1. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

2. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

3. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

4. Key-pair creation and storage infrastructure MUST be within a TEE.

5. The level of protection should correspond with the value of the assets these keys are protecting.

6. The WikiLeaks pool MUST use only one type for any KEL.

7. Non-delegated pre-rotated keys are at the next level of delegation hierarchy and MUST have the very highest level of protection. There is no recovery mechanism within KERI to regain control over a non-delegated AID once its pre-rotated key has been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and control over a non-delegated AID once its pre-rotated keys have been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and control over a non-delegated AID once its pre-rotated keys have been captured.

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

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

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

11. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

12. The WikiLeaks pool MUST use only one type for any KEL.

13. Key-pair creation and storage infrastructure MUST be within a TEE.

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

15. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

16. The level of protection should correspond with the value of the assets these keys are protecting.

17. Non-delegated pre-rotated keys are at the next level of delegation hierarchy and MUST have the very highest level of protection. There is no recovery mechanism within KERI to regain control over a non-delegated AID once its pre-rotated key has been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and control over a non-delegated AID once its pre-rotated keys have been captured. The only recourse is to abandon the AID and stand up a new AID and reestablish the reputation and control over a non-delegated AID once its pre-rotated keys have been captured.

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

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

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

21. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

22. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

23. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

24. Key-pair creation and storage infrastructure MUST be within a TEE.

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

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

27. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

28. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

29. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

30. Key-pair creation and storage infrastructure MUST be within a TEE.

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

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

33. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

34. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

35. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

36. Key-pair creation and storage infrastructure MUST be within a TEE.

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

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

39. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

40. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

41. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

42. Key-pair creation and storage infrastructure MUST be within a TEE.

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

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

45. The Witness Pool configuration MUST include a minimum of 5 Witnesses with the sufficient threshold as per KAACE (NOTE: this prevents a single web host provider from hosting a majority of Witnesses.)

46. Autonomic Identifiers (AIDs) MUST be a threshold multisig with weighting requirements that have been determined by GLEIF.

47. The next or pre-rotated set of keys MUST be protected with the highest level of protection.

48. Key-pair creation and storage infrastructure MUST be within a TEE.

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

50. Key-pairs MUST be generated using a cryptographic algorithm with at least 128 bits of cryptographic strength. This includes using a source of entropy of at least 128 bits of cryptographic strength for the salt or seed used to generate the private key of the key pair.
1. The GLEIF Watcher Signing Key Pair key store MUST reside on the Watcher Service host but MUST use dedicated user-only permissions on the key store directory and its contents.

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

3. While used, the encryption key store MUST reside on a different device or host from that of the Watcher service.

Qualified vLEI Issuer Management Policies

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

4. Qualified vLEI issuers policy for approving rotation of the issuing keys for the GLEIF-Delegated issuing identifier.

- MUST use a OOK (out-of-band) MFA (multi-factor authorization) mechanism to approve delegated key rotation.
- Must be at least a 2 or 3 thresholded multi-sig scheme.

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

Qualified vLEI Issuer CERT Profile

1. For added security, Qualified vLEI Issuers:
   a. MUST use Delegated AIDs from GLEIF for issuing AIDs or all types.
   b. MUST use at least a 2 or 3 thresholded multi-sig scheme.

2. Qualified vLEI Issuer Key Compromise Recovery

1. Qualified vLEI Issuer Key Compromise Monitoring

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

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

Qualified vLEI Issuer Watchers

1. The Challenger MUST verify that:
   a. Corresponding Issuer Qualification
   b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
   c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

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

Qualified vLEI Issuer Endorser Support: Witness Pool or Ledger Registrar

1. The Challenger MUST include a cryptographic nonce generated in real-time.

2. The Responder’s AID.

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

4. Make a recovery rotation event that forks their KEL and submit the recovering rotation event explanation to GLEIF for publication in GLEIF’s public key recovery event registry.

5. The Challenger MUST include a cryptographic nonce generated in real-time.

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

- MUST use at least a 2 or 3 thresholded multi-sig scheme.
- MUST use at least a 2 or 3 thresholded multi-sig scheme.

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

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

9. The Challenge Message is sent to the:
   a. Fully Signed Request contains the same cryptographic nonce as the Challenge Message.
   b. The signatures of the Responders were generated by the private keys that control the Issuers’ AIDs.

10. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

11. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

12. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

13. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

14. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

15. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

16. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

17. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

18. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

19. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

20. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.

21. The Challenger MUST verify that:
    a. Corresponding Issuer Qualification
    b. Delegated AID of a Qualified vLEI Issuer MUST set the Do Not Delegate configuration trait to Qualified vLEI Issuer Delegation
    c. The Delegated AID of a Qualified vLEI Issuer MUST use Delegated AIDs from GLEIF for issuing vLEIs or all types.
**MUST' statements** Technical Requirements Part 2: vLEI Credentials

<table>
<thead>
<tr>
<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>
<tbody>
<tr>
<td>Identification Version Upgrades:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Previous versions explicitly cited by policies in this document MUST be supported for a period 18 months.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>New versions MUST be implemented within a period 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.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Security and Privacy</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. All vLEI Credential schema MUST be SIS compliant.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. All instantiated vLEI Credentials MUST be ACDC compliant.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4. All SADs MUST use the cryptoBlake3-256 digest.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Requirements for vLEI ACDC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. Issuer and Holder Identifiers MUST be KERI AIDs that use the did:keri Method.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. All vLEI Credentials MUST include an ACDC version string field.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. All vLEI Credentials MUST support SIS certification.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4. All vLEI Credentials MUST include a SAD (as evidence of immutability).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Specification Version Upgrades</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Security and Privacy</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. All signatures for the vLEI Credentials MUST use Ed25519 Signatures CESR Proof Format.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. All vLEI Credential schema MUST be SIS compliant.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. All instantiated vLEI Credentials MUST be ACDC compliant.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4. All SADs MUST use the cryptoBlake3-256 digest.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Requirements for vLEI ACDC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. Issuer and Holder Identifiers MUST be KERI AIDs that use the did:keri Method.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. All vLEI Credentials MUST include an ACDC version string field.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. All vLEI Credentials MUST support SIS certification.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4. All vLEI Credentials MUST include a SAD (as evidence of immutability).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>The following ACDC sections MUST include a SAD - Attribute (data payload) section, Schema section and Rules section.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7. All source links MUST include the SAD of the referenced ACDC.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8. ACDCs have three primary forms that MUST be supported separately by Issuers, Holders and Verifiers using the following rules:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Form 1 – the Fully-expanded Form in which the schema, attributes and rules are fully expanded and embedded.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Form 2 – Schema compacted Form in which only the SAD of each major section is included.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Form 3 – Schema compacted Form in which only the SAD of the schema section is included.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9. Issuers MUST support the issuance of vLEI Credentials in any or all three forms:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10. Issuers MUST provide the SADs at issuance to Holders when issuing forms 2 and 3, by either including the SAD in the presentation or including a reference to the highly-available service endpoint from which the SAD can be retrieved.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vLEI Credential Schema</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. vLEI Credential schema MUST be compliant the SAD and SIS specifications.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. All vLEI Credential schema MUST include a SAD (as evidence of immutability).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. Each vLEI Credential MUST be in-compliance with its specific vLEI Credential Governance Framework.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>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.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Composable Event Streaming Representation (CESR)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. The Proof Format for vLEI Credentials MUST comply with the CESR Proof Format specification.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. Each vLEI Credential Issuer MUST maintain a highly-available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3. vLEI Credential Issuers MUST comply with the Issuance Exchange Protocol Specification for ACDC and KERI.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Credential Registry and Revocation Registry Requirements</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. Each vLEI Credential Issuer MUST maintain a highly-available issuance and registration registry in compliance with the Public Transaction Event Log (PTEL) Specification.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Exchange Protocols</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>1. All vLEI Credential Issuers MUST comply with the Issued Exchange Protocol Specification for AAI and IAI.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
The following steps MUST be performed in the order listed and completed during this OOBI session.

1. All Controllers MUST establish their own Private Key Stores.
2. All Controllers MUST keep their private keys secret.
3. A given Controller MUST control one and only one key pair from each set of keys.
4. The KERI protocol MUST be used to transfer control authority from one set of keys to another.

3. All Controllers MUST be authenticated by all other Controllers in the multi-signing group.
4. The controllers MUST have a Continuity Policy for the survival of control authority in the event of a disaster or a failure of the multi-signing group.
5. The controllers MUST have a Continuity Policy for the survival of control authority in the event of a disaster or a failure of the multi-signing group.

1. The GRAC MUST be designated as the GLEIF Root AID Genesis Controller (GRAGC).
2. Each GRAC MUST verify the signature of every other GRAC.
3. One of the GRACs MUST issue a Challenge Message in every other GLEIF Controller as defined in the Technical Requirements Part 1 for the purpose of cryptographic authentication of their Controller AID. The Challenge Message MUST be unique to the OOBI session.
4. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
5. Each GRAC MUST verify that the signature of every other GRAC.
6. The GRACs MUST be designated as the GLEIF Root AID Genesis Controller (GRAGC).
7. One of the GRACs MUST issue a Challenge Message in every other GLEIF Controller as defined in the Technical Requirements Part 1 for the purpose of cryptographic authentication of their Controller AID. The Challenge Message MUST be unique to the OOBI session.
8. Each GRAC MUST verify the signature of every other GRAC.
9. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
10. Each GRAC MUST verify that the signature of every other GRAC.
11. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
12. Each GRAC MUST verify that the signature of every other GRAC.
13. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
14. Each GRAC MUST verify that the signature of every other GRAC.
15. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
16. Each GRAC MUST verify that the signature of every other GRAC.
17. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
18. Each GRAC MUST verify that the signature of every other GRAC.
19. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
20. Each GRAC MUST verify that the signature of every other GRAC.
21. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
22. Each GRAC MUST verify that the signature of every other GRAC.
23. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
24. Each GRAC MUST verify that the signature of every other GRAC.
25. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
26. Each GRAC MUST verify that the signature of every other GRAC.
27. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
28. Each GRAC MUST verify that the signature of every other GRAC.
29. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
30. Each GRAC MUST verify that the signature of every other GRAC.
31. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
32. Each GRAC MUST verify that the signature of every other GRAC.
33. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
34. Each GRAC MUST verify that the signature of every other GRAC.
35. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
36. Each GRAC MUST verify that the signature of every other GRAC.
37. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
38. Each GRAC MUST verify that the signature of every other GRAC.
39. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
40. Each GRAC MUST verify that the signature of every other GRAC.
41. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
42. Each GRAC MUST verify that the signature of every other GRAC.
43. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
44. Each GRAC MUST verify that the signature of every other GRAC.
45. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
46. Each GRAC MUST verify that the signature of every other GRAC.
47. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
48. Each GRAC MUST verify that the signature of every other GRAC.
49. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
50. Each GRAC MUST verify that the signature of every other GRAC.
51. Each GRAC MUST verify in real time that a response to the Challenge Message was received from every other GRAC.
The following steps MUST be performed in the order listed and completed during this OOBI session for the GLEIF External Delegated AID (GEDA).

a. The set of GGDACs MUST each rotate their participating AIDs.

b. The set of GGDACs MUST each rotate their participating AIDs.

c. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

d. Each GDAC MUST verify the signature of every other GDAC.

e. Each GDAC MUST verify the signature of every other GDAC.

f. One of the GDACs MUST be designated as the GLEIF Delegated AID Genesis Controller (GDAGC).

The following steps MUST be performed in the order listed and completed during this OOBI session for the two GLEIF Delegated AIDs, respectively, the GLEIF Internal Delegated AID (GIDEA) and the GLEIF External Delegated AID (GIDEA).

a. The set of GGDACs MUST each rotate their participating AIDs.

b. The set of GGDACs MUST each rotate their participating AIDs.

c. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Root AIDWitness.

d. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Root AIDWitness.

e. Each GDDAC must verify the signature of every other GDAGC.

f. Each GDDAC must verify the signature of every other GDAGC.

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

a. The set of GDACs MUST each rotate their participating AIDs.

b. The set of GDACs MUST each rotate their participating AIDs.

c. Each GDAC must verify the signature of every other GDAC.

The following steps MUST be performed in the order listed and completed during this OOBI session for the Delegated AID Inception Event.

a. Each QDAC must verify the signature of every other QDAC.

b. Each QDAC must verify the signature of every other QDAC.

c. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

d. Each QDAC must verify the signature of every other QDAC.

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

f. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

g. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

h. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

i. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

j. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

k. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

l. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

m. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

n. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

o. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

p. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

q. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

r. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

s. The QDAGC MUST select the AIDs and Service Endpoints from the QVI Delegated AID Witness Pool.

The following steps MUST be performed in the order listed and completed during this OOBI session for the GLEIF External Delegated AID (GEDA).

a. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

b. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

c. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

d. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

e. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

f. Each GDDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

The following steps MUST be performed in the order listed and completed during this OOBI session for the Delegated AID Inception Event.

a. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

b. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

c. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

d. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

e. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.

f. Each QDAC must verify that the Delegated AID Inception Event is fully witnessed by every Witness.
b. GLEIF MUST designate one of the GDACs as the GEAKEC.

X; covered as part of KERI Key Management

X; requirement in Identifier Governance Framework

c. The GEAKEC MUST select the AIDs from the set of GDACs for the
ordered set of authorized participant members in the multi-sig group
and configure and approve the weight threshold and ordered set of
participants for both the current and next public key set and threshold of
participants.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

d. Using the current public key, the next public key digest from each of
the participating AID Rotation Events, and the digest of the QVI
Delegated AID Inception Event, the GEAKEC generate a GLEIF
Delegated AID Rotation Event and publish this to the GDACs and to the
GLEIF Delegated AID Witnesses.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Key Management

e. Each GDAC MUST verify the set of public keys, the next public key
digest, the Witness identifiers, the threshold, the next threshold and
delegated Inception Event digests in that Rotation Event.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

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

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

X; covered as part of KERI Key Management

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

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

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

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

8. GLEIF Root AID Publication

a. The GLEIF HTTPS website.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

b. The HTTPS websites of at least ten members of the GLEIF
Regulatory Oversight Committee.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

c. The HTTPS websites of all QVIs.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

d. In the KERI Event Log for all GLEIF KERI Witnesses.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

e. Published to at least 3 international newspapers in separate
national jurisdictions.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

f. Published to public registries (to be specified).

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

9. Abandonment

1. Voluntary Abandonment

GLEIF MUST abandon its GLEIF Root AID if GLEIF no longer holds the role of
root of trust for the vLEI Ecosystem.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations

2. Private Key Compromise or Natural Disaster

If in the extremely unlikely event of the failure of all key recovery provisions
specified in Technical Requirements Part 1: KERI Infrastructure, GLEIF
MUST abandon its Root AID and Delegated Internal and External AIDs and
create and publish its new Root AID and Delegated Internal and External
AIDs.

X; requirement in Identifier Governance Framework

X; covered as part of KERI Identifier Operations
Involuntary revocation of vLEI Credentials MUST follow the process specified in Involuntary Revocation.

The GAR MUST approve issuance of a QVI vLEI Credential after the completion of a QVI vLEI Issuer Qualification Program and has been issued a QVI vLEI Credential.

The Issuer MUST:

1. use the QVI's vLEI Credential scheme defined in section 8.1.
2. include all Claims marked as Required in section 8.1.

1. Identity Authentication


- The GAR MUST perform initial identity verification of the QVI's Legal Entity Identity using the GLEIF-supplied vLEI software.

- The GAR MUST perform the revocation within the timeframe specified in Appendix 5, Service Level Agreement (SLA).

2. Identity Representation

- A credential wallet MUST be set up for the QVI.

- The QVI MUST designate a QAR to act on its behalf.

- A GAR and the QAR MUST participate in a real-time audio video session in which the GAR and the QAR are present. An example is a continuous video meeting attended by all parties on both audio and video.

- The following steps MUST be performed in this order and completed during the audio video session:

  1. The GAR MUST perform initial verification of the QAR's Legal Entity Identity using the GLEIF-supplied vLEI software.

  2. The QAR MUST use its unique identifier (such as a QAR code or a chat) to share the QAR's Controller External Autonomic Identifier (AID) with the GAR.

  3. An QAR MUST use an QAR protocol (such as a QAR code or a chat) to share the QAR AID with the GAR.

  4. A QAR MUST send a Challenge Message from the GLEIF Controller General AID to the QAR AID as defined in the Technical Requirements Part 4 QBI Infrastructure for the purpose of cryptographic authentication of the QBI AID. The Challenge Message MUST be unique to the QBI AID.

  5. The QAR MUST verify that the Challenge Message was received from the GLEIF.

  6. The QAR MUST verify that the response to the Challenge Message has been received, the GAR must verify the signature of the QAR.

  7. The QAR MUST propose issuance of a QVI vLEI Credential after the completion of Identity assurance in sections 6.3 above.

- A QAR MUST handle all Identity Assurance requests in a fair and equal manner and ensure that all Legal Entities receive an equal level of service.

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

2. Identity Revocation

- The QVI vLEI Credential must contain the ID of the QVI.

- If the GAR observes that the QAR has not completed the required actions in a timely manner, the GAR MUST take appropriate action to ensure compliance.

- The GAR and the QAR MUST establish a real-time OOBI session in which the GAR and the QAR are present. An example is a continuous video meeting attended by all parties on both audio and video.

- The following steps MUST be performed in this order and completed during the video meeting:

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

  2. The GAR MUST use the QVI AID to the QVI AID as defined in the Technical Requirements Part 4 QBI Infrastructure for the purpose of cryptographic authentication of the QVI AID. The Challenge Message MUST be unique to the QVI AID.

  3. The QVI vLEI Credential MUST be set up for the QVI.

- A GLEIF Authorized Representative (GAR) MUST perform identity assurance of the QVI's Legal Entity Identity using the GLEIF-supplied vLEI software.

- A QAR MUST revoke a Legal Entity vLEI Credential upon receipt of a revocation message from the QAR.

- The GAR MUST perform identity assurance of the QVI's Legal Entity Identity using the GLEIF-supplied vLEI software.
Ecosystem Governance Framework.

Issuer MUST:
1. use the legal entity's LEI (Legal Entity Identifier) as the identifier of a Legal Entity in the LEI system.
   Requirement satisfied by: Compliance with vLEI Governance Framework
2. Use the digital signature for identifying, authenticating, and for the Management.
   Requirement satisfied by: Compliance with vLEI Governance Framework

Identity Assurance:
1. A Qualified vLEI Issuer (QVI) MUST verify that the Issuer is supplied by the Issuer to the Issuer for which the request has been made.
   Requirement satisfied by: Compliance with vLEI Issuer Qualification Program
2. A QVI MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
3. The Legal Entity MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
4. A QAR (Qualified Accredited Revocation Agent) MUST perform the revocation of a vLEI Credential that has been reported.
   Requirement satisfied by: Compliance with vLEI Governance Framework
5. The Legal Entity MUST call the vLEI Reporting API with each issuance event of Legal Entity vLEI Credentials.
   Requirement satisfied by: Compliance with vLEI Governance Framework

Identity Authentication:
1. The Legal Entity Identity Verification process outlined in section 6.3 MUST be completed before
   Requirement satisfied by: Compliance with vLEI Governance Framework
2. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
3. Each AVR MUST use the Legal Entity's AID to authenticate the Legal Entity to the QAR.
   Requirement satisfied by: Compliance with vLEI Governance Framework
4. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
5. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential upon receipt of a fully
   Requirement satisfied by: Compliance with vLEI Governance Framework
6. The Issuer MUST ensure that the Issuer is supplied by the Issuer for the Issuer for the Issuer for which the request has been made.
   Requirement satisfied by: Compliance with vLEI Governance Framework
7. A QAR MUST perform the revocation of a vLEI Credential that has been reported.
   Requirement satisfied by: Compliance with vLEI Governance Framework

Issuer Compliance:
1. A Qualified vLEI Issuer (QVI) MUST verify that the Issuer is supplied by the Issuer to the Issuer for which the request has been made.
   Requirement satisfied by: Compliance with vLEI Governance Framework
2. A Qualified vLEI Issuer (QVI) MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
3. The Legal Entity MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
4. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
5. Each AVR MUST use the Legal Entity's AID to authenticate the Legal Entity to the QAR.
   Requirement satisfied by: Compliance with vLEI Governance Framework
6. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
7. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential upon receipt of a fully
   Requirement satisfied by: Compliance with vLEI Governance Framework

Issuer Qualification Program:
1. A Qualified vLEI Issuer (QVI) MUST verify that the Issuer is supplied by the Issuer to the Issuer for which the request has been made.
   Requirement satisfied by: Compliance with vLEI Governance Framework
2. A Qualified vLEI Issuer (QVI) MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
3. The Legal Entity MUST verify the identity assurance of the Identity Assurance to the Issuer of the Legal Entity that has been verified.
   Requirement satisfied by: Compliance with vLEI Governance Framework
4. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
5. Each AVR MUST use the Legal Entity's AID to authenticate the Legal Entity to the QAR.
   Requirement satisfied by: Compliance with vLEI Governance Framework
6. The QAR MUST use an OOBI protocol (such as a QR code or live chat) to share the QVI with the Legal Entity.
   Requirement satisfied by: Compliance with vLEI Governance Framework
7. The Legal Entity MUST notify the QVI to revoke an ECR vLEI Credential upon receipt of a fully
1. The Legal Entity must: X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   a. a Qualified vLEI Issuer (QVI) must verify that the identity of the Legal Entity has been validated and certified. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. The legal entity vLEI credential must include the legal entity’s vLEI, along with any additional information required by the Legal Entity and OOR Person. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. The legal entity vLEI credential must include a unique identifier (the LEI) for the legal entity, as defined in ISO 17442. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. The legal entity vLEI credential must be issued by an Official Organizational Role (OOR) of the Legal Entity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. The legal entity vLEI credential must be signed by the OOR, as defined in section 8.1. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

2. The OOR Person must: X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   a. be a QAR that has been approved to sign an OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. be authorized to represent the Legal Entity in the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. be a member of the Legal Entity’s management team or a direct contact person. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. be a person with the specific qualifications required by the Legal Entity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. be authorized to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. be independent of the Legal Entity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

3. The OOR vLEI Credential Issuance Process must: X; covered as part of the OOR vLEI Issuance process with KERI (crytographic trust requirement)
   a. require the Legal Entity to submit a request for an OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. require the Legal Entity to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. require the Legal Entity to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. require the QAR to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. require the QAR to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. require the Legal Entity to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   g. require the OOR Person to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   h. require the OOR vLEI Credential to be transmitted to the Qualified vLEI Issuer. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

4. The OOR vLEI Issuance Process must: X; covered as part of the OOR vLEI Issuance process with KERI (crytographic trust requirement)
   a. require the Legal Entity and OOR Person to authenticate their identities using a trusted identity assurance service. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. require the Legal Entity and OOR Person to perform a cryptographic authentication of the OOR Person’s AID. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. require the Legal Entity and OOR Person to ensure that the OOR vLEI Credential is issued in accordance with KERI standards. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. require the Legal Entity and OOR Person to ensure that the OOR vLEI Credential is issued in accordance with KERI standards. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. require the Legal Entity and OOR Person to ensure that the OOR vLEI Credential is issued in accordance with KERI standards. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. require the Legal Entity and OOR Person to ensure that the OOR vLEI Credential is issued in accordance with KERI standards. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   g. require the Legal Entity and OOR Person to ensure that the OOR vLEI Credential is issued in accordance with KERI standards. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

5. The OOR vLEI Issuance Process must: X; covered as part of the OOR vLEI Issuance process with KERI (crytographic trust requirement)
   a. require the Legal Entity to submit a request for an OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. require the Legal Entity to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. require the Legal Entity to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. require the QAR to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. require the QAR to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. require the Legal Entity to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   g. require the OOR Person to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   h. require the OOR vLEI Credential to be transmitted to the Qualified vLEI Issuer. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

6. The OOR vLEI Issuance Process must: X; covered as part of the OOR vLEI Issuance process with KERI (crytographic trust requirement)
   a. require the Legal Entity to submit a request for an OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. require the Legal Entity to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. require the Legal Entity to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. require the QAR to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. require the QAR to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. require the Legal Entity to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   g. require the OOR Person to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   h. require the OOR vLEI Credential to be transmitted to the Qualified vLEI Issuer. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance

7. The OOR vLEI Issuance Process must: X; covered as part of the OOR vLEI Issuance process with KERI (crytographic trust requirement)
   a. require the Legal Entity to submit a request for an OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   b. require the Legal Entity to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   c. require the Legal Entity to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   d. require the QAR to verify the OOR Person’s identity. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   e. require the QAR to approve the issuance of the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   f. require the Legal Entity to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   g. require the OOR Person to sign the OOR vLEI Credential. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
   h. require the OOR vLEI Credential to be transmitted to the Qualified vLEI Issuer. X; requirement in Credential Governance Framework X; assessment and demonstration of Qualified vLEI Issuer compliance
Usage of a valid vLEI Credential does not assert that the legal entity is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any law.

Issuance of a valid vLEI Credential only establishes that the information in the requirements in the Identity Verification sections, 6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.
**ECR vLEI Credentials for AVRs**

**Voluntary revocation**

A QAR, another QAR then approves the issuance and signs the ECR vLEI Credential. A workflow MUST be implemented in the operations of the QVI which requires, in accordance with section 6.1.a of the Credential Framework:

- a. The QAR MUST perform manual verification of the ECR Person’s legal identity for which the QAR has already performed Identity Assurance: An example, the QCR Person usually present one or more identity credentials and the QAR compares the credentials verified during identity Assurance to the QVI.

- b. A QAR MUST use an OOOI protocol (such as a QR code or link to chat) to share the QAR Autonomic Identifier (AQI) with the AVR.

- c. The following steps MUST be performed in this order and completed during this OOOI session:
  
  i. The QAR MUST verify that the credentials verified during Identity Assurance are still valid and accept the offer in the QVI vLEI Request to issue an ECR vLEI Credential. The Challenge Message MUST be unique to the OOOI session.
  
  ii. The QAR Person never view the legal entity and return a response to the Challenge Message, after which the ECR Person MUST acknowledge that the QAR Person has completed the steps.
  
  iii. The QAR MUST verify in real-time that the response to the Challenge Message was received from the QAR Person.
  
  iv. When the response to the Challenge Message has been received by the QAR, the QAR MUST verify the QAR Person’s signature.
  
  v. The QAR MUST perform manual verification of the ECR Person’s legal identity for which the QAR has already performed Identity Assurance: An example, the QCR Person usually present one or more identity credentials and the QAR compares the credentials verified during identity Assurance to the QVI.

- d. The QAR MUST issue a vLEI vLEI Credential (ECR vLEI Credential) to the QVI. The QAR MUST verify that the LEI supplied for the vLEI vLEI Credential who will issue ECR vLEI Credentials has the entity status of Active and an LEI registration status other than Lapsed, Retired, Suspended or Not Listed.

The following steps MUST be performed in this order and completed during this OOOI session:

- a. The legal entity must allow an OOOI session to create an ECR vLEI Credential, after receipt of a Fully Signed revocation request the by the QVI vLEI Credential, the above-mentioned Identity Assurance, Identity Authentication and out-of-band validations are performed by a VAQ. Another QAR then approves the issuance and signs the ECR vLEI Credential.

- b. The QAR vLEI vLEI Credential(s) MUST perform the revocation within the timeframes specified in the agreement that has delegated the issuance of Legal Entity Engagement Context Role vLEI Credentials to one or more QAR vLEI vLEI Credentials issued by Qualified vLEI Issuers as a value-added service.

- c. The QAR vLEI vLEI Credential(s) MUST verify that the LEI supplied for the vLEI vLEI Credential who will issue ECR vLEI Credentials has the entity status of Active and an LEI registration status other than Lapsed, Retired, Suspended or Not Listed.

Usage of a valid vLEI vLEI Credential allows the authorizing vLEI vLEI Credential to be used in transactions and services as required by the vLEI vLEI Credential. A QAR Autonomic Identifier (AQI) of the ECR vLEI Credential is used in transactions and services as the authorized vLEI vLEI Credential. A QAR, another QAR then approves the issuance and signs the ECR vLEI Credential. The Challenge Message MUST be unique to the OOOI session.

- a. The QAR MUST perform manual verification of the ECR Person’s legal identity for which the QAR has already performed Identity Assurance: An example, the QCR Person usually present one or more identity credentials and the QAR compares the credentials verified during identity Assurance to the QVI.

- b. A QAR MUST verify that the legal entity identifier (LEI) of the legal entity has an entity status of Active and an LEI registration status other than Lapsed, Retired, Suspended or Not Listed.

- c. The QAR MUST verify that the LEI supplied for the vLEI vLEI Credential who will issue ECR vLEI Credentials has the entity status of Active and an LEI registration status other than Lapsed, Retired, Suspend
iv. The ECR Person MUST use an OOBI protocol (such as a QR code or live chat) to share its AID with the AVR.

v. The AVR MUST send a Challenge Message to the ECR Person's AID as defined in the Technical Requirements Part 1 for the purposes of cryptographic authentication of the ECR Person's AID. The Challenge Message MUST be unique to the OOBI session.

vi. The ECR Person MUST use its Private Key Store to sign and return a response to the Challenge Message, after which the ECR Person MUST acknowledge that this action has been completed.

vii. The AVR MUST verify in real time that the response to the Challenge Message was received from the ECR Person.

viii. When the response to the Challenge Message has been received by the AVR, the AVR MUST verify the ECR Person's signature.

Issuance

1. The ECR Person Identity Verification process outlined in section 6.5 MUST be completed before ECR vLEI Credential issuance can begin.

2. A workflow MUST be put in place by the Legal Entity for ECR vLEI Role Credentials to meet the requirement for two AVRs to sign the ECR vLEI Role Credentials at issuance.

ECR vLEI Credentials for AVRs

a. ECR vLEI Credentials MUST be issued to the AVRs of a Legal Entity.

b. The ECR vLEI Credentials for AVRs MUST be issued by a QVI.

The following text MUST appear in the Rules section of the Authentic Chained Data Container (ACDC) vLEI Credentials:

Usage of a valid vLEI Credential does not assert that the Legal Entity is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws.

Issuance of a valid vLEI Credential only establishes that the information in the requirements in the Identity Verification sections, 6.3 and 6.5, of the Credential Governance Framework were met in accordance with the vLEI Ecosystem Governance Framework.