The vLEI Ecosystem Governance Framework MUST enable vLEIs to be issued to any Legal Entity issued a LEI in the Global LEI System.

GLEIF MUST not provide funds of any form whatsoever for QVI operations.

The QVI MUST ensure that its operations regarding vLEIs are sustainably financed.

There MUST be availability targets defined for all vLEI services included in the Appendix 5 of the vLEI Issuer Qualification.

All revisions to the vLEI Ecosystem Governance Framework MUST be approved by GLEIF using its Change Management Process.

All revisions to Controlled Documents MUST be identified with a revision number that is a sequential integer.

All revisions to the Primary Document MUST be identified with a revision number that is a sequential integer.

QVIs MUST ensure that third parties comply with the vLEI Ecosystem Governance Frameworks when providing vLEI services to a Legal Entity.

All LEIs contained in vLEIs MUST maintain a LEI Entity Status of Active and a LEI Registration Status of Issued, Pending Transfer or Withdrawn in the Global LEI System.

Nothing in the vLEI Ecosystem Governance Framework SHOULD require vLEI Ecosystem stakeholders to breach applicable law in order to perform its obligations under the vLEI Ecosystem Governance Framework.

vLEI Issuers MUST verify that a Holder’s Autonomic Identifier (AID) is controlled by the Holder.

vLEI Issuers MUST provide verifiable proof of the authenticity of their digital identity data.

The vLEI Ecosystem Governance Framework MUST ensure the protection of digital identity data when applicable.

The vLEI Ecosystem Governance Framework MUST enable interoperability, for the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST ensure that vLEIs are uniquely, having only one global identity and this identity should include a digital identity.

The vLEI Ecosystem Governance Framework MUST ensure that every Legal Entity in the Global LEI System regarding their entity and relationships.

The vLEI Ecosystem Governance Framework MUST fulfill GLEIF’s intention to make the vLEI infrastructure widely available as an open and non-proprietary approach and to use open source whenever possible.

The vLEI Ecosystem Governance Framework MUST deliver on GLEIF’s vision that every Legal Entity be able to be identified uniquely, having only one global identity and this identity should include a digital identity.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST enable the digital identity data of an entity to be displayed, transmitted, processed, presented, and verified interoperably using open, public, and publicly transparent, as well as verifiable, the ability of identity rights holders to observe or trace a copy of their digital identity data to the entity or system of their choice.

The vLEI Ecosystem Governance Framework MUST ensure that vLEIs are uniquely, having only one global identity and this identity should include a digital identity.

The vLEI Ecosystem Governance Framework MUST ensure that every Legal Entity in the Global LEI System regarding their entity and relationships.

The vLEI Ecosystem Governance Framework MUST fulfill GLEIF’s intention to make the vLEI infrastructure widely available as an open and non-proprietary approach and to use open source whenever possible.

The vLEI Ecosystem Governance Framework MUST deliver on GLEIF’s vision that every Legal Entity be able to be identified uniquely, having only one global identity and this identity should include a digital identity.
2. Qualified vLEI Issuers MUST successfully install, test and implement the GLEIF-supplied vLEI software within stated timeframes.

Qualified vLEI Issuers MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this policy as evidenced in the Annual vLEI Issuer Qualification.

If a Qualified vLEI Issuer uses third-party providers in functions that involve the handling of vLEI Data, the Qualified vLEI Issuer also adequately addresses physical security and entry control according to industry best practices.

If a Qualified vLEI Issuer performs handling of vLEI Data in its own data center, the Qualified vLEI Issuer’s security policies MUST provide for timely detection of security incidents, and immediately report any security events and their disposition.

The vLEI Ecosystem’s Internal Control Environment (EIR) is certified as part of GLEIF’s ISO 20000 Certification during vLEI Issuer Qualification, including certification, evaluation, in scope resulting from accredited third-party audits, such as ISO 27001, Statement on Compliance for Information Security Officers (SSAE SOC 2), or other industry standards.

4. Qualified vLEI Issuers MUST maintain and follow documented incident response procedures and guidelines for computer security events and their disposition.

5. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.

6. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.

7. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.

8. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.

9. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.

10. Qualified vLEI Issuers MUST maintain and follow documented information security policies and procedures. Change Management is followed by GLEIF and is certified as part of GLEIF’s ISO 27001 Certification during vLEI Issuer Qualification.
<table>
<thead>
<tr>
<th>Section</th>
<th>Sub-section</th>
<th>There are no 'MUST' Statements in the Governance Requirements Controlled Document</th>
<th>Requirement satisfied by vLEI Ecosystem Governance Framework</th>
<th>Requirement to be satisfied by ISO 20000 Certification</th>
<th>Requirement satisfied by vLEI Issuer Qualification Program</th>
</tr>
</thead>
</table>
## Business Requirements

1. There MUST be availability targets defined for all vLEI services included in Appendix 5 of the vLEI Issuer Qualification Agreement, Qualified vLEI Issuer Service Level Agreement (SLA).
2. The QVI MUST be solely responsible for managing the revenue that is produced and the costs that are incurred in the running of its vLEI operations.
3. The GLEIF MUST not contribute funds of any form whatsoever for QVI operations.
An Endorser MUST use either a Witness Pool or a Ledger Registrar for Endorsement

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

GLEIF policies for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier:

- The time and place of key rotation MUST be kept confidential among the key holders until after the rotation has been completed.
- The rotated key MUST be protected from unauthorized access.
- The rotated key MUST be shared on the following social media:
- The rotated key MUST be stored as a file on a public GLEIF GitHub repository.
- The rotated key MUST be published to at least one ecosystem discovery mechanism.
- Both Authentic Chained Data Container (ACDC) Issuer and Issuee AIDs MUST be transferable.

The next or pre-rotated set of keys MUST be protected with the highest level of protection. This level of protection should be compatible with the value of the assets kept in the keys they are protecting.

Non-delegated pre-rotated keys are at the root level of a delegation hierarchy and MUST have the very highest level of protection.

The next or pre-rotated set of keys MUST be protected with the highest level of protection. This level of protection should be compatible with the value of the assets kept in the keys they are protecting.

Non-delegated pre-rotated keys are at the root level of the delegation hierarchy and MUST have the very highest level of protection.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

The rotated key MUST be published to at least one ecosystem discovery mechanism.

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

6.11 Policies

Policies

6.10 Challenge

Revocation
Issuance and

6.8 Key
Monitoring
Compromise

6.5 Key

6.4 Watchers

6.3.2 Ledger

6.3.1 Witness

2.
a.
3.
1.
1.
c.
a.
1.
1.
5.
4.
3.
1.
4.
3.
1.
5.
1.

The Challenger MUST verify that:

The Challenger MUST verify that:

The Challenger MUST verify that:

The Challenger MUST verify that:

The Challenger MUST verify that:

New members MUST be able to Spot Check through Identity Authentication and the Challenge Response process any new members.

Contact sharing with new members of a group multi-sig AID MUST be performed by a threshold satisfying number of existing members in order to inform their key management process that a key recovery may be required.

Qualified vLEI Issuers MUST monitor their public VDR 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.

Send a key recovery event explanation to GLEIF for publication in GLEIF’s public registry of Qualified vLEI Issuer recovery events.

GLEIF may anchor a confirmation seal in its KEL.

Make a recovery rotation event that forks their KEL and submit the recovering rotation event and signatures to GLEIF in order that an investigation to GLEIF.

Report to GLEIF all key compromise recovery operations within 24 hours of gaining knowledge of the key compromise.

In any case of key compromise, a Qualified vLEI Issuer MUST:

Encryption keys protecting private keys SHOULD be rotated prophylactically at least quarterly and MUST be rotated whenever the encryption key store directory and its contents.

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

Event that occurs less than six months from the last QVI Rotation Event.

GLEIF External GARs MUST approve a QVI Rotation Event that occurs no less than six months from the last QVI Rotation Event.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

The encryption key store MUST reside on a different device or host from that of the Registrar service.

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

Larger pools MUST use KAACE software remotely distributed.

When signing the new keys, new members should be added to the Witness service and their new keys and key commitments added to the key store.

New members MUST be able to Spot Check through Identity Authentication and the Challenge Response process any new members.

The Fully Signed Response contains the same cryptographic nonce as the Challenge Message.

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

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

The Key Recover event explanation to GLEIF for publication in GLEIF’s public registry of Qualified vLEI Issuer recovery events.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

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

The encryption key store MUST reside on a different device or host from that of the Witness service.

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

Larger pools MUST use KAACE software remotely distributed.

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

When used, the encryption key store MUST reside on a different device or host from that of the Registrar service.
## Requirement satisfied by vLEI

**Ecosystem Governance Framework**

**Requirement to be satisfied by ISO 20000 Certification**

**Requirement satisfied by vLEI Issuer Qualification Program**

1. **Credential Specifications**

   1.2 **Specification Version Upgrades**

   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.**

## Security and Privacy

1. **All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.**

2. **All vLEI Credential schema MUST be SIS compliant.**

3. **All instantiated vLEI Credentials MUST be ACDC compliant.**

4. **All SAIDs MUST use the cryptoBlake3-256 digest.**

## Requirements for vLEI ACDCs

1. **Issuer and Holder Identifiers MUST be KERI AIDs that use the did:keri Method.**

2. **All vLEI Credentials MUST include an ACDC version string field.**

3. **All vLEI Credentials MUST support JSON serialization.**

4. **All vLEI Credentials MUST include a SAID (as evidence of immutability).**

5. **The following ACDC sections MUST include a SAID – Attributes, data payload, sections, Reference source and Roles sections.**

   - Issuer MUST support the issuance of vLEI Credentials in any of all three forms.
   - 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.

## 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 Issuer MUST be in compliance with its specific vLEI Credential Governance Framework.**

4. **All vLEI credential Issuers MUST be in accordance with the ACDC specification.**

## Composable Event Streaming (CESR)

1. **The Proof Format for vLEI credentials MUST comply with the CESR Proof Format specification.**

## Credential Registry and Revocation Registry Requirements

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

## Exchange Protocols

1. **All vLEI credential Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.**
## 2. Official vLEI Credential Schema

### 2.1 Requirements

1. The digest algorithm employed for generating schema SAIDs MUST have an approximate cryptographic strength of 128 bits.

2. The SAID MUST be generated in compliance with the IETF-SAID internet draft specification and MUST be encoded using CESR. The CESR encoding indicates the type of cryptographic digest used to generate the SAID.

3. The schema MUST be JSON-Schema 2020-12 compliant. The table in 2.3 below provides the normative SAIDs for each of the official schema.
The following steps MUST be performed in the order listed and completed during the OOBi verification for the GLEIF Root AID to the External GAR Lead.

1. Creation of the External Delegated AID GLEIF Authorized Representative Pool

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

2. Creation of the External Delegated AID GLEIF Authorized Representative Pool

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

3. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

4. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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 GARs.

5. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

6. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

7. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

8. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

9. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

10. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

11. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

12. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

13. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

14. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

15. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

16. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

17. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

18. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

19. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

20. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

21. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

22. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

23. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

24. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

25. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

26. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

27. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

28. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

29. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

30. Creation of the Internal Delegated AID GLEIF Authorized Representative Pool

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

AIDs Delegated AID and GLEIF of GLEIF Root Publication

The following steps MUST be performed in the order listed and completed during the GLEIF 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 this section.

1. Each Internal GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.
2. Each Internal GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.
3. Each Internal GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that event and publish this to the other participating Internal GARs and to the Root AID Witnesses.
4. GLEIF Internal Delegated AID Inception Event, the Internal GAR Lead MUST generate a GLEIF Internal Delegated AID Rotation Event.

The set of publication points MUST include at least 4 of the list of publication points initially highlighted below:

- The HTTPS websites of all QVIs.
- The HTTPS website of the GLEIF Regulatory Oversight Committee.
- The GLEIF HTTPS website.
- The set of publication points MUST be published in a sufficiently strongly correlated and fault-tolerant manner to establish it as the unique AID for GLEIF.
- Each External GAR MUST verify that the Root AID Rotation Event is fully witnessed by every Root AID Witness.
- Each External GAR MUST sign and publish to the Root AID Witnesses their signature on the Root AID Rotation Event.
- Each External GAR MUST verify the set of public keys, the next public key digest, and delegated Inception Event digests in that event and publish this to the other participating External GARs and to the Root AID Witnesses.
- GLEIF External Delegated AID Inception Event, the External GAR Lead MUST generate a GLEIF External Delegated AID Rotation Event using the current public key, the next public key digest from each of the participating AID Rotation Events, and the digests of the AID Rotation Inception Events.
- A threshold satisficing subset of External GARs MUST each rotate their participating AIDs.
- The GLEIF Root AID and Delegated Internal and External AIDs MUST be published in a sufficiently strongly correlated and fault-tolerant manner to establish it as the unique AID for GLEIF.
- The requirement in GLEIF Identifier Management Operations.

Governance Framework

Operations
6.2 Credential Status: Final

6.3 QVI

6.7 QVI vLEI

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

The External GAR Lead then submits a request to issue the Qualified vLEI Issuer vLEI Credential to QVI vLEI to the External GAR Lead to perform Identity Assurance on the QARs.

External GAR multi-sig group trust External GAR Lead to anchor because the External GARs already have trusted the External GAR match those that the External GAR Lead verified according to section 6.3 above.

Unless otherwise pre-approved by the GLEIF Root GARs, GLEIF External AID MUST use an Interaction Event to approve the and the GEDA in the Delegated AID Inception Event.

Each QAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, Witness AIDs, and the GEDA, the QAR Lead MUST generate the QVI Delegated AID Inception Event and publish this to the other

Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated

The QAR Lead MUST select the AIDs from the set of QARs for the ordered set of authorized participant members in the multi-sig

The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

Infrastructure for the purposes of cryptographic authentication of their individual single signature AID. The Challenge Message

this provides the participating AID and the service endpoint whereby the other QARs may obtain the KEL of its participating AID.

An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.

The following steps MUST be performed in this order and completed during this OOBI session.

An External GAR and the QAR MUST establish a real-time OOBI session in which the External GAR and the QAR are present. An

An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.

The Issuer MUST ensure that the Issuer of the QVI vLEI Credential is GLEIF.

The following steps MUST be performed in this order and completed during this OOBI session.

An External GAR MUST identify an External GAR who will present to the QVI AID to the External GAR.

The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

An External GAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID to the External GAR.

The External GAR Lead then submits a request to issue the Qualified vLEI Issuer vLEI Credential to QVI vLEI to the External GAR Lead to perform Identity Assurance on the QARs.

External GAR multi-sig group trust External GAR Lead to anchor because the External GARs already have trusted the External GAR match those that the External GAR Lead verified according to section 6.3 above.

Unless otherwise pre-approved by the GLEIF Root GARs, GLEIF External AID MUST use an Interaction Event to approve the and the GEDA in the Delegated AID Inception Event.

Each QAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, Witness AIDs, and the GEDA, the QAR Lead MUST generate the QVI Delegated AID Inception Event and publish this to the other

Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated

The QAR Lead MUST select the AIDs from the set of QARs for the ordered set of authorized participant members in the multi-sig

The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

Infrastructure for the purposes of cryptographic authentication of their individual single signature AID. The Challenge Message

this provides the participating AID and the service endpoint whereby the other QARs may obtain the KEL of its participating AID.

An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.

The following steps MUST be performed in this order and completed during this OOBI session.

An External GAR and the QAR MUST establish a real-time OOBI session in which the External GAR and the QAR are present. An

An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.

The Issuer MUST ensure that the Issuer of the QVI vLEI Credential is GLEIF.

The following steps MUST be performed in this order and completed during this OOBI session.

An External GAR MUST identify an External GAR who will present to the QVI AID to the External GAR.

The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

An External GAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID to the External GAR.

The External GAR Lead then submits a request to issue the Qualified vLEI Issuer vLEI Credential to QVI vLEI to the External GAR Lead to perform Identity Assurance on the QARs.

External GAR multi-sig group trust External GAR Lead to anchor because the External GARs already have trusted the External GAR match those that the External GAR Lead verified according to section 6.3 above.

Unless otherwise pre-approved by the GLEIF Root GARs, GLEIF External AID MUST use an Interaction Event to approve the and the GEDA in the Delegated AID Inception Event.

Each QAR MUST verify the set of public keys, the next public key digest, the Witness identifiers, the threshold, the next threshold, Witness AIDs, and the GEDA, the QAR Lead MUST generate the QVI Delegated AID Inception Event and publish this to the other

Using the current public key and the next public key digest from each of the participating AID Inception Events, the Delegated

The QAR Lead MUST select the AIDs from the set of QARs for the ordered set of authorized participant members in the multi-sig

The QAR Lead MUST either configure or select the AIDs and Service Endpoints for the QVI Delegated AID Witness Pool.

Infrastructure for the purposes of cryptographic authentication of their individual single signature AID. The Challenge Message

this provides the participating AID and the service endpoint whereby the other QARs may obtain the KEL of its participating AID.

An QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI AID with the External GAR.

The following steps MUST be performed in this order and completed during this OOBI session.

An External GAR and the QAR MUST establish a real-time OOBI session in which the External GAR and the QAR are present. An

An External GAR MUST lead for the anchoring action for the QVI External Delegated AID described below.

The Issuer MUST ensure that the Issuer of the QVI vLEI Credential is GLEIF.
6.3 Legal Entity Qualifications

6.1 Policies

6.2 Issuer Section

3. Version Date: [Image]

3.4. 2. b. Revocation

1. Voluntary

A QAR MUST call the vLEI Reporting API with each revocation event of Legal Entity vLEI Credentials. A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).

A QAR and the LARs MUST establish a real-time OOBI session in which the QAR and all LARs are present. An example is a video call. The Legal Entity MUST designate a set of one or more LARs to act on its behalf.

3.3. The Legal Entity Identifier (LEI) of the Legal Entity has an entity status of Active and an LEI registration status other than Lapsed, Retired, Duplicate, Annulled or Merged (will be deprecated in March 2022) in the Global LEI System.

A Qualified vLEI Issuer has a LEI issued by a LEI Issuer. The LEI of a Qualified vLEI Issuer and the LEI of the Legal Entity Holder of the Legal Entity vLEI Credential are the same. A vLEI holder is a Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date.

A vLEI holder that has been provisioned on the LEI page of the Legal Entity to reflect Legal Entity vLEI credentials that have been issued by GLEIF.

A QAR and the Legal Entity vLEI Credential Issuance Issuer MUST establish a real-time OOBI session in which the QAR and all LARs are present. An example is a video call. The Legal Entity vLEI Credential Issuance Issuer MUST designate a set of one or more LARs to act on its behalf.

A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity has an entity status of Active and an LEI registration status other than Lapsed, Retired, Duplicate, Annulled or Merged (will be deprecated in March 2022) in the Global LEI System.

A QAR MUST verify the LEI of a Legal Entity, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. Another QAR then approves the issuance and signs the Legal Entity vLEI Credential. The QAR MUST perform manual verification of each LAR's legal identity for which the QAR has already performed Identity Assurance and Identity Authentication.

A QAR and the LARs MUST establish a real-time OOBI session in which the QAR and all LARs are present. An example is a video call. The Legal Entity MUST designate a set of one or more LARs to act on its behalf.

A QAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).

The Legal Entity Identifier (LEI) field value MUST be the LEI of Legal Entity Holder. The LEI of the Legal Entity Holder MUST be the same as the LEI of the Legal Entity. The field values in the credential MUST be as follows:

3.4. 2. c. Issuance

The QAR MUST verify in real time that a response to the Challenge Message was received from each LAR. The Challenge Message MUST be unique to the OOBI session. The QAR MUST perform Identity Assurance of a person serving in the role of a Legal Entity Authorized Representative (LAR) to at least Identity Assurance Level 2 (IAL2) as defined in NIST 800-63A. A Qualified vLEI Issuer in the vLEI Ecosystem with qualification up to date. The Issuer MUST:

A QAR and the LARs MUST establish a real-time OOBI session in which the QAR and all LARs are present. An example is a video call. The Legal Entity MUST designate a set of one or more LARs to act on its behalf.

A QAR MUST verify the Legal Entity Identifier (LEI) of the Legal Entity has an entity status of Active and an LEI registration status other than Lapsed, Retired, Duplicate, Annulled or Merged (will be deprecated in March 2022) in the Global LEI System.

A QAR MUST verify the LEI of a Legal Entity, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. Another QAR then approves the issuance and signs the Legal Entity vLEI Credential. The QAR MUST perform manual verification of each LAR's legal identity for which the QAR has already performed Identity Assurance and Identity Authentication.
The "engagementContextRole" field value MUST be the Engagement Context Role to be assigned in the vLEI ECR Credential.

The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity.

The "LEI" field value MUST be the LEI of Legal Entity Holder.

The field values in the credential MUST be as follows:

- The QAR then MUST revoke the vLEI Role Credential.
- To revoke a previously issued vLEI Role Credential, the LAR(s) MUST revoke the QVI AUTH vLEI Credential related to a specific Issuer Policies
- A LAR and the OOR Person or ECR Person MUST establish a real-time OOBI session in which the LAR and the OOR Person or ECR Person are present. An example is a continuous web meeting attended by all parties on both audio and video.
- A LAR MUST perform identity assurance of an OOR Person or ECR Person designated by the Legal Entity to receive vLEI Role Credentials.
- The Issuer MUST be a LAR of a Legal Entity that holds a valid Legal Entity vLEI Credential that was issued by the QVI with which the Legal Entity has contracted to issue vLEI Role Credentials.
- The Issuer MUST issue the vLEI Role Credentials for the time period for which the vLEI Role Credential is valid, as defined in the vLEI Ecosystem Governance Framework 1.0 Trust Assurance Framework.
- The "signaturePolicy" field value MUST be included as a requirement in the legal entity vLEI Ecosystem Governance Framework.
- The "field values in the credential MUST be as follows:

  1. The "signaturePolicy" field value MUST be included as a requirement in the legal entity vLEI Ecosystem Governance Framework.
  2. The "signaturePolicy" field value MUST be included as a requirement in the legal entity vLEI Ecosystem Governance Framework.
The OOR Person MUST be able to sign the Challenge Message using its Private Key Store.

The OOR Person MAY use any additional means of authentication in order to perform the OOR Certification process and complete the OOBI session for an OOR Person serving in an Official Organizational Role (OOR Person).

A QAR MAY request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

A QAR MUST validate the name and the Official Organizational Role of an OOR Person using one or more official public sources.

If the OOR Person is not able to use their OOR Credential to obtain an OOR Person Role in the LEI database of the Legal Entity, the QAR MAY request the Legal Entity to provide the required documentation.

When the Identity Assurance is performed by a QAR, the Identity Assurance MUST be in the same Supervised Remote In-person or other equivalent level of assurance as specified 6.d. below (essentially including the IAL3 requirement for a Supervised Remote In-person session).

The OOR Person MUST use its Private Key Store to sign and return the response to the Challenge Message, after which the OAR MUST verify in real time that the response was received from the OOR Person.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

A QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the OOR Credential has been made.

A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issuance which has occurred.

The QAR MUST verify the source reference to the Legal Entity that issued the OOR Credential.

The Legal Entity Identifier (LEI) of the Legal Entity MUST be contained in the Legal Entity's vLEI Credential with the Legal Entity Identifier (LEI) of the Legal Entity.

The LEI page on the vLEI Registry MUST reflect OOR vLEI credential issuances that have occurred.

The QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the OOR Credential has been made.

A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issuance which has occurred.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

The QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the OOR Credential has been made.

A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issuance which has occurred.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

The QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the OOR Credential has been made.

A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issuance which has occurred.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify in real time that the response to the Challenge Message was received from the OOR Person.

The QAR MUST request from the LAR(s) copies of documents of the Legal Entity, such as Board minutes or resolutions, statutes or articles of incorporation, or any other documents that may be required to perform an OOR Certification. If the name and the Official Organizational Role of the OOR Person cannot be validated using one or more official public sources, the OOR Credential MUST be cancelled.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.

A QAR MUST verify that the LEI supplied for the Credential is the LEI of the Legal Entity for which the issuance request for the OOR Credential has been made.

A QAR MUST validate the Legal Entity Identifier (LEI) of the Legal Entity has a LEI Entity Status of Active and a LEI Registration Status of Issuance which has occurred.

The OOR Credential MUST be able to sign the Challenge Message using their Private Key Store.
To follow, the **Issuer** may apply by Qualifiable vLEI Issuer to the Legal Entity vLEI Issuer according to section 6.1 of the Issuer Policies

**6.1 Issuer Policies**

To follow, the **Issuer** may apply by Qualifiable vLEI Issuer to the Legal Entity vLEI Issuer according to section 6.1 of the Issuer Policies

**6.2 Credential**

The Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. The QAR performs the following Identity Assurance steps during the QAR Event, according to section 6.1 of the Issuer Policies.

**6.3 Revocation**

The Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. The QAR performs the following Identity Assurance steps during the QAR Event, according to section 6.1 of the Issuer Policies.

**6.4 Legal Entity**

The Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. The QAR performs the following Identity Assurance steps during the QAR Event, according to section 6.1 of the Issuer Policies.

**6.5 ECR Person**

The Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. The QAR performs the following Identity Assurance steps during the QAR Event, according to section 6.1 of the Issuer Policies.

**6.6 Issuer Policies**

The Legal Entity vLEI Credential, that the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a QAR. The QAR performs the following Identity Assurance steps during the QAR Event, according to section 6.1 of the Issuer Policies.
The "personLegalName" field value MUST be the Legal Name of the Person in the Engagement Context Role at the Legal Entity.

The "engagementContextRole" field value MUST be the Engagement Context Role.

For an Issuer in 6.1.2, the Sources section of the ECR vLEI Credential MUST contain a source reference to the Legal Entity vLEI Credential (via SAID) held by the Legal Entity issuing this ECR vLEI Credential. The value of the "LEI" field of the Legal Entity vLEI Credential MUST equal the value of the "LEI" field in this ECR vLEI Credential.