Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v4.0

Authorization vLEI Credential Framework

Public
Document Version 1.4
2026-03-25

Version	1.4
Date of version	2026-03-25
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework Authorization vLEI Credential Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pqzNrYoS?service=vlei-documents&relativeRef=/egf/docs/2026-03-25_vLEI-EGF-v4.0-Authorization-vLEI-Credential-Framework_v1.4_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 content 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.
2.0	1.2	December 15, 2023	Updated 'and' to 'or' in initial sentence in section 6.3 Identity Verification; added frequency of GLEIF checking TEL in section 6.7;

EGF Version	Document Version	Date	Description of Change
			updated specification references and links in section 9 Privacy Considerations and in sections 10.1 and 10.2 Schema; updated GLEIF-IT hosted link to schema in sections 10.1 and 10.2 Schema.
3.0	1.3	April 16, 2025	Updated references to Identity Verification sections in section 6.3.1.a.
4.0	1.4	March 25, 2026	Renamed credential to eliminate Qualified vLEI Issuer/QVI since Legal Entities issuing ECR credentials are required to use AUTH credentials as well; clarified section 3, Purpose, to reflect the above; clarified section 4, Scope, to reflect the above; deleted section 6.3, Identity Verification; updated and clarified now section 6.3, Issuance, to reflect the above; clarified now section 6.4, Revocation, to reflect the above; updated ACDC specification link in section 9, Privacy Considerations and section 10, 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 Authorization vLEI Credentials (AUTH vLEI Credentials). There are two variants of this AUTH credential as defined by their schema. The first variant is the OOR Authorization vLEI Credential (OOR AUTH vLEI Credential). The second variant is the ECR Authorization vLEI Credential (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 AUTH vLEI Credential is to enable simple, safe, secure instruction and authorization by a Legal Entity Authorized Representative (LAR) sent to a Qualified vLEI Issuer (QVI) for the issuance and revocation of Official Organizational Role vLEI Role Credentials (OOR vLEI Credentials) or Engagement Context Role vLEI Credentials (ECR vLEI Credentials), or to its LARs for the issuance and revocation of ECR vLEI Credentials directly by the Legal Entity.

The AUTH vLEI Credentials will become part of the chain of the vLEI Role Credentials.

4 Scope

The scope of this Credential Framework is for Legal Entities and QVIs for which Legal Entities have contracted for vLEI services for the issuance of OOR vLEI Credentials, and optionally for the issuance of ECR vLEI Credentials, and for Legal Entities that will issue ECR vLEI Credentials directly.

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 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 AUTH vLEI Credentials shall be designed to fulfil a request for the authorization by a LAR regardless of context, including in-person, online, or using a mobile device.

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 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 Issuance

1. The LAR MUST complete the Identity Verification requirements specified in the Legal Entity Official Organizational Role (OOR) vLEI Credential Framework and the Legal Entity Engagement Context Role (ECR) vLEI Credential Framework prior to issuing OOR AUTH vLEI Credentials and ECR AUTH vLEI Credentials.
2. The LAR also MUST follow the usage rules in the Legal Entity Official Organizational Role (OOR) vLEI Credential Framework for the inclusion of OOR long names, code, abbreviations and Latin Transliteration of OOR long names in creating OOR AUTH vLEI Credentials.
3. 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 or ECR Person, as elements within the appropriate AUTH vLEI Credential for the issuance of the associated vLEI Role Credential.
4. The signatures on the AUTH vLEI Credential MUST match the signing threshold of the AID of the Legal Entity vLEI Credential.
5. In addition, a workflow SHOULD be implemented in the operations of a Legal Entity which requires one LAR to prepare the 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.

6. A LAR MUST issue AUTH vLEI Credential explicitly authorizing the QARs of a QVI to issue each vLEI Role Credential. The AUTH vLEI Credential will become part of the chain of the vLEI Role Credentials.
7. A LAR also MUST issue an ECR AUTH vLEI Credential for ECR vLEI Credentials which the Legal Entity will issue directly.

6.4 Revocation

1. To revoke a previously issued vLEI Role Credential, the LAR(s) MUST revoke the AUTH vLEI Credential related to a specific issuance of a vLEI Role Credential.
2. The QAR or a LAR (for ECR vLEI Credentials issued directly by the Legal Entity) then MUST revoke the vLEI Role Credential.

6.5 Level of Assurance

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

6.6 Monitoring

1. GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect revocations of AUTH vLEI Credentials by LARs, at least daily. 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 or ECR 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 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 OOR AUTH vLEI credential.

It is the sole responsibility of QVIs as Issuees of ECR AUTH vLEI Credentials to present these Credentials in a privacy-preserving manner using the Issuance and Presentation Exchange (IPEX) protocol section of the Authentic Chained Data Container (ACDC) specification https://trustoverip.github.io/kswg-acdc-specification/

10 Credential Definition

10.1 Schema OOR AUTH vLEI Credential

1. The 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/GLEIF-IT/vLEI-schema/blob/main/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 specified in the vLEI OOR Credential.

   Note: the Schema for the OOR AUTH vLEI Credential will be updated to include OOR codes, abbreviations and Latin Transliteration of OOR long names.

   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 Authentic Chained Data Container (ACDC) specification.

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

10.2 Schema ECR AUTH vLEI Credential

1. The 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/GLEIF-IT/vLEI-schema/blob/main/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 specified 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 ECR AUTH 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 here: https://trustoverip.github.io/kswg-acdc-specification/