Enabling global identity
Protecting digital trust

verifiable LEI (vLEI) Ecosystem Governance Framework v1.0

GLEIF Identifier Governance Framework

Public
Document Version 1.0
2022-12-16

Version	1.0
Date of version	2022-12-16
Document Name	verifiable LEI (vLEI) Ecosystem Governance Framework GLEIF Identifier Governance Framework
Document DID URL	did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2022-12-13_GLEIF-Identifier-GF-Prep-1.0-Publication_v0.7_work.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.

1 Introduction

This is a Controlled Document of the verifiable LEI (vLEI) Ecosystem Governance Framework. It is the authoritative Governance Framework for the purpose, principles, policies, and specifications that apply to the use of the GLEIF Root Autonomic Identifier (AID) and its GLEIF Delegated AIDs in the vLEI Ecosystem.

2 Terminology

All terms in First Letter Capitals are defined in the vLEI Glossary.

3 Purpose

The GLEIF Root AID provides the Root of Trust for the ecosystem tree of trust. Each branch in that tree is a Chain of Trust. The Delegated AID Chain of Trust branch provides trust for delegated GLEIF AIDs and Qualified vLEI Issuer Delegated AIDs. The vLEI Chain of Trust branch, that attaches to the Delegated AID Chain of Trust branch, provides trust for all vLEIs within the vLEI ecosystem.

Scope

The scope of this Identifier Governance Framework is limited to the GLEIF Root AID and its Delegated AIDs.

4 Principles

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

4.1 Highest Duty of Care

GLEIF shall exercise the highest duty of care in generating and administering the GLEIF AID and all its Delegated AIDs as these are the security foundation of the entire vLEI Ecosystem.

4.2 Self-Certifying (Autonomic) Identifiers

All identifiers in the vLEI Ecosystem shall be self-certifying identifiers (specifically KERI Autonomic Identifiers or AIDs), i.e., it must be possible to verify directly using cryptography alone as defined by the Key Event Receipt Infrastructure (KERI) protocol that the identifier was generated from a specific set of cryptographic key pair(s).

4.3 Cryptographic Root of Trust

All AIDs in the vLEI Ecosystem shall be generated from a random number seed large enough to provide adequate cryptographic security for the branch of the tree of trust that provides the Chain of Trust for which a given AID is the head.

5 AID Generation

1. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key pairs generated from a cryptographically-secure pseudo-random number generator (SPRNG) or a true random number generator with at least 128 bits of cryptographic Root (see section 3.1 of Technical Requirements Part 1 KERI Infrastructure).
2. The AID MUST then be derived from a cryptographic digest of a serialization of the public keys of the first set of key pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters associated with the supporting infrastructure for the Root Identifier as specified in the Technical Requirements Part 1 KERI Infrastructure.
3. The cryptographic digest MUST have at least 128 bits of cryptographic strength.

6 AID Controllers

1. All Controllers MUST establish their own Private Key Store.
2. All Controllers MUST keep their private keys secret.
3. A given Controller MUST control one and only one key pair from each set of keys.
4. The KERI protocol MUST be used to transfer control authority from one set of keys to another.
5. Continuity and Survivorship
    a. GLEIF MUST have a Continuity Policy for the survival of control authority of all Controllers for the GLEIF Root AID and its Delegated AIDs, including Escrow Agents.

b. QVIs and Legal Entities SHOULD have a Continuity Policy for the survival of control authority of their Controllers.

7 GLEIF AID Genesis

The policies in this section apply to the genesis event for the GLEIF Root AID, the GLEIF Internal Delegated AID (GIDA) and the GLEIF External Delegated AID (GEDA).

1. GLEIF MUST establish a list of initial GLEIF Controllers that specifies:
    a. The legal identity of each Controller.
    b. Which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.
    c. A set of policies MUST be put in place that ensure fault-tolerance with respect to common mode failures of the multi-sig signing authority of the set of GLEIF Controllers, e.g., a Designated Survivor policy and/or restrictions on joint travel and in-person attendance of meetings).
2. GLEIF MUST establish real-time Out-of-Band Interaction (OOBI) session(s) in which all initial GLEIF Controllers are present. An example is a continuous web meeting attended by all parties on both audio and video. The essential feature is that there is a mutual live presentation by all participants that verifies their live participation in the session.
    a. Each session MUST be recorded, and the recording stored in high-security storage.
3. All GLEIF Controllers MUST mutually authenticate each other's legal identities before proceeding with any further steps. An example is each Controller visually presenting one or more legal identity credentials for all other Controllers to verify against the list of initial GLEIF Controllers.
4. The Root AID GLEIF Authorized Representative, the Internal Delegated AID GLEIF Authorized Representative and the External Delegated AID GLEIF Authorized Representative are GLEIF Controllers.
5. Creation of GLEIF Root AID

    The following steps MUST be performed in the order listed and completed during each OOBI session for the GLEIF Root AID.

    a. Each Root AID GLEIF Authorized Representative (Root GAR) MUST generate its own single signature AID that is a participating member in the group of AIDs that will be used to create the GLEIF Root AID.
    b. Each Root GAR MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Root GAR. For each Root GAR this provides the participating AID and the service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.
    c. Each Root GAR MUST send a Challenge Message to every other Root GAR as defined in the Technical Requirements Part 1 for the purposes of cryptographic

authentication of their Root GAR AID. The Challenge Message MUST be unique to each OOBI session.

d. Each Root GAR MUST verify in real time that a response to the Challenge Message was received from every other Root GAR.

e. Each Root GAR MUST verify the signature of every other Root GAR.

f. One of the Root GARs MUST be designated as the Root AID GLEIF Authorized Representative Lead (Root GAR Lead).

g. The Root GAR Lead MUST select the AIDs from the set of Root GAR s for the ordered set of authorized participant members in the multi-sig group and configure and approve the weight threshold and ordered set of participants for both the current and next set and threshold of participants.

h. The Root GAR Lead MUST select the AIDs and Service Endpoints for the GLEIF Root AID Witness Pool.

i. Using the current public key and the next public key digest from each of the participating AID Inception Events and the Root Witness AIDs, the Root GAR Lead MUST generate the GLEIF Root AID Inception Event and publish this to the other Root GARs and to the Root AID Witnesses designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the Root AID Witnesses.

j. Each Root GAR MUST verify the set of public keys, the next public key digest, the threshold, the next threshold, and Root AID Witness identifiers in the Root AID Inception Event.

k. Each Root GAR MUST verify the set of service endpoints for the Root AID Witnesses.

l. Each Root GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Inception Event.

m. Each Root GAR MUST verify that the Root AID Inception Event is fully witnessed by every Root AID Witness.

6. Creation of the GLEIF Internal Delegated AIDs

The following steps MUST be performed in the order listed and completed during each OOBI session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in this section, and the GLEIF External Delegated AID (GEDA) in section 7.

a. Each Internal Delegated AID GLEIF Authorized Representative (Internal GAR) that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GIDA.

b. Each Internal GAR MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Internal GARs. For each Internal GAR, this provides the participating AID and the service endpoint whereby the other Internal GARs may obtain the KEL of its participating AID.

c. Each Internal GAR MUST send a Challenge Message to every other Internal GAR as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their GIDA. The Challenge Message MUST be unique to each OOBI session.

d. Each Internal GAR MUST verify in real time that a response to the Challenge Message was received from every other Internal GAR.

e. Each Internal GAR MUST verify the signature of every other Internal GAR.

f. One of the Internal GAR s MUST be designated as the Internal Delegated AID GLEIF Authorized Representative (Internal GAR Lead)

g. The Internal GAR Lead MUST select the AIDs and Service Endpoints for the GLEIF Internal Delegated AID Witness Pool.

h. The Internal GAR Lead MUST select the AIDs from the set of Internal GAR for the ordered set of authorized participant members in the multi-sig group and configure and approve the weight threshold and ordered set of participants for both the current and next set and threshold of participants.

i. Using the current public key and the next public key digest from each of the participating AID Inception Events, the Internal Delegated Witness AIDs, and the GLEIF Root AID, the Internal GAR Lead MUST generate the GLEIF Internal Delegated AID Inception Event and publish this to the other Internal GARs and to the Delegated AID Witnesses designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the Internal Delegated AID Witnesses.

j. Each Internal GAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, and the Root AID in the Internal Delegated AID Inception Event.

k. Each Internal GAR MUST verify the set of Witness endpoints for the GIDA.

l. Each Internal GAR MUST sign and publish to the Internal Delegated AID Witnesses its signature on the Internal Delegated AID Inception Event.

m. Each Internal GAR MUST verify that the Internal Delegated AID Inception Event is fully witnessed by every Witness.

7. Creation of the GLEIF External Delegated AIDs

The following steps MUST be performed in the order listed and completed during each OOBI session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in section 6 and the GLEIF External Delegated AID (GEDA) in this section.

a. Each External Delegated AID GLEIF Authorized Representative (External GAR) that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GEDA.

b. Each External GAR MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other External GARs. For each

External GAR, this provides the participating AID and the service endpoint whereby the other External GARs may obtain the KEL of its participating AID.

c. Each External GAR MUST send a Challenge Message to every other External GAR as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their GEDA. The Challenge Message MUST be unique to each OOBI session.

d. Each External GAR MUST verify in real time that a response to the Challenge Message was received from every other External GAR.

e. Each External GAR MUST verify the signature of every other External GAR.

f. One of the External GARs MUST be designated as the External Delegated AID GLEIF Authorized Representative Lead (External GAR Lead).

g. The External GAR Lead MUST select the AIDs and Service Endpoints for the GLEIF External Delegated AID Witness Pool.

h. The External GAR Lead MUST select the AIDs from the set of External GARs for the ordered set of authorized participant members in the multi-sig group and configure and approve the weight threshold and ordered set of participants for both the current and next set and threshold of participants.

i. Using the current public key and the next public key digest from each of the participating AID Inception Events, the External Delegated Witness AIDs, and the GLEIF Root AID, or the External GAR Lead MUST generate the GLEIF External Delegated AID Inception Event and publish this to the other External GARs and to the External Delegated AID Witnesses designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the External Delegated AID Witnesses.

j. Each External GAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, and the Root AID in the External Delegated AID Inception Event.

k. Each External GAR MUST verify the set of Witness endpoints for the GEDA.

l. Each External GAR MUST sign and publish to the External Delegated AID Witnesses their signature on the External Delegated AID Inception Event.

m. Each External GAR MUST verify that the External Delegated AID Inception Event is fully witnessed by every Witness.

8. Rotation Event to delegate the GLEIF Internal Delegated AIDs

The following steps MUST be performed in the order listed and completed during this OOBI session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in this section and the GLEIF External Delegated AID (GEDA) in section 9.

The anchor in this Rotation Event is the mechanism by which the delegation is authorized by the Delegator. The Rotation Event with the anchoring digest of the Inception Event of the Delegated AID, when Fully Signed, is a verifiable cryptographic commitment to the

delegation. The Delegated AIDs are not verifiable until they are anchored in the KEL of the Delegator e.g., the Root AID. A new event must be created to include these anchors.

(Delegation in KERI is cooperative. It requires a cryptographic commitment from both the Delegator and the Delegate.)

a. A threshold satisficing subset of Internal GARs MUST each rotate their participating AIDs.

b. Using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digest of the GLEIF Internal Delegated AID Inception Event, the Internal GAR Lead MUST generate a GLEIF Internal Delegated AID Rotation Event and publish this to the other participating Internal GARs and to the Root AID Witnesses.

c. Each Internal GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that Rotation Event.

d. Each Internal GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.

e. Each Internal GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.

9. Rotation Event to delegate the GLEIF External Delegated AIDs

The following steps MUST be performed in the order listed and completed during this OOBI session for each of the two GLEIF Delegated AIDs, namely, the GLEIF Internal Delegated AID (GIDA) in section 8 and the GLEIF External Delegated AID (GEDA) on this section.

The anchor in this Rotation Event is the mechanism by which the delegation is authorized by the Delegator. The Rotation Event with the anchoring digest of the Inception Event of the Delegated AID, when Fully Signed, is a verifiable cryptographic commitment to the delegation. The Delegated AIDs are not verifiable until they are anchored in the KEL of the Delegator e.g. the Root AID. A new event must be created to include these anchors.

(Delegation in KERI is cooperative. It requires a cryptographic commitment from both the Delegator and the Delegate.)

a. A threshold satisficing subset of External GARs MUST each rotate their participating AIDs.

b. Using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digest of GLEIF External Delegated AID Inception Event, the External GAR Lead MUST generate a GLEIF External Delegated AID Rotation Event and publish this to the other participating External GARs and to the Root AID Witnesses.

c. Each External GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that Rotation Event.

d. Each External GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.

e. Each External GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.

f. Each participating External GAR MUST verify the delegated Inception Event digest in that Interaction Event.

g. Each participating External GAR MUST sign and publish to the GLEIF External Delegated AID Witnesses their signature on the GLEIF External Delegated AID Interaction Event.

h. Each participating External GAR MUST verify that the GLEIF External Delegated AID Interaction Event is fully witnessed by every Witness.

8 Publication of GLEIF Root AID and GLEIF Delegated AIDs

1. The GLEIF Root AID and GLEIF Delegated Internal and External AIDs MUST be published in a sufficiently strongly correlated and fault-tolerant manner to establish them as unique AIDs for GLEIF.
2. The set of publication points MUST include at least 4 of the list of publication points initially (highlighted below) following the creation of the GLEIF Root AID and GLEIF Delegated Internal and External AIDs.

    a. The GLEIF HTTPS website.

    b. The HTTPS website of the GLEIF Regulatory Oversight Committee.

    c. The HTTPS websites of all QVIs.

    d. In the KERI Event Log hosted by GLEIF KERI Witnesses.

    e. Published to at least 3 international newspapers in separate national jurisdictions (applies only to the GLEIF Root AID).

    These publications are: Financial Times UK edition, South China Morning Post - Business and American Banker.

    f. Published to github repositories

    The Web of Trust github repository

    Public GLEIF-controlled github repository

    g. Published to public registries

    IANA (IETF RFCs) registries

    ISO registries

9 Abandonment

1. Voluntary abandonment
   GLEIF MUST abandon its GLEIF Root AID if GLEIF no longer holds the role of root of trust for the vLEI Ecosystem.
2. Private key compromise or natural disaster
   If in the extremely unlikely event of the failure of all key recovery provisions specified in Technical Requirements Part 1: KERI Infrastructure, GLEIF MUST abandon its Root AID and Delegated Internal and External AIDs and create and publish its new Root AID and Delegated Internal and External AIDs.