials that the QVI has issued.
    b. Then, the terminated QVI MUST transfer a copy of its revocation log to GLEIF.
4. GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect OOR 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

1. 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

1. The OOR vLEI Credential MUST be an Authentic Chained Data Container (ACDC) that MUST use for its schema at the time of issuance, the JSON Schema found in:

   https://github.com/WebOfTrust/vLEI/blob/dev/schema/acdc/legal-entity-official-organizational-role-vLEI-credential.json

2. **The field values in the credential MUST be as follows:**

   The "LEI" field value MUST be the LEI of Legal Entity Holder.

   The "personLegalName" field value MUST be the Legal Name of the Person in the Official Role at the Legal Entity.

   The "officialRole" field value MUST be the the Official Organizational Role.

   Additional data elements can be specified about the OOR Person through issuance of another ACDC credential containing these additional elements by using the chaining capabilities of ACDC credentials to chain this additional ACDC credential to the Legal Entity Official Organizational Role vLEI Credential.

1. The Sources section of the OOR vLEI Credential MUST contain a source reference to the QVI AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this OOR vLEI Credential. The Sources section of that QVI AUTH vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential that was issued by the QVI to the Legal Entity and contain the same value for the “LEI” field as the Legal Entity vLEI Credential.

The elements in this type of credential can be returned in response to a presentation request as defined in the IPEX protocol (see below).

The ACDC specification is covered in the ACDC protocol specification which can be found in: https://github.com/WebOfTrust/ietf-keri

The issuance and presentation exchange protocols are covered in the Issuance and Presentation Exchange (IPEX) protocol specification, which can be found in: https://github.com/WebOfTrust/IETF-IPEX