Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v4.0

Legal Entity Official Organizational Role
vLEI Credential Framework

Public
Document Version 1.5
2026-03-25

Version	1.5
Date of version	2026-03-25
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Legal Entity Official Organizational Role vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pqzNrYoS?service=vlei-documents&relativeRef=/egf/docs/2026-03-25_vLEI-EGF-v4.0-Legal-Entity-Official-Organizational-Role-vLEI-CredentialFramework_v1.5_Final.pdf
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 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	Restructured section 6.5 OOR Person Identity Verification to indicate clearly requirements for Legal Entity Authorized Representatives (LARs) and for Qualified vLEI Issuers (QVIs) and to account for Legal Entities with a sole employee; moved requirement for LARs to issue the Legal Entity OOR Authorization vLEI Credential from section 6.6.2 to section 6.5.1.i.; updated section 9 Credential Definition to clarify the requirement for the 'personLegalName' field value.
2.0	1.2	December 15, 2023	Added the usage rules that the LAR must follow for specifying OOR roles in QVI OOR

EGF Version	Document Version	Date	Description of Change
			AUTH vLEI Credentials in section 6.5.1.j. and 6.5.2.c. OOR Person Identity Verification; updated sections 6.5.1.2. and 6.1.2.2., OOR Person Identity Verification, with examples of acceptable documentation that can be used by QARs to validate the name and Official Organizational Role of an OOR Person; deleted repeated 'on the' in section 6.5.5.1.f. OOR Person Identity Verification; added the usage rules that a QAR must follow for Official Organizational Role Codes and Reference Data included in OOR vLEI Credentials in section 6.6, Issuance; updated GLEIF-IT hosted link to schema in section 9.1.1, Schema; updated inclusion of Issuance and Presentation (IPEX) protocol within the Authentic Chained Data Container (ACDC) specification in section 9.1.3., Schema; added credential usage paragraph in section 9.1.5., Schema.
2.0	1.3	April 10, 2024	Added requirement not to use video filters and avatars during OOBI sessions in sections 6.5.1.1.i., 6.5.1.2.b.ii., and 6.5.2.2.b.ii., OOR Person Identity Verification; corrected omission of the step of the sharing of the Legal Entity Autonomic Identifier (AID) in section 6.5.1.1.i.i., OOR Person Identity Verification; corrected omission of the step of the sharing of the QVI Autonomic Identifier (AID) in sections 6.5.1.2.c.i. and 6.5.2.2.c.i.,OOR Person Identity Verification.

EGF Version	Document Version	Date	Description of Change
3.0	1.4	April 16, 2025	Added option for Identity Assurance to be performed by the presentation of digital identity credentials from specific digital identity schemes in section 6.3.1.c., OOR Person Identity Verification; added requirement not to display on-screen (share) passcodes and passwords during OOBI sessions in sections 6.5.1.1.ii., 6.5.1.2.b.iii., and 6.5.2.2.b.iii., OOR Person Identity Verification; clarified requirements for revocation of OOR vLEI Credentials by the Legal Entity in section 6.7, Revocation, including deletion of the OOR vLEI details on the LEI page of the Legal Entity instead of indicating the Revoked status of an OOR vLEI on the LEI page.
4.0	1.5	March 25, 2026	Deletion of section 6.3, Legal Entity Identity Verification and section 6.4, Legal Entity Authorized Representative (LAR) Identity Verification; rewrite of now section 6.3, Official Organizational Role Person (OOR Person) Identity Verification; updated usage rules for QVIs for OOR long names, OOR codes, OOR abbreviations and Latin Transliteration of OOR long names and updated section 6.41, Issuance; updated now section 6.5, Revocation; updated ACDC specification link in section 9.1, Schema; updates for consistency and clarification.

1 Introduction

This is a Controlled Document of the verifiable LEI (vLEI) Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). It is the authoritative Credential Framework for the Legal Entity Official Organizational Role vLEI Credential (OOR 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 OOR vLEI Credential is to enable the simple, safe, secure identification of an OOR vLEI Credential Holder to any Verifier that accepts a OOR vLEI Credential.

4 Scope

The scope of this Credential Framework is limited to Issuers, Holders, and Verifiers of OOR vLEI Credentials.

5 Principles

The following principles guide the development of policies in this Credential Framework. Note that they apply in addition to the Core Policies defined in the vLEI Ecosystem Governance Framework.

5.1 Binding to Holder

The OOR vLEI Credential shall be designed to provide a strong binding to the OOR vLEI Credential Holder that a request for verification of the OOR vLEI Credential can be satisfied by the Legal Entity, the OOR vLEI Credential Holder, and/or against one or more public sources.

5.2 Context Independence

The OOR vLEI Credential shall be designed to fulfil a request for the legal identity of the OOR vLEI Credential Holder regardless of context, including in-person, online, or using a mobile device.

6 Issuer Policies

6.1 Qualifications

The Issuer MUST:

1. be a Qualified vLEI Issuer (QVI) that has been contracted by a Legal Entity holding a valid Legal Entity vLEI Credential to issue OOR vLEI Credentials.

6.2 Credential

The Issuer MUST:

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

6.3 Official Organizational Role Person (OOR Person) Identity Verification

1. Identity Verification (Assurance and Authentication) of a person serving in an Official Organizational Role (OOR Person) MUST be performed prior to authorization of the issuance by a LAR and prior to the approval by a QAR of the issuance of an OOR vLEI Credential. Identity Verification is a necessary process to ensure that digital identities have been verified in a secure manner to prevent impersonation, identity fraud, and ultimately, unauthorized access or use of a vLEI credential.

   Identity Assurance is the process by which a person who will receive a vLEI Credential needs to prove that they are the real person they claim to be.

   Once the identity of the person has been assured, a second step, Identity Authentication, follows. Identity Authentication ensures that the person who has been identity assured to receive a vLEI Credential also is in control of the cryptographic identifier which will be used in the credential as well as is in control of the wallet in which their vLEI Credential will be held.

   Requiring both Identity Assurance and Identity Authentication prior to the issuance

of a vLEI Credential leverages the most effective and secure means currently available to ensure that the correct person is the holder of the credential and receives their credential securely.

a. Identity Assurance and Identity Authentication MUST be performed using a real-time Out-of-Band-Introduction (OOBI) session. An example is a continuous web meeting attended by all parties on both audio and video in which the LAR and the OOR Person or the QAR and the OOR Person are present.

b. If a continuous web meeting is used for the OOBI session:

    i. Video filters and avatars MUST not be used during the OOBI session.

    ii. Passcodes and passwords MUST not be displayed on screen (shared) during the OOBI session.

c. Identity Assurance MAY be performed either:

    i. to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A (https://pages.nist.gov/800-63-3/sp800-63a.html) using OOBI session types compliant with IAL2; or

    ii. By presentation of a valid digital identity credential by the OOR Person from one of the following digital identity schemes:

        Europe

        Please refer to the following published list schemes in the EU. Only High and/or Substantial Level of Assurance schemes MAY be used for vLEI Identity Assurance.

        https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

        Asia

        Australia my Gov
        Bhutan Bhutan NDI
        China cyberspace ID
        Hong Kong iAM Smart
        India Aadhaar
        Philippines PhilSys
        Singapore SingPass
        Thailand Thai National ID

Latin America

Brazil e-CPF

d. Identity Assurance of an OOR Person

i. Identity Assurance MAY be performed either:

a. By a LAR or a QAR; or

b. As an alternative, a Legal Entity or a QVI MAY use a third-party service provider to perform Identity Assurance of OOR Persons.

c. Proper security access controls MUST be put in place between the QVI and the third-party provider so that the QAR can view the results of identity assurance and confirm that the persons that the third party has conducted identity assurance according to the requirements of the vLEI Ecosystem Governance Framework.

6.3.1 For a Legal Entity with more than one authorized signer or employee

1. Identity Assurance of an OOR Person by a LAR

a. Preparing for authorization of an OOR vLEI Credential by a LAR

i. A credential wallet MUST be set up for the OOR Person.

b. This Credential Framework outlines a comprehensive process of Identity Assurance to support in small or large organizations alike a process in which LARs can verify the identities of colleagues and other representatives of their organizations which they have not met or know personally.

i. Identity Verification (Assurance and Authentication) of an OOR Person MUST be performed prior to authorization of the issuance of an OOR vLEI Credential if the identity of a colleague and other representative of their organizations is not well known in their role in the organization to at least one of the LARs.

ii. For a colleague or other representative of their organizations who are well known in their role in the organization to at least one of the LARs, the LARs MAY choose to restrict Identity Assurance to validating the legal name of the OOR Person on the identity credential which the OOR Person will use in Identity Assurance conducted by the QVI in order to complete the requirements of the vLEI Authorization Credential.

c. If Identity Assurance is performed, Identity Assurance MUST be completed prior to Identity Authentication.

d. Identity Authentication always MUST be performed.

e. The LAR MUST obtain the consent of the OOR Person for their name and OOR to be published on the LEI page of the Legal Entity on gleif.org. This confirmation will be indicated in the OOR Authorization vLEI Credential (OOR AUTH vLEI Credential).

f. The LAR MUST request the OOR Person to generate its AID.

2. Identity Authentication of an OOR Person by a LAR

Then the following steps MUST be performed in this order and completed during a continuous web meeting OOBI session.

a. The LAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.

b. The LAR MUST use an OOBI protocol (such as a QR code or live chat) to share the Legal Entity AID with the OOR Person.

c. The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the LAR.

d. The LAR MUST send a Challenge Message to the OOR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the OOR Person's AID. The Challenge Message MUST be unique to the OOBI session.

e. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.

f. The LAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

g. When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the OOR Person's signature.

3. Preparation of the OOR AUTH vLEI Credential by the LARs

a. The LAR MUST create a OOR AUTH vLEI Credential to be issued to the QVI as required in the Authorization vLEI Credential Framework.

b. The LAR MUST follow the usage rules below for specifying OOR long names in OOR AUTH vLEI Credentials.

c. The OOR long name MUST be specified in the OOR AUTH vLEI Credential.

d. If the OOR long name is included in the ISO 5009 Official Organization Role lists, then the long name of the role and its corresponding OOR code MUST be included in the OOR AUTH vLEI Credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.

e. If the OOR long name is specified in public documents, but not in the ISO 5009 Official Organization Role lists, used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the OOR AUTH vLEI Credential.

f. If the OOR long name is specified in other documents provided by the Legal Entity, but not in the ISO 5009 Official Organization Role lists, and used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the OOR AUTH vLEI Credential.

g. The OOR AUTH vLEI Credential MUST be signed by a threshold satisfying number of LARs using the Legal Entity vLEI Credential.

4. Preparing for issuance of an OOR vLEI Credential by a QVI

a. Based on the information contained in the OOR AUTH vLEI Credential received by the QVI:

i. A QAR MUST validate 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 using the GLEIF API.

ii. A QAR MUST validate 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 using the GLEIF API.

iii. A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources. An example of documentation that can be used to validate the name and Official Organizational Role of an OOR Person are a certified copy of documentation accessed directly by the QAR from a business registry.

iv. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the QAR MUST

request from the LAR(s) copies of documents of the Legal Entity. Examples of documentation that can be provided by the Legal Entity to validate the name and Official Organizational Role of an OOR Person are a notarized copy of statutes or articles, Board minutes or a certificate of incumbency provided by the Legal Entity. Use of documents not certified or notarized or documents found on websites or through links provided solely by the Legal Entity are not acceptable for this validation.

v. If the name and the Official Organizational Role of the OOR Person cannot be validated using official public sources or copies of documents of the Legal Entity, then the QAR MUST notify the LAR that an OOR vLEI Credential cannot be issued and the LAR MAY authorize instead the issuance of an ECR vLEI Credential.

b. Identity Verification of an OOR Person by a QVI

i. Identity Verification (Assurance and Authentication) of an OOR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an OOR vLEI Credential.

ii. Identity Assurance MUST be completed prior to Identity Authentication.

iii. Identity Authentication of an OOR Person by a QAR

Then the following steps MUST be performed in this order and completed during a continuous web meeting OOBI session.

a. A QAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.

b. A QAR MUST ask the OOR Person verbally to confirm the AID that was sent in the OOR AUTH vLEI Credential. If the AID provided by the OOR Person does not match the AID sent in the OOR AUTH vLEI Credential, the OOBI session ends.

c. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the OOR Person.

d. The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the QAR.

e. The QAR MUST send a Challenge Message to the OOR Person's AID as defined in the Technical Requirements Part 1 for the purposes of

cryptographic authentication of the OOR Person's AID. The Challenge Message MUST be unique to the OOBI session.

f. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.

g. The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

h. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.

i. A Challenge Message MAY be sent from the OOR Person to the QAR, signed and returned by the QAR to the OOR Person and the QAR's signature verified by the OOR Person.

6.3.2 For a Legal Entity with a sole authorized signer or employee

1. Preparing for authorization of an OOR vLEI Credential by a sole authorized signer or employee (who is at the same time DAR, LAR and OOR Person)

   a. A credential wallet MUST be set up for the OOR Person.

   b. The LAR as OOR Person MUST generate its AID for an Official Organizational Role vLEI Credential to include in the OOR AUTH vLEI Credential.

   c. Since the OOR Person also is the only LAR, as the sole authorized signer, the LAR MUST issue a OOR AUTH vLEI Credential to the QVI.

      i. The LAR MUST follow the usage rules below for specifying OOR long names in QVI OOR AUTH vLEI Credentials.

         1. The OOR long name MUST be specified in the OOR AUTH vLEI Credential.

         2. If the OOR long name is included in the ISO 5009 Official Organization Role lists, then the long name of the role and its corresponding OOR code MUST be included in the OOR AUTH vLEI Credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.

         3. If the OOR long name is specified in public documents, but not in the ISO 5009 Official Organization Role lists, used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the OOR AUTH vLEI credential.

4. If the OOR long name is specified in other documents provided by the Legal Entity, but not in the ISO 5009 Official Organization Role lists, and used by the QVI to validate the person in the role, then the role as specified in these documents MUST be included in the OOR AUTH vLEI credential.

d. The OOR Person as LAR MUST indicate consent that their name and OOR to be published on the LEI page of the Legal Entity on gleif.org when preparing the OOR AUTH vLEI Credential.

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

a. Based on the information contained in the OOR AUTH vLEI Credential received by the QVI:

i. A QAR MUST validate 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 using the GLEIF API.

ii. A QAR MUST validate 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 using the GLEIF API.

iii. A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources. An example of documentation that can be used to validate the name and Official Organizational Role of an OOR Person are a certified copy of documentation accessed directly by the QAR from a business registry.

iv. If the long name that the QAR has validated using public sources does not match the OOR long name in the OOR AUTH vLEI Credential, then the QAR MUST notify the LAR.

v. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the QAR MUST request from the LAR(s) copies of documents of the Legal Entity. Examples of documentation that can be provided by the Legal Entity to validate the name and Official Organizational Role of an OOR Person are a notarized copy of statutes or articles, Board minutes or a certificate of incumbency provided by the Legal Entity. Use of documents not certified or notarized or documents found on websites or through links provided solely by the Legal Entity are not acceptable for this validation.

vi. If the name and the Official Organizational Role of the OOR Person cannot be validated using official public sources or copies of documents of the Legal Entity, then the QAR MUST notify the OOR Person as LAR that an OOR vLEI Credential cannot be issued and the OOR Person as LAR MAY authorize instead the issuance of an ECR vLEI Credential.

b. Identity Verification of an OOR Person by a QAR

i. Identity Verification (Assurance and Authentication) of a person serving in an OOR Person by its QVI MUST be performed prior to approval by a QAR of the issuance of an OOR vLEI Credential.

i. Identity Assurance of the OOR Person

ii. The OOR Person already has been identity assured in its role as a LAR.

iii. Identity Authentication of the OOR Person by a QAR
The following steps MUST be performed in this order during a continuous web meeting OOBI session.

a. A QAR MUST perform manual verification of the OOR Person's legal identity in the identity credential which was presented during Identity Assurance.

b. A QAR MUST ask the OOR Person verbally to confirm the AID that was sent in the OOR AUTH vLEI Credential. If the AID provided by the OOR Person does not match the AID sent in the OOR AUTH vLEI Credential, the OOBI session ends.

c. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the OOR Person.

d. The OOR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the QAR.

e. The QAR MUST send a Challenge Message to the OOR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the OOR Person's AID. The Challenge Message MUST be unique to the OOBI session.

f. The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person MUST acknowledge that this action has been completed.

g. The QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

h. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the OOR Person's signature.

i. A Challenge Message MAY be sent from the OOR Person to the QAR, signed and returned by the QAR to the OOR Person and the QAR's signature verified by the OOR Person.

6.4 Issuance

1. The Legal Entity validation and OOR Person Identity Verification process outlined in section 6.3 MUST be completed before OOR vLEI Credential issuance can begin.

2. The QAR MUST follow the usage rules specified below for OOR long names, OOR codes, OOR abbreviations and Latin Transliteration of OOR long names included in OOR vLEI Credentials. The usage rules followed by LARs for preparing the OOR AUTH vLEI Credential are specified in section 6.3. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.

   a. Usage rules for QARs for OOR long names and OOR codes, if applicable

      i. If the OOR long name and code, if applicable, specified in the OOR AUTH vLEI Credential does not match either the OOR long name and code specified in the ISO 5009 Official Organization Role lists or the OOR long name in the documents provided by the Legal Entity, then the QAR MUST inform the LAR.

   b. Usage rules for QARs for abbreviations of OOR roles

      i. If an OOR abbreviation exists for an OOR role:

         1. If an OOR abbreviation is included in the ISO 5009 Official Organization Role lists for the corresponding OOR role, then the abbreviation listed MUST be included in the OOR vLEI credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.

         2. If the OOR abbreviation is specified in other documents used by the QVI to validate the person in the role, then the abbreviation as specified in these documents MUST be included in the OOR vLEI credential

   c. Usage rule for QARs for the Latin Transliteration of OOR long names

      i. For all OORs included in the ISO 5009 Official Organization Role lists, the standard requires long names of OORs in non-Latin character sets to be

transliterated into Latin characters. If a Latin transliteration exists for an OOR long name in the ISO 5009 lists, the Latin transliteration MUST appear in the OOR vLEI Credential. The ISO 5009 Official Organization Role lists can be accessed using the GLEIF API.

3. A workflow MUST be implemented in the operations of the QVI which requires two QARs to be involved in the issuance and signing an OOR 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 OOR vLEI Credential.

4. A QAR MUST send the issued OOR vLEI Credential to the OOR Person who MUST sign the Admit message to accept the credential.

5. The QAR then MUST confirm that the OOR Person has Fully Signed the Admit message for the OOR vLEI Credential.

6. A QAR MUST call the vLEI Reporting API for each issuance event of OOR vLEI Credentials.

7. GLEIF MUST update the list of vLEI Credentials on the LEI page of the Legal Entity to reflect OOR vLEI credential issuances that have been reported by QVIs.

6.5 Revocation

1. To revoke an OOR vLEI Credential:

   a. The Legal Entity MUST revoke OOR vLEI Credentials if the OOR Person no longer holds the OOR specified in the OOR vLEI Credential, either as a result of changing roles or termination of employment, or if the OOR Person rescinds consent for their name and OOR to be published on the LEI page of the Legal Entity on gleif.org.

   b. To revoke a previously issued OOR vLEI Credential, the LAR(s) MUST revoke the OOR AUTH vLEI Credential related to a specific issuance of an OOR vLEI Credential.

   c. A QAR then MUST revoke the OOR vLEI Credential.

   d. The QAR MUST perform the revocation within the timeframe specified in Appendix 5 Service Level Agreement (SLA).

   e. A QAR MUST call the vLEI Reporting API for each revocation event of OOR vLEI Credentials.

f. GLEIF MUST remove the details of the OOR vLEI Credential that have been published on the LEI page of the Legal Entity on gleif.org when notified through the vLEI Reporting API about the revocation of an OOR vLEI Credential.

2. If the QVI has been terminated:

   a. By the end of the Grace Period for the Qualified vLEI Issuer vLEI Credential that has been revoked by GLEIF, all OOR vLEI Credentials will have become unverifiable because the chain of authority has been broken.

   b. Validators MUST treat as invalid any OOR vLEI Credentials once the Grace Period has expired. The expiration date of the Grace Period is 90 days after the revocation date of the QVI credential.

6.6 Level of Assurance

1. The OOR vLEI Credential SHOULD be issued with only a single Level of Assurance. Future versions of this Credential Framework MAY define multiple Levels of Assurance.

6.7 Monitoring

1. GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance of OOR vLEI Credentials which were not reported using the vLEI Reporting API.

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 Credential Definition

9.1 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/GLEIF-IT/vLEI-schema/blob/main/legal-entity-official-organizational-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 Official Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.

    c. The "officialRole" field value MUST be the Official Organizational Role.

    d. Additional data elements can be specified about the OOR 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 Official Organizational Role vLEI Credential.

3. The Sources section of the OOR vLEI Credential MUST contain a source reference to the OOR AUTH vLEI Credential (via SAID) that the issuing QVI received authorizing the issuance of this OOR vLEI Credential. The Sources section of that OOR 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.

    The elements in this type of credential can be returned in response to a presentation request as defined in the Issuance and Presentation Exchange (IPEX) protocol section of the ACDC specification.

    The ACDC specification can be found in: https://trustoverip.github.io/kswg-acdc-specification/

4. Usage of a valid, unexpired, and non-revoked vLEI Credential, as defined in the associated Ecosystem Governance Framework, 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 or that an implied or expressly intended purpose will be fulfilled. It is recommended that upon presentation of OOR vLEI Credentials that the credentials are verified. The Legal Entity is responsible for the use of OOR vLEI credentials that it has authorized and assumes liability for misuse of OOR vLEI Credentials by its official representatives.