Enabling global identity
Protecting digital trust

verifiable LEI (vLEI) Ecosystem Governance Framework v4.0

Legal Entity vLEI Credential Framework

Public
Document Version 1.5
2026-03-25

Version	1.5
Date of version	2026-03-25
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Legal Entity vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052blyxZNBn9pqzNrYoS?service=vlei-documents&relativeRef=/egf/docs/2026-03-25_vLEI-EGF-v4.0-Legal-Entity-vLEI-Credential-Framework _v1.5_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.;

EGF Version	Document Version	Date	Description of Change
			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.
3.0	1.4	April 16, 2025	Added option for Identity Assurance to be performed by the presentation of digital identity credentials from specific digital identity schemes in sections 6.3.1.a. and 6.3.2.a., Legal Entity Identity Verification; added requirement not to display on-screen (share) passcodes and passwords during OOBI sessions in section 6.3.3.d., Legal Entity Identity Verification; updated section 6.4, Issuance, to detail the formation of the LAR multi-sig group and signing of the Legal Entity vLEI Credential.

EGF Version	Document Version	Date	Description of Change

4.0	1.5	March 25, 2026	Additions to and renaming of section 6.3, Identity Verification of the Legal Entity and the Legal Entity's Designated Authorized Representative (DAR);
			renaming of section 6.4 to Appointment of the Legal Entity Authorized Representatives (LARs);
			rewrite of section 6.5, Identity Verification of the LARs;
			additions to section 6.7, Revocation;
			updated ACDC specification link in section 9, Schema;
			updates for consistency and clarification.

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 request for verification of 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 request for the legal identity of the Legal Entity vLEI Credential Holder regardless of context, including in-person, online, or using a mobile device.

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 Identity Validation of the Legal Entity's Designated Authorized Representative (DAR)

1. Prior to the signing of the contract between the QVI and the Legal Entity:
   a. A QAR would have verified the signing authority of the DAR.
   b. Identity Assurance of the DAR also would have been performed using the same requirements that are described in section 6.5 below for vLEI Credential issuance.

6.4 Appointment of the Legal Entity Authorized Representatives (LARs)

1. 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.

6.5 Identity Verification of the LARs

1. Identity Verification (Assurance and Authentication) of the LARs
   The Identity Verification (Assurance and Authentication) of the LARs MUST be performed prior to authorization of the issuance and approval of the Legal Entity vLEI Credential. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.

   Identity Assurance is the process by which a person who will receive a vLEI Credential needs to prove that they are the real person they claim to be.

   Once the identity of the person has been assured, a second step, Identity Authentication, follows. Identity Authentication ensures that the person who has been identity assured to receive a vLEI Credential also is in control of the cryptographic identifier which will be used in the credential as well as is in control of the wallet in which their vLEI Credential will be held.

   Requiring both Identity Assurance and Identity Authentication prior to the issuance of a vLEI Credential leverages the most effective and secure means currently available to ensure that the correct person is the holder of the credential and receives their credential securely.

   a. Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which a QAR and the LARs are present.

   b. If a continuous web meeting is used for the OOBI session:

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

      ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session.

   c. Identity Assurance MAY be performed either:

      i. to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html) using OOBI session types compliant with IAL2; or

ii. By presentation of a valid digital identity credential by the LARs from one of the following digital identity schemes:

Europe

Please refer to the following published list schemes in the EU. Only High and/or Substantial Level of Assurance schemes MAY be used for vLEI Identity Assurance.

https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

Asia

Australia my Gov
Bhutan Bhutan NDI
China cyberspace ID
Hong Kong iAM Smart
India Aadhaar
Philippines PhilSys
Singapore SingPass
Thailand Thai National ID

Latin America

Brazil e-CPF

d. Identity Assurance of the LARs by a QVI

i. Identity Assurance MAY be performed either:

a. By a QAR; or

b. As an alternative, the QVI MAY use a third-party service provider to perform Identity Assurance on the LARs.

c. 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 the third party has conducted identity assurance according to the requirements of the vLEI Ecosystem Governance Framework.

2. Identity Authentication of the LARs
    a. A credential wallet MUST be set up for each LAR.
    b. Identity Authentication MUST be performed using a continuous web meeting OOBI session.
        i. One session MAY be established with a QAR and all of the LARs attending or separate sessions with a QAR and each of the LARs, for asynchronous identity authentication of LARs, MAY be held during a timeframe set by the QVI for the complete set of signatures of the LAR multi-sig group to satisfy the required signature threshold.
    c. The following steps MUST be performed in this order and completed during the continuous web meeting OOBI session(s).
        i. The QAR MUST perform manual verification of each LAR's legal identity in the identity credential which was presented during Identity Assurance.
        ii. One of the LARs MUST be designated as the LAR Lead.
        iii. The LAR Lead MUST initiate the set of LARs to create a multi-sig group which will generate the AID to which the Legal Entity vLEI Credential will be issued if the AID has not been created prior to the beginning of Identity Authentication.
        iv. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (AID) with each LAR.
        v. Each LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the QAR.
        vi. 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.
        vii. Each LAR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which each LAR MUST acknowledge that this action has been completed.
        viii. The QAR MUST verify in real time that a response to the Challenge Message was received from each LAR.
        ix. 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.
3. Addition or Replacement of DARs and LARs
    a. When new DARs are appointed to replace or add LARs, Identity Assurance of a person serving in the role of a new DAR MUST be performed.

   b. When DARs replace or add LARs after the issuance of the Legal Entity vLEI Credential, Identity Verification of the new LAR(s) needs to be performed.

6.6 Issuance

1. After the conclusion of the Identity Verification of the LARs, 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 creates and signs the Legal Entity vLEI Credential. The second QAR then approves the issuance and signs the Legal Entity vLEI Credential as an Interaction Event.
3. A QAR MUST send the issued Legal Entity vLEI Credential to the LARs who MUST multi-sign the Admit message to accept the credential by the Legal Entity.
4. The QAR then MUST confirm that the LARs have Fully Signed the Admit message for the Legal Entity vLEI Credential.
5. A QAR MUST call the vLEI Reporting API for each issuance event of Legal Entity vLEI Credentials.
6. 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.

6.7 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 with 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. If the QVI has been terminated:

a. By the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, all Legal Entity vLEI Credentials will have become unverifiable because the chain of authority has been broken.

b. Validators MUST treat as invalid any Legal Entity vLEI Credentials once the Grace Period has expired. The expiration date of the Grace Period is 90 days after the revocation date of the QVI credential.

6.8 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.

6.9 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://trustoverip.github.io/kswg-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.