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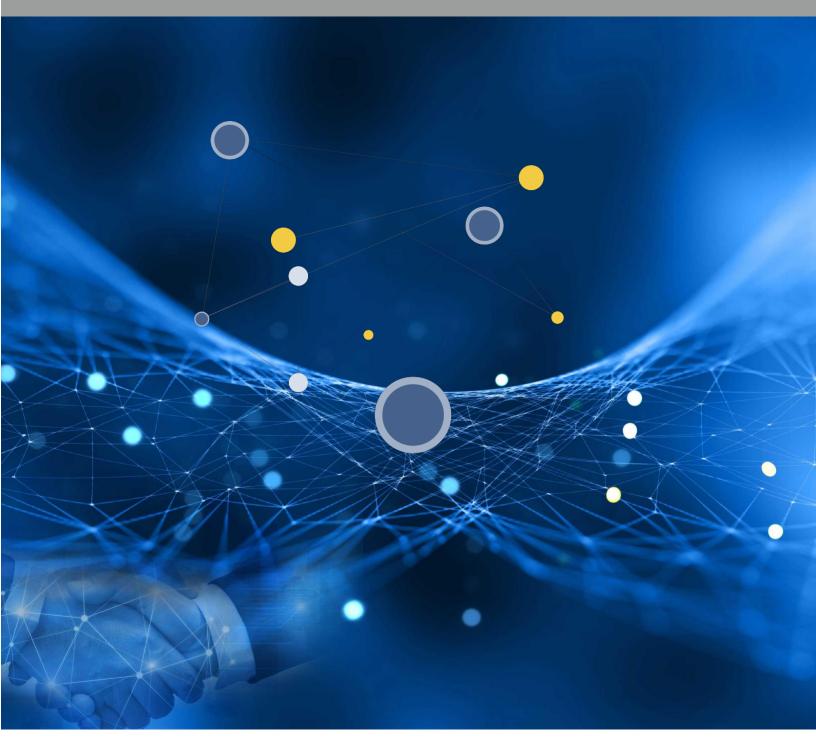
verifiable LEI (vLEI)
Ecosystem Governance
Framework

Qualified vLEI Issuer
vLEI Credential
Goverance Framework

2021-12-15, v1.0 draft
Trust over IP Review

Document Name:	Qualified vLEI Issuer vLEI Credential Governance Framework
Document DID:	
Version Number:	V1.0 draft for Trust over IP Review
Version Date:	
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	
Copyright:	

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. For more information about the vLEI Ecosystem Governance Framework, please see the following section on the GLEIF website at [INSERT URL HERE].

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.

verifiable LEI (vLEI)   Qualified vLEI Issuer   2021-12-15, v1.0 draft
Ecosystem Governance   vLEI Credential   Trust over IP Review
Framework   Goverance Framework

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. Invlude 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 webmeeting attended by all parties on both audio and video.

verifiable LEI (vLEI)   Qualified vLEI Issuer   2021-12-15, v1.0 draft
Ecosystem Governance   vLEI Credential   Trust over IP Review
Framework   Goverance Framework

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

62   d. The following steps MUST be performed in this order and completed during
63   this OOBI session.

64   i.   The GAR MUST perform manual verification of the QAR's legal
65   identity for which the GAR has already performed Identity Assurance.
66   An example is the QAR visually presenting one or more legal identity
67   credentials and the GAR compares the credentials verified during
68   Identity Assurance to the QAR Person.

69   ii.   The GAR MUST use an OOBI protocol (such as a QR code or live chat)
70   to share the GLEIF Controller External Autonomic Identifier (AID) with
71   the QAR.

72   iii.   An QAR MUST use an OOBI protocol (such as a QR code or live chat)
73   to share the QVI AID with the GAR.

74   iv.   The GAR MUST send a Challenge Message from the GLEIF Controller
75   External AID to the QVI AID as defined in the Technical Requirements
76   Part 1 KERI Infrastructure for the purposes of cryptographic
77   authentication of the QVI AID.

78   v.   The QAR MUST use its Private Key Store to sign and return the
79   response to the Challenge Message, after which the QAR must
80   acknowledge that this action has been completed.

81   vi.   The GAR must verify in real time that the response to the Challenge
82   Message was received from the QAR.

83   vii.   When the response to the Challenge Message has been received, the
84   GAR must verify the signature of the QAR.

85   6.4   Issuance

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

88   6.5   Revocation

89   1. Voluntary revocation
90   a. A QAR MUST revoke a QVI vLEI Credential upon receipt of a Fully Signed
91   revocation request by the QAR(s) using the GLEIF-supplied vLEI software.
92   b. A GAR MUST perform the revocation within the timeframe specified in
93   Appendix 5, Service Level Agreement (SLA).
94   2. Involuntary revocation
95   a. Involutary revocation of vLEI Credentials MUST follow the process specified in
96   Appendix 5, Service Level Agreement (SLA).

97   6.6   Level of Assurance

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

101

verifiable LEI (vLEI)   Qualified vLEI Issuer   2021-12-15, v1.0 draft
Ecosystem Governance   vLEI Credential   Trust over IP Review
Framework   Goverance Framework

102 **6.7 Grace Period**

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

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

7 Holder Policies

115 There are no restrictions on the Holders of vLEI Credentials specified in the vLEI Ecosystem.
116 Restrictions may be introduced in other Ecosystems that use the vLEI Ecosystem.

8 Verifier Policies

118 There are no restrictions on the Verifiers of vLEI Credentials specified in the vLEI Ecosystem.
119 Restrictions may be introduced in other Ecosystems that use the vLEI Ecosystem.GLEIF vLEI
120 credentials are chained credentials following the ToIP ACDC standard
121 (https://github.com/trustoverip/TSS0033-technology-stack-acdc).

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

9 Credential Definition

130 **9.1 Schema**

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

132 The credential elements, schema and the vLEI Credential examples can be found in:
133 https://github.com/WebOfTrust/keripy/blob/master/docs/Peer2PeerCredentials.md
134
135 This document covers both issuance and presentation exchange protocols.
136 The URL of the vLEI Ecosystem Governance Framework is:

137 [Add URL of the vLEI EGF when assigned]

verifiable LEI (vLEI)   Qualified vLEI Issuer   2021-12-15, v1.0 draft
Ecosystem Governance   vLEI Credential   Trust over IP Review
Framework   Goverance Framework