



Enabling global identity
Protecting digital trust

verifiable LEI (vLEI) Ecosystem Governance Framework v1.0

Legal Entity Engagement Context Role vLEI Credential Framework

Public
Document Version 1.1
2023-08-30



Version	1.1
Date of version	2023-08-30
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Legal Entity Engagement Context Role vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052blyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2023-08-30_verifiable-LEI-(vLEI)-Ecosystem-Governance-Framework-Legal-Entity-Engagement-Context-Role-vLEI-Credential-Framework_v1.1_final.docx
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. 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	<p>Clearly indicated 'or' for requirements in section 6.1 Qualifications;</p> <p>updated the '10.1' and '10.2' to '9.1' and '9.2' in section 6.2 Credential;</p> <p>clarified section headings in sections 6.3, 6.4, 6.5 (Legal Entity, Legal Entity Authorized Representative (LAR) and ECR Person Identity Verification) and 6.6 Issuance to indicate requirements for issuance by a QVI and issuance by a Legal Entity;</p> <p>added the option for Legal Entity Authorized Representatives (LARs) to use of Third-Party Services for Identity Assurance in section 6.5;</p> <p>clarified section headings in section 6.7 Revocation to indicate requirements for revocation by a QVI and revocation by a Legal Entity;</p>



			updated section 9 Credential Definition to clarify the requirement for the 'personLegalName' field value.

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 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.

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 Person.



5.2 Context Independence

The ECR vLEI Credential shall be designed to fulfil a Proof Request for the legal identity of the ECR Person regardless of context, including in-person, online, or over the phone.

6 Issuer Policies

6.1 Qualifications

The Issuer MUST:

1. be a QVI with which a Legal Entity holding a valid Legal Entity vLEI Credential has contracted with for the issuance of ECR vLEI Credentials, offered by QVIs as a value-added service; or
2. be a Legal Entity holding a valid Legal Entity vLEI Credential who will issue ECR vLEI Credentials directly to ECR Persons.

6.2 Credential

The Issuer MUST:

1. use the ECR vLEI Credential schema elements defined in section 9.1.
2. include the Claims marked as Required in section 9.1.

6.3 Legal Entity Identity Verification

6.3.1 For issuance by a QVI:

1. Identity Assurance
 - a. A Qualified vLEI Issuer 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 has a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Pending Archival 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.



6.3.2 For issuance by a Legal Entity:

1. Identity Assurance for the Legal Entity is not applicable for the issuance of an ECR vLEI Credential.
2. Identity Authentication for the Legal Entity is not applicable for the issuance of an ECR vLEI Credential.

6.4 Legal Entity Authorized Representative (LAR) Identity Verification

6.4.1 For issuance by a QVI:

Identity Assurance and Identity Authentication for the LAR are specified section 6.3 of the Legal Entity vLEI Credential Governance Framework.

6.4.2 For issuance by a Legal Entity:

1. The LARs of the Legal Entity MUST act as the Issuer of ECR vLEI Credentials when these credentials are issued directly by a Legal Entity.

6.5 ECR Person Identity Verification

6.5.1 For issuance by a QVI for a Legal Entity with more than one authorized signer or employee

1. Preparing for authorization of an ECR vLEI Credential by a LAR
 - a. A credential wallet MUST be set up for the ECR Person.
 - b. Identity Assurance of a person serving in an Engagement Context Role (ECR Person) MUST be performed prior to authorization of the issuance of an ECR vLEI Credential.
 - c. Identity Assurance of an ECR Person MAY be performed either by a LAR or through the use of Third-Party Services by the Legal Entity.
 - d. Identity Assurance MAY be performed by a Third-Party Services for the Identity Assurance of ECR Persons as long as proper security access controls are put in place between the Legal Entity and the third-party provider and the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.
 - e. Identity Assurance of an ECR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (<https://pages.nist.gov/800-63-3/sp800-63a.html>). Even when IAL2 is used for Identity Assurance, a real-time OOBI session is required (essentially including the IAL3 requirement for a Supervised Remote In-person session).



- f. Upon completion of Identity Assurance, the LAR MUST request the ECR Person to generate its AID.
- g. Then the following steps MUST be performed in this order and completed during this OOB session.
 - i. The LAR 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. The Challenge Message MUST be unique to the OOB session.
 - ii. The ECR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed.
 - iii. The LAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.
 - iv. When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the ECR Person's signature.
- h. The LAR MUST issue a Legal Entity ECR AUTH vLEI Credential to the QVI as required in the Legal Entity QVI AUTH vLEI Credential Framework.

2. Preparing for issuance of an ECR vLEI Credential by a QVI

- a. Identity Authentication by a QAR
 - i. A QAR and the ECR Person MUST establish a real-time OOB session in which the QAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.
 - ii. A QAR MUST perform manual verification of the ECR Person's legal identity for which the LAR, or third-party service provider, already has performed Identity Assurance. An example: the ECR Person visually presents one or more identity credentials verified during Identity Assurance to the QAR.
 - iii. A QAR MUST ask the ECR Person verbally to confirm the AID that was sent in the Legal Entity ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOB session ends.
 - iv. If the AID provided by the ECR Person matches the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOB session continues with Identity Authentication by the QAR.



- b. The following steps **MUST** be performed in this order and completed during this OOB session.
 - i. 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. The Challenge Message **MUST** be unique to the OOB session.
 - ii. 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.
 - iii. The QAR **MUST** verify in real time that the response to the Challenge Message was received from the ECR Person.
 - iv. When the response to the Challenge Message has been received by the QAR, the QAR **MUST** verify the ECR Person's signature.

6.5.2 For issuance by a QVI for a Legal Entity with a sole employee

1. Preparing for authorization of an ECR vLEI Credential by a sole employee (who is at the same time DAR, LAR and ECR Person)
 - a. A credential wallet **MUST** be set up for the ECR Person.
 - b. Since the ECR Person also is the only LAR, the single employee as the LAR **MUST** issue a Legal Entity ECR AUTH vLEI Credential to the QVI.
2. Preparing for issuance of an ECR vLEI Credential by a QVI
 - a. QAR and the ECR Person **MUST** establish a real-time OOB session in which the QAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.
 - b. A QAR **MUST** ask the ECR Person verbally to confirm the AID that was sent in the Legal Entity ECR AUTH vLEI Credential. If the AID provided by the ECR Person does not match the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOB session ends.
 - c. If the AID provided by the ECR Person matches the AID sent in the Legal Entity ECR AUTH vLEI Credential, the OOB session continues.
 - d. Identity Assurance



- v. Identity Assurance of the ECR Person who is the sole employee MUST be performed prior to the issuance of an ECR vLEI Credential.
- vi. Identity Assurance of an ECR Person that is a sole employee MUST be performed either by a QAR or through the use of Third-Party Services by the QVI since an ECR Person that is a sole employee is unable to identity assurance itself.
- vii. Identity Assurance MAY be performed by a Third-Party Services for the Identity Assurance of ECR Persons as long as proper security access controls are put in place between the QVI and the third-party provider and the third-party provider follows the requirements of the vLEI Ecosystem Governance Framework.
- viii. Identity Assurance of an ECR person MUST be performed to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (<https://pages.nist.gov/800-63-3/sp800-63a.html>). Even when IAL2 is used for Identity Assurance, a real-time OOB session is required (essentially including the IAL3 requirement for a Supervised Remote In-person session).

e. Identity Authentication

- ix. The following steps MUST be performed in this order and completed during this OOB session.
- x. 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. The Challenge Message MUST be unique to the OOB session.
- xi. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed.
- xii. The QAR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.
- xiii. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the ECR Person's signature.



6.5.3 For issuance by a Legal Entity with more than one authorized signer or employee

The following applies except when the ECR Person is a sole employee, most likely a sole proprietor, who simply would issue an ECR vLEI Credential to their own wallet.

1. Identity Assurance

- a. A LAR, or a Third-Party Services engaged by the Legal Entity ,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>). Even when IAL2 is used for Identity Assurance, a real-time OOB session is required as specified 2.b below (essentially including the IAL3 requirement for a Supervised Remote In-person session).

2. Identity Authentication

- a. A credential wallet MUST be set up for the ECR Person.
- b. A LAR and the ECR Person MUST meet in person or establish a real-time OOB session in which the LAR and the ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.
- c. The following steps MUST be performed in this order and completed during this OOB session.
 - i. The LAR MUST perform manual verification of the ECR Person's legal identity for which the LAR has already performed Identity Assurance. An example: the ECR Person visually presents one or more legal identity credentials and the LAR compares to the credentials verified during Identity Assurance.
 - ii. The LAR MUST use an OOB protocol (such as a QR code or live chat) to share the Legal Entity AID with the ECR Person.
 - iii. The ECR Person MUST use an OOB protocol (such as a QR code or live chat) to share its AID with the LAR.
 - iv. The LAR 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. The Challenge Message MUST be unique to the OOB session.
 - 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 LAR 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 LAR, the LAR MUST verify the ECR Person's signature.

6.6 Issuance

6.6.1 For issuance by a QVI:

1. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before ECR 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 an ECR vLEI Credential. The first QAR will perform the required above-mentioned Identity Authentication and out-of-band validations and then signs the credential. Another QAR then approves the issuance and signs the ECR vLEI Credential.

6.6.2 For issuance by a Legal Entity:

1. The ECR Person Identity Verification process outlined in section 6.5 MUST be completed before ECR vLEI Credential issuance can begin.
2. A workflow MUST be put in place by the Legal Entity for ECR vLEI Role Credentials to meet the requirement for two LARs to sign the ECR vLEI Role Credentials at issuance.

6.7 Revocation

6.7.1 For revocation by a QVI:

1. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential.
2. To revoke a previously issued ECR vLEI Credential, the LAR(s) MUST revoke the QVI AUTH ECR vLEI Credential related to a specific issuance of an ECR vLEI Credential.
3. The QAR then MUST revoke the ECR vLEI Credential.
4. The QAR MUST perform the revocation within the timeframe specified in the agreement that has delegated the issuance of ECR vLEI Credentials to one or more QVIs, offered by QVIs as a value-added service.
5. At the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, the QVI MUST revoke all of the ECR vLEI Credentials that the QVI has issued.
6. Then the terminated QVI MUST transfer a copy of its revocation log to GLEIF.



6.7.2 For revocation by a Legal Entity:

The Legal Entity SHOULD put in place its own processes specifying how LARs are to be notified when ECR vLEI Credentials should be revoked and the timeframe in which the ECR vLEI Credentials are to be revoked.

6.8 Level of Assurance

The ECR 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.

7 Holder Policies

7.1 Restrictions

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.

7.2 Privacy Considerations

It is the sole responsibility of Holders as Issuers of an ECR vLEI Credential to present that Credential in a privacy-preserving manner using the mechanisms provided in the Issuance and Presentation Exchange (IPEX) protocol specification and the Authentic Chained Data Container (ACDC) specification. <https://github.com/WebOfTrust/IETF-IPEX> and <https://github.com/trustoverip/tswg-acdc-specification>

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 ECR 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/legal-entity-engagement-context-role-vLEI-credential.json>



2. The field values in the credential must be as follows:

- a. The "LEI" field value MUST be the LEI of Legal Entity Holder.
- b. The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.
- c. The "engagementContextRole" field value MUST be the the Engagement Context Role.

Additional data elements can be specified about the ECR Person 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 Legal Entity Engagement Context vLEI Credential.

3. For an Issuer that is a QVI, the Sources section of the ECR vLEI Credential MUST contain a source reference to the QVI AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this ECR vLEI Credential. The Sources section of that QVI AUTH vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential that was issued by the QVI to the Legal Entity and contain the same value for the "LEI" field as the Legal Entity vLEI Credential.
4. For an Issuer that is a Legal Entity, the Sources section of the ECR vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential (via SAID) held by the Legal Entity that is issuing this ECR vLEI Credential. The value of the "LEI" field of the Legal Entity vLEI Credential MUST match the value of the "LEI" field in this ECR vLEI Credential.

The elements in this type of credential can be returned in response to a presentation request in a manner that provides for graduated disclosure and contractually protected disclosure 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>

