Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v1.0

Qualified vLEI Issuer Identifier and vLEI Credential Governance Framework

Public
Document Version 1.2
2023-08-30

Version	1.2
Date of version	2023-08-30
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Qualified vLEI Issuer Identifier and vLEI Credential Governance Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2023-08-30_verifiable-LEI-(vLEI)-Ecosystem-Governance-Framework-Qualified-vLEI-Issuer-Identifer-vLEI-Credential-Governance-Framework_v1.2_final.docx
Governing Authority	Global Legal Entity Identifier Foundation (GLEIF)
Copyright	

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	April 3, 2023	Corrected QVI External AID to GLEIF External AID in section 6.5.2.b.
	1.2	August 30, 2023	Updated section 6.3 Legal Entity Identification to include requirements for multi-sig and thresholds for signing of the Legal Entity vLEI Credential; corrected 'AVR' to 'LAR' in section 6.3.2.c.i; added section 6.3.3 for Addition or Replacement of QARs.

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 Qualified vLEI Issuer Delegated AIDs and the vLEI Credential (QVI vLEI Credential). It specifies the purpose, principles, policies, and specifications that apply to the use of the Qualified vLEI Issuer Delegated AIDs and the QVI vLEI 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 QVI vLEI Credential is to:

- enable a QVI to issue, verify and revoke Legal Entity vLEI Credentials, Legal Entity Official Organizational Role vLEI Credentials and Legal Entity Engagement Context Role vLEI Credentials;
- revoke this Credential in the case that a QVI has been terminated for not successfully completing Annual vLEI Issuer Qualification, for not remediating qualification issues documented as a result of Annual vLEI Issuer Qualification, or if the LEI of a QVI lapses or is retired, which would prevent the terminated vLEI Issuer from any further issuance, verification or revocation of vLEIs;
- introduce a grace period within this Credential to allow GLEIF to be able to manage the transition of Legal Entities for which Legal Entity vLEI Credentials, Legal Entity Official Organization Role vLEI Credentials, as well as Legal Entity Engagement Context Role vLEI Credentials, to contract with new QVIs.

4 Scope

The scope of this Identifier and Credential Governance Framework is limited to GLEIF and the Issuer, Holders, and Verifiers of the QVI Delegated AIDs and the QVI vLEI Credential.

5 Principles

The following principles guide the development of policies in this Identifier and 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

1. The QVI vLEI Credential MUST be designed to provide a strong enough binding to the QVI vLEI Credential Holder that a Proof Request for the QVI vLEI Credential can be satisfied only by the QVI vLEI Credential Holder.

5.2 Context Independence

1. The QVI vLEI Credential MUST be designed to fulfil a Proof Request for the operational status of the QVI regardless of context, including in-person, online, or over the phone.

6 Issuer Policies

6.1 Qualifications

1. The Issuer MUST ensure that the Issuer of the QVI vLEI Credentials is GLEIF.

6.2 Credential

The Issuer MUST:

1. Use the QVI vLEI Credential schema defined in section 10.1.
2. Include the Claims marked as Required in section 10.1.

6.3 QVI Identity Verification

1. Identity Assurance
    a. An External GLEIF Authorized Representative (External GAR) MUST perform identity assurance of each person serving in the role of QVI Authorized Representative (QAR) 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. A minimum of two QARs MUST form the QVI multi-sig group.
    c. An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.
    d. The External GAR Lead MAY be a different External GAR than the External GAR Lead for the creation of the GLEIF External Delegated AIDs.
2. Identity Authentication
    a. A credential wallet MUST be set up for the QVI.
    b. The QVI MUST designate a QAR to act on its behalf.
    c. An External GAR and each QAR MUST establish a real-time OOBI session in which the External GAR and the QAR are present. An example is a continuous web meeting attended by all parties on both audio and video.

d. The following steps MUST be performed in this order and completed during this OOBI session.
    i. The External GAR MUST perform manual verification of the QAR's legal identity for which the External GAR has already performed Identity Assurance. An example is the QAR visually presenting one or more legal identity credentials and the External GAR compares the credentials verified during Identity Assurance to the QAR Person.
    ii. The External GAR MUST use an OOBI protocol (such as a QR code or live chat) to share the GLEIF External Delegated AID (GEDA) with the QAR.
    iii. An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.
    iv. The External GAR MUST send a Challenge Message from the GEDA to the QVI AID as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of the QVI AID. The Challenge Message MUST be unique to the OOBI session.
    v. The QAR MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the QAR MUST acknowledge that this action has been completed.
    vi. The External GAR MUST verify in real time that the response to the Challenge Message was received from the QAR.
    vii. When the response to the Challenge Message has been received, the External GAR MUST verify the signature of the QAR.

3. Addition or Replacement of QARs
    a. When QVIs replace or add QARs after the issuance of the Qualified vLEI Issuer vLEI Credential, the steps within 1. Identity Assurance and Identity Authentication MUST be followed, beginning with 6.3.1.

6.4 Creation of QVI Delegated AIDs

1. The creation of the QVI Delegated AIDs follows the successful completion of Identity Verification by the External GAR Lead of each QAR.
2. The following steps MUST be performed in the order listed and completed during an OOBI session for a given QVI Delegated AID.
    a. Each Delegated AID QVI Authorized Representative (QAR) that is a participating member in the group of AIDs MUST generate its own individual single signature AID that will be used to create the QVI Delegated AID.

b. Each QAR MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID with the other QAR s. For each QAR, this provides the participating AID and the service endpoint whereby the other QARs may obtain the KEL of its participating AID.

c. Each QAR MUST send a Challenge Message to every other QAR as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their individual single signature AID. The Challenge Message MUST be unique to the OOBI session.

d. Each QAR must verify in real time that a response to the Challenge Message was received from every other QAR.

e. Each QAR must verify the signature of every other QAR.

f. One of the QARs must be designated as the Delegated AID QVI Authorized Representative (QAR Lead).

g. The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

h. The QAR Lead MUST select the AIDs from the set of QARs for the ordered set of authorized participant members in the multi-sig group and configure and approve the weight threshold and ordered set of participants for both the current and next set and threshold of participants.

i. Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated Witness AIDs, and the GEDA, the QAR Lead MUST generate the QVI Delegated AID Inception Event and publish this to the other QARs and to the Delegated AID Witnesses designated by that Inception Event.

j. Each QAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, and the GEDA in the Delegated AID Inception Event.

k. Each QAR MUST verify the set of Witness endpoints for the QVI Delegated AID.

l. Each QAR MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.

m. Each QAR MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.

n. GLEIF MUST designate one of the External Delegated AID GLEIF Authorized Representative (External GARs) as the External Delegated AID GLEIF Authorized Representative (External GAR Lead).

6.5 Delegation of the QVI Delegated AIDs

1. Unless otherwise pre-approved by the GLEIF Root GARs, GLEIF External AID MUST use an Interaction Event to approve the delegation of the QVI Delegated AIDs.

2. The following steps MUST be performed in the order listed and completed during this OOBI session for the GLEIF External Delegated AID (GEDA).

   The anchor in this Interaction Event is the mechanism by which the delegation is authorized by the Delegator. The Interaction Event with the anchoring digest of the Inception Event of the GEDA when Fully Signed, is a verifiable cryptographic commitment to the delegation.

   (Delegation in KERI is cooperative. It requires a cryptographic commitment from both the Delegator and the Delegate.)

   a. The QAR Lead initiates a set of QARs to create a mulit-sig group and the QARs mutually are authenticated.

   b. The QAR Lead initiates the creation of the Inception Event using the published GLEIF External AID as the Delegator.

   c. The External GAR Lead verifies that the set of QARs in the multi-sig group in this Inception Event to delegate the QVI External AID match those that the External GAR Lead verified according to section 6.3 above.

   d. The External GAR Lead submits request to the External GAR multi-sig group to anchor the Interaction event. All members of the External GAR multi-sig group trust External GAR Lead to anchor because the External GARs already have trusted the External GAR Lead to perform Identity Assurance on the QARs.

   e. The External GAR Lead then submits a request to issue the Qualified vLEI Issuer vLEI Credential to QVI vLEI to the External GAR multi-sig group as an Interaction Event.

6.6 QVI vLEI Credential Issuance

1. The GAR MUST approve issuance of a QVI vLEI Credential after the completion of QVI Identity Verification in section 6.3 above.

6.7 QVI vLEI Credential Revocation

1. Voluntary revocation

   a. An External QAR MUST revoke a QVI vLEI Credential upon receipt of a Fully Signed revocation request by the QAR(s) using the vLEI software.

   b. An External GAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).

2. Involuntary revocation
    a. Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).

6.8 Level of Assurance

a. The QVI 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 Grace Period

The QVI vLEI Credential includes a grace period which would commence on the revocation date of this credential and continue for up to 90 Days if a vLEI Issuer has been terminated for not successfully completing Annual vLEI Issuer Qualification, for not remediating documented qualification issues, agreement or service level breaches, ceases operation or if the LEI of a QVI lapses or is retired.

The QVI vLEI Credential would be revoked, initiating the grace period, which would prevent the terminated vLEI Issuer from any further issuance, verification or revocation of vLEIs, and will allow GLEIF to be able to manage the transition of Legal Entities holding valid Legal Entity vLEI Credentials, as well as Legal Entity Official Organization Role vLEI Credentials and Legal Entity Engagement Context Role vLEI Credentials, to contract with new QVIs.

7 QVI Self-issuance of vLEIs

1. Following the issuance of Qualified vLEI Issuer vLEI Credentials to organizations which GLEIF qualifies as Qualified vLEI Issuers (QVIs), QVIs MAY issue a Legal Entity vLEI Credential and Legal Entity Official Organizational vLEI Role Credentials to themselves as Legal Entities.
2. GLEIF MUST oversee the assignment of these vLEI Credentials issued by QVIs to themselves.
3. GLEIF MAY announce a date after which QVIs qualified by GLEIF MUST contract with third-party QVI organizations for the issuance of their Legal Entity vLEI Credential and Legal Entity Official Organizational vLEI Role Credentials. In the event the GLEIF announces such a date, that date will be published with advance notice so that Verifiers will be able to update their tooling in order to distinguish correctly between compliant QVI self-issued Legal Entity vLEIs and OOR vLEI Role Credentials issued before that date and non-compliant QVI self-issued Legal Entity vLEIs and OOR vLEI Role Credentials issued after that date.

8 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.

9 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. GLEIF vLEI credentials are chained credentials following the ToIP ACDC standard (https://github.com/trustoverip/tswg-acdc-specification).

1. Each vLEI MAY be part of a provenance chain of vLEIs.
2. When part of a chain, each chained vLEI MUST include a reference to one or more preceding vLEIs in its provenance chain.
3. If any preceding vLEIs in the provenance chain or a given vLEI is revoked, then that given vLEI MUST not verify.
4. The schema for each type of vLEI defines what type or types of vLEIs MUST or MAY be referenced in its provenance section.

10 Credential Definition

10.1 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/qualified-vLEI-issuer-vLEI-credential.json

2. The field values in the credential MUST be as follows:
   a. The "LEI" field value MUST be the LEI of the QVI.
   b. The "gracePeriod" field value MUST be at least 90 (ninety) Days.

   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