GLEIF

Enabling global identity
Protecting digital trust

verifiable LEI (vLEI) Ecosystem Governance Framework v1.0

Qualified vLEI Issuer Authorization 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 Qualified vLEI Issuer Authorization vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2023-08-30_verifiable-LEI-(vLEI)-Ecosystem-Governance-Framework-Qualified-vLEI-Issuer-Authorization-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 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	Corrected ‘9.1’ and ‘9.2’ to ’10.1’ and ’10.2’ in section 6.2 Credential; updated section 6.3 Identity Verification to refer to the Identity Assurance and Identity Authentication sections in the OOR and ECR vLEI Credential Frameworks; updated section 6.4 Issuance to include requirements for multi-sig and thresholds for issuance of the QVI AUTH vLEI Credentials; updated section 9 Privacy Considerations with the requirement for OOR Person consent; updated section 10 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 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 simple, safe, secure instruction and authorization by a Legal Entity Authorized Representative (LAR) sent to a QVI 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 MUST be 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 10.1 and 10.2 for authorizing the associated OOR vLEI or ECR vLEI AUTH credentials respectively.
2. include the Claims marked as Required in the schema indicated in 10.1 and 10.2.

6.3 Identity Verification

LARs MUST 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. The requirements for Identity Assurance for the issuance of vLEI Role Credentials specified in the preparing for authorization of OOR and ECR vLEI Credentials MUST be followed for the issuance of QVI AUTH vLEI Credentials. For OOR vLEI Credentials, the relevant section in the Credential Framework is 6.5.1.1. For ECR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.1., 6.5.2.d. and 6.5.3.1.
2. Identity Authentication
    a. The requirements for Identity Authentication for the issuance of vLEI Role Credentials specified in the preparing for authorization of OOR and ECR vLEI Credentials MUST be followed for the issuance of QVI AUTH vLEI Credentials. For OOR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.2.b. and 6.5.2.2.b. For ECR vLEI Credentials, the relevant sections in the Credential Framework are 6.5.1.2.a., 6.5.2.2.e. and 6.5.3.2.

6.4 Issuance

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

1. The LAR MUST include the OOR Person's or ECR Person's AID obtained during Identity 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. The signatures on the QVI AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential.

3. In addition, a workflow SHOULD be implemented in the operations of a Legal Entity which requires one LAR to prepare the QVI AUTH vLEI Credential for the issuance of a vLEI Role Credential which then is approved and signed by the remaining LARs needed to satisfy the signing threshold of the AID of the Legal Entity vLEI Credential.

4. 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.

6.4.2 For a Legal Entity with a sole employee

1. The LAR MUST include the OOR Person's or ECR Person's AID obtained during Identity 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. The signatures on the QVI AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential, which in this case is a sole signer.

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 OOR AUTH vLEI Credentials. The LAR is responsible for obtaining the consent of the OOR Person for their name and OOR to be published on the on the LEI page of the Legal Entity on gleif.org and indicate this confirmation in the QVI OOR AUTH vLEI credential.

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:

https://github.com/WebOfTrust/vLEI/blob/dev/schema/acdc/oor-authorization-vlei-credential.json

2. The field values in the credential MUST be as follows:
    a. The "AID" field value MUST be the AID of OOR Person.
    b. The "LEI" field value MUST be the LEI of Legal Entity Holder.
    c. The "personLegalName" field value MUST be the Legal Name of the Person in the Official Organizational Role at the Legal Entity as it appears in the identity credential provided by the OOR Person for Identity Assurance.
    d. The "officialRole" field value MUST be the the Official Organizational 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:
    a. The "AID" field value MUST be the AID of ECR Person.
    b. The "LEI" field value MUST be the LEI of Legal Entity Holder.
    c. 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 ECR Person for Identity Assurance.
    d. 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