Issuing LE vLEIs

Please email vlei-support@provenant.net to give feedback or get support with this information.

This document covers issuance of vLEIs that prove the identity of the legal identity. For information about issuing vLEIs to individuals, see Issuing OOR vLEIs and Issuing ECR vLEIs.

Although many normative documents from GLEIF cover some aspect of this process, the primary reference is the Legal Entity vLEI Credential Governance Framework (LE-vLEI-FW).

Preconditions

The Provenant portion of the steps outlined in this document MUST be completed by a Provenant QAR, not just general staff.

Unsolicited Issuance

If an organization does not yet have the ability to use KERI infrastructure (lacks a wallet and formally defined LARs), then a request for an LE vLEI begins in meetings or casual conversations. However, from a formal standpoint, the onboarding process begins when someone who claims to be associated with the LE sends an email to vlei-support@provenant.net, requesting that Provenant engage with the LE associated with LEI to issue a vLEI for the LE. Conversations MUST move to this official channel to begin an audit trail with SLAs. See Communicating with Customers.

The person who sends this email MUST NOT be confused with the role that is called a *Legal Entity Authorized Representative* (*LAR,* formerly *AVR*) in 6.3.2.a of LE-vLEI-FW. Anybody can submit the request that starts this process, because the identity of that person is not important. However, only LARs can act for the LE identified by LEI x in an official capacity. The steps we follow guarantee that we properly maintain this distinction.

The steps to follow for unsolicited issuances, after the preconditions have been met, are:

1. Call GLEIF's lei-records API to confirm that the LE identified by LEI x already has an LEI with LE status=ACTIVE and registration status other than Lapsed, Retired, Duplicate, Annulled, or Merged, with an expiration date at least 30 days later than the likely issuance date of the vLEI. Save the JSON returned from the API as evidence, in the LE's customer folder in the Provenant vault.

(for glossary, gov fw, and other reference docs see Resources)

2. As required by 6.3.1.a of LE-vLEI-FW, perform identity assurance on the legal entity to make sure that the LE in question is behind this request and wants to proceed. This process is documented in Assuring LE Identity and Intent.

3. Ask the company to designate one or more LARs. Encourage them to designate at least three, with a 2-of-3 multisig scheme.

4. Complete identity assurance on each LAR, and give them a wallet and AID.

    a. Complete steps 1 through 4, then steps 5a-f, as described in the "Assurance" section of Assuring and Authenticating Individual Identity.

    b. Create a wallet for the LAR and give them control of it.

    c. Help them to create an AID that they will use in their LAR capacity.

    d. End the Zoom meeting and complete step 5g from the doc.

5. After step 4 has been completed with all LARs, start a zoom meeting at which all LARs attend as a group.

6. Call GLEIF's lei-records API (again) for the LEI in question, to confirm that the LE continues to have an LEI with ACTIVE status. Save the updated JSON in the LE's customer folder in the Provenant vault.

7. Authenticate each LAR. See the "Authenticating" section of Assuring and Authenticating Individual Identity (or could send a challenge to the AID we know they control from step 4c...)

8. Help LARs jointly create the AID for the legal entity and set up multisig AID.

9. Complete the OOBI exchange/challenge as described in 6.3.2.d of LE-vLEI-FW.

10. Assist the LARs to generate a fully signed issuance request for the LE vLEI. Have them send this issuance request to Provenant. At this point, the remaining workflow is identical to that for Solicited Issuance.

11. End the meeting. Save the recording into the LE's customer folder in the Provenant vault. (This step may be postponed while the steps of solicited issuance are completed on the meeting, if desired.)

Solicited Issuance

Solicited issuance begins when Provenant receives a fully signed issuance request for an LE that is associated with LEI $\boldsymbol{\mathcal{X}}$.

(for glossary, gov fw, and other reference docs see Resources)

12. Validate the issuance request.

13. One QAR, designated QAR1, acts as the facilitator of the request. Assign the QAR1 role to a member of Provenant's QVI staff.

14. A second QAR, designated QAR2, acts as final approver. Assign the QAR2 role to a different member of Provenant's QVI staff.

15. QAR1 saves a copy of the fully signed issuance request in the LE's customer folder in the Provenant vault.

16. If it has been more than 7 days since the last time Provenant called [GLEIF's lei-records API](), call it again to confirm that the LE continues to have an LEI with ACTIVE status. Save the updated JSON in the LE's customer folder in the Provenant vault.

17. If the LE has any LARs that have not been identity assured by Provenant, then QAR1 performs step 4 for all the unfamiliar LARs, thus rebuilding the relationship between LE and LARs in a way that Provenant can stand behind.

18. QAR1 submits all evidence of proper process to QAR2 and proposes that the issuance be approved.

19. QAR2 reviews the evidence and approves (or rejects if needed).

20. Assuming approval, QAR2 signs the LE vLEI credential and releases it for distribution to the LARs (or, if multisig is absent, to the LE wallet).

21. Provenant automation performs the following steps:

    a. Send an email announcing issuance to each LAR for the LE.

    b. Call GLEIF's vLEI reporting API to guarantee that GLEIF has a record of the issuance event.

    c. Generate an invoice and email it to the LE.

(for glossary, gov fw, and other reference docs see [Resources]())