verifiable LEI (vLEI)EcosystemGovernance Framework: Legal Entity Engagement Context Role vLEI Credential Governance Framework

Document Name:	Legal Entity Engagement Context Role 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:	

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 Legal Entity Engagement Context Role vLEI Credential (ECR 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 ECR vLEI Credential is to enable the simple, safe, secure identification of an ECR vLEI Credential Holder to any Verifier that accepts an ECR vLEI Credential.

4 Scope

The scope of this Credential Governance Framework is limited to Issuers, Holders, and Verifiers of the ECR 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 ECR vLEI Credential shall be designed to provide a strong enough binding to the ECR vLEI Credential Holder that a Proof Request for the ECR vLEI Credential can be satisfied only by the Legal Entity vLEI Credential or the ECR vLEI Credential Holder.

5.2 Context Independence

The ECR vLEI Credential shall be designed to fulfill a Proof Request for the legal identity of the ECR 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 Legal Entity holding a valid Legal Entity vLEI Credential, or be a Legal Entity holding a valid Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials to one or more QVIs, offered by QVIs as a value-added service.

6.2 Credential

The Issuer MUST:

1. use the ECR vLEI Credential schema elements defined in section 8.1. Additional schema elements may be added depending on the requirement of a use case.
2. include the Claims marked as Required in section 8.1.

6.3 Legal Entity Identity Verification

1. Identity Assurance
    a. A QVI Authorized Representative (QAR) MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the Credential has been made.
    b. A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity is Issued and Active in the Global LEI System.
2. Identity Authentication
    a. Identity Authentication for the Legal Entity is not applicable for the issuance of an ECR vLEI Credential.

6.4 Authorized vLEI Requestor (AVR) Identity Verification

Identity Assurance and Identity Authentication for the AVR are specified section 6.4 of the Legal Entity vLEI Credential Governance Framework.

6.5 ECR Person Identity Verification

1. Identity Assurance
    a. A QAR MUST perform identity assurance of a person serving in an Engagement Context Role (ECR Person) 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 ECR Person.
    b. A QAR and the ECR Person MUST establish a real-time OOBI session in which the QAR and the ECR Person are present. An example is a continuous webmeeting attended by all parties on both audio and video.
    c. The following steps MUST be performed in this order and completed during this OOBI session.

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

6.6 Issuance

The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before OOR vLEI Credential issuance can begin.

6.7 Revocation

1. Voluntary revocation
    a. The Legal Entity MUST notify the Qualified vLEI Issuer to revoke ECR vLEI Credential using a request that must be signed by the private key of the AID of the Legal Entity, e.g., if the Engagement Context Role no longer applies to the Holder of the Credential.
    b. The Qualified vLEI Issuer MUST specify or provide the means by which the Legal Entity must notify the Qualified vLEI Issuer of the revocation.
    c. The Qualified vLEI Issuer MUST perform the revocation within the timeframe specified in the agreement that has delegated the issuance of ECR vLEI Credentials to one or more Qualified vLEI Issuers, offered by Qualified vLEI Issuers as a value-added service.

2. Involuntary revocation
    a. Involutary revocation of vLEI Credentials SHALL follow the same process specified for the revocation of ECR vLEI Credentials in Appendix 5, Qualified vLEI Issuer Service Level Agreement (SLA).

6.8 Level of Assurance

The ECR 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.

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 Reserved Context

1. ECR vLEI Credentials for AVRs
    a. ECR vLEI Credentials MUST be issued to the AVRs of a Legal Entity.
    b. The ECR vLEI Credentials for AVRs MUST be issued by a QVI.

10 Credential Definition

10.1 Schema

The ECR vLEI Credential MUST contain the following elements at a minimum - the LEI of the Holder of the Legal Entity vLEI Credential, the Legal Name of the Person in the Engagement Context Role at the Legal Entity and the Engagement Context Role itself. The Legal Entity MAY include additional elements in this credential, some of which may be private information pertinent to the Legal Entity and the Person in the Engagement Context Role.

The elements in this type of credential can be returned in response to a proof request (partial visibility).

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.

The following text MUST appear in the Rules section of the Automatic Chained Data Container (ACDC) vLEI Credentials.

Usage of a valid vLEI Credential 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.

Issuance of a valid vLEI Credential only establishes that the information in the requirements in the Identity Verification sections, 6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.

[Add URL of the vLEI EGF when assigned]