verifiable LEI (vLEI) Ecosystem Governance Framework: Qualified vLEI Issuer vLEI Credential Governance Framework

Document Name:	Qualified vLEI Issuer vLEI Credential Governance Framework
Document DID:	DID URLs for all documents will be published with the v1.0 Draft of the Ecosystem Governance Framework.
Version Number:	v0.9 Draft for Publication
Version Date:	2022-02-07
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	The Governance Authority DID will be published with the v1.0 Draft of the Ecosystem Governance Framework.
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.

3

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 Qualified vLEI Issuer vLEI Credential (QVI 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 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 Credential Governance Framework is limited to GLEIF as the Issuer, Holders, and Verifiers of the QVI vLEI Credential.

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 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

The QVI vLEI Credential MUST be designed to fulfill 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

The Issuer MUST:

1. Ensure that the Issuer of the QVI vLEI Credentials is GLEIF.
2. Confirm that the QVI successfully has completed the vLEI Issuer Qualification Program.

6.2 Credential

The Issuer MUST:

1. Use the QVI vLEI Credential schema defined in section 8.1.
2. Include the Claims marked as Required in section 8.1.

6.3 QVI Identity Verification

1. Identity Assurance
    a. A GLEIF Authorized Representative (GAR) MUST perform identity assurance of a 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)
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. A GAR and the QAR MUST establish a real-time OOBI session in which the 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 GAR MUST perform manual verification of the QAR's legal identity for which the GAR has already performed Identity Assurance. An example is the QAR visually presenting one or more legal identity credentials and the GAR compares the credentials verified during Identity Assurance to the QAR Person.
    ii. The GAR MUST use an OOBI protocol (such as a QR code or live chat) to share the GLEIF Controller External Autonomic Identifier (AID) 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 GAR.
    iv. The GAR MUST send a Challenge Message from the GLEIF Controller External AID 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 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 GAR must verify the signature of the QAR.

6.4 Issuance

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

6.5 Revocation

1. Voluntary revocation
    a. A QAR MUST revoke a QVI vLEI Credential upon receipt of a Fully Signed revocation request by the QAR(s) using the GLEIF-supplied vLEI software.
    b. A 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).

6.6 Level of Assurance

The QVI vLEI Credential V1 SHOULD be issued with only a single Level of Assurance. Future versions of this credential governance framework MAY define multiple Levels of Assurance.

6.7 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 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. GLEIF vLEI credentials are chained credentials following the ToIP ACDC standard (https://github.com/trustoverip/TSS0033-technology-stack-acdc).

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.

9 Credential Definition

9.1 Schema

The QVI vLEI Credential MUST contain the LEI of the QVI.

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.