Enabling global identity
Protecting digital trust

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

Public
EGF Version 1.0
Document Version 0.3
2022-10-31

Version	0.4
Date of version	2022-10-31
Document Name	Qualified vLEI Issuer Authorization vLEI Credential Governance Framework
Document DID URL	DID URLs for all documents will be published with the v1.0 Draft of the Ecosystem Governance Framework
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.

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 Authorization vLEI Credentials (QVI AUTH vLEI Credentials). There are two variants of this AUTH credential as defined by their schema. The first variant is the Qualified vLEI Issuer OOR Authorization vLEI Credential (QVI OOR AUTH vLEI Credential). The second variant is the Qualified vLEI Issuer ECR Authorization vLEI Credential (QVI ECR AUTH vLEI Credential). This document specifies the purpose, principles, policies, and specifications that apply to the use of these Credentials 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 AUTH vLEI Credential is to enable the simple, safe, secure authorization by a Legal Entity Authorized Representative (LAR) to be sent to a QVI accompanying all instructions sent to QVIs for the issuance and revocation of vLEI Role Credentials.

4 Scope

The scope of this Credential Governance Framework is limited to Legal Entities and QVIs for which Legal Entities have contracted for vLEI services.

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 AUTH vLEI Credentials shall be designed to provide a strong binding between and the Legal Entity Authorized Representatives (LARs) so the Qualified vLEI Issuer Authorized Representatives (QARs) cannot act to issue or to revoke vLEI Role Credentials without instructions and authorization from a LAR.

5.2 Context Independence

The QVI AUTH vLEI Credentials shall be designed to fulfil a Proof Request for the authorization by a LAR regardless of context, including in-person, online, or over the phone.

6 Issuer Policies

6.1 Qualifications

1. The Issuer MUSTbe a LAR of a Legal Entity that holds a valid Legal Entity vLEI Credential that was issued by the QVI with which the Legal Entity has contracted to issue vLEI Role Credentials.

6.2 Credential

The Issuer MUST:

1. use the QVI AUTH vLEI Credential schema defined in sections 9.1 and 9.2 for authorizing the associated OOR vLEI or ECR vLEI AUTH credentials respectively.
2. include the Claims marked as Required in the schema indicated in 9.1 and 9.2.

6.3 Identity Verification

LARs will need to include the Autonomic Identifiers (AIDs) of Official Organizational Role Persons (OOR Persons) and Engagement Context Role Persons (ECR Persons) as an element within the QVI AUTH vLEI Credentials issued for each vLEI Role Credential.

1. Identity Assurance
    a. A LAR MUST perform identity assurance of an OOR Person or ECR Person designated by the Legal Entity to receive vLEI Role Credentials 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 as specified in 2.e.i 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 OOR Person or ECR Person.
    b. A LAR and the OOR Person or ECR Person MUST establish a real-time OOBI session in which the LAR and the OOR Person or 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 OOBI session.
        i. The LAR MUST perform manual verification of the OOR Person's or ECR Person's legal identity for which the LAR has already performed Identity Assurance. An example, the OOR Person or ECR Person visually presenting one or more legal identity credentials and the LAR compares the credentials verified during Identity Assurance to the OOR Person or ECR Person.
        ii. The LAR MUST use an OOBI protocol (such as a QR code or live chat) to share its Autonomic Identifier (AID) with the OOR Person or ECR Person.
        iii. The OOR Person or ECR Person MUST use an OOBI 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 OOR Person's or ECR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the OOR Person's or ECR Person's AID. The Challenge Message MUST be unique to the OOBI session.
        v. The OOR Person or ECR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OOR Person or 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 OOR Person or ECR Person.
        vii. When the response to the Challenge Message has been received by the LAR, the LAR MUST verify the OOR Person's or ECR Person's signature.

6.4 Issuance

1. The LAR MUST include the OOR Person's or ECR Person's AID obtained during Identify Verification of the OOR Person or ECR Person, as well as the name and role of the OOR Person and ECR Person, as elements within the appropriate QVI AUTH vLEI Credential for the issuance of the associated vLEI Role Credential.
2. A workflow MAY be implemented in the operations of a Legal Entity which requires two LARs to be involved in the issuance and signing of a QVI AUTH vLEI Credential. The first LAR would prepare the QVI AUTH vLEI Credential for the issuance of a vLEI Role Credential. Another LAR then approves and signs the QVI AUTH vLEI Credential.
3. A LAR MUST issue QVI AUTH vLEI Credential explicitly authorizing the QARs of a QVI to issue each vLEI Role Credential. The QVI AUTH vLEI Credential will become part of the chain of the vLEI Role Credentials.

6.5 Revocation

1.To revoke a previously issued vLEI Role Credential, the LAR(s) MUST revoke the QVI AUTH vLEI Credential related to a specific issuance of a vLEI Role Credential.

2. The QAR then MUST revoke the vLEI Role Credential.

6.6 Level of Assurance

1. The QVI AUTH 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.

6.7 Monitoring

1. GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect revocations of QVI AUTH vLEI Credentials by LARs. This will advise GLEIF in the case of a terminated QVI or QVI leaving the vLEI Ecosystem to follow up on revocation of any OOR vLEI Credentials.

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 Privacy Considerations

Privacy Considerations are applicable to QVI ECR AUTH vLEI Credentials. It is the sole responsibility of QVIs as Issuees of QVI ECR AUTH vLEI Credentials to present these Credentials 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

10 Credential Definition

10.1 Schema QVI OOR AUTH vLEI Credential

1. The QVI OOR AUTH 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:

2. **The field values in the credentialbe as follows:**

   The "AID" field value MUST be the AID of OOR Person.

   The "LEI" field value MUST be the LEI of Legal Entity Holder.

   The "personLegalName" field value MUST be the Legal Name of the Person in the Official Role at the Legal Entity.

   The "officialRole" field value MUST be the the Official Role to be assigned in the vLEI OOR Credential.

   The elements in this type of credential can be returned in response to a presentation request as defined in the IPEX protocol (see below).

10.2 Schema QVI ECR AUTH vLEI Credential

1. The QVI ECR AUTH 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/ecr-authorization-vlei-credential.json

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

   The "AID" field value MUST be the AID of ECR Person.

   The "LEI" field value MUST be the LEI of Legal Entity Holder.

   The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity.

   The "engagementContextRole" field value MUST be the the Engagement Context Role to be assigned in the ECR vLEI Credential.

3. The Sources section MUST contain a source reference to the Legal Entity vLEI Credential (via SAID) held by the Legal Entity issuer of this credential. The Issuer of the referenced Legal Entity vLEI Credential MUST be the target holder of this QVI ECR AUTH vLEI Credential.

   The elements in this type of credential can be returned in response to a presentation request 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