verifiable LEI (vLEI) Ecosystem Governance Framework: GLEIF Identifier Governance Framework

verifiable LEI (vLEI)
Ecosystem Governance
Framework

GLEIF Identifier
Governance Framework

2021-12-15, v1.0 draft
Trust over IP Review

Document Name:	GLEIF Identifier Governance Framework
Document DID:	
Version Number:	V1.0 draft for Trust over IP Review
Version Date:	
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	
Copyright:	

1 Introduction

This is a Controlled Document of the GLEIF 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. For more information about the vLEI Ecosystem Governance Framework, please see the following section on the GLEIF website at [INSERT URL HERE].

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 delegrated 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 (CSPRNG) 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 Controllers.
    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 and the GLEIF External Delegated AID.

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 GLEIF Internal AID and the GLEIF External AID.
    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 a real-time Out-of-Band Interaction (OOBI) session in which all initial GLEIF Controllers are present. An example is a continuous webmeeting attended by all parties on both audio and video.
    a. This 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 futher 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. Creation of GLEIF Root AID

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

    a. Each GLEIF Root AID Controller 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 GLEIF Controller MUST use an OOBI protocol (such as a QR code or live chat) to share its own AID and Service Endpoints with the other Controllers. For each GLEIF Controller, this provides the participating AID and the service endpoint whereby the other Controllers may obtain the Key Event Log (KEL) of its participating AID.
    c. Each Controller MUST send a Challenge Message to every other GLEIF Controller as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of their Controller AID.
    d. Each Controller MUST verify in real time that a response to the Challenge Message was received from every other Controller.
    e. Each Controller MUST verify the signature of every other Controller.

f. One of the Controllers MUST be designated as the GLEIF Genesis Controller.

g. The GLEIF Genesis Controller MUST select the AIDs and Service Endpoints from the GLEIF Root AID Witness Pool.

h. 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 GLEIF Genesis Controller MUST generate the GLEIF Root AID Inception Event and publish this to the other Controllers 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.

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

j. Each Controller MUST verify the set of service endpoints for the Root AID Witnesses.

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

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

5. Creation of the GLEIF 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.

a. Each GLEIF Delegated AID Controller that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the GLEIF Delegated AID.

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

c. Each Controller MUST send a Challenge Message to every other Controller as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their Controller AID.

d. Each Controller must verify in real time that a response to the Challenge Message was received from every other Controller.

e. Each Controller must verify the signature of every other Controller.

f. One of the Controllers must be designated as the GLEIF Delegated AID Genesis Controller.

g. The GLEIF Delegated AID Controller MUST select the AIDs and Service Endpoints from the GLEIF Delegated AID Witness Pool.

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

i. Each Controller MUST verify the set of public keys, the next public key digest, the Witness identifiers and the Root AID in the Delegated AID Inception Event.

j. Each Controller MUST verify the set of Witness endpoints for the GLEIF Delegated AID.

k. Each Controller MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.

l. Each Controller MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.

6. Rotation Event to delegate the GLEIF Delegated AIDs

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. The set of GLEIF Root AID Controllers 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 Delegated AID Inception Event, the GLEIF Genesis Controller MUST generate a GLEIF Delegated AID Rotation Event and publish this to the other Controllers and to the Root AID Witnesses.

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

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

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

7. Creation of QVI Delegated AIDs

The following steps MUST be performed in the order listed and completed during an OOBI session for a given QVI Delegated AID.

a. Each QVI Delegated AID Controller that is a participating member in the group of AIDs MUST generate its own single signature AID that will be used to create the QVI Delegated AID.

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

c. Each Controller MUST send a Challenge Message to every other Controller as defined in the Technical Requirements Part 1 KERI Infrastructure for the purposes of cryptographic authentication of their Controller AID.

d. Each Controller must verify in real time that a response to the Challenge Message was received from every other Controller.

e. Each Controller must verify the signature of every other Controller.

f. One of the Controllers must be designated as the QVI Delegated AID Genesis Controller.

g. Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated Witness AIDs, and the GLEIF External Delegated AID, the QVI Delegated AID Genesis Controller MUST generate the QVI Delegated AID Inception Event and publish this to the other Controllers and to the Delegated AID Witnesses designated by that Inception Event.

h. Each Controller MUST verify the set of public keys, the next public key digest, the Witness identifiers and the GLEIF External Delegated AID in the Delegated AID Inception Event.

i. Each Controller MUST verify the set of Witness endpoints for the QVI Delegated AID.

j. Each Controller MUST sign and publish to the Delegated AID Witnesses their signature on the Delegated AID Inception Event.

k. Each Controller MUST verify that the Delegated AID Inception Event is fully witnessed by every Witness.

8. Interaction Event to delegate QVI Delegated AIDs

The anchor in this Interaction Event is the mechanism by which the delegation is authorized by the Delegator. The Interaction Event with the anchoring digest of the

Inception Event of the Delegated AID, when Fully Signed, is a verifiable cryptographic commitment to the delegation.

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

a. GLEIF MUST designate on of the GLEIF External Delegated AID Controllers as the GLEIF External AID Interaction Event Controller.

b. Using the current public key from each of the participating AID Controllers and the digest of the QVI Delegated AID Inception Event, the GLEIF External AID Interaction Event Controller MUST generate a GLEIF Delegated AID Interaction Event and publish this to the other Controllers and to the GLEIF Delegated AID Witnesses.

c. Each Controller MUST verify the delegated Inception Event digest in that Interaction Event.

d. Each Controller MUST sign and publish to the GLEIF Delegated AID Witnesses their signature on the GLEIF Delegated AID Interaction Event.

e. Each Controller MUST verify that the GLEIF Delegated AID Interaction Event is fully witnessed by every Witness.

9. Rotation Event to delegate QVI Delegated AIDs

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.

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

a. The set of GLEIF External Delegated AID Controllers MUST each rotate their participating AIDs.

b. GLEIF MUST designate on of the GLEIF External Delegated AID Controllers as the GLEIF External AID Rotation Event Controller.

c. Using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digest of the QVI Delegated AID Inception Event, the GLEIF External AID Rotation Event Controller MUST generate a GLEIF Delegated AID Rotation Event and publish this to the other Controllers and to the GLEIF Delegated AID Witnesses.

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

e. Each Controller MUST sign and publish to the GLEIF External AID Witnesses their signature on the GLEIF External AID Rotation Event.

f. Each Controller MUST verify that the GLEIF External AID Rotation Event is fully witnessed by every Witness.

8 GLEIF Root AID Publication

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 the following:
   a. The GLEIF HTTPS website.
   b. The HTTPS websites of at least ten members of the GLEIF Regulatory Oversight Committee.
   c. The HTTPS websites of all QVIs.
   d. In the KERI Event Log for all GLEIF KERI Witnesses.
   e. Published to at least 3 international newspapers in separate national jurisdictions.
   f. Published to public registries (to be specified).

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.