Enabling global identity
Protecting digital trust

verifiable LEI (vLEI)
Ecosystem Governance Framework v2.0

Technical Requirements Part 1:
KERI Infrastructure

Public
Document Version 1.2
2023-12-15

verifiable LEI (vLEI) Ecosystem Governance Framework Technical Requirements

Part 1: KERI Infrastructure

This Controlled Document specifies the technical requirements for KERI (Key Event Receipt Infrastructure) Infrastructure for use by GLEIF and Qualified vLEI Issuers (QVIs) within the vLEI Ecosystem Governance Framework.

The DID URL for this Controlled Document is: did:keri:EINmHd5g7iV-UldkkkKyBIH052bIyxZNBn9pq-zNrYoS?service=vlei-documents&relativeRef=/egf/docs/2023-12-15_vLEI-EGF-v2.0-Technical-Requirements-Part-1-KERI-Infrastructure_v1.2_final.pdf

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	April 3, 2023	Replaced 'Verifiable Data Registries (VDRs)' in section 5.6 with 'GLEIF Witness Network'
2.0	1.2	December 15, 2023	Updated link to KERI specification in section 1.1; clarification in section 5.6 GLEIF Witness Network that GLEIF must set up and maintain its own Witness pool; formatting, editing (for example, consistent capitalization of defined terms).

1 KERI Specifications

1.1 Specification References

The draft specification for KERI family of capabilities can be found at:
https://github.com/trustoverip/tswg-keri-specification

1.2 Specification Version Upgrades

These policies govern migrating to revisions of the KERI specifications.

1. Previous versions explicitly cited by policies in this document MUST be supported for a period of 18 months.
2. New versions MUST be implemented within a period of 12 months after final approval of the new version, unless otherwise superseded by revised policies in a new version of the vLEI Ecosystem Governance Framework.
3. After upgrading to a new version, implementers MUST NOT begin using any breaking changes until the end of the time period required to adopt new versions. For example, v2.0 must be compatible with v1.0 until the end of the v2.0 adoption period. So v2.0 must be used in a v1.0 compatible mode.

2 Endorser (Backer) Management

An Endorser provides a secondary root-of-trust for a KEL (Key Event Log). Two types of Endorsers will be supported initially for the vLEI infrastrcture: Witnesses and Registrars.

2.1 Witness Pool

A Witness Pool:

1. MUST use a KERI Agreement Algorithm for Control Establishment (KAACE) sufficient majority threshold on a minimum pool of 5 Witnesses.
2. SHOULD use access control independent of the Controller keys for configuring the Witness host and accepting events for witnessing. (NOTE: this avoids poisoning of Witnesses by Controller key compromise and adds an extra layer of security.)
3. MUST publish Witnesses to at least one ecosystem discovery mechanism:
    a. Well-Known URI IETF RFC-8615 on a web site(s)associated with entity. The value of the /well-known/oobi resource is a OOBI (out-of-band-introduction) to witness or witnesses
    b. Publish OOBIs for witnesses on web site(s) discoverable by search engines.
    c. KERI Distributed Hash Table (DHT)
    d. DID method resolvers
    e. Ledgers

2.2 Registrar (Ledger)

A Registrar (Ledger):

1. SHOULD use only one Registrar at a time for a given KEL;
2. MUST use a GLEIF Approved DID Method (one for each authorized ledger):
    a. Security guarantees are based on the particular ledger.
    b. A DID method MUST be approved down to the ledger-specific level.

2.3 Hybrid (Witness Pool and Ledger Registrar)

A Hybrid (Witness Pool and Ledger Registrar)

1. MUST use only one type for any KEL.
2. MAY use different types for each Delegated KEL at any level of a delegation hierarchy.

3 Watcher Management

Validators need to be protected by their Watcher network.

1. Validators SHOULD choose Watchers carefully or else the integrity of the network will be affected.
2. Validators MAY choose any number of Watchers.
3. If a Validator is managing its own Watcher pool:
    a. The Validator SHOULD use a minimum pool of three with a threshold of sufficient majority threshold of 2 for consensus establishment;
    b. If using more than three Watchers, Validators SHOULD use a KAACE sufficient majority threshold pool size greater than three.
4. If using a Watcher service, Validators SHOULD use a Watcher service that at a minimum self-asserts compliance with the GLEIF vLEI EGF.

4 Key Management

Unless otherwise specified, the term key-pair refers to an asymmetric (public, private) key-pair for digital signatures. The private key is used to generate signatures and the public key is used to validate signatures. Ecosystem key management policies are grouped into three sets of policies for protecting three different infrastructures:

1. Key-pair creation and storage infrastructure;
2. Signature creation infrastructure;
3. Signature verification infrastructure.

4.1 Key-Pair Creation and Storage Infrastructure

4.1.1 Strength

All key-pairs MUST be generated using a cryptographic algorithm with at least 128 bits of cryptographic strength. This includes using a source of entropy of at least 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.

NOTE: Well known libraries provide cryptographic strength pseudo random number generators (CSPRNGs) sufficient to meet this condition. When practical, a true random number generator is preferable to a CSPRNG. In general, the codes in the CESR (Composable Event Streaming Representation) tables only support cryptographic operations with a minimum strength of 128 bits.

Examples of compliant asymmetric digital signature algorithms include Ed25519 and EcDSASecp256k1. Unless otherwise specified, all key management policies assume use of the KERI protocol for managing the authoritative key state for any Autotomic Identifier (AID).

4.1.2 Autonomic Identifiers (AIDs)

AIDs are self-certifying identifiers that are imbued with self-management capabilities via the KERI protocol. There are two main classes of AIDs in KERI: 1) transferable AIDs, and 2) non-transferable AIDs. Key management policies are different for the two classes of AIDs.

1. Both Authentic Chained Data Container (ACDC) Issuer and Issuee AIDs MUST be transferable.

4.1.3 Key Pre-Rotation for Transferable AIDs

In KERI, the authoritative key state of a transferable AID consists of two sets of key-pairs. The first set is the current set of signing keys and the second set is the pre-committed set of one-time rotation keys that after rotation will become the next or pre-rotated set of signing keys. These two sets provide the basis for KERI's pre-rotation mechanism.

1. The next or pre-rotated set of keys MUST be protected with the highest level of protection. This level of protection should be commensurate with the value of the assets these keys are protecting.
2. Non-delegated pre-rotated keys are at the root level of a delegation hierarchy and MUST have the very highest level of protection. There is no recovery mechanism within KERI to regain control over a non-delegated AID once its pre-rotated keys have been captured. The only recourse is to abandon the AID and stand up a new AID and re-establish the reputation and associations of the new AID. This re-establishment process is ecosystem dependent and is not part of KERI.
3. Delegated pre-rotated keys MAY have a lower level of protection because the Delegator may recover the loss or compromise of delegated pre-rotated keys. Valid KERI delegations are cooperative in that they require verified signatures from both the Delegator and Delegatee thus requiring an attacker to compromise both sets of keys.

4.1.4 Non-Transferable AIDs

Non-transferable AIDs are self-certifying but are not meant for long term persistent use and hence their key-pair(s) are not rotatable. Instead, the identifier is abandoned and replaced with a new identifier with a new set of key-pair(s). These may also be called ephemeral AIDs. Within KERI, the primary use for non-transferable (ephemeral) AIDs are for the Witness identifiers. Because Witnesses are used in a pool, the pool forms a threshold structure which provides protection from the exploit of a minority of the key-pairs of the ephemeral Witness AIDs in the pool. If a given Witness AID has its key(s) compromised, then the Witness AID itself is abandoned and replaced. Thus, the Witness pool management policy protects Witness ephemeral AIDs.

4.2 Signature Creation Infrastructure

When statements are signed by the private key(s) for a given AID, the private key becomes exposed in the sense that it must be used in some computing device in order to compute the signature. Computing devices used to create a signature of, or sign, a statement are part of the signature creation infrastructure. A typical attack on signing infrastructure would be to observe or capture the private key while in the memory of the computing or signing device.

Another layer of protection is provided by the Witness pool which must endorse all events.

1. The signature creation or signing infrastructure for AIDs SHOULD be protected within some form of a TEE (Trusted Execution Environment).
2. A separate layer of access control SHOULD be imposed on a Controller's Witnesses with Multi-factor Authentication (MFA) such that a Witness will only endorse events with MFA. This provides a threshold structure where an attacker must also compromise the access integrity of a sufficient number of Witnesses.

4.3 Signature Verification Infrastructure

An attack against signature verification infrastructure typically requires replacing the signature verification code with malicious code that falsely reports signature verification on signed statements. KERI provides a specific protection mechanism for signature verification via a Watcher pool where an event is only accepted as verified if a sufficient majority of the Watchers in a pool agree on the verification status of the signature(s) on that event. This provides a threshold structure where an attacker must compromise the code integrity of a sufficient number of Watchers for successful attack. Because the composition of a Watcher pool does not need to be publicly disclosed, an attacker must also discover that composition to ensure a successful attack.

1. Best practices for code delivery and library usage MUST be observed for signature verification infrastructure. Because the signature verification infrastructure need never be publicly disclosed an attacker must first discover what computing devices are being used to verify signatures.
2. Either a TEE or a Watcher pool or both SHOULD be used to protect a signature verification infrastructure. The entity harmed primarily by a compromise of a signature verification infrastructure is the Verifier, not the Controller, and the degree of protection should be commensurate with the degree of risk associated with faulty verification.

5 GLEIF KERI Profile

This section specifies policies for GLEIF's own use of KERI.

5.1 GLEIF Root AID Inception Event

1. GLEIF MUST hold a recorded GLEIF Root AID genesis event with at least a minimum of three Witnesses.

   The OOBI for the KEL for the GLEIF Root AID: (https://www.gleif.org/.well-known/keri/oobi/EDP1vHcw_wc4M__Fj53-cJaBnZZASd-aMTaSyWEQ-PC2)

   a. MUST be stored on the following GLEIF servers protected by extended validation HTTPS certificates:

      i. EU-FI-HTZ-01 65.21.253.212 Prod 1 Helsinki

      ii. NA-CA-OVH-01 51.79.54.121 Prod 1 Canada

      iii. AF-ZA-AZR-01 102.37.159.99 Prod 1 South Africa

      iv. SA-BR-AWS-01 54.233.109.129 Prod 1 Brazil

      v. AS-CN-ALI-01 8.210.213.186 Prod 1 China

      vi. OC-AU-OVH-01 51.161.130.60 Prod 2 Sydney

      vii. NA-US-HTZ-01 5.161.49.239 Prod 2 Ashburn

      viii. AS-JP-AZR-01 20.78.61.227 Prod 2 Japan

      ix. AF-ZA-AWS-01 13.244.119.106 Prod 2 South Africa

      x. EU-UK-ALI-01 8.208.27.153 Prod 2 United Kingdom

   b. MUST be stored at the HTTPS URLs of the following affiliated organizations:

      i. Qualified vLEI Issuers

   c. MUST be stored as a file on a public GLEIF GitHub repository.

   d. MUST be shared on the following social media:

      i. LinkedIn and X (formerly Twitter)

5.2 GLEIF Root AID

1. Non-delegated pre-rotated keys are at the root level of the delegation hierarchy and MUST have the very highest level of protection.
2. The GLEIF Root AID MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.
3. Key Pair Creation and Storage Infrastructure MUST be within a TEE.
4. Each key-pair in a thresholded multi-sig MUST use a non-co-located TEE.
5. Signature Creation Infrastructure SHOULD be within a TEE.

6. Signature Verification Infrastructure SHOULD be within a TEE.

5.3 GLEIF Root Witness Pool

1. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.
2. The number of Witnesses on any single web host provider MUST be less than the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)
3. The number of Witnesses on any single continent MUST be less than the sufficient threshold as per KAACE.
4. The number of Witnesses in any single political jurisdiction MUST be less than the sufficient threshold as per KAACE.
5. GLEIF Root Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents.
6. The secrets in the key store MUST be encrypted with the key loaded dynamically whenever the Witness service is started.
7. The key store MUST reside on a different device or host from that of the Witness service.
8. The Witness encryption key store SHOULD be a Hardware Security Module (HSM).
9. The Witness signing key store MAY be a TEE.

5.4 GLEIF Internal Delegated AIDs (GIDAs)

The GLEIF Internal AID is the identifier used by GLEIF to be able to participate in the vLEI Ecosystem and Infrastructure as a vLEI Holder. The policies for GIDAs are identical to the policies for the GLEIF Root AID except:

1. Key Pair Creation and Storage Infrastructure SHOULD be within a TEE.
2. Each key-pair in a thresholded multi-sig SHOULD use a non-co-located TEE.

5.5 GLEIF External Delegated AIDs (GEDAs)

These policies are used by GLEIF to issue the Qualified vLEI Issuer vLEI Credentials and Qualified vLEI Issuer Delegated AIDs. The policies for the GEDAs are the same as GLEIF Internal Delegated AID policies except:

1. GLEIF MUST set the Do Not Delegate configuration property on Qualified vLEI Issuer Delegated AIDs.

   NOTE: This may change in the future to enable horizontal scalability.

5.6 GLEIF Witness Network

These policies are for issuance and revocation state of vLEIs.

1. GLEIF MUST set up and maintain its own Witness pool.

5.7 GLEIF Watcher Network

1. The GLEIF Watcher Network SHOULD be protected by a Watcher pool of at least 3 members with a threshold of 2.
2. Larger pool sizes MUST use KAACE sufficient majority thresholds.
3. The GLEIF Watcher Signing Key Pair key store MAY reside on the Watcher Service host but MUST use dedicated user only permissions on the key store directory and its contents.
4. The secrets in the key store SHOULD be encrypted with the key loaded dynamically whenever the Watcher service is started.
5. When used, the encryption key store MUST reside on a different device or host from that of the Watcher service.
6. The Watcher encryption key store MAY be an HSM.
7. The Watcher signing key store MAY be a TEE.

5.8 GLEIF Key Management

1. The specific holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.
2. Signing keys SHOULD be rotated prophylactically no more often than once every six months and no less often once every two years but on an unpredictable schedule.
3. Signing keys MUST be rotated whenever there is a likelihood of key compromise.
4. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.
5. Encryption keys protecting private keys SHOULD be rotated prophylactically at least quarterly and MUST be rotated whenever the associated signing key store host configuration changes.
6. GLEIF policies for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier:
    a. MUST use an OOB (out-of-band) MFA (multi-factor authorization) mechanism to approve Delegated AID rotation;
    b. SHOULD use an off-the-shelf MFA tool.

6 Qualified vLEI Issuer KERI Profile

This section specifies the KERI policies that apply to Qualified vLEI Issuers.

6.1 Qualified vLEI Issuer Distribution

1. GLEIF SHOULD encourage and promote a diverse distribution of Qualified vLEI Issuers across political jurisdictions and geographies.

6.2 Delegated AIDs

1. For added security, Qualified vLEI Issuers:
    a. MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.
    b. MUST use at least multi-sig scheme of at least 3 signers with a threshold of 2.
    c. MAY use a TEE to protect their Delegated pro-rotated AID keys.
2. Key Pair Creation and Storage Infrastructure SHOULD be within a TEE.
3. Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.
4. Signature Creation Infrastructure SHOULD be within a TEE.
5. Signature Verification Infrastructure SHOULD be within a TEE.

6.3 Endorser Support: Witness Pool or Ledger Registrar

1. An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement.

6.3.1 Witness Pool

1. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.
2. The Witness Signing Key Pair key store MAY reside on the Witness Service host but MUST use dedicated user only permissions on the key store directory and its contents.
3. The secrets in the key store SHOULD be encrypted with the key loaded dynamically whenever the Witness service is started.
4. The encryption key store MUST reside on a different device or host from that of the Witness service.
5. The Witness encryption key store SHOULD be an HSM.
6. The Witness signing key store MAY be a TEE.

6.3.2 Ledger Registrar

1. The Registrar Signing Key Pair key store MAY reside on the Registrar Service host but MUST use dedicated user only permissions on the key store directory and its contents.

2. The secrets in the key store SHOULD be encrypted with the key loaded dynamically whenever the Registrar service is started.
3. The encryption key store MUST reside on a different device or host from that of the Registrar service.
4. The Registrar encryption key store SHOULD be an HSM.
5. The Registrar signing key store MAY be a TEE.

6.4 Watchers

1. Watchers SHOULD be protected by a Watcher pool of at least 3 members with a threshold of 2.
2. Larger pool sizes MUST use KAACE sufficient majority thresholds.
3. Watcher Signing Key Pair key store MAY reside on the Watcher Service host but MUST use dedicated user only permissions on the key store directory and its contents.
4. The secrets in the key store SHOULD be encrypted with the key loaded dynamically whenever the Watcher service is started.
5. When used, the encryption key store MUST reside on a different device or host from that of the Witness service.
6. The Watcher encryption key store MAY be an HSM.
7. The Watcher signing key store MAY be a TEE.

6.5 Key Management

1. The specific holders of cryptographic keys MUST be kept confidential and shall be determined by Qualified vLEI Issuer internal policy.
2. Signing keys SHOULD be rotated prophylactically no more often than once every six months and no less often once every two years but on an unpredictable schedule.
3. GLEIF External GARs (GLEIF Authorized Representatives) MUST approve a QVI Rotation Event that occurs no less than six months from the last QVI Rotation Event.
4. Qualified vLEI Issuer Authorized Representatives (QARs) MUST contact GLEIF External GARs for approval of any QVI Rotation Event that occurs less than six months from the last QVI Rotation Event.
5. Signing keys MUST be rotated whenever there is a likelihood of key compromise.
6. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.
7. Encryption keys protecting private keys SHOULD be rotated prophylactically at least quarterly and MUST be rotated whenever the associated signing key store host configuration changes.

6.6 Delegation

1. The Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to True. (NOTE: This may change in future versions in order to accommodate horizontal scalability of the vLEI signing infrastructure.)

6.7 Key Compromise Monitoring

Qualified vLEI Issuers:

1. MUST monitor their public Witnesses for their vLEI issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to inform their key management process that a key recovery may be required.
2. SHOULD provide a capability for challenging the issuance, revocation or data contained within vLEIs.

6.8 Key Compromise Recovery

In case of key compromise:

1. A Qualified vLEI Issuer MUST:
    a. Report to GLEIF all key compromise recovery operations within 24 hours of gaining knowledge of the key compromise.
    b. Investigate as expeditiously as possible at its own expense the source of the key compromise and make a full report of the investigation to GLEIF.
    c. Make a recovery Rotation Event that forks their KEL and submit the recovering Rotation Event and signatures to GLEIF in order that GLEIF may anchor a confirmation seal in its KEL.
    d. Send a key recovery event explanation to GLEIF for publication in GLEIF's public registry of Qualified vLEI Issuer recovery events.

2. GLEIF MAY at its sole discretion:
    a. Publicly disclose the compromise.
    b. Reissue all compromised vLEI Credentials at the sole expense of the Qualified vLEI Issuer regardless of any contractual terms to the contrary.

6.9 vLEI Issuance and Revocation Policies

1. Qualified vLEI Issuers MUST monitor their public Witnesses for their vLEI issuance and revocation registry for erroneous or malicious issuances and revocations (primarily issuances) in order to inform their key management process that a key recovery may be required.

6.10 Challenge Message Policies

In various policies throughout this Governance Framework, Challenge Messages are required for cryptographic authentication during real-time Out of Band Introduction (OOBI) sessions.

1. The Challenge Message MUST include a cryptographic once generated in real time.
2. The Challenge Response Message MUST be Fully Signed by the Responder.
3. The Challenger MUST verify that:
    a. The Fully Signed Response contains the same cryptographic once as the Challenge Message.
    b. The signatures of the Responders were generated by the private keys that control Responder's AID.

6.11 Policies for Sharing Authenticated AIDs

When new GARs of the GLEIF External AID or GLEIF Internal AID or QARs of the a Qualified vLEI Issuer AID are rotated into the the GAR or QAR group multisig AID, it will be necessary for the the new GARs/QARs to prepopulate their local database with contact information for authenticated AIDs from the existing GARs /QARs database.

1. Contact sharing with new members of a group multisig AID MUST be performed by a threshold satisfying number of existing members.
2. New members MUST be able to Spot Check through Identity Authentication and the Challenge Response process any new authenticated AID they receive from existing members or their new group multisig AID.