The vLEI Ecosystem Governance Framework MUST provide GLEIF’s role to support and contribute to a global, persistent organizational identity to a public good.

Policy:

1. An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement.
2. Larger pool sizes MUST use KAACE sufficient majority thresholds.
3. Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.
4. All QVIs MUST successfully complete Annual vLEI Issuer Qualification.
5. QVIs MUST ensure that third-parties comply with the vLEI Ecosystem Governance Framework when providing vLEI services to all revisions of the vLEI Ecosystem Governance Framework.
6. All QVIs MUST confirm that the digital identity of vLEI data has been uniquely, having only one global identity and this identity should include a digital identity.
7. All QVIs MUST ensure that third parties comply with the vLEI Ecosystem Governance Framework when providing vLEI services to the Primary Document.
8. All QVIs MUST ensure that third parties comply with the vLEI Ecosystem Governance Framework when providing vLEI services to all revisions of the vLEI Ecosystem Governance Framework.
9. All revisions to the Primary Document MUST be identified with a revision number that is a sequential integer.

The specific holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.

Investigate as expeditiously as possible at its own expense the source of the key compromise and make a full report on the investigation.

The vLEI Ecosystem Governance Framework MUST support GLEIF’s intention to deliver the vLEI infrastructure using a technology architecture compliant with FIDO2, W3C Standards, and compliant with FIDO2, W3C Standards.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

Each key-pair in a thresholded multi-sig MUST use a non-co-located key store.

The vLEI Ecosystem Governance Framework MUST provide GLEIF’s role to support and contribute to a global, persistent organizational identity to a public good.

The specific holders of cryptographic keys MUST be kept confidential and shall be determined by GLEIF internal policy.

Investigate as expeditiously as possible at its own expense the source of the key compromise and make a full report on the investigation.

The vLEI Ecosystem Governance Framework MUST support GLEIF’s intention to deliver the vLEI infrastructure using a technology architecture compliant with FIDO2, W3C Standards, and compliant with FIDO2, W3C Standards.
vLEI Issuance and Revocation Policies
1. Qualified vLEI Issuers MUST monitor their public VDR for their vLEI or VC 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.

Challenge Message
1. The Challenge Message MUST include a cryptographic nonce generated in real time.

3. The Challenge Response Message MUST be Fully Signed by the Responder.

4. The Challenger MUST verify that:
   a. The Fully Signed Response contains the same cryptographic nonce as the Challenge Message.
   b. The signatures of the Responders were generated by the private keys that control the Responder’s AID.

Qualified vLEI Issuer Delegation
1. The Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to True.

Qualified vLEI Issuer Key Compromise Monitoring
1. Monitor all key compromise inquiries immediately and inform the key management team of any compromise.

Qualified vLEI Issuer Key Compromise Recovery
1. In any case of key compromise, 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, make a full report of the investigation to GLEIF, and maintain such records for at least three years.
   c. Keep all records and information that are relevant to and resulting from both key compromise and key recovery operations.
   d. Make key recovery operations transparent for publication in GLEIF’s public registry of Qualified vLEI Issuer recovery events.

Signing Keys
1. Signing keys MUST be rotated whenever there is a likelihood of key compromise.

2. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.

Qualified vLEI Issuer Key Compromise Monitoring
1. Qualified vLEI Issuers MUST monitor their public VDR for their vLEI or VC 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.

Qualified vLEI Issuer Key Compromise Recovery
1. In any case of key compromise, 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, make a full report of the investigation to GLEIF, and maintain such records for at least three years.
   c. Keep all records and information that are relevant to and resulting from both key compromise and key recovery operations.
   d. Send a key recovery event explanation to GLEIF for publication in GLEIF’s public registry of Qualified vLEI Issuer recovery events.
2. Qualified vLEI Issuers MUST successfully install, test and implement the GLEIF-supplied vLEI software within stated timeframes.

1. GLEIF MUST provide technical changes/upgrades to Qualified vLEI software to Qualified vLEI Issuers.

Developer Security Policies

2. GLEIF and Qualified vLEI Issuers MUST maintain records to evidence the availability of their services.

1. GLEIF and Qualified vLEI Issuers MUST maintain defined availability targets as part of the vLEI Ecosystem Governance Framework.

Availability Policies

2. Qualified vLEI Issuers MUST define and execute an appropriate response plan to investigate suspected unauthorized access to vLEI Data. This plan MUST include procedures and forms that GLEIF and the Qualified vLEI Issuers use responsive to communicate security events and their disposition.

vLEI Data. This plan MUST include procedures and forms that GLEIF and the Qualified vLEI Issuers use responsively to communicate security events and their disposition.

2. vLEI Ecosystem Member employment verification policies and procedures MUST include, but may not be limited to, criminal background checks and proof of identity validation.

3. These policies MUST be mandatory for all employees of the vLEI Ecosystem Member involved with vLEI Transactions or vLEI Data. The vLEI Ecosystem Member MUST designate its Information Security Manager or another Office to provide reasonable oversight for such policies, including formal governance and management, employee education, and compliance verification.

4. vLEI Ecosystem Member employment verification policies and procedures MUST include, but may not be limited to, criminal background checks and proof of identity validation.

5. Qualified vLEI Issuers MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this document.

6. Qualified vLEI Issuers MUST confirm that they respect and comply with data protection legislation as applicable and as evidenced in the Annual vLEI Issuer Qualification.

7. Qualified vLEI Issuers MUST make available evidence of stated compliance with these policies and any relevant accreditations document.

8. vLEI Ecosystem Member Privacy Policies

9. Qualified vLEI Issuers MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this document.

10. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

11. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

12. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

13. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

14. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

15. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

16. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

17. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

18. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

19. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

20. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

21. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

22. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

23. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

24. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.

25. Requirement satisfied by vLEI Issuer Qualification, including certificates, attestations, or reports mirroring how accredited third-party audits, such as ISO 27001, Statement on Standards for Information and Services Organization (SSO), or other industry standards.
4. The encryption key store MUST reside on a different device or host from that of the Witness service.

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. The secrets in the key store MUST be encrypted with the key loaded into the key store.

1. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.

3. The number of Witnesses on any single continent MUST be less than 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 number is based on the number of vLEIs issued in the last year, the threshold is subject to change).

1. Non-delegated pre-rotated keys are at the root level of the delegation hierarchy and MUST have the very highest level of protection. This level of protection should be commensurate with the value of the assets these keys are protecting.

2. The KEL for the GLEIF Root AID Genesis Event:

a. The KEL for the GLEIF Root AID Genesis Event:

b. The KEL for the GLEIF Root AID Genesis Event:

1. Key Pair Creation and Storage Infrastructure MUST be within a TEE.

2. The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.

3. The number of Witnesses on any single web host provider MUST be less than the sufficient threshold as per KAACE.

2. New versions MUST be implemented within a period 12 months after final approval of the new version, unless otherwise specified by the governing body.

1. The next or pre-rotated set of keys MUST be protected with the highest level of protection. This level of protection and the associated key store MUST use dedicated user only permissions on the key store directory and its contents. The secrets in the key store MUST be encrypted with the key loaded into the key store.

4. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.

1. For added security, Qualified vLEI Issuers:

**Table 1:**

<table>
<thead>
<tr>
<th>Requirement satisfied by vLEI Ecosystem Governance Framework</th>
<th>Requirement satisfied by ISO 30113 Certification Program</th>
<th>Requirement satisfied by vLEI Certification Program</th>
<th>Requirement satisfied by ISO 30118 Certification Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Issuer role within the GLEIF AID issuance and lifecycle process</td>
<td>1. By the issuer</td>
<td>1. By the issuer</td>
<td>1. By the issuer</td>
</tr>
<tr>
<td>4. The encryption key store MUST reside on a different device or host from that of the Witness service, unless otherwise specified by the governing body in a new version of the vLEI Issuer Governance Framework.</td>
<td>4. Statement and demonstration of compliance</td>
<td>4. Controlled by the vLEI Management Architecture</td>
<td>4. Controlled by the vLEI Management Architecture</td>
</tr>
<tr>
<td>2. After upgrading to a new version, issuers MUST begin using any new features changes until the end of the three month period to adopt new versions. For example, vLEI ID MUST be compatible with v0 and the end of the v1.0 adoption period. It will need to be suitably spaced before the v1.0 compliance</td>
<td>2. Statement and demonstration of compliance</td>
<td>2. Controlled by the vLEI Management Architecture</td>
<td>2. Controlled by the vLEI Management Architecture</td>
</tr>
<tr>
<td><strong>Section 4:</strong> Qualified vLEI Issuer Ledger Registrar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Qualified vLEI Issuer Ledger Registrar MUST be used in v1.0 compatible mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Qualified vLEI Issuer Ledger Registrar MUST be used in v1.0 compatible mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Qualified vLEI Issuer Ledger Registrar MUST be used in v1.0 compatible mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Qualified vLEI Issuer Ledger Registrar MUST be used in v1.0 compatible mode.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1:** GLEIF Key Management Policies

- The Witness Pool configuration MUST include a minimum of 5 with the sufficient threshold as per KAACE.
- The number of Witnesses on any single continent MUST be less than the sufficient threshold as per KAACE.
- The number of Witnesses on any single web host provider MUST be less than the sufficient threshold as per KAACE.
1. The specific holders of cryptographic keys MUST be kept confidential and shall be determined by Qualified vLEI Issuer internal policy.

2. Signing keys MUST be rotated whenever there is a likelihood of key compromise.

3. The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.

4. When used, the encryption key store MUST reside on a different device or host from that of the Witness service.

Qualified vLEI Issuer Delegation

1. The Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to True.

Qualified vLEI Issuer Key Compromise Recovery

1. In any case of key compromise, 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 in order to both identify the key holder and recover the key.
   c. Make a key recovery event explanation that is signed by the key holder and submit the signed recovery event to GLEIF in order to announce the key recovery event in GLEIF's public registry of Qualified vLEI Issuer recovery events.
   d. Send a key recovery event explanation to GLEIF for publication in GLEIF's public registry of Qualified vLEI Issuer recovery events.

Qualified vLEI Issuance and Revocation Policies

1. Qualified vLEIs MUST monitor their public VDR for their vLEI or VC 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.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. All vLEI Credential schema MUST be ACDC compliant.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. All vLEI Credentials MUST include an ACDC version string field.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. All vLEI Credentials MUST include a SAID (as evidence of immutability).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Issuer and holder identifiers MUST be KERI AIDs that use the did:keri Method.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. All vLEI Credentials MUST include an ACDC version string field.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. All vLEI Credentials MUST be in compliance with its specific vLEI Credential Governance Framework.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. vLEI Issuer Event Streaming Representation (CESR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. The Proof Format for all Credentials MUST comply with the OASIS Proof Format specification.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Each vLEI Issuer MUST maintain a highly available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. All vLEI Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Security and Privacy**

1. All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.
2. All vLEI Credential schema MUST be ACDC compliant.
3. All vLEI Credentials MUST include an ACDC version string field.
4. All vLEI Credentials MUST include a SAID (as evidence of immutability).

**vLEI Credential Schema**

1. vLEI Credential schema MUST be compliant the SAID and SIS specifications.
2. All vLEI Credential schema MUST include a SAID (as evidence of immutability).
3. Each vLEI Credential MUST be in compliance with its specific vLEI Credential Governance Framework.
3.1. Each vLEI Credential MUST be chained to its source(s), if any, as required by the applicable vLEI Credential Governance Framework in accordance with the ACDC specification.

**Composable Event Streaming Representation (CESR)**

1. The Proof Format for all Credentials MUST comply with the OASIS Proof Format specification.
2. Each vLEI Issuer MUST maintain a highly available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.
3. All vLEI Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.

**Credential Registry and Revocation Registry Requirements**

1. Each vLEI Issuer MUST maintain a highly available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.

**Compliance**

1. Each vLEI Issuer’s ACDC certificates chain MUST be signed by a trusted authority in a new version of the vLEI Ecosystem Governance Framework.
The following steps MUST be performed in the order listed and completed during this OOBI session for each of the two
pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters
that there is a mutual live presentation by all participants that verifies their live participation in the session.

3. The service MUST be recorded and the recording stored in high-security storage.

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

1. Each Root AID GLEIF Authorized Representative (Root GAR) MUST generate its own single signature AID that is
designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the
Internal Delegated AID Inception Event and publish this to the Internal GARs and to the Delegated AID Witnesses

j. The Internal GAR Lead MUST select the AIDs from the set of Internal GARs for the ordered set of authorized
participants for both the current and next set and threshold of participants.

i. GLEIF MUST establish a list of initial GLEIF Controllers that specifies:

a. Which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

b. Which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

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

d. Each External GAR MUST verify in real-time that a response to the Challenge Message was received from every
External GAR, which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

e. Each Root AID Witness MUST verify that the Root AID transition event is fully arrived at by every Root AID Witness.

f. Each Root GAR MUST verify that the Root AID transition event is fully arrived at by every Root AID Witness:

1. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key
pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters
that there is a mutual live presentation by all participants that verifies their live participation in the session.

2. Each Internal 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.

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

h. The Root GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF External Delegated AID and the Delegated AID Witness pools:

a. Each of the Internal GARs MUST be designated as the Internal Delegated AID GLEIF Authorized Representative (Internal GAR) for each of the
Internal Delegated AID Inception Event.

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

c. Each Internal GAR MUST verify the signature of every other Internal GAR, which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

d. Each Internal GAR MUST verify the signature of every other Internal GAR, which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

2. The Root GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF Root AID and the Delegated AID Witness pools:

3. The Internal GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF Internal Delegated AID and the Delegated AID Witness pools:

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

a. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key
pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters
that there is a mutual live presentation by all participants that verifies their live participation in the session.

b. Each Root AID GLEIF Authorized Representative (Root GAR) MUST generate its own single signature AID that is
designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the
Internal Delegated AID Inception Event and publish this to the Internal GARs and to the Delegated AID Witnesses

j. The Internal GAR Lead MUST select the AIDs from the set of Internal GARs for the ordered set of authorized
participants for both the current and next set and threshold of participants.

i. Each Root AID GLEIF Authorized Representative (Root GAR) MUST generate its own single signature AID that is
designated by that Inception Event. The published Inception Event includes as an attachment OOBIs for each of the
Internal Delegated AID Inception Event and publish this to the Internal GARs and to the Delegated AID Witnesses

h. The Internal GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF Internal Delegated AID and the Delegated AID Witness pools:

7. Release of Internal AID Witness Information:

6. Creation of GLEIF Internal Delegated AID:

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

2. Each Internal GAR MUST verify the signature of every other Internal GAR, which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

1. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key
pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters
that there is a mutual live presentation by all participants that verifies their live participation in the session.

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

The following steps MUST be performed in the order listed and recorded during the OOBIs as evidence for the Root GAR
service endpoint whereby the other Root GARs may obtain the Key Event Log (KEL) of its participating AID.

h. The Internal GAR Lead MUST select the AIDs and Service Endpoints from the GLEIF Internal Delegated AID and the Delegated AID Witness pools:

2. Each Internal GAR MUST verify the signature of every other Internal GAR, which Controllers shall control the GLEIF Root AID, the GIDA and the GEDA.

1. An AID conformant with this Governance Framework MUST be created from two sets of asymmetric signing key
pairs and a cryptographic digest of second set of key pairs, as well as any other identifiers and configuration parameters
that there is a mutual live presentation by all participants that verifies their live participation in the session.
The following steps MUST be performed in the order listed and completed during the 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) in section 9.

1. Rotation Event to delegate the GLEIF External Delegated AIDs

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

   b. The External GAR Lead MUST select the AIDs from the set of External GARs for the ordered set of authorized participant witnesses.

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

   d. The QAR Lead MUST select the AIDs from the set of QARs for the ordered set of authorized participant witnesses.

   e. Each QAR MUST verify the set of Witness endpoints for the GEDA.

   f. Each QAR MUST send a Challenge Message to every other QAR as defined in the Technical Requirements Part 1 of the Governance Framework.

   g. Each QAR MUST verify the set of Witness endpoints for the GLEIF External Delegated AID.
Credential Schema

The QVI vLEI Credential MUST contain the LEI of the QVI.

Involuntary revocation of vLEI Credentials MUST follow the process specified in Appendix 5, Service Level Agreement (SLA).

Involuntary Revocation

1. A QVI Identity Verification is completed as required in section 6.3.
2. The External GAR issues a QVI vLEI Credential after completion of QVI Identity Verification in section 6.3.
3. The External GAR uses a QVI vLEI Credential to connect the QVI to the GLEIF-supplied vLEI software.
4. The QVI MUST designate a QAR to act on its behalf.
5. The QAR MUST perform manual verification of the QAR's legal identity for which the External GAR is acting as its agent.
6. The QAR MUST perform revocation process with KERI as described in section 7.2.1.
7. The QVI vLEI Credential MUST include a reference to one or more preceding vLEIs in its provenance chain.
8. If any preceding vLEIs in the provenance chain or a given vLEI is revoked, then that given vLEI MUST not verify.

Issuance

QVI Identity Verification

The Issuer MUST:

- Issue the QVI vLEI Credential to the QVI.
- The Issuer MUST include a reference to one or more preceding vLEIs in its provenance chain.
- The Issuer MUST perform revocation process with KERI as described in section 7.2.1.
- The Issuer MUST ensure that all sub-signatures of the Issuer vLEI are signed using the Issuer vLEI.
- The Issuer MUST ensure that the Issuer vLEI is signed using the Issuer vLEI.
The Issuer MUST:

- a. The Legal Entity MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

1. Issuance

- a. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

2. Identity Verification

- a. The Issuer MUST verify the complete set of signatures.
- b. The Issuer MUST perform 3-factor authentication in conjunction with 2-factor authentication.
- c. The Issuer MUST keep all Challenge Messages unique to the OOBI session.
- d. The Issuer MUST implement a revocation process with KERI.
- e. The Issuer MUST implement the vLEI Reporting API to enable QVIs to report each issuance event of Legal Entity vLEI Credentials.

3. Legal Entity AID

- a. A LAR MUST use an OOBI protocol such as a QR code or live chat to share the Legal Entity AID with the QAR.
- b. A LAR MUST use the Legal Entity AID to verify the Identity Assurance level of the Legal Entity.
- c. A LAR MUST use the Legal Entity AID to verify the registration status for the Legal Entity.
- d. A LAR MUST verify the complete set of signatures.

4. Qualification to be satisfied by ISO 20000 Certification

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

5. Requirement satisfied by vLEI Issuer Qualification Program

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

6. Requirement satisfied by UDI Implementation Framework

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

7. Requirement satisfied by vLEI Ecosystem Governance Framework

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

8. Requirement satisfied by Trust Assurance Framework

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

9. Requirement satisfied by vLEI Ecosystem Governance Framework

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

10. Requirement satisfied by KERI Operations

- a. The Issuer MUST satisfy the minimum Legal Entity qualification level of the vLEI Ecosystem.
- b. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
- c. The Issuer MUST meet the requirements specified in the vLEI Issuer Qualification Program.
- d. The Issuer MUST be a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.
6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework. The following text MUST appear in the Rules section of the Authentic Chained Data Container (ACDC) vLEI Credentials.

GLEIF MUST monitor the QVI Transaction Event Logs (TELs) to detect the issuance or revocation of OOR vLEI Credentials which

Monitoring

A QAR MUST call the vLEI Reporting API with each issuance event of OOR vLEI Credentials for which the Legal Entity has

Issuance

A QAR MUST use the OOR Person’s Private Key (PK) to sign the OOR vLEI Credential and publish it to the OOR vLEI Credential database. An IDA in a credential wallet MUST be set up for the OOR Person.

Part 2 for the purposes of cryptographic authentication of the OOR Person’s AID.

Another ODR may request the OOR vLEI Credential to be updated after OOR vLEI Credential issuance is complete. A QAR MUST perform revocation within the timeframe specified in Appendix 5, Qualified vLEI Issuer Service Level Agreement (SLA).

A QAR MUST use an ODR protocol (such as a QR code or live chat) to share the QVI Autonomic Identifier (QVI-AID) with the OOR Person. The QVI-AID includes the Claims marked as Required in section 8.1.

In addition, a Qualified vLEI Issuer (QVI) that has been contracted by a Legal Entity holding a valid Legal Entity vLEI Credential to

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance

Qualified vLEI Issuer compliance
6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.

Issuance of a valid vLEI Credential only establishes that the information in the requirements in the Identity Verification sections, A QAR MUST perform identity assurance of an ECR Person at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A. (See Appendix A for a table of IALs.)

The Issuer MUST:

1. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

2. A workflow MUST be implemented in the operations of the QVI which requires, prior to issuing and signing an ECR vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

5. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before

1. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

2. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

3. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

4. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

5. The Legal Entity MUST perform the Trust Assurance Step as defined in section 6.5 and complete the AIA for the ECR vLEI Credential

6. A QAR Authorized Representative (QAR) MUST verify in real time that the response to the Challenge Message was received from the ECR Person

7. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the QAR vLEI Credential holder's AID with the ECR Person.

8. The QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity. This check is covered as part of the Credential issuance process with KERI

9. The Legal Entity vLEI Credential holder's AID MUST be used to enroll the Legal Entity's vLEI Legal Entity vLEI Credential that has delegated the issuance of ECR vLEI Credentials

10. The Legal Entity and ECR Person Identity Verification process outlined in sections 6.3 and 6.5 MUST be completed before