Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v2.0

Legal Entity vLEI Credential Framework

Public
Document Version 1.3
2024-04-10

Version	1.3
Date of version	2024-04-10
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Legal Entity vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2024-04-10_vLEI-EGF-v2.0-Legal-Entity-vLEI-Credential-Framework_v1.3_final.pdf
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.

Change History

This section records the history of all changes to this document.

EGF Version	Document Version	Date	Description of Change
1.0	1.1	August 30, 2023	Updated section 6.3 Legal Entity Identification to include Identity Assurance requirements for DARs, requirements for the appointment of LARS and for multi-sig and thresholds for signing of the Legal Entity vLEI Credential by LARs; corrected ‘AVR’ to ‘LAR’ in section 6.3.2.c.i.; added section 6.4 for Addition or Replacement of DARs and LARs.
2.0	1.2	December 15, 2023	Added to section 6.3 examples of acceptable documentation that QARs, or Third-Party Service providers, can use in the Identity Assurance of DARs; added Note that a DAR also can be a LAR in section 6.3.1.f.;

			clarified the presentation of Legal Entity vLEI Credentials by LARs in section 6.3.1.f.; corrected reference to Legal Entity vLEI Credential in section 6.4.4.; added section 6.7, Monitoring, for the issuance of Legal Entity vLEI Credentials; updated GLEIF-IT hosted link for schema in section 9.1.1., Schema; updated references to specification references and links in section 9.1.3., Schema; added usage of credentials paragraph to section 9.1.4., Schema.
2.0	1.3	April 10, 2024	Clarified signing requirements for the Legal Entity vLEI Credential in section 6.3.1.f.iv., Legal Entity Identity Verification; clarified credential wallet set up in section 6.3.3.a., Legal Entity Identity Verification; added requirement not to use video filters and avatars during OOBI sessions in section 6.3.3.c., Legal Entity Identity Verification; corrected omission of step for creation of the Legal Entity Autonomic Identifier (AID) in section 6.3.3.d.iii., Legal Entity Identity Verification.

1 Introduction

This is a Controlled Document of the verifiable LEI (vLEI) Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). It is the authoritative Credential 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.

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 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 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 fulfil 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 vLEI software for hosting Witnesses, Watchers and for Key Management.
4. The Issuer MUST be a Qualified vLEI Issuer (QVI) that has been contracted by a Legal Entity for the issuance of a Legal Entity vLEI Credential.

6.2 Credential

The Issuer MUST:

1. use the Legal Entity 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 of the Legal Entity's Designated Authorized Representative (DAR)
    a. A QVI Authorized Representative (QAR) MUST perform identity assurance of a person serving in the role of a Legal Entity Designated Authorized Representative (DAR) that will designate the Legal Entity Authorized Representatives (LARs) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html).

    b. As an alternative to a., the QVI MAY use Third-Party Services to perform identity assurance on the DAR.
        i. Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance to ensure that the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.

    c. The QAR MUST verify the signing authority of the DAR. Examples of authorization documentation that can be provided are a certified copy of documentation accessed directly by the QAR from a business registry, or a notarized copy of statutes or certificate of incumbency provided by the Legal Entity. Use of documents not certified or notarized or documents found on websites or through links provided solely by the Legal Entity are not acceptable as proof of signing authority.

    d. A QAR MUST verify that the LEI supplied for the Credential by the DAR is the LEI of the Legal Entity for which the issuance request for the Credential has been made.

e. 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.

f. The DAR SHOULD designate at least three (3) LARs if the Legal Entity has 3 or more authorized signers or authorized employees that can be designated for signing credentials in order to use the greater security of KERI multi-sig protocols.

   i. The Legal Entity MAY appoint less than three (3) LARs if less than 3 authorized signers exist or less than 3 employees can be designated for signing credentials on behalf of the Legal Entity. Note: the DAR also MAY be designated as a LAR.

   ii. If 2 or more LARs have been designated, the signing threshold MUST require at least 2 LARs to sign the Legal Entity vLEI Credential.

   iii. Only one LAR signature is required for a Legal Entity with a sole employee or authorized signatory.

   iv. The Legal Entity vLEI Credential MUST be multi-signed by a threshold satisfying number of LARs before the credential can be used or presented..

2. Identity Assurance of the Legal Entity Authorized Representative(s) (LAR(s))

   a. A QAR MUST perform identity assurance of a person serving in the role of a Legal Entity Authorized Representative (LAR) 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 in 3.b.

   b. As an alternative to a., the QVI MAY use Third-Party Services to perform identity assurance on the LARs.

      i. Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance and confirm that the persons that have been identity assured are the LARs that join the real-time OOBI session specified in 3. b.), as well as to ensure that the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.

3. Identity Authentication

   a. A credential wallet MUST be set up for each LAR.

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

   c. Video filters and avatars MUST not be used during the OOBI session.

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

      i. The QAR MUST perform manual verification of each LAR's legal identity for which the QAR has already performed identity Assurance. An example is each LAR visually presenting one or more legal identity credentials and the

QAR compares the credentials verified during Identity Assurance to the LAR 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 LARs.

iii. A LAR MUST create the Legal Entity AID.

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

v. 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. The Challenge Message MUST be unique to the OOBI session.

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

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

viii. 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.

4. Addition or Replacement of DARs and LARs

   a. When new DARs are appointed to replace or add LARs, a QAR MUST perform identity assurance of a person serving in the role of a new DAR as specified in 6.3.1a and 6.3.1.b.

   b. When DARs replace or add LARs after the issuance of the Legal Entity vLEI Credential, the steps within 1. Identity Assurance and Identity Authentication MUST be followed, beginning with 6.3.2.a.

6.4 Issuance

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

2. A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing a Legal Entity vLEI Credential. The first QAR will perform the required above-mentioned Identity Assurance, or confirm if a third-party provider is used), Identity Authentication and out-of-band validations and then will sign the credential. Another QAR then approves the issuance and signs the Legal Entity vLEI Credential.

3. A QAR MUST call the vLEI Reporting API for each issuance event of Legal Entity vLEI Credentials.

4. GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect Legal Entity vLEI credential issuances that have been reported by QVIs.

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 LAR(s) of the Legal Entity, e.g., if the Legal Entity chooses to no longer be the Holder of this Credential.
    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 for each revocation event of Legal Entity 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.
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 Framework MAY define multiple Levels of Assurance.

6.7 Monitoring

1. GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance of Legal Entity 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 Legal Entity 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/GLEIF-IT/vLEI-schema/blob/main/legal-entity-vLEI-credential.json

2. The field values in the credential MUST be as follows:
   a. "LEI" field value MUST be the LEI of Legal Entity Holder.
   b. Additional data elements can be specified about the Legal Entity 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 related Legal Entity vLEI Credential.
3. The Sources section MUST contain a source reference to the Qualified vLEI Issuer vLEI Credential of the QVI that issued this Legal Entity vLEI Credential.
   The elements in this type of credential can be returned in response to a presentation request as defined in the Issuance and Presentation Exchange (IPEX) protocol section in the ACDC specification.
   The ACDC specification can be found in: https://github.com/trustoverip/tswg-acdc-specification
4. Usage of a valid, unexpired, and non-revoked vLEI Credential, as defined in the associated Ecosystem Governance Framework, 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 or that an implied or expressly intended purpose will be fulfilled. It is recommended that upon presentation of Legal Entity vLEI Credentials that the credentials are verified. The Legal Entity is responsible for the use of Legal Entity vLEI credentials that it has authorized and assumes liability for misuse of Legal Entity vLEI Credentials by its representatives.